## Nokia Contact Information
### Corporate Headquarters

<table>
<thead>
<tr>
<th>Web Site</th>
<th><a href="http://www.nokia.com">http://www.nokia.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>1-888-477-4566 or 1-650-625-2000</td>
</tr>
<tr>
<td>Fax</td>
<td>1-650-691-2170</td>
</tr>
</tbody>
</table>
| Mail Address   | Nokia Inc.  
313 Fairchild Drive  
Mountain View, California  
94043-2215 USA |

### Regional Contact Information

<table>
<thead>
<tr>
<th>Region</th>
<th>Address</th>
<th>Telephone/Email</th>
</tr>
</thead>
</table>
| Americas        | Nokia Inc.  
313 Fairchild Drive  
Mountain View, CA 94043-2215 USA | US: 1-877-997-9199  
Outside USA and Canada: +1 512-437-7089  
tel: info.ipnetworking_americas@nokia.com |
| Europe, Middle East, and Africa | Nokia House, Summit Avenue  
Southwood, Farnborough  
Hampshire GU14 ONG UK | Tel: UK: +44 161 601 8908  
Tel: France: +33 170 708 166  
et: info.ipnetworking_emea@nokia.com |
| Asia-Pacific    | 438B Alexandra Road  
#07-00 Alexandra Technopark  
Singapore 119968 | Tel: +65 6588 3364  
et: info.ipnetworking_apac@nokia.com |

### Nokia Customer Support

<table>
<thead>
<tr>
<th>Web Site</th>
<th><a href="https://support.nokia.com/">https://support.nokia.com/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td><a href="mailto:tac.support@nokia.com">tac.support@nokia.com</a></td>
</tr>
</tbody>
</table>
| Americas       | 1-888-361-5030 or 1-613-271-6721  
Fax: 1-613-271-8782 |
| Europe         | Voice: +44 (0) 125-286-8900  
Fax: +44 (0) 125-286-5666 |
| Asia-Pacific   | Voice: +65-67232999  
Fax: +65-67232897 |
Contents

About This Guide .................................................. 17
Document Organization ........................................... 17
Document Conventions ............................................ 18
  Cautions and Notes ............................................ 18
  Command Syntax Conventions ................................. 18
  Additional Documentation ................................. 20

1 Introducing the Command-Line Interface ............... 21
  Environment Commands ....................................... 23
  Transaction Mode ............................................ 26
  General CLI Features ........................................ 28
  Commands and Command Operations ........................ 28
  Command Completion ........................................ 29
    Using Tab to Expand Commands ........................... 29
    Using Esc to Expand Commands ............................ 30
    Viewing Related Commands ................................ 30
  Using Default Values ....................................... 31
  Command Help ................................................ 32
  Command Recall ............................................... 32
    Executing Previous Commands ............................. 33
    Reusing Parts of Commands ................................ 33
  Command-Line Movement and Editing ........................ 34
  Exiting an Output Screen .................................... 35
  Setting Configuration Locks ................................ 35
  Monitoring the File System and Processes ................. 36
  Loading Commands From a File .............................. 37
## 2 Interface Commands

Using IPSO Shell Commands ........................................ 38
Saving Configuration Changes ...................................... 38

General Commands .................................................. 39
Viewing All Interfaces .............................................. 39
  Interface Names .................................................. 39
Deleting Any Logical Interface .................................... 40
Viewing Tunnels ..................................................... 41
Viewing Status and Statistics ...................................... 41
ARP ............................................................................. 42
ARP Commands ......................................................... 42
ATM Interfaces ........................................................ 45
  Physical ATM Interfaces ........................................... 45
Logical ATM Interfaces .............................................. 47
  ARP Entries for IPoA Interfaces ................................. 53
Ethernet Interfaces .................................................... 55
  Physical Ethernet Interfaces ...................................... 56
Logical Ethernet Interfaces ....................................... 57
Transparent Mode ..................................................... 59
  Configuring Transparent Mode .................................. 59
Link Aggregation ....................................................... 61
Point-to-Point Over Ethernet ....................................... 63
  Configuring Profiles ............................................. 63
  Configuring PPPoE Logical Interface .......................... 65
  Configuring PPPoE Physical Interface ......................... 66
FDDI Interfaces ........................................................ 68
  Physical FDDI Interfaces ......................................... 69
Logical FDDI Interfaces ............................................ 70
ISDN Interfaces ......................................................... 71
  Physical ISDN Interfaces ......................................... 71
Logical ISDN Interfaces ............................................ 74
Loopback Interfaces .................................................... 84
Logical Loopback Interfaces ............................................. 84
Logical or Physical Loopback Interfaces ............................... 85
Modem Interfaces ............................................................ 85
Serial Interfaces .............................................................. 88
Physical Serial Interfaces .................................................. 88
Any Physical Interface ...................................................... 88
HSSI, X.21, V.35 Interfaces ............................................... 90
T1 Interfaces ................................................................. 91
E1 Interfaces ................................................................. 99
Frame Relay Encapsulation .............................................. 105
PPP Encapsulation .......................................................... 108
Logical Serial Interfaces ................................................... 109
VPP Interfaces .................................................................. 111
Create Appropriate Static Routes ...................................... 112
VPP Interface Commands .................................................. 112

3 Network Security and Access Commands ......................... 115
Network Access and Services ............................................. 115
Licenses ............................................................................. 119
Configuring Software Licenses .......................................... 120
IPsec Commands .............................................................. 121
General IPsec Commands ................................................. 121
Proposal Commands ......................................................... 122
Filter Commands ............................................................ 124
Certificate Commands ...................................................... 126
Policy Commands ............................................................ 133
Rule Commands .............................................................. 135
Miscellaneous IPsec Commands ......................................... 140
AAA ................................................................................. 142
Viewing AAA Configuration .............................................. 142
Configuring Service Modules .......................................... 142
Configuring Service Profiles ............................................ 143
Configuring Authentication Profiles ................................. 146
Configuring Account Profiles .............................................. 148
Configuring Session Profiles ............................................ 151
Configuring RADIUS ....................................................... 153
Configuring TACPLUS ...................................................... 156
SSH ................................................................. 158
  Enabling/Disabling SSH Service ........................................ 158
Configuring Server Options .............................................. 159
  Configuring Server Access Control .................................... 159
  Configuring Server Authentication of Users ....................... 160
  Configuring User Login Environment ................................ 162
  Configuring Server Protocol Details ................................. 162
  Configuring Service Details .......................................... 164
  Configuring Server Implementation .................................. 166
Configuring and Managing SSH Key Pairs ............................. 167
  Managing New Host Keys ............................................. 167
  Generating New User Identity Keys ................................. 168
  Managing Authorized Keys .......................................... 170
Voyager Web Access (SSL) .................................................. 172
  Enabling SSL Voyager Web Access .................................. 172
  Generating a Certificate and Private Key ......................... 174
  Installing a Certificate and Private Key ......................... 176
User Management .......................................................... 177
  Adding New Users .................................................... 178
  Deleting a User ...................................................... 180
  Changing the Admin and Monitor Password ...................... 180
  Configuring S/Key for Admin and Monitor ...................... 181
Show Commands .......................................................... 182
Group Management ........................................................ 183
  Managing Groups .................................................... 184
  Show Commands ...................................................... 184
VPN Acceleration ........................................................ 185
  Configuring VPN Acceleration .................................... 185
  Displaying VPN Accelerator Information ........................ 185
## 4 Routing Commands ................................................. 187

- **BGP** .......................................................... 187
  - External BGP ............................................... 188
  - BGP Confederations ....................................... 195
  - BGP Route Reflection ..................................... 197
  - BGP Route Dampening ..................................... 198
  - Internal BGP ............................................... 200
  - BGP Communities .......................................... 207
  - BGP Show Commands ....................................... 207

- **OSPF** .......................................................... 208
  - OSPF Areas ................................................. 209
  - OSPF Interfaces ........................................... 210
  - OSPF Virtual Links ........................................ 216
  - OSPF Global Settings ..................................... 219
  - OSPF Show Commands ...................................... 222

- **RIP** ............................................................ 229
  - RIP Interfaces ............................................. 230
  - General RIP Properties .................................. 230
  - RIP Show Commands ....................................... 233

- **IGRP** ........................................................... 233
  - General IGRP Properties .................................. 234
  - IGRP Interfaces ........................................... 234
  - IGRP Show Commands ...................................... 238

- **IGMP** .......................................................... 239
  - IGMP Interfaces ............................................ 239
  - IGMP with IP Clustering ................................... 240
  - IGMP Show Commands ...................................... 242

- **PIM** ............................................................ 242
  - PIM Interfaces ............................................. 243
  - PIM With IP Clustering .................................... 243
  - Sparse Mode PIM ........................................... 243
  - Timer and Assert Rank Parameters for Dense Mode and Sparse Mode .................................. 244
Show PIM Commands ........................................... 253
Route Aggregation ........................................... 254
BOOTP .......................................................... 257
   BOOTP Interfaces ........................................... 257
   BOOTP Show commands ................................... 258
DVMRP .......................................................... 258
   DVMRP Interfaces ........................................... 259
   DVMRP Timers .............................................. 260
   DVMRP Show Commands ................................... 261
Static Routes .................................................. 262
   Configuring Static Routes ................................. 262
VRRP ........................................................... 265
   All Implementations ....................................... 266
   Simplified Method Monitored-Circuit VRRP ........... 267
   Full Method Monitored-Circuit VRRP ................... 270
      VRRP Show Commands ................................. 271
   VRRPv2 ..................................................... 272
      VRRPv2 Interfaces ..................................... 272
ICMP Router Discovery ....................................... 274
   ICMP Router Discovery Interfaces ....................... 274
   ICMP Router Discovery Show Commands ............... 276
IP Broadcast Helper .......................................... 276
   IP Broadcast Helper Forwarding ......................... 277
   IP Broadcast Helper Interfaces ......................... 277
   IP Broadcast Helper Show Commands ................... 278
Network Time Protocol ....................................... 278
   Configuring an NTP Server .............................. 278
   Adding an NTP Server .................................... 279
   Deleting an NTP Server .................................. 279
   NTP Show Commands ..................................... 280
Dial on Demand Routing ..................................... 280
   Dial on Demand Routing Commands .................... 281
Routing Option Commands ................................... 284
Equal-cost Path Splitting (Load Sharing) ...................... 284
Protocol Rank .................................................. 285
Trace Routing Commands ...................................... 286
Configuring the Trace Log File ................................ 286
Trace Option Variables ......................................... 287
Show Route Summary Commands ............................... 297
Route Summary Commands ..................................... 297
Show Routing Daemon (IPSRD) Commands .................... 299
Show MFC Commands ............................................ 300

5 Traffic Management Commands .............................. 303
IP Clustering Commands ....................................... 303
General Clustering Commands ................................ 303
Clustering Administration ..................................... 317
Managing Join-Time Shared Features ......................... 318
Configuring Join-Time Shared Features ....................... 320
Installing IPSO Images on a Cluster ......................... 321
Access List Commands ......................................... 322
ACL Node Commands ........................................... 323
ACL Ruleset Commands ........................................ 325
Aggregation Class Commands ................................ 331
Set, Change, and View Aggregation Classes ................. 331
Queue Class Commands ........................................ 332
Set, Change, and View Queue Classes ....................... 332
ATM QoS ......................................................... 336
Configuring ATM QoS Descriptors ............................ 336
DSCP to VLAN Priority Commands ........................... 338
Configuring DSCP to VLAN Mapping ......................... 339

6 System Configuration Commands ......................... 341
System Configuration Summary ............................... 341
Configuring DHCP .............................................. 341
DHCP Service Commands ...................................... 341
Configuring DHCP Clients ........................................... 342
Configuring DHCP Servers ........................................ 344
Configuring Subnets .................................................. 344
Configuring Fixed-IP Addresses ................................. 348
Configuring Dynamic Domain Name System (DDNS) Service 351
Configuring Dynamic Domain Name System (DDNS) Zones 353
Backup and Restore Files ........................................... 354
Manually Backing Up .............................................. 354
Scheduling Backups ............................................... 355
Transferring Backup Files to a Remote Server .................. 357
Configuring Automated Transfers ............................ 358
Transferring Backup Files Manually ......................... 359
Restore Files from Locally Stored Backup Files .......... 360
Restore Files from Backup Files Stored on Remote Server ... 361
Show Backup Commands ........................................... 362
Schedule Jobs Through Crontab File .......................... 365
Scheduling Jobs ..................................................... 366
Adding Jobs ......................................................... 366
Deleting Jobs ....................................................... 366
Show Cron Commands ............................................. 368
System Failure Notification Configuration ................. 369
Enabling System Failure Notification ......................... 369
Show System Failure Notification ........................... 370
DNS ................................................................. 370
Setting DNS ........................................................ 370
Show DNS ........................................................ 371
Deleting DNS ....................................................... 371
Static Host Address Assignment Configuration .......... 372
Adding New Host Names ........................................ 372
Modifying Host Names ........................................... 372
Deleting Host Names .............................................. 373
7 SNMP Commands ........................................ 405
SNMP Description ........................................ 405
SNMP Command Set ........................................ 406
Enabling/Disabling and Setting SNMP .................. 408
Enabling and Disabling SNMP Traps .................... 411
Enabling/Disabling and Changing SNMPv3 USM Users .. 415
Show SNMP Implementation and Trap Commands ...... 418
Show SNMPv3 Users Commands ......................... 419

8 IPv6 Commands ........................................ 425
Configuration Summary .................................. 425
Interface Commands ..................................... 425
Neighbor Discovery Protocol ............................ 427
Tunnels .................................................. 430
IPv6 to IPv4 ............................................ 434
IPv6 Over IPv4 .......................................... 435
IPv6 Routing Configuration .............................. 436
RIPng .................................................. 436
   Interfaces ......................................... 437
   Show Commands ................................... 437
Route Aggregation ...................................... 438
Static Routes .......................................... 439
ICMP Router Discovery .................................. 442
   Interfaces ......................................... 442
   Show Commands ................................... 447
VRRP for IPv6 .......................................... 447
   All implementations ................................ 447
VRRPv3 ................................................ 448
   Monitored Circuit for IPv6 Interfaces ............... 451
VRRP for IPv6 Show Commands ......................... 455
Show Routing Summary Commands ..................... 455
Host Name Configuration ............................... 456
Network Access and Services ......................... 457
9 Monitoring Commands ........................................... 459
   Current and Historical Network Reports ................. 459
   Configuring How Much Data is Stored .................. 459
   Configuring CPU Utilization Reports ...................... 460
   Configuring Memory Utilization Reports ................ 461
   Configuring Interface Linkstate Reports ................. 462
   Configuring Rate Shaping Bandwidth Reports .......... 463
   Configuring Interface Throughput Reports .............. 464
Useful System Information .................................. 465
   Displaying Useful System Statistics .................... 466
   Displaying Interface Settings ............................ 466
   Displaying System Logs .................................. 466
   Displaying Interface Traffic Statistics ................. 469
   Displaying the Interface Monitor ....................... 469
   Displaying Resource Statistics ......................... 470
   Displaying the Forwarding Table ....................... 471
Displaying Hardware Monitors .............................. 473
   Displaying a Temperature Sensor Information .......... 473
   Displaying a Watchdog Timer Information ............... 474
   Displaying Voltage Sensor Information ................ 475
   Displaying Power Supply Information .................. 477
   Displaying Fan Sensor Information ..................... 478
   Displaying a Network Interface Card Slot Status .... 479

10 Command-Line Utilities ................................. 481

   List of Commands .......................................... 545

Index .......................................................... 637
About This Guide

You can now use a command-line interface (CLI) to configure and monitor IPSO systems. The CLI complements Nokia Network Voyager, the Nokia web-based interface for IPSO systems, by allowing you to chose the interface you are most comfortable with.

Everything that you can accomplish with Voyager can also be done with the CLI. You can enter CLI commands individually and you can also create batch files of CLI commands to automate configuration tasks. You should have a fundamental knowledge of routing principals, security software, firewalls, and command-line interfaces on UNIX-based systems.

This guide provides all of the information you need to create and implement command-line interface (CLI) commands that are applicable to IPSO 3.8.

Document Organization

This guide is organized into the following chapters:

- Chapter 1, “Introducing the Command-Line Interface”
- Chapter 2, “Interface Commands”
- Chapter 4, “Routing Commands”
- Chapter 3, “Network Security and Access Commands”
- Chapter 5, “Traffic Management Commands”
- Chapter 7, “SNMP Commands”
Document Conventions

The following sections provide document conventions used throughout this guide.

Cautions and Notes

⚠️ **Caution**
Cautions indicate potential equipment damage, equipment malfunction, loss of performance, loss of data, or interruption of service.

---

**Note**
Notes provide information of special interest or recommendations.

Command Syntax Conventions

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

---

**Note**
The Nokia CLI prompt is omitted from the examples shown in this guide.
Command Syntax Example 1

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

save clienv

Text you enter is shown as monospace font; for example, set clienv.

Each line that is indented under an earlier component of the command is an argument for that command; for example, debug, echo-cmd, on-failure, output, rows, and syntax-check are all arguments for the set clienv command.

If more than one choice is applicable in the command string, the alternative, mutually exclusive choices are surrounded by angle brackets (<>) and separated by vertical lines (|) or by a hyphen if the choices cover a range; for example, <pretty | structured | xml> and <0-65535>. If a default value is applicable, that value is shown underlined; for example, pretty.

If a phrase or term in the command syntax is italicized, then that term or phrase is a placeholder for an entry you select. In the above example, where the line reads rows integer, your actual entry might be rows 5.

Command Syntax Example 2

set [slot <1-15>] interface log_if_name address ip_address

If one of more phrases or terms are surrounded by square brackets, as in [slot <1-15>], then the information inside the square brackets is optional and might or might not be included in your use of the command.
Additional Documentation

For supporting documentation, see the following documents:

- *Voyager Reference Guide*, which is on the IPSO 3.8 CD
- IPSO 3.8 *Getting Started Guide and Release Notes*, which is included in the release pack
1 Introducing the Command-Line Interface

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

To use the CLI:

1 Log on to the platform using a command-line connection (SSH, console, or telnet) over a TCP/IP network as an admin, cadmin, or monitor user.
   If you log in as a cadmin (cluster administrator) user, you can change and view configuration settings on all the cluster nodes. See Chapter 5, “Traffic Management 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 the one of the procedures explained in the next section.
# Invoking the CLI

You can execute CLI commands from the CLI shell and the IPSO shell. The IPSO shell is what you see when you initially log on to the platform.

<table>
<thead>
<tr>
<th>Execute From</th>
<th>To Implement</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSO shell</td>
<td>Enter <code>clish</code> 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 <code>clish -c &quot;cli_command&quot;</code></td>
<td>Lets you execute a single CLI command. You must place double-quotiation marks around the CLI command</td>
</tr>
<tr>
<td>Command files</td>
<td>• Enter <code>clish -f filename</code> &lt;br&gt; • Enter <code>clish</code> to invoke the shell. Then enter load commands <code>filename</code></td>
<td>Lets you load commands from a file that contains commands. The argument must be the name of a regular file.</td>
</tr>
</tbody>
</table>
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>-d</td>
<td>Sets the debug level; Enter an integer from 0 to 5 as the parameter</td>
</tr>
<tr>
<td>-o</td>
<td>Sets output format; enter either pretty, structured, or xml.</td>
</tr>
<tr>
<td>-s</td>
<td>Use with -c or -f to force a permanent configuration save. For example, enter clish -s -f filename or clish -s -c &quot;cli_command&quot;</td>
</tr>
<tr>
<td>-i</td>
<td>Use before -f 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

debug <0-5>  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
   Default: 0

echo-cmd <on | off>  Specifies to echo all commands. When using the load commands command, all commands are echoed before being executed.
   Default: off

on-failure <stop | continue>  Continue specifies to continue executing commands from a file or a script and only to display error messages. Stop specifies to stop executing commands from a file or a script when the system encounters an error.
   Default: stop

output <pretty | structured | xml>  Specifies the command-line output format.
   Default: pretty

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.
   Default: Specified by your console or xterm window.
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**

- `debug`: Displays the configured debug level.
- `echo-cmd`: Displays whether or not echo-cmd is enabled.
- `on-failure`: Displays whether or not on-failure is enabled.
- `output`: Displays the configured output.
- `rows`: Displays the number of screen rows configured.
- `syntax-check`: Displays whether or not syntax-check is enabled.

**syntax-check <on | off>**

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

**Default:** off

**save clienv**

Specifies to save the environment variables that the user modifies with the `set clienv` commands.
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/JaVED1rk2DiPm1XHF/;
    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>
  inatarp  - 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 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, like you can with 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 *nn*th 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 *n*th 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.
- **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 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.
1 Introducing the Command-Line Interface

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

**Arguments**

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

### 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**

- `fsinfo` Displays the number of file systems, the directories in which they are mounted, and their capacity.
- `processes` Displays the currently running processes
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.
2 Interface Commands

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

General Commands

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

Viewing All Interfaces

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

```plaintext
show interfaces
```

Interface Names

When a physical interface is installed, the system automatically creates a corresponding logical interface and supplies default names for the physical and logical interface. To make an interface functional, you need to configure both the physical interface and at least one corresponding logical interface (you can create multiple logical interfaces for a single physical interface in some cases).
The `show interfaces` command displays the physical and logical names of all the installed interfaces (as well as other information). You use these names when viewing or configuring specific interfaces.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if_name</code></td>
<td>Physical or logical interface name is acceptable.</td>
</tr>
<tr>
<td><code>phys_if_name</code></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><code>log_if_name</code></td>
<td>Only a logical interface name is acceptable. The default name for a logical interface is the name of the physical interface with <code>unit_number</code> appended (in which <code>unit_number</code> uniquely identifies the logical interface). For example, the default name for the first logical interface created for physical Ethernet interface <code>eth-s1p1</code> is <code>eth-s1p1c0</code>. 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
2 Interface Commands

show interface if_name status

To see various statistics about an interface, enter
show interface if_name statistics

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

ARP

This section contains commands to configure the Address Resolution Protocol (ARP).

ARP Commands

Use the following commands to configure ARP behavior.

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

Use the following commands to show the current ARP settings.

show arp
    keep-time
    retry-limit
    accept-multicast-replies
    all

Arguments

all Shows all the current configuration settings.
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
```

**keep-time <60–86400>**  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).

**Default:** 14400 seconds (4 hours).

**retry-limit <1–100>**  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).

**Default:** 3

**accept-multicast-arprep lies <on | off>**  Specifies or shows whether the router accepts ARP replies with a multicast address.

**Default:** off
Use the following commands to show the current proxy, static, and dynamic ARP entries.

```
show arp proxy all
show arp static all
show arp dynamic all
```

**Arguments**

- `arp proxy all`  
  Shows all the proxy ARP entries for the system.

- `arp static all`  
  Shows all the static ARP entries for the system.
Use the following commands to delete ARP addresses.

```
delete
   arpproxy address ip_address
   arps static address ip_address
```

**ATM Interfaces**

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

**Physical ATM Interfaces**

Use the following commands to configure and view the settings of physical ATM interfaces.

```
set interface phys_if_name
   active <on | off>
   framing <sonet | sdh>
   transmitclock <freerun | looptiming>
   atm-oam <on | off>
   vc-max maxVPI/maxVCI
```
## 2 Interface Commands

```
show interface phys_if_name
  all
  framing
  transmitclock
  atm-oam
  vc-max
  statistics
  lb-status
  status
```

### 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>active &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> on</td>
</tr>
<tr>
<td>framing &lt;sonet</td>
<td>sdh&gt;</td>
</tr>
<tr>
<td></td>
<td>type of transmission network this interface is connected to.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> sonet</td>
</tr>
<tr>
<td>transmitclock</td>
<td>&lt;freerun</td>
</tr>
<tr>
<td></td>
<td>internal clock. If two ATM</td>
</tr>
<tr>
<td></td>
<td>interfaces are connected directly with each other, at least one of them must use an internal clock. The loop-timing choice causes the interface to derive the transmit clock from the recovered receive clock.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> freerun</td>
</tr>
</tbody>
</table>

---

CLI Reference Guide for Nokia IPSO 3.9
Use the following commands to create logical ATM interfaces.

**atm-oam <on | off>**
Specifies whether OAM cell processing is enabled at the ATM VC layer. If OAM is enabled, the interface sends LB responses and RDI cells to active VCs when needed.
**Default:** off

**vc-max maxVPI/maxVCI**
Specifies or shows the ranges of virtual path identifiers (VPIs) and virtual channel identifiers (VCIs) for the ATM interface. The possible values are
- 0/4095: The VPI must be 0 and the range of possible VCIs is 1–4095.
- 1/2047: The range of VPIs is 0–1 and the range of possible VCIs is 1–2047.
- 3/1023: The range of VPIs is 0–3 and the range of possible VCIs is 1–1023.
- 255/15: The range of VPIs is 0–255 and the range of possible VCIs is 1–15.

To see information about setting the actual VPI and VCI values, see page 48.

**statistics**
Shows traffic and error information about the interface.

**lb-status**
Shows the loopback status of virtual channels.

**status**
Shows whether the interface is active or inactive.

**Logical ATM Interfaces**

Use the following commands to create logical ATM interfaces.
add interface phys_if_name [unit <1-255>] type
   ipoa vcs [VPI/]VCI(s) [logical-name log_if_name]
   p2p vc [VPI/]VCI [logical-name log_if_name]

Arguments

unit <1-255> Identifies a specific logical interface. The
default name of the logical interface is the
name of the physical interface followed by c
and this number. For example, entering
add interface atm-s1p1 unit 0
creates the logical interface atm-s1p1c0.

ipta vcs [VPI/]VCI{s} Creates a logical interface that is part of an IP
over ATM connection (also called a logical IP
subnet, or LIS).
You can specify a virtual path identifier (the
default is 0) and one or more virtual channel
identifiers. The acceptable values for VPI
and VCI(s) depend on the values you set
using the command set interface
phys_if_name vc-max (see page 47).
You can create multiple VCIs by specifying
ranges (for example, 8-15) or using commas
to separate individual VCIs (for example,
8,11,15).
The following are additional examples of
valid values for VCI(s) and VPI/VCI(s):
  • 8
  • 5,8-11
  • 3/5,8
  • 1/5-8,11,15-17
Use the following commands to configure logical ATM interfaces.

```
set interface log_if_name
  mtu <768—9180>
  address ip_address[/mask <8–30>]
  destination address
  unnumbered <yes | no>
  proxy-interface log_if_name
  enable | disable
  vcs [VPI/]VCI(s)
```

**Arguments**

- **mtu <768—9180>**
  Specifies the maximum transfer unit for the interface. The value must be an integer.
  **Default:** 1500

- **address ip_address[/mask <8–31>]**
  Specifies a local IP address for the logical interface. For ATM over IP interfaces, you must include the subnet mask length of the IP subnet connected to the interface.
## Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination address</strong></td>
<td>Specifies an IP address for the remote end of a point-to-point link—this should be the address of the interface at the other end of the link. This command is valid only for point-to-point interfaces.</td>
</tr>
<tr>
<td>**unnumbered &lt;yes</td>
<td>no&gt;**</td>
</tr>
<tr>
<td><strong>proxy-interface log_if_name</strong></td>
<td>Use when unnumbered mode is enabled to specify the interface from which the address for this interface is taken. <code>log_if_name</code> is the logical name of the other (numbered) interface. This command is valid only for point-to-point interfaces.</td>
</tr>
<tr>
<td>**enable</td>
<td>disable**</td>
</tr>
</tbody>
</table>
Use the following command to view the settings for a logical ATM interface.

```
show interface log_if_name
  all
  status
  unnumbered
  address
  destination
  mtu
  proxy-interface
  vcs
  type
  statistics
```

**Arguments**

- `all` Shows all the current configuration settings.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Shows whether the interface is active or inactive.</td>
</tr>
<tr>
<td>unnumbered</td>
<td>Shows whether the interface is unnumbered.</td>
</tr>
<tr>
<td>address</td>
<td>Shows the local IP address configured on the logical interface, if any. This argument is valid only for numbered interfaces.</td>
</tr>
<tr>
<td>instance</td>
<td>Shows the routing instance that this address belongs to.</td>
</tr>
<tr>
<td>destination</td>
<td>For point-to-point interfaces, this field contains the IP address configured for the remote end of the link. For broadcast media, this field contains the network address and the network mask length of the IP subnet connected to the interface. This argument is valid only for numbered interfaces.</td>
</tr>
<tr>
<td>mtu</td>
<td>Shows the maximum transmission unit of the interface.</td>
</tr>
<tr>
<td>proxy-interface</td>
<td>For unnumbered interfaces, this shows the logical name of the numbered interface from which the address for this interface is taken. (If you have changed the logical name of the proxy interface from the default name, this command does not show you the new name—it shows the original (default) name of the interface.) Only point-to-point interfaces can be configured as unnumbered.</td>
</tr>
<tr>
<td>vcs</td>
<td>Shows the virtual channel identifier(s) of the interface (IPoA or point-to-point).</td>
</tr>
</tbody>
</table>
Use the following command to create ARP entries for IP over ATM logical interfaces.

```
add interface log_if_name atmarp vc [VPI/]VCI(s) remote ip_address
```

Static ARP entries map IP addresses to virtual channels (the combination of a VPI and VCIs). They can be created for an interface only if the interface has an IP address assigned to it.

For a given physical ATM interface, only one logical interface can be assigned a static ARP entry at a given time—that is, a physical ATM interface supports only one association of an IP address to a virtual channel at a time.

**Arguments**

- **type**: Shows the type of the interface—IP over ATM (ipoa) or point-to-point (p2p).
- **statistics**: Shows traffic and error information for the interface.

**ARP Entries for IPoA Interfaces**

Use the following command to create ARP entries for IP over ATM logical interfaces.

```
add interface log_if_name atmarp vc [VPI/]VCI(s) remote ip_address
```

Static ARP entries map IP addresses to virtual channels (the combination of a VPI and VCIs). They can be created for an interface only if the interface has an IP address assigned to it.

For a given physical ATM interface, only one logical interface can be assigned a static ARP entry at a given time—that is, a physical ATM interface supports only one association of an IP address to a virtual channel at a time.

**Arguments**

- **vc [VPI/]VCI(s)**: Specifies the virtual path identifier and one or more of virtual channel identifier(s) of the logical interface. (The default VPI value is 0.) These VPI and VCI values specified here must match values already assigned to the logical interface being proxied.

The following are additional examples of valid values for **VCI(s)** and **VPI/VCI(s)**:

- 8
- 5,8-11
- 1/5-8,11,15-17


2 Interface Commands

remote ip_address  Specifies the IP address of the remote end of the virtual channel. Packets received by
                     log_if_name that are addressed to the remote IP address will be forwarded to it.

Use the following commands to view and delete ARP entries for IP over ATM logical interfaces.

show interface log_if_name atmarp
    static
    dynamic

delete interface log_if_name atmarp
    static vc VCI
    dynamic vc VCI

Arguments

static  Specifies a static ATM ARP entry (configured manually).

dynamic Specifies a dynamic ATM ARP entry (configured by the system).

vc VCI  Specifies the virtual channel identifier of the ATM ARP entry.

Use the following commands to configure global InATMARP protocol settings.

set inatmarp
    keep-time <1-900>
    timeout <1-30>
    max-retries <1-100>
    holdoff-time <1-900>
The InATMARP protocol is used to resolve IP addresses to ATM addresses in a logical IP subnet (LIS) on top of an ATM network.

Use the following command to view all the global InATMARP protocol settings.

```
show inatmarp
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>keep-time &lt;1–900&gt;</td>
<td>Specifies the number of seconds to keep resolved dynamic ATM ARP entries.</td>
<td>900</td>
</tr>
<tr>
<td>timeout &lt;1–30&gt;</td>
<td>Specifies the InATMARP request retransmission interval in seconds. This value must be less than a third of the keep-time value.</td>
<td>5</td>
</tr>
<tr>
<td>max-retries &lt;1–100&gt;</td>
<td>Specifies the number of times the system should retry InATMARP requests until holding off requests for the holdoff time.</td>
<td>5</td>
</tr>
<tr>
<td>holdoff-time &lt;1–900&gt;</td>
<td>Specifies the number of seconds to hold off InATMARP requests after the maximum number of retries has been reached.</td>
<td>60</td>
</tr>
</tbody>
</table>

**Ethernet Interfaces**

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

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

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

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

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>speed 10M</td>
<td>100M</td>
</tr>
<tr>
<td>Default:</td>
<td>10M</td>
</tr>
</tbody>
</table>

**Note**

Ethernet is the only interface type supported by the IP2250 appliance.
Logical Ethernet Interfaces

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

```
add interface log_if_name vlanid <2–4094> address ip_address/masklen <0–31>
```
2 Interface Commands

```plaintext
add interface log_if_name
    address ip_address/mask

set interface log_if_name
    vlanid <2–4094>
    logical-name new_log_if_name
    enable | disable
    MTU <1500–16,000>

show interface log_if_name vlanid
```

Arguments

- **vlanid <2–4094>**
  Specifies the virtual LAN that the logical interface is assigned to. You cannot assign a virtual LAN ID to the first logical interface for a given physical interface.

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

- **logical-name new_log_if_name**
  Specifies a new logical name for the interface or shows the current logical name. If a logical interface is part of an IPSO cluster, do not change its logical name.

- **enable | disable**
  Enables or disables the logical interface.
  **Default:** disable

- **MTU <1500–16,000>**
  Specifies the maximum transfer unit for the interface. The value must be an integer.
  **Default:** 1500
Transparent Mode

Transparent mode support gives you the ability to have firewall functionality on a layer 2 device like a switch or bridge. Some of the 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 support, you configure interfaces on the firewall router to act as ports on a bridge. The interfaces then forward traffic using layer 2 addressing. Nokia’s transparent mode supports only Ethernet 10/100/1000 Mbps. See “Logical Ethernet Interfaces” for more information on configuring Ethernet.

NOTE: Transparent mode support will not provide full-fledged bridging functionality such as loop detection or spanning tree.

Note
The Kona appliance does 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 <any interger greater than 0>
    interface logical_if_name
```

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

```
delete xmode
    id <any interger greater than 0>
    interface logical_if_name
```

Use the following commands to configure a transparent mode group.
2 Interface Commands

```
set xmode id <any interger greater than 0>
  state <on | off>
  vrrp_enabled <on | off>
```

Use the following commands to view transparent mode configurations.

```
show
  xmode id <any interger greater than 0> info
  xmode id <any interger greater than 0> interfaces
  xmode id <any interger greater than 0> stat
  xmode id <any interger greater than 0> state
  xmode id <any interger greater than 0> vrrp_enabled
  xmodes
```

**Arguments**

- `id <any interger greater than 0>`: Specifies an interger associated with a transparent mode group. When you use the argument with the `add xmode` command you will create a transparent mode group. For example, entering `add xmode id 100` on the command line will create a transparent mode group XMG 100.

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

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

- `vrrp_enabled <on | off>`: Enables or disable VRRP for a transparent mode group. **Default**: off

- `info`: Shows the configuration of the specified transparent mode group.

- `interfaces`: Shows the interfaces associated with the specified transparent mode group.
Link Aggregation

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.

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 ae10 and its logical name is ae10c0.

<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, for example, number of known neighbors, packet statistics, VRRP statistics relating to transparent mode, etc.</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>
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.

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

```
add linkaggregation
  group <1-1024>
  port phys_if_name [type primary]

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.

Use the following commands to view link aggregation settings.

```
show
  linkaggregation
  groups
  group <1-1024>
```
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.
2 Interface Commands

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.

delete 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 65.

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

Configuring PPPoE Logical Interface

Use the following commands to add a logical pppoe interface in dynamic mode.

add interface pppoe0 mode dynamic profile-name profile_name
            interface-name log_if_name
            enable off | on

Use the following commands to add 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

Use the following commands to add 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

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.

```plaintext
set interface pppoe0
    admin-status enable | disable
    link_trap on | off
```

**Arguments**

- `profile_name`: The name used to identify the profile with the associated logical interface. The profile name may be 1 to 31 characters long.
- `interface phys_if_name`: Specifies the physical ethernet interface.
- `mode <connect-on-demand | keep-alive>`: Specifies the available connection modes.
  - connect-on-demand: The interface comes up when IP traffic is generated.
  - keep-alive: The interface is always up.
- `noauth`: Specifies no authentication will be used.
- `authype <PAP | CASE>`: If you specify an authentication type, you must also specify the user name and password.
- `username user_name`: Specifies the user name when using authentication. The user name may be 1 to 63 characters long.
- `password pass_word`: Specifies the password the user must log in with. The password may be 1 to 31 characters long.
timeout <30-259200; 300>

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.

peername name

Specifies the PPPoE server from which the system will accept connections. When this is not specified, the system will accept connections from any PPPoE server. The name can be 1 to 63 characters long.

description name

Specifies an identity that the user may use to remember the profile.

mss mss_value

Specifies the size in bytes of the maximum segment size.

mtu <136-1492>

Specifies the size in bytes of the maximum transmission unit.
### Interface Commands

- **mode <unnumbered | dynamic | static>**
  Specifies how the logical interface will be assigned an IP address.

  - **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.

- **local-ipaddress ip_address**
  Used with mode static command to specify the local interface address.

- **remote-ipaddress ip_address**
  Used with mode static command to specify the remote interface address.

- **enable <off | on>**
  Enables or disables the logical interface.

- **admin-status disable|enable**
  Enable or disable the logical interface.

- **link_trap on | off**
  Enable or disable the link-trap for the logical interface.

### FDDI Interfaces

Use the commands explained in this section to configure physical and logical FDDI interfaces.
Physical FDDI Interfaces

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

```
set interface phys_if_name
  active <on | off>
  duplex <half | full>

show interface phys_if_name
  all
  duplex
  status
  statistics
```

**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>all</td>
<td>Shows a variety of information about the interface (not including traffic and error statistics).</td>
</tr>
<tr>
<td>duplex &lt;half</td>
<td>full&gt;</td>
</tr>
<tr>
<td>status</td>
<td>Shows whether the interface is active or inactive.</td>
</tr>
<tr>
<td>statistics</td>
<td>Shows traffic and error information for the interface.</td>
</tr>
</tbody>
</table>
Logical FDDI Interfaces

Use the following command to change the IP address of a logical FDDI interface.

```
add interface log_if_name address ip_address/mask <8-31>
```

Use the following command to enable or disable a logical FDDI interface.

```
set interface default_log_if_name
   enable | disable
   logical-name log_if_name
```

Use the following command to view information about a logical FDDI interface.

```
show interface default_log_if_name
   address
   status
   statistics
   logical-name
   all
```

### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_address/mask &lt;8-31&gt;</code></td>
<td>Specifies the IP address and subnet mask length for the logical interface.</td>
</tr>
<tr>
<td><code>default_log_if_name</code></td>
<td>Specifies the default logical name of the interface (such as fddi-s1p1c0).</td>
</tr>
<tr>
<td>`enable</td>
<td>disable`</td>
</tr>
<tr>
<td><code>address</code></td>
<td>Shows the IP address assigned to the logical interface.</td>
</tr>
<tr>
<td><code>status</code></td>
<td>Shows whether the interface is active or inactive.</td>
</tr>
</tbody>
</table>

---

2 Interface Commands
ISDN Interfaces

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

**Physical ISDN Interfaces**

The commands explained in this section let you configure and view the settings for physical ISDN interfaces.

```
set interface phys_if_name
  status <on | off>
  switch-type etsi
  line-topology [point-to-point | multi]
  tei-option [automatic | manual]
  tei-assignment [first-call | power-up]
  tei <0-63>
  local-number number
  local-sub-number number
  logging [warn | info | error]
  disconnect-channel <1 | 2>
```

---

**statistics**

Shows traffic and error information for the interface.

**logical-name**

Specifies a new logical name for the interface or shows the current logical name.

**all**

Shows a variety of information about the interface (not including traffic and error statistics).
show interface phys_if_name
   all
   status
   switch-type
   line-topology
   tei-option
   tei-assignment
   tei
   local-number
   local-sub-number
   logging
   disconnect-channel
   chan-state
   chan-link
   chan-call-info
   chan-last-call-info

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows all the current configuration information.</td>
</tr>
<tr>
<td>status &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>switch-type etsi</td>
<td>Specifies that the service provider’s switch is compliant with ETSI (European Telecommunications Standards Institute) standards. Default: etsi</td>
</tr>
<tr>
<td>line-topology [point-to-point</td>
<td>multi]</td>
</tr>
</tbody>
</table>
tei-option
[automatic | manual] Specifies whether the terminal endpoint identifier is assigned automatically or manually.
**Default:** automatic

tei-assignment
[first-call | power-up] Defines when terminal endpoint identifier negotiation occurs. The first-call parameter specifies that TEI negotiation occurs when the first ISDN call is placed or received. The power-up parameter specifies that the TEI is negotiated when the system is powered on.
**Default:** first-call

etei <0–63> Specifies the terminal endpoint identifier. This argument is valid only if tei-option has been set to manual.

local-number number If multiple devices are connected to a single ISDN line, use this argument to prevent the system from answering calls not intended for it. If you configure a local number, the system will answer only calls that have number as the called-party number in the setup message. If you configure a local number, the system will attempt to answer all calls. You can also configure a local subnumber that the system will check (in addition to the local number).

local-sub-number number If you configure a local subnumber, the system will answer only calls that have number as the called-party subaddress in the setup message.
2 Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging [warn</td>
<td>info</td>
</tr>
<tr>
<td></td>
<td>• error: An unrecoverable error condition occurred.</td>
</tr>
<tr>
<td></td>
<td>• warning: An event that may require attention occurred.</td>
</tr>
<tr>
<td></td>
<td>• informational: A noteworthy event occurred.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> error</td>
</tr>
<tr>
<td>disconnect-channel &lt;1</td>
<td>2&gt;</td>
</tr>
<tr>
<td>chan-state &lt;1–2&gt;</td>
<td>Shows the state of the specified B channel (whether its active or not).</td>
</tr>
<tr>
<td>chan-link &lt;1–2&gt;</td>
<td>Shows whether the link of the specified B channel is up or down.</td>
</tr>
<tr>
<td>chan-call-info &lt;1–2&gt;</td>
<td>Shows status information about the current call on the specified B channel</td>
</tr>
<tr>
<td>chan-last-call-info &lt;1–2&gt;</td>
<td>Shows status information about the last call made or received on the specified B channel.</td>
</tr>
</tbody>
</table>

Logical ISDN Interfaces

Use the following command to create logical ISDN interfaces.

```
add interface phys_if_name encapsulation <ppp | multilink-ppp>
```
Arguments

encapsulation Specifies the encapsulation protocol.
<ppp | multilink-ppp>

Use the following commands to add and delete incoming numbers for logical ISDN interfaces.

add interface log_if_name incoming-number number

delete interface log_if_name incoming-number number

Arguments

incoming-number number Specifies or deletes the remote numbers that can call into this interface. Incoming calls are checked against the incoming numbers configured for each logical interface. A call will be accepted on the first interface configured to accept incoming calls with an incoming number that matches the calling number in the incoming SETUP packet. If no match is found, the call is rejected. (This functionality requires that the network supports calling line identification.)

If an interface is configured to accept incoming calls (set to incoming or both—see page 78 for more information) and is not configured with any incoming numbers, it will accept any incoming calls.

Logical interfaces that are not configured to accept incoming calls or that are already connected will not accept incoming calls.
Use the following commands to configure logical ISDN interfaces and view the corresponding configuration settings.

```
set interface log_if_name
   enable | disable
   description description
   direction <outgoing | incoming | both>
   rate <64kbps | 56kbps>
   idle-time <0–999999>
   minimum-call-time <0–999999>
   remote-number number
   remote-sub-number number
   calling-number number
   calling-sub-number number
   local-name name
   local-password password
   remote-auth-method <pap | chap | none>
   remote-name name
   remote-password password
   bandwidth-util-level <0–100>
   bandwidth-util-period <0–999>
   echo-interval <0–255>
   max-echo-failures <0–255>
   max-mrru <0–99999>
   fragment-size <0–99999>
   address ip_address
   destination ip_address
   unnumbered <yes | no>
   proxy-interface if_name
   connect-channel
   lcp-options <magic-number | no-magic-number | mru | no-mru
   |mrru| no-mrru
   |short-seq-num | no-short-seq-num | endpoint-disc
   |no-endpoint-disc>
```
show interface log_if_name
   encapsulation
   status
   description
   direction
   rate
   idle-time
   minimum-call-time
   remote-number
   remote-sub-number
   calling-number
   calling-sub-number
   local-name
   local-password
   remote-auth-method
   remote-name
   remote-password
   bandwidth-util-level
   bandwidth-util-period
   echo-interval
   max-echo-failures
   max-mrru
   fragment-size
   address
   destination
   unnumbered
   proxy-interface
   connect-channel
   lcp-options
   incoming-number number

Arguments

enable | disable  Enables or disables the logical interface.

Default: disable

encapsulation  Specifies or shows whether the logical interface is configured to use PPP or multilink PPP encapsulation.
### Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Shows whether the logical interface is active or inactive.</td>
</tr>
<tr>
<td>description description</td>
<td>Specifies or shows a text string usually used to describe the purpose of the connection. To include spaces in the description, enclose the description in quotation marks.</td>
</tr>
<tr>
<td>direction incoming</td>
<td>Specifies or shows the direction of ISDN calls supported by the interface. Default: outgoing</td>
</tr>
<tr>
<td>rate 64kbps</td>
<td>Specifies or shows the connection speed for outgoing calls. Default: 64kbps</td>
</tr>
<tr>
<td>idle-time 0-999999</td>
<td>Specifies or shows the number of seconds an outgoing call is idle before the call is disconnected. A value of 0 indicates that an outgoing call never times out. Default: 120</td>
</tr>
<tr>
<td>minimum-call-time 0-999999</td>
<td>Specifies or shows the minimum number of seconds a call must be connected before it can be disconnected by an idle timeout. A value of 0 indicates that a call can be disconnected immediately. If the service provider has a minimum charge for each call, it is recommended that the minimum call time be set to 0. Default: 120</td>
</tr>
<tr>
<td>remote-number number</td>
<td>Specifies or shows the number to call when establishing an outgoing call.</td>
</tr>
<tr>
<td>remote-sub-number number</td>
<td>Specifies or shows the subaddress to use when establishing an outgoing call.</td>
</tr>
</tbody>
</table>
calling-number number Specifies or shows the calling number to insert in a setup message. If not specified, no calling number is sent.

calling-sub-number number Specifies or shows the calling subaddress to insert in a setup message. If not specified, no subaddress is sent.

local-name name Specifies or shows the name used to identify this host to a remote host when the remote host attempts to authenticate this host. This name must match the name for this host that is configured on the remote host. To include spaces in the name, enclose the description in quotation marks.

local-password password Specifies or shows the password returned to a remote host for PAP authentication or the secret used to generate the challenge response for CHAP authentication. To include spaces in the password, enclose the description in quotation marks.

remote-auth-method <pap | chap | none> Specifies or shows the method this host uses to authenticate a remote host.

• pap: password authentication protocol
• chap: challenge handshake password authentication protocol
• none: no authentication protocol—therefore, local-name and local-password do not apply
## Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote-name name</td>
<td>Specifies or shows the name of the remote host that this logical interface connects to. This name must match the name the remote host uses to identify itself. The name is used with the endpoint discriminator to form a multilink protocol bundle on this host.</td>
</tr>
<tr>
<td>remote-password password</td>
<td>Specifies or shows the password returned by the remote host specified with <code>remote-name</code> for PAP authentication or the secret used to validate the challenge response for CHAP authentication.</td>
</tr>
<tr>
<td>bandwidth-util-level &lt;0-100&gt;</td>
<td>Specifies or shows the percentage of bandwidth utilization at which bandwidth will be dynamically added or subtracted. When the utilization of the interface exceeds the percentage threshold defined by this value for longer than the time specified with <code>bandwidth-util-period</code>, a second channel is added. After a second channel has been added, if utilization falls below this threshold for longer than the time specified with <code>bandwidth-util-period</code>, the second channel is removed. This argument is valid only for interfaces that use multilink PPP encapsulation. <strong>Default:</strong> 70</td>
</tr>
</tbody>
</table>
bandwidth-util-period <0–999>
Specifies or shows the number of seconds utilization must remain above the threshold set by bandwidth-util-level before a second channel will be added. Once a second channel has been added, this value specifies the number of seconds that utilization of the interface must remain below the threshold before the second channel is removed. This argument is valid only for interfaces that use multilink PPP encapsulation.
Default: 10

echo-interval <0–255>
Specifies or shows the number of seconds between echo-request message transmissions (which test for an active remote system). This value must match the echo interval time configured on the system at the remote end of the link or the link state will fluctuate.
Default: 0

max-echo-failures <0–255>
Specifies or shows the maximum number of echo-request messages that can be sent without a reply being received. If no reply has been received after this number of requests have been sent, this system will consider the link to be down.
Default: 30

max-mrru <0–99999>
Specifies or shows the maximum size of a packet when all fragments have been reassembled (a reconstructed receive unit). This argument is valid only for interfaces that use multilink PPP encapsulation and only if you have enabled the mrru LCP option.
Default: 1500
### Interface Commands

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fragment-size &lt;0–99999&gt;</code></td>
<td>Specifies or shows the maximum size of a packet fragment that may be sent over a multilink protocol link. If set to zero, then packets will not be fragmented. This argument is valid only for interfaces that use multilink PPP encapsulation. <strong>Default:</strong> 0</td>
</tr>
<tr>
<td><code>address ip_address</code></td>
<td>Specifies or shows the IP address of the interface. You must enter a valid IP address. IPSO does not support dynamically assigning IP addresses for ISDN interfaces. Do not enter 0.0.0.0.</td>
</tr>
<tr>
<td><code>destination ip_address</code></td>
<td>Specifies or shows the IP address of the remote router’s point-to-point interface.</td>
</tr>
<tr>
<td>`unnumbered &lt;yes</td>
<td>no&gt;`</td>
</tr>
<tr>
<td><code>proxy-interface log_if_name</code></td>
<td>Use when unnumbered mode is enabled to specify the interface from which the address for this interface is taken. log_if_name is the logical name of the other (numbered) interface.</td>
</tr>
<tr>
<td><code>connect-channel</code></td>
<td>Use this argument to manually initiate a connection call on the B channel.</td>
</tr>
</tbody>
</table>
lcp-options
<magic-number | no-magic-number | c-number | mru | no-mru | mrru | no-mrru | short-seq-num | no-short-seq-num | endpoint-disc | no-endpoint-disc>

Specifies or shows link control protocol options.

- **magic-number/no-magic-number**: Specifies whether or not this system can negotiate and use a magic number to detect looped-back links.
- **mru/no-mru**: Specifies whether or not this system can negotiate a maximum receive unit value.
- **mrru/no-mrru**: Specifies whether or not this system can negotiate a maximum receive reconstructed unit value (which specifies the size of the reassembled multilink PPP packet). This argument is valid only for interfaces that use multilink PPP encapsulation. If you enable this option, then the maximum MRRU that can be negotiated is the value you set with the `max-mrru` argument.
- **short-seq-num/no-short-seq-num**: Specifies whether or not to use a short multilink protocol fragment sequence number (12 bits) to reduce fragment header overhead. This argument is valid only for interfaces that use multilink PPP encapsulation.
- **endpoint-disc/no-endpoint-disc**: Specifies whether or not this system can negotiate an endpoint discriminator to identify this host to multilink protocol peers. This argument is valid only for interfaces that use multilink PPP encapsulation.
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`
- `delete interface log_if_name address ip_address`
- `set interface log_if_name logical-name log_name`
- `show interface log_if_name addresses`

`incoming-number number` Shows the remote numbers that can call into this interface.
Logical or Physical Loopback Interfaces

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

```plaintext
show interface if_name
   status
   disabled-proto
   enabled-proto
   all
```

**Arguments**

- `if_name`: You can specify the logical or physical name of the interface.
- `status`: Displays whether the interface is active or not.
- `disabled-proto`: Displays protocols that are not enabled for the interface.
- `enabled-proto`: Displays protocols that are enabled for the interface.
- `all`: Displays all configuration options for the interface.

Modem Interfaces

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

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

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

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com2</td>
<td>com3</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>active</td>
<td>Shows whether the modem on the specified port is active.</td>
</tr>
<tr>
<td>inactivity-timeout &lt;0–5&gt;</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. Default: 0</td>
</tr>
</tbody>
</table>
### Modem Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>poll-interval &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. <strong>Default</strong>: 0</td>
</tr>
<tr>
<td>`enable-dialback</td>
<td>disable-dialback`</td>
</tr>
<tr>
<td><code>dialback-number</code></td>
<td>Specifies or shows the number that the system will call after it drops an incoming call.</td>
</tr>
<tr>
<td><code>phone_num</code></td>
<td></td>
</tr>
</tbody>
</table>
| `type <5oC1 | 5oC2>` | Specifies the type of PC Card (PCMCIA) modem that is installed.  
  - `5oC1`: Ositech Five of Clubs I  
  - `5oC2`: Ositech Five of Clubs II |
| `country-code`            | Specifies or shows the country code of the number that the system will call after it drops an incoming call.  
  - `0–99`: use when the modem type is `5oC1`  
  - `00–FF`: use uppercase hexadecimal when the modem type is `5oC2` |
| `status`                  | Shows whether there is a modem on the specified port.                                                                                       |
Serial Interfaces

Use the commands explained in this section to configure physical and logical serial interfaces. The commands for configuring physical interfaces are explained immediately below. To learn about configuring logical interfaces, see “Logical Serial Interfaces” on page 109.

Physical Serial Interfaces

Some commands apply to any physical serial interface and others are applicable only to specific types of interfaces.

Any Physical Interface

Use the following commands to configure and view the settings of any physical serial interface.

```
set interface phys_if_name
  active <on | off>
  encaps <chdlc | ppp | fr>
  keepalive <0—255>
  clocking <external | internal>
  queue-mode <disable | min-latency | max-bw>
```

```
show interface phys_if_name
  status
  encaps
  keepalive
  clocking
  speed
  queue-mode
```

Arguments

```
active <on | off>  Specifies whether this interface is on or off.
```
Serial Interfaces

<table>
<thead>
<tr>
<th>status</th>
<th>Shows whether this interface is on or off.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>encaps</strong></td>
<td>Specifies the datalink protocol to run over the device. This setting must match the datalink protocol of the system at the remote end of the point-to-point link.</td>
</tr>
<tr>
<td>&lt;chdlc</td>
<td>ppp</td>
</tr>
<tr>
<td>• chdlc: Cisco HDLC. Using this option creates a logical interface for this physical interface.</td>
<td></td>
</tr>
<tr>
<td>• ppp: point to point protocol. Using this option creates a logical interface for this physical interface.</td>
<td></td>
</tr>
<tr>
<td>• fr: frame relay. Using this option does not create a logical interface for this physical interface. To create a logical interface that uses frame relay encapsulation, you must also specify a datalink connection identifier (DLCI). See page 107 for more information.</td>
<td></td>
</tr>
<tr>
<td><strong>keepalive &lt;0–255&gt;</strong></td>
<td>Specifies the number of seconds between keepalive protocol message transmissions. These messages periodically test to find out if the remote system is active. This value must match the keepalive value configured on the remote system, or the link state will fluctuate. Setting the keepalive to 0 turns prevents this system from sending keepalive transmissions (that is, setting this to 0 turns off link-failure detection).</td>
</tr>
<tr>
<td><strong>Default:</strong> If you are using Cisco HDLC or frame relay encapsulation, the default is 10. If you are using PPP encapsulation, the default is 5.</td>
<td></td>
</tr>
</tbody>
</table>
HSSI, X.21, V.35 Interfaces

Use the following commands to configure and view the settings of a physical HSSI, X.21, or V.35 interface.

```
set interface phys_if_name
    channel-mode <full-duplex | loopback>
    speed <1-45000000 | 1-2048000 | 1-10000000>

show interface phys_if_name
    channel-mode
    speed
```
Serial Interfaces

Arguments

channel-mode  
<full-duplex | loopback>

- **full-duplex**: Specifies bidirectional data transfer. This is the usual operating mode of the device.
- **loopback**: The device will loop all received external traffic back to the sender and will loop all data transmitted from this system back to it. This mode should be used only for diagnosing configuration problems.

**Default**: full-duplex

speed

<1-45000000 | 1-2048000 | 1-10000000>

If this interface is set to use internal clocking, you must also use this command to set the internal clock speed (bits per second). This determines the data-transfer rate of the point-to-point link. If the interface can generate only certain clock speeds and rate you configure is not one of these values, the next highest valid speed is used. The ranges of possible values are identified below:

- HSSI interfaces: 1-45000000
- V.35 interfaces: 1-2048000
- X.21 interfaces: 1-2048000

T1 Interfaces

Use the following commands to configure and view the settings of a physical T1 interface.
2 Interface Commands

```plaintext
set interface phys_if_name
    channel-mode <normal | l1b | clb | rlb | plb>
    line-type <short-haul | long-haul>
    cable-length <0—655>
    transmit-loss <0 | -7.5 | -15 | -22>
    receiver-gain <-30 | -36>
    invert-data | noinvert-data
    timeslot channel(s)
    encoding <ami | b8zs>
    framing <sf | esf>
    channel-speed <64Kbps | 56Kbps>
    jitter-attenuator <off | rx | tx>
    jabuffer-depth <32 | 128>
    fdl-type <ansi | none>
    density-enforcer <on | off>
    speed
```

```plaintext
show interface phys_if_name
    channel-mode
    line-type
    cable-length
    transmit-loss
    receiver-gain
    invert-data
    timeslot
    encoding
    framing
    channel-speed
    jitter-attenuator
    jabuffer-depth
    fdl-type
    density-enforcer
    speed
```
**Arguments**

<table>
<thead>
<tr>
<th>channel-mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>normal</strong></td>
<td>Normal data transfer.</td>
</tr>
<tr>
<td><strong>llb</strong></td>
<td>(local loopback): The device will loop all transmitted data back into its receiver. This option should be used only for diagnosing configuration problems.</td>
</tr>
<tr>
<td><strong>clb</strong></td>
<td>(local channel loopback): The device will loop all transmitted data back to the internal receiver of this system. This mode should be used only for diagnosing configuration problems.</td>
</tr>
<tr>
<td><strong>rlb</strong></td>
<td>(remote loopback): The device will loop all received external traffic back to the transmitter without processing the incoming data. This mode should be used only for diagnosing configuration problems.</td>
</tr>
<tr>
<td><strong>plb</strong></td>
<td>(remote payload loopback): The device will loop all received external traffic back to the transmitter internally after processing the incoming data. This mode should be used only for diagnosing configuration problems.</td>
</tr>
</tbody>
</table>

**Default:** normal

Nokia T1 interface cards have built in CSU/DSU devices and provide the following channel mode options:
### Interface Commands

#### line-type

```
<short-haul | long-haul>
```

Specifies or shows whether this device is connected to a short-haul (DSX-1) or long-haul (CSU) line.

- **short-haul**: Select this option if the cable connected to this interface is less than or equal to 655 feet long.
- **long-haul**: Select this option when the interface is connected to repeatered lines more than a total of 655 feet long.

**Default:** short-haul

#### cable-length <0—655>

Specifies or shows the length of the cable (in feet) from the interface to the remote end of the link. The line build-out value (which allows signal strength to be properly adjusted) is automatically based on this value.

This argument is valid only if the line type is set to **short-haul**.

**Default:** 224

#### transmit-loss

```
<0 | -7.5 | -15 | -22>
```

Specifies or shows the line build-out value (the number of decibels by which the transmit signal is decreased).

This argument is valid only if the line type is set to **long-haul**.

**Default:** -15

#### receiver-gain <-30 | -36>

Specifies or shows the number of decibels by which the received signal is increased using pulse equalization.

This argument is valid only if the line type is set to **long-haul**.

**Default:** -30
invert-data | noinvert-data

You should enable data inversion when you have chosen any of the following settings:

• AMI line encoding
• 64Kbps channel speed
• pulse-density enforcer enabled

Data inversion turns the HDLC 0-bit-stuffing mechanism into a 1-bit-stuffing mechanism, which ensures that the data stream meets the rules required by ANSI T1.403. Data inversion is not required when B8ZS encoding or 56Kbps channel speed is configured. These settings guarantee that ANSI T1.403 pulse-density requirements are maintained.

Default: noinvert-data

timeslot channel(s)

Use this argument to selectively enable or show the DS0 channels that make up the T1 line, that is, configure fractional T1 lines. All the DS0 channels are enabled by default. If you use this argument to specify channels, those channels remain enabled and all the remaining channels are disabled.

You can enable multiple channels by specifying ranges (for example, 2–7) and/or using commas to separate individual channels (for example, 2, 5, 7). The acceptable range of channel values is 1–24.

The following are additional examples of valid values:

• 2 (all the other channels are disabled)
• 2, 7 (all the other channels are disabled)
• 2, 7, 11–18 (all the other channels are disabled)
encoding <ami | b8zs>

Specifies the line encoding used by the T1 channel. This setting must match the line encoding of the CSU/DSU at the remote end of the link.

- **ami**: Specifies alternate mark inversion encoding. When using this encoding, you can also enable the pulse-density enforcer to ensure that there are enough pulses on the line to maintain line synchronization.
- **b8zs**: Specifies bipolar 8-zero substitution. When you use this encoding, the pulse-density enforcer is automatically turned off.

**Default**: b8zs

framing <sf | esf>

Specifies or shows the framing format, which is used to divide the data stream into DS0 channels and to synchronize with the remote CSU/DSU. This setting must match the frame format used by the CSU/DSU at the remote end of the link.

- **sf**: Specifies superframe (or D4) framing, an older format that combines as many as 12 T1 frames into a superframe. If you use this format, you cannot use the fdl-type argument to specify that performance reports should be sent over the facilities data link.
- **esf**: Specifies extended superframe framing, which combines 24 T1 frames into a superframe. It also provides CRC checking on frames and a facilities data link for data monitoring and reporting.

**Default**: esf
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>channel-speed</strong></td>
<td>Specifies or shows the speed of the DS0 channels in the T1 line. This setting must match the channel speed used by the CSU/DSU at the remote end of the link.</td>
</tr>
<tr>
<td>64Kbps</td>
<td>All 8 bits of the channel are used to carry data. This is the most common configuration.</td>
</tr>
<tr>
<td>56Kbps</td>
<td>Only 7 of the 8 bits of each channel are used to carry data. This option is used on some older trunk lines.</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>64Kbps</td>
</tr>
<tr>
<td><strong>jitter-attenuator</strong></td>
<td>Jitter attenuation helps eliminate errors caused by random variations in a clock signal. It is usually used to eliminate fluctuations in the clock signal derived from the received bit stream.</td>
</tr>
<tr>
<td>off</td>
<td>Jitter attenuation is disabled.</td>
</tr>
<tr>
<td>rx</td>
<td>Jitter attenuation is enabled on the receiver (input).</td>
</tr>
<tr>
<td>tx</td>
<td>Jitter attenuation is enabled on the transmitter (output). This setting is appropriate when the built-in CSU (on the Nokia T1 interface card) is providing the clock signal for the link.</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>rx</td>
</tr>
</tbody>
</table>
jabuffer-depth <32 | 128>  Specifies or shows the jitter attenuator buffer length (in bits). The jitter attenuator buffer length is used to ensure the accuracy of the processed clock signal. This argument is valid only if jitter attenuation is enabled.
- 32: The buffer is 32 bits long. This setting is used when high clock accuracy is expected.
- 128: The buffer is 128 bits long. Use this setting when you expect significant amounts of jitter.

Default: 32

fdl-type <ansi | none>  Specifies or shows whether to send performance reports to the remote CSU/DSU. These performance reports are sent on the facilities data link (a dedicated channel) and do not affect data throughput on the T1 link. This argument is valid only if the interface is using extended superframe (esf) framing.
- ansi: Performance reports conforming to the ANSI T1.403 standard will be sent every second.
- none: No performance reports will be sent.

Default: ansi
Serial Interfaces

density-enforcer <on | off> Specifies or shows whether to use the pulse-density enforcer to force the transmit and receive data streams to meet the framing rules specified by the ANSI T1.403 standard. Nokia recommends that you enable the pulse-density enforcer when you use AMI line encoding. The enforcer is automatically disabled when B8ZS encoding is configured. Default: off

speed Shows the internal clock speed (in bps). This is the data-transfer rate of the point-to-point link.

E1 Interfaces

Use the following commands to configure and view the settings of a physical E1 interface.

set interface phys_if_name
  channel-mode <normal | llb | clb | rlb | plb>
  encoding <ami | hdb3>
  framing <el | el-noframe>
  crc4-framing | no-crc4-framing
  timeslot-16-framing | no-timeslot-16-framing
  timeslot channel(s)
  line-type <short-haul | long-haul>
  invert-data | noinvert-data
2  Interface Commands

```
show interface phys_if_name
  channel-mode
  encoding
  framing
  crc4-framing
  timeslot-16-framing
  timeslot
  line-type
  invert-data
```
### Arguments

**channel-mode**

Nokia E1 interface cards have built-in CSU/DSU devices and provide the following channel mode options:

- **normal**: Normal data transfer.
- **llb** (local loopback): The device will loop all transmitted data back into its receiver. This option should be used only for diagnosing configuration problems.
- **clb** (local channel loopback): The device will loop all transmitted data back to the internal receiver of this system. This mode should be used only for diagnosing configuration problems.
- **rlb** (remote loopback): The device will loop all received external traffic back to the transmitter without processing the incoming data. This mode should be used only for diagnosing configuration problems.
- **plb** (remote payload loopback): The device will loop all received external traffic back to the transmitter internally after processing the incoming data. This mode should be used only for diagnosing configuration problems.
2 Interface Commands

encoding <ami | hdb3>

Specifies or shows the line encoding used by the E1 channel. This setting must match the line encoding of the CSU/DSU at the remote end of the link.

- **ami**: Specifies alternate mark inversion encoding. When using this encoding, you can also enable the pulse-density enforcer to ensure that there are enough pulses on the line to maintain line synchronization.
- **hdb3**: Specifies high density bipolar (order 3) encoding.

framing <e1 | e1-noframe>

Specifies or shows the framing format, which is used to divide the data stream into DS0 channels and to synchronize with the remote CSU/DSU. This setting must match the frame format used by the CSU/DSU at the remote end of the link.

- **e1**: Specifies E1 framing.
- **e1-noframe**: All timeslots will be used for data. If you use this framing format, you cannot use CRC 4 error checking and cannot configure fractional E1 channels.

crc4-framing | no-crc4-framing

Specifies or shows whether to use CRC 4 error checking. This argument is valid only if framing is set to **e1**.

**Default**: crc4-framing
timeslot-16-framing | no-timeslot-16-framing

Specifies or shows whether to use timeslot 16 for signaling or whether it should be available for use as a data channel.

- **timeslot-16-framing**: Specifies that timeslot 16 is used for line supervision signaling (for example, to determine if a telephone is on-hook or off-hook) and is thus not available to be used as a data channel. Enabling timeslot 16 framing is generally useful in telephony applications.

- **no-timeslot-16-framing**: Specifies that timeslot 16 is not used for signaling purposes (and is thus available to be used as a data channel).

This argument is valid only if framing is set to `e1`.

**Default**: no-timeslot-16-framing
timeslot channel(s) Use this argument to selectively enable or show the DS0 channels that make up the E1 line, that is, configure fractional E1 lines. All the DS0 channels are enabled by default. If you use this argument to specify channels, those channels remain enabled and all the remaining channels are disabled.
You can enable multiple channels by specifying ranges (for example, 2-7) and/or using commas to separate individual channels (for example, 2, 5, 7). The acceptable range of channel values is 1-31.
The following are additional examples of valid values:
• 2 (all the other channels are disabled)
• 2, 7 (all the other channels are disabled)
• 2, 7, 11-18 (all the other channels are disabled)
This argument is valid only if framing is set to e1.

line-type <short-haul | long-haul> Specifies or shows whether this device is connected to a short-haul (DSX-1) or long-haul (CSU) line.
• short-haul: Select this option if the cable connected to this interface is less than or equal to 655 feet long.
• long-haul: Select this option when the interface is connected to repeatered lines more than a total of 655 feet long.
Default: long-haul
If you set an interface to use frame relay encapsulation, use the following commands to configure and view the settings of the physical interface.

```
set interface phys_if_name
    dte | dce
    active-status-monitor <on | off>
    lmi-type <ansi | ccitt | fr-consortium>
    n391 <1—255>
    n392 <1—10>
    n393 <1—10>
    dlci-length <10 | 11 | 13>
```

```
add interface phys_if_name
dlci <16—1007>
```

```
show interface phys_if_name
dlci
```

You should enable data inversion when you are using AMI line encoding. Data inversion turns the HDLC 0-bit-stuffing mechanism into a 1-bit-stuffing mechanism.

Default: noinvert-data

**Frame Relay Encapsulation**

If you set an interface to use frame relay encapsulation, use the following commands to configure and view the settings of the physical interface.

```
set interface phys_if_name
    dte | dce
    active-status-monitor <on | off>
    lmi-type <ansi | ccitt | fr-consortium>
    n391 <1—255>
    n392 <1—10>
    n393 <1—10>
    dlci-length <10 | 11 | 13>
```

```
add interface phys_if_name
ndlci <16—1007>
```

```
show interface phys_if_name
    dte | dce
    active-status-monitor
    lmi-type
    n391
    n392
    n393
    dlci-length
```

**invert-data | noinvert-data**

You should enable data inversion when you are using AMI line encoding. Data inversion turns the HDLC 0-bit-stuffing mechanism into a 1-bit-stuffing mechanism.

Default: noinvert-data
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| dte | dce | Specifies or shows whether the interface operates in DCE or DTE mode.  
• DTE is typically appropriate when the interface is connected to a frame relay switch.  
• DCE mode is typically used if the interface is connected directly to a DTE device.  
**Default:** dte |
| active-status-monitor | Specifies or shows whether to monitor the connection status (and include the status in LMI status messages). You may want to turn off monitoring for testing purposes or when the interface is connected to a device that does not provide this status information.  
**Default:** on |
| lmi-type | Specifies or shows the LMI protocol used to communicate with a frame relay switch.  
• ansi: ANSI T1.617 Annex D specification  
• ccitt: CCITT Q.933 Annex A specification  
• fr-consortium: frame relay consortium specification  
**Default:** ansi |
| n391 | Specifies the number of partial LMI status requests (keepalives) to send before sending a full status request.  
**Default:** 6 |
n392 <1—10>
This is the LMI error threshold counter (n392), which is used with n393 to monitor the reliability of the link. Use this argument to specify the number of errored events that must occur before the link is considered unreliable.

**Default:** 3

n393 <1—10>
This is the LMI monitored event counter (n393), which is used with n392 to monitor the reliability of the link. Use this argument to specify the number of events (out of which there must be the number of errored events specified by the n392 argument) before the link is considered unreliable. This argument also specifies the number of monitored events that must occur without errors before the link is considered reliable again.

If you use the default values for n392 and n393, the link is considered unreliable if three out of four monitored events produce errors. If this occurs, the link is considered reliable again when four monitored events occur without any errors.

**Default:** 4

dlci-length
<10 | 11 | 13>
Specifies or shows the number of bits in the datalink connection identifier (DLCI) in the frame relay address. This argument is valid only if lmi-type is set to fr-consortium.

**Default:** 10

dlci <16—1007>
Creates a logical interface with the specified datalink connection identifier.
PPP Encapsulation

If you set an interface to use PPP encapsulation, use the following commands to configure and view the settings of the interface.

```
set interface phys_if_name
  keepalive-failures <1-255>
  magic-number | no-magic-number
  mru | no-mru

show interface phys_if_name
  keepalive-failures
  magic-number
  mru
```

**Arguments**

- **keepalive-failures**
  - *<1-255>*
  - Specifies or shows the number of times the remote system must fail to respond to keepalive protocol messages before this system considers the link down.
  - **Default:** 30

- **magic-number**
  - *| no-magic-number*
  - Specifies or shows whether this system can negotiate and use a magic number to detect looped-back links. This may need to be disabled if the remote system does not support the option.
  - **Default:** magic-number

- **mru**
  - *| no-mru*
  - Specifies or shows whether this system can negotiate a maximum receive unit value. This may need to be disabled if the remote system does not support the option.
  - **Default:** mru
Logical Serial Interfaces

Use the commands explained in this section to configure and view logical serial interfaces.

When you configure a physical serial interface to use PPP or Cisco HDLC encapsulation, a logical serial interface is automatically created for that physical interface. If you configure a physical serial interface to use frame relay encapsulation, a logical interface for it is not created until you also specify a datalink connection identifier (DLCI). (See page 89 for information about how to specify the encapsulation format for a physical serial interface. See page 107 for information about how to specify the DLCI for a physical interface.)

```
set slot <1-15> interface log_if_name
   logical-name log_if_name
   address ip_address
   destination ip_address
   unnumbered <yes | no>
   proxy-interface log_if_name
   enable | disable
   mtu <128-65535>
```

```
show slot <1-15> interface log_if_name
   all
   logical-name
   address
   destination
dlci
   unnumbered
   proxy-interface
   mtu
   status
   statistics
```

**Arguments**

| all | Shows all the current configuration settings. |
logical-name

Specifies a new logical name for the interface or shows the current logical name.

log_if_name

address ip_address

Specifies or shows the IP address of the logical interface.

destination ip_address

Specifies or shows the IP address of the remote router’s point-to-point interface.

dlci

Shows the datalink connection identifier of this interface. This is applicable only if the physical interface uses frame relay encapsulation.

unnumbered <yes | no>

Specifies or shows whether the interface is unnumbered. In unnumbered mode the interface does not have its own unique IP address—the address of another interface is used. Specify the other interface with the proxy-interface log_if_name form of this command.

Default: no

proxy-interface

log_if_name

Use when unnumbered mode is enabled to specify the interface from which the address for this interface is taken. log_if_name is the logical name of the other (numbered) interface.

mtu <128-65535>

Valid when physical media is HSSI.

enable | disable

Enables or disables the logical interface.

Default: disable

status

Displays whether the interface is active or not.
Each GPLC in an IP3000 Series system is divided into two “domains.” The local domain is under the control of the GPLC, and the other is under the control of the CRP. Unexported interfaces on the GPLC are part of the local domain, and exported interfaces are part of the domain controlled by the CRP.

Virtual point-to-point (VPP) interfaces provide connections between these domains. They allow processes running in the local domain of a GPLC to communicate and exchange traffic with the CRP and other GPLCs.

The system automatically creates two VPP interfaces for each GPLC. Interface vpp0 is in the local domain of the GPLC. Interface vpp1 is in the CRP’s domain—the system automatically exports vpp1 interfaces to the CRP. The default logical names for these interfaces are vpp0c0 and vpp1c0.

If you want the system to pass traffic and communicate between the two domains, you must configure both logical VPP interfaces to work with each other. You can configure VPP interfaces to be numbered or unnumbered. If the VPP interfaces are unnumbered, you may want to use the loopback interfaces on the CRP and GPLC as the proxy interfaces. This approach is advantageous because the loopback interfaces will not go down. See “Loopback Interfaces” on page 84 for more information.

If both of the VPP interfaces are numbered, both of the following must be true:

- the address of the exported interface must match the destination address of the unexported interface
- the address of the unexported interface must match the destination address of the exported interface

| statistics | Shows traffic and error information for the interface. |
If one of the VPP interfaces is numbered, its destination address must be the address of the proxy interface for the unnumbered interface.

Create Appropriate Static Routes

To pass traffic between unexported interfaces and the CRP, you must also configure appropriate static routes (on both the GPLC that has the unexported routes and the CRP). If the VPP interfaces are unnumbered, you must use logical-name as the gateway type when you create the static routes.

VPP Interface Commands

Use the following commands to configure and view the settings for VPP interfaces. When configuring or viewing the settings for unexported VPP interfaces, you must specify the chassis slot with the argument slot. When configuring or viewing the settings for exported VPP interfaces, do not use the argument slot. (The default logical name of an exported VPP interface identifies the chassis slot that the relevant GPLC is installed in. For example, the default logical name of the exported VPP interface of a GPLC installed in chassis slot 3 is vpp-s3/1c0.)

```
set interface log_if_name
  enable | disable
  address ip_address
  destination ip_address
  unnumbered <yes | no>
  proxy-interface log_if_name
  logical-name log_if_name
```
show interface log_if_name
    all
    status
    address
    destination
    unnumbered
    proxy-interface
    logical-name

**Arguments**

- **all**
  
  Shows all the current configuration settings.

- **status**
  
  Shows whether the interface is active.

- **enable | disable**
  
  Enables or disables the logical interface.

- **address ip_address**
  
  Specifies or shows the IP address of the logical interface.

- **destination ip_address**
  
  Specifies or shows the IP address of the point-to-point interface at the other end of the link.

- **unnumbered <yes | no>**
  
  Specifies or shows whether the interface is unnumbered. In unnumbered mode the interface does not have its own unique IP address—the address of another interface is used. Specify the other interface with the `proxy-interface log_if_name` form of this command.

- **proxy-interface log_if_name**
  
  Use when unnumbered mode is enabled to specify the interface from which the address for this interface is taken. `log_if_name` is the logical name of the other (numbered) interface.

- **logical-name log_if_name**
  
  Specifies a new logical name for the interface or shows the current logical name.
3 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.

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>
  cli-http <yes | no>
  cli-https <yes | no>
  com2-login <yes | no>
  com3-login <yes | no>
  com4-login <yes | no>
```
3 Network Security and Access Commands

Use the following command to configure a PCMCIA modem.

```
set modem com4 <country code>
```

Use the following commands to view network access configurations.

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

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>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp &lt;yes</td>
<td>no&gt;</td>
<td>Specifies FTP access to the platform.</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Specifies a port on which the ftpd server listens.</td>
<td>21</td>
</tr>
<tr>
<td>tftp &lt;yes</td>
<td>no&gt;</td>
<td>Specifies TFTP access to the platform.</td>
</tr>
<tr>
<td>telnet &lt;yes</td>
<td>no&gt;</td>
<td>Specifies TELNET access to the platform.</td>
</tr>
<tr>
<td>admin-net-login &lt;yes</td>
<td>no&gt;</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>cli-http &lt;yes</td>
<td>no&gt;</td>
<td>Specifies remote execution of CLI over HTTP.</td>
</tr>
<tr>
<td>cli-https &lt;yes</td>
<td>no&gt;</td>
<td>Specifies remote execution of CLI over HTTPS.</td>
</tr>
<tr>
<td>com2-login &lt;yes</td>
<td>no&gt;</td>
<td>Specifies login on the serial port ttyd1 com2 that may be connected to an external modem.</td>
</tr>
<tr>
<td>com3-login &lt;yes</td>
<td>no&gt;</td>
<td>Specifies login on the serial port ttyd2 com3 that may be connected to an external modem.</td>
</tr>
<tr>
<td>com4-login &lt;yes</td>
<td>no&gt;</td>
<td>Specifies login on the serial port ttyd3 com4 that may be connected to an external modem.</td>
</tr>
</tbody>
</table>
### Network Security and Access Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>`echo &lt;yes</td>
<td>no&gt;`</td>
<td>Specifies echo service, which sends back any data received by the platform to the originating source.</td>
</tr>
<tr>
<td>`discard &lt;yes</td>
<td>no&gt;`</td>
<td>Specifies discard service, which discards any data received by the platform.</td>
</tr>
<tr>
<td>`chargen &lt;yes</td>
<td>no&gt;`</td>
<td>Specifies chargen service, which sends back any data without regard to input. The data sent is a repeating sequence of printable characters.</td>
</tr>
<tr>
<td>`daytime &lt;yes</td>
<td>no&gt;`</td>
<td>Specifies daytime service, which sends the current date and time as a character string without regard to the input.</td>
</tr>
<tr>
<td>`time &lt;yes</td>
<td>no&gt;`</td>
<td>Specifies time service, which sends back the time, in seconds, since midnight January 1, 1900 the originating source. The value is sent as a binary number.</td>
</tr>
</tbody>
</table>
To purchase a license or increase your limit on your current license, call your Nokia representative or call (650) 625-2000 or (888) 477-4566 or email sales@iprg.nokia.com.

modem com4 <country code>

For the Ositech Five of Clubs card, use the following country codes. For the US, enter 22; for Canada, enter 20; for Australia, enter 1; for Belgium, enter 2; for Denmark, enter 3; for Finland, enter 4; for France, enter 5; for Germany, enter 6; for Greece, enter 16; for Iceland, enter 99; for Ireland, enter 7; for Italy, enter 8; for Luxembourg, enter 9; for the Netherlands, enter 10; for Portugal, enter 12; for Spain, enter 13; for Sweden enter 14; for Switzerland, enter 25; and for United Kingdom, enter 16.

For the Ositech Five of Clubs II card, use of the following country codes. For the US, enter B5; for Canada, enter 20; for Australia, enter 09; for Belgium, enter 0F; for Denmark, enter 31; for Finland, enter 3C; for France, enter 3D; for Germany, enter 42; for Greece, enter 46; for Iceland, enter 57; for Italy, enter 59; for Luxembourg, enter 69; for the Netherlands, enter 7B; for Norway, enter 82; for Portugal, enter B8; for Spain, enter A0; for Sweden, enter A5; for Switzerland, enter A6; and for United Kingdom, enter B4.
Configuring Software Licenses

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

```plaintext
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.

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

Use the following commands to show your software licenses.

```plaintext
show
    licensing
    licensing bgp-key
    licensing dvmrp-rip-key
    licensing dvmrp-ospf-key
    licensing igrp-key
    licensing dvmrp-key
```

**Arguments**

- `bgp-key license_key` Enables BGP feature.
- `dvmrp-rip-key license_key` Enables DVMRP with RIP feature.
- `dvmrp-ospf-key license_key` Enables DVMRP with OSPF feature.
IPsec Commands

This section describes the CLI commands you use to configure 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**
The IP2250 appliance does 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.

```
add ipsec proposal name

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

Arguments

proposal name Specifies a unique identifier for the proposal:
• Format: single word, no spaces allowed
• Example: 3des-md5

type <esp | ah> Specifies the type of proposal to add.
Default: esp

auth <sha1 | md5> Specifies the algorithm used to generate and
verify a hash for every packet.
Default: md5

crypto Specifies the algorithm used to encrypt the
<des | 3des | blowfish packets. AH proposals cannot have an
| null> encryption algorithm.
Default: des

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

show ipsec proposal
    all
    name

Arguments

proposal all Shows information about all proposals.

proposal name Shows information about a specified proposal.
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 133).

```plaintext
delete ipsec proposal
   all
   name
```

**Arguments**

- `proposal all` Deletes all proposals. You cannot delete proposals that are linked to a policy.
- `proposal name` Specifies the name of the proposal to delete.

**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.

```plaintext
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

filter name
    Specifies a name for the filter:
    • Format: single word, no spaces allowed
    • Example: 3des-md5

address ip_address
    Specifies the IP address of the desired subnetwork with host bits as zeroes (0):
    • Example: 10.2.0.0

mask <0—32>
    Specifies the mask length for the network.

address6 ip6_address
    Specifies the IPv6 address of the desired subnetwork:
    • Example: 1000:50:32::

mask6 <0—128>
    Specifies the mask length for the network.

proto
    Specifies the protocol of the packet to filter.
    Default: any

port <0—65535>
    Specifies the port number of the packet to filter, if appropriate, ignored otherwise.

Use the following command to show information about the specified filter:

show ipsec filter
    all
    name
3 Network Security and Access Commands

**Arguments**

<table>
<thead>
<tr>
<th>Command</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.

```
delete ipsec filter
    all
    name
```

**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.
- **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.
3 Network Security and Access Commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file name</td>
<td>Specifies the file, including the path, containing the CA certificate or the signed DEV certificate. <strong>Note:</strong> This parameter is valid only if the source is PEM</td>
</tr>
</tbody>
</table>
| 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  
  - 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. |

Use the following command to show information about the specified certificate or all certificates:

```
show ipsec x509cert all
   options <attrs | content | decoded>

name options <attrs | content | decoded>
```
**Arguments**

x509cert all  
**Shows information about all certificates.**

x509 name  
**Shows information about the specified certificate.**

options  
**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.

**Default:** attrs

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**

x509cert all  
**Deletes all certificates.**

x509 name  
**Specifies the name of the certificate to delete.**

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.
  - **Default:** 1024

- **sig-algo <dsa | rsa>**
  - Specifies the algorithm to use to generate the keys.
  - **Default:** 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, Nokia.

org-unit name Specifies the name of your subunit within your company or organization, for example, Nokia Engineering Department.

dns-name name Specifies the common DNS name (fully qualified domain name), for example: www.dns.nokia.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

e-mail Specifies the email address to contact the person responsible for this system or for its certificate, for example, webmaster@engineering.nokia.com. The CA sends notification to this address.

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

**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.
  - **Default**: **attrs**

Use the following command to delete all x509 certificate requests or a specific certificate request:

```plaintext
delete ipsec x509certreq
    all
    name
```

**Arguments**

- **x509certreq all**
  - Deletes all x509 certificate requests.

- **x509certreq name**
  - Specifies the name of the certificate request to delete.
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**

- `policy name` Specifies the name of the policy to add.
Use the following command to view information about the specified policy or all policies:

```
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>
```
show ipsec policy
  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. 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**

- **rule name**
  - Specifies the name of the rule to add.

- **mode**
  - Specifies the rule mode. The rest of the command depends on this value. Transport mode rules accept values only for policy name, source filter, and destination filter.
  - **Default:** tunnel
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<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>
<td>10.2.0.1</td>
</tr>
<tr>
<td>ip_address</td>
<td></td>
<td></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>
<td>10.2.0.2</td>
</tr>
<tr>
<td>ip_address</td>
<td></td>
<td></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>
<td>1000:50:32::1</td>
</tr>
<tr>
<td>ip6_address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote-address6</td>
<td>Specifies the IPv6 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>
<td>1000:50:32::2</td>
</tr>
<tr>
<td>ip6_address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>policy name</td>
<td>Specifies an existing policy for the rule.</td>
<td></td>
</tr>
<tr>
<td>src-filter name</td>
<td>Specifies an existing source filter for the rule.</td>
<td></td>
</tr>
<tr>
<td>dst-filter name</td>
<td>Specifies an existing destination filter for the rule.</td>
<td></td>
</tr>
<tr>
<td>inc-end-points</td>
<td>Specifies whether the tunnel end points are included in the filter.</td>
<td>off</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
<td></td>
</tr>
<tr>
<td>logical-interface</td>
<td>Specifies whether a separate logical interface is needed for this tunnel mode rule.</td>
<td>on</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
<td></td>
</tr>
</tbody>
</table>
The following command can be used to display information about a specified rule. Also, you can show all tunnel mode rules, all transport mode rules, or all rules.

```
show ipsec rule
   all [mode <tunnel | transport>]
   name
```

### Arguments

- `rule all` Shows information about all rules.
- `mode` Specifies whether to show all tunnel mode rules or all transport mode rules. This parameter is optional.
  - Default: `tunnel`
- `rule name` Shows information about a specific rule.

**hello-prot <on | off>**

Specifies whether the Hello protocol is running on the tunnel. Determines the end-to-end connectivity of a tunnel interface, modifying the link state if necessary.

**Default:** `off`

**hello-inv <0—21666>**

Specifies the time in seconds between Hello packets. The Hello Protocol must be running to set this value.

**Default:** `1`

**dead-inv <0—65000>**

Specifies the time in seconds before the interface is considered down. The Dead interval should be 3 times or more than the Hello interval. The Hello protocol must be running to set this value.

**Default:** `3`
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode</td>
<td>Specifies the rule mode. This allows you to delete all tunnel mode rules or all transport mode rules. <strong>Default:</strong> tunnel</td>
</tr>
<tr>
<td>rule name</td>
<td>Specifies the name of the rule.</td>
</tr>
<tr>
<td>policy name</td>
<td>Specifies the name of the policy to be detached from the rule.</td>
</tr>
<tr>
<td>src-filter name</td>
<td>Specifies an existing source filter for the rule.</td>
</tr>
<tr>
<td>dst-filter name</td>
<td>Specifies an existing destination filter for the rule.</td>
</tr>
<tr>
<td>rule all</td>
<td>Delete all rules. If you do not use the optional mode parameter, you delete all tunnel and transport mode rules.</td>
</tr>
</tbody>
</table>

### Miscellaneous IPsec Commands

Use the following command to configure various IPsec functionality:
set ipsec
    log-level <error | debug | info>
    hardware-accl <on | off>
    allow-interfaceless-tunnels <on | off>

Arguments

log-level <error | debug | info>
    Specifies the IPsec logging level. This affects the logging IPsec sends to SYSLOG.
    Default: error

hardware-accl <on | off>
    Turns hardware acceleration on or off for all interfaces. When you turn hardware acceleration on, it is enabled for all the interfaces.
    Default: off

allow-interfaceless-tunnels <on | off>
    Specifies whether to allow IPsec tunnels that are not associated with logical interfaces. In a new installation this flag is turned off.
    Default: off

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

ldap url
    Specifies the URL of the LDAP server.

Use the following commands to view miscellaneous information about IPsec properties:
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.
AAA

show aaa
    services
    service name

Arguments

service name          The name of an application or service that is to use AAA.
profile name          A service profile entry created by the command add aaa profile 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 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.
3 Network Security and Access Commands

```
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.
```

```
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.
```

```
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

**authprofile name**  
An authentication profile entry. The following authentication profiles are included in the IPSO operating system:

- base_httpd_authprofile
- base_login_authprofile
- base_other_authprofile
- base_snmpd_authprofile
- base_sshd_authprofile

**acctprofile name**  
An account profile entry. The following account profiles are included in the IPSO operating system:

- base_httpd_acctprofile
- base_login_acctprofile
- base_other_acctprofile
- base_snmpd_acctprofile
- base_sshd_acctprofile
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.

```
delete aaa authprofile name
```

Use the following command to change authentication profile configurations.

```
set aaa authprofile name
   authtype name
   authcontrol name
```

Use the following command to view authentication profile configurations.

```
```
show aaa
    authprofiles
    authprofile name
    authprofile name authtype
    authprofile name authcontrol

Arguments

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:
   • base_httpd_authprofile
   • base_login_authprofile
   • base_other_authprofile
   • base_snmpd_authprofile
   • base_sshd_authprofile

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
### Configuring Account Profiles

Use the following command to create an account profile entry.

```
add aaa acctprofile name accttype name acctcontrol name
```

---

<table>
<thead>
<tr>
<th>authcontrol name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 <code>required</code> is only effective when multiple authentication profiles are defined for a given service profile. The IPSO operating system includes the following control values:</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>required—The result is retained and the next algorithm is invoked.</td>
<td></td>
</tr>
<tr>
<td>requisite—A result of <code>error</code> is reported immediately and no further algorithms are invoked. Otherwise, the result is retained and the next algorithm is invoked.</td>
<td></td>
</tr>
<tr>
<td>sufficient—A result of <code>error</code> is ignored; If a previous algorithm has reported <code>error</code>, or the result of this algorithm is <code>error</code>, the next algorithm is invoked.</td>
<td></td>
</tr>
<tr>
<td>optional—A result of <code>error</code> is ignored and a result of <code>success</code> is retained. The next algorithm is always invoked.</td>
<td></td>
</tr>
<tr>
<td>nokia-server-auth-sufficient—Same as “sufficient,” except a result of <code>error</code> for this module is reported immediately and no further modules are invoked.</td>
<td></td>
</tr>
</tbody>
</table>
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
accttype name

The name of the account management algorithm. The IPSO operating system includes the following account management algorithms:

- PERMIT—(pam.permit.so.1.0) This algorithm returns PAM_SUCCESS when invoked.
- UNIX—(pam.unix.acct.so.1.0) This algorithm provides the basic UNIX accounting mechanism by checking if the password is still valid. If the password is expired, the algorithm logs in appropriate messages. The algorithm also prompts for a password change if the password is going to expire soon.
Configuring Session Profiles

Use the following command to create a session profile entry.

```bash
add aaa sessprofile name sesstype name sesscontrol name
```

Use the following command to delete an session profile entry.

```bash
delete aaa sessprofile name
```

Use the following command to change session profile configurations.

```bash
acctcontrol name
```

The name of a control value. The control value determines how the results of multiple accounting algorithms are applied and when additional algorithms are invoked. A control value other than `required` is only effective when multiple accounting 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.
3 Network Security and Access Commands

set aaa sessprofile name
    sesstype name
    sesscontrol name

Use the following command to view session profile configurations.

show aaa
    sessprofiles
    sessprofile name
    sessprofile name sesstype
    sessprofile name sesscontrol

Arguments

<table>
<thead>
<tr>
<th>sessprofile name</th>
<th>The name of a new session profile (add) or existing session profile (delete, set, show). The IPSO operating system includes the following session profiles:</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>sessstype name</th>
<th>The name of the session management algorithm. The IPSO operating system includes the following session management algorithms:</th>
</tr>
</thead>
<tbody>
<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>
sesscontrol name  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.

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
  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>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>base_httpd_authprofile</td>
<td></td>
</tr>
<tr>
<td>base_login_authprofile</td>
<td></td>
</tr>
<tr>
<td>base_other_authprofile</td>
<td></td>
</tr>
<tr>
<td>base_snmpd_authprofile</td>
<td></td>
</tr>
<tr>
<td>base_sshd_authprofile</td>
<td></td>
</tr>
</tbody>
</table>
### AAA

<table>
<thead>
<tr>
<th><strong>priority integer</strong></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>
<tbody>
<tr>
<td><strong>host IPv4 address</strong></td>
<td>The IP address of the RADIUS server in dot-delimited format.</td>
</tr>
<tr>
<td><strong>port 1-65535</strong></td>
<td>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). <em>port</em> also takes the keyword <em>unset</em>, which indicates that no value is set in the database so the default is used. <strong>Default:</strong> 1812</td>
</tr>
<tr>
<td><strong>secret name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>prompt secret</strong></td>
<td>Prompts you to enter the “shared secret” during the run of the command.</td>
</tr>
<tr>
<td><strong>timeout integer</strong></td>
<td>The number of seconds to wait, after contacting the server, for a response. The default value 3 seconds.</td>
</tr>
<tr>
<td><strong>maxtries integer</strong></td>
<td>The number of attempts to make to contact the server. <strong>Default:</strong> 3 (includes the first attempt, so a value of 3 means two retries)</td>
</tr>
</tbody>
</table>
Configuring TACPLUS

Use the following command to configure TACPLUS for use in a single authentication profile.

```
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.

```
delete aaa tacplus-servers authprofile name priority integer
```

Use the following commands to change the configuration of a TACPLUS entry.

```
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.

```
new-priority integer Changes the priority number of the server.
list Displays a list of all servers associated with an authentication profile.
```
show aaa tacplus-servers authprofile name priority integer
  host
  port
  timeout

Arguments

| authprofile name       | An authentication profile entry. The following authentication profiles are included in the IPSO operating system:
|                       | • base_httpd_authprofile
|                       | • base_login_authprofile
|                       | • base_other_authprofile
|                       | • base_snmpd_authprofile
|                       | • base_sshd_authprofile

| priority integer      | 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.

| host IPv4 address      | The IP address of the TACPLUS server in dot-delimited format.

| 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. |

**Default:** 1812
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.

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

show ssh server
  enable
```
Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable &lt;0</td>
<td>1&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 1</td>
</tr>
</tbody>
</table>

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.

```bash
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.

```bash
show ssh server
  allow-groups
  allow-users
  deny-groups
  deny-users
  permit-root-login
```
### Configuring Server Authentication of Users

Use the following commands to configure the type of authentication the server will use to authenticate users.

<table>
<thead>
<tr>
<th>Arguments</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 indentifications 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 indentifications 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>
```
set ssh server
    pubkey-authentication <0 | 1>
    password-authentication <0 | 1>
    rhosts-authentication <0 | 1>
    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>Argument</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.</td>
</tr>
<tr>
<td></td>
<td>If this is set to 0, other forms of authentication may be used.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>combined with successful RSA host authentication.</td>
</tr>
<tr>
<td>rsa-authentication</td>
<td>Default: 1</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>
```
3 Network Security and Access Commands

rsa-authentication <0 | 1>  Specifies whether pure RSA authentication is allowed (for version 1 of the protocol only).
   Default: 1

Configuring User Login Environment

Use the following commands to configure the user environment.

    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

print-motd <0 | 1>  Specifies whether text from /etc/motd is displayed when the user logs in interactively.
   Default: 1

use-login <0 | 1>  Specifies whether the login utility is used for interactive logins.
   Default: 0

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
listen-addr2
port
protocol
server-key-bits

Arguments

ciphers name  The following list of ciphers are used as the default setting:
• 3des-cbc
• blowfish
• arcfour
• cast128-cbs
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.
Default: 1
### Configuring Service Details

Use the following commands to configure service details.

```plaintext
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.

```plaintext
listen-addr  ip_address
listen-addr2 ip_address
port <1-65535>
protocol <1 | 2 | 1,2>
server-key-bits
<512 | 640 | 768 | 864 |
| 1024>
```

- `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. **Default:** 1,2
- `server-key-bits` defines the number of bits in the server key. **Default:** 768
show ssh server
  gateway-ports
  ignore-rhosts
  ignore-user-known-hosts
  key-regeneration-time
  login-grace-time
  max-starups

Arguments

gateway-ports <0 | 1>  Specifies whether remote hosts are allowed to connect to ports forwarded for the client. The value for no is zero (0).
   Default: 0

ignore-rhosts <0 | 1>   Specifies that .rhosts and .shosts files will not be used in authentication. This is relevant only if rhosts authentication or rhosts+RSA authentication is enabled. The value for yes is 1.
   Default: 1

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).
   Default: 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.
3 Network Security and Access Commands

**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.

```
set ssh server
  log-level name
  strict-modes <0 | 1>
```

Use the following commands to show service detail configurations.

```
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 sshd. The following are the values you can designate from least to most verbose:</td>
</tr>
<tr>
<td></td>
<td>• QUITE</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>
Configuring and Managing SSH Key Pairs

The commands in the following section allow you to configure and manage SSH key pairs.

Managing New Host Keys

Use the following commands to generate new host keys.

$$\text{set ssh hostkey}$$

\[
\begin{align*}
\text{v1 size integer} \\
\text{v2 dsa size integer}
\end{align*}
\]

Use the following commands to view host keys.

$$\text{show ssh hostkey}$$

\[
\begin{align*}
\text{v1} \\
\text{v2 dsa} \\
\text{v2 dsa ssh2-format}
\end{align*}
\]

Arguments

$$\text{v1 size integer}$$

Generates new RSA public/private key pair that will be used by the SSH server to authenticate itself to clients using SSH protocol version 1. Specify the size of the key in bits. The value of 1024 is recommended.

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.

Default: 1
Generating New User Identity Keys

Use the following commands to generate new user identity keys.

set ssh identity
    v1 user name size integer <passphrase name | prompt-passphrase>
    v2 user name size integer <passphrase name | prompt-passphrase>

Use the following commands to view identity keys.

show ssh identity
    v1 user name
    v2 dsa user name
    v2 dsa user name ssh2-format

v2 dsa size integer Generates new DSA public/private key pair that will be used by the SSH server to authenticate itself to clients using SSH protocol version 2. Specify the size of the key in bits. The value of 1024 is recommended.

v2 dsa Displays the DSA public key that will be used by the SSH server using the OpenSSH version of SSHv2.

v2 dsa ssh2-format Displays the DSA public key using SSHv2.
### Arguments

**v1 user name size integer**

<passphrase_name | prompt _passphrase>

Creates a new RSA public/private key pair that will be used to authenticate the given user to other SSH servers when connecting using SSH protocol version 1.

- **user name** The user for which you want to create a new key pair.
- **size integer** Key size in bits, for example 1024.
- **(Optional) passphrase_name** The passphrase the user will enter when using the key.
- **(Optional) prompt_passphrase** Prompts you to enter the passphrase on the command line.

**v2 dsa user name size integer**

<passphrase_name | prompt _passphrase>

Creates a new DSA 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** The user for which you want to create a new key pair.
- **size integer** Key size in bits, for example 1024.
- **(Optional) passphrase name** The passphrase the user will enter when using the key.
- **(Optional) prompt-passphrase** Prompts you to enter the passphrase on the command line.

**v2 dsa user name ssh2-format**

Displays the DSA public/private key in SSHv2.
Managing Authorized Keys

Use the following commands to add authorized keys.

```
add ssh authkeys
  v1 user name bits integer exponent integer modulus name comment name
  v2 dsa user name <openssl-format name | ssh2-format file name>
    comment name
```

Use the following commands to delete authorized keys.

```
delete ssh authkeys
  v1 user name id id number
  v2 dsa user name id id number
```

Use the following commands to view authorized keys configured for various user accounts.

```
show ssh authkeys
  v1 user name list
  v1 user name id id number
  v2 dsa user name list
  v2 dsa user name id id number
```
### Arguments

**v1 user name bits integer exponent integer modulus name comment name**

Associates an RSA authorized key to an account so that the owner of that key is allowed access without needing a password.

- **user name** Identifies the account to which you are giving the key access.
- **bits integer** Key size, for example 1024.
- **exponent integer** Usually the second number making up an RSA key, for example 35.
- **modulus name** A very long number that is usually the third value of an RSA key.
- **comment name** An added comment to help you identify the key. This is optional.

**v2 dsa user name
<openssh-format name | ssh2-format file name> comment name**

Associates an OpenSSH DSA authorized key to an account so that the owner of that key is allowed access without needing a password.

- **user name** Identifies the account to which you are giving the key access.
- **openssh-format name** The text of OpenSSH key.
- **ssh2-format file name** The file containing the SSHv2 formatted key.
- **comment name** An added comment to help you identify the key. This is optional.

**id id number**

The identification number associated with a particular key.

**list**

Shows “id” values associated with keys.
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>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon-enable</td>
<td>Enables and disables web configuration for the platform.</td>
<td>1</td>
</tr>
</tbody>
</table>

**Default:** 1
Voyager Web Access (SSL)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port &lt;1-65535&gt;</strong></td>
<td>Specifies the port number on which the Voyager web configuration tool can be accessed when <em>not</em> using SSL-secured connections. 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></td>
<td><strong>Default:</strong> 80</td>
</tr>
<tr>
<td><strong>ssl-port &lt;1-65535&gt;</strong></td>
<td>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 <a href="https://hostname/">https://hostname/</a> to <a href="https://hostname:PORTNUMBER/">https://hostname:PORTNUMBER/</a></td>
<td><strong>Default:</strong> 443</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
```
### Arguments

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-name name</td>
<td>Identifies where the certificate will go. The name is most commonly the fully qualified domain name for your platform, for example, <a href="http://www.ship.wwwidgets.com">www.ship.wwwidgets.com</a>. If you are generating a request for a certificate authority, the issuer may impose a different standard.</td>
</tr>
<tr>
<td>email-address name</td>
<td>Specifies an e-mail address that could be used for contacting the person responsible for platform and its certificate, for example, “<a href="mailto:webmaster@ship.wwwidgets.dom">webmaster@ship.wwwidgets.dom</a>”</td>
</tr>
<tr>
<td>cert-file path</td>
<td>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.</td>
</tr>
<tr>
<td>cert-request-file path</td>
<td>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.</td>
</tr>
<tr>
<td>key-file path</td>
<td>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.</td>
</tr>
</tbody>
</table>
User Management

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

**Arguments**

- **cert-file path**
  Specifies a file that contains the certificate you want to copy. The keyword should be followed by the path name to the file on the IPSO system. Use absolute pathnames.

- **key-file path**
  Specifies a file that contains the private key you want to copy. The keyword should be followed by the path name to a file on the IPSO system. Use absolute pathnames.

- **passphrase name**
  Enter the passphrase you used when generating the certificate and private key or certificate request. Using this syntax will echo your passphrase as you type.

- **prompt-passphrase**
  Prompts you to enter the passphrase you used when generating the certificate and private key or certificate request. Using this syntax will not echo your passphrase as you type.

**User Management**

Use the commands in “Adding New Users” and “Deleting a User” 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.

### Adding New 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 USM users, see the SNMP section.

```plaintext
set user
  name passwd
  name oldpass passwd newpass passwd
  name info string
  name uid <0-65535>
  name gid <0-65535>
  The default gid value is 10.
  name homedir Unix path name
  name shell string
  name homepage Tcl script name

add user
  name uid <0-65535> homedir Unix path name
```

**Note**  
You can use the `add user` command to add new users, but you must use the `set user name passwd` command to set the password and allow the user to log on to the system.
## Arguments

**name passwd**

Specifies the new user name. The command then prompts you to enter the user’s existing password followed by the user’s new password and to reenter the new password to verify it. For a new user or if you do not know the user’s password, hit enter after being prompted to enter the user’s existing password. This command sets the user’s new password. Use alphanumeric characters. A user password of at least 8 characters gives the user SNMPv3 USM permissions. If you do not want the specified user to have USM permissions, set the password with fewer than 8 characters.

**name oldpass passwd newpass passwd**

Specifies to configure a new password for the specified user. Enter the current password after `oldpass` and the new password after `newpass`.

**user name info 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.

**user name uid <0-65535>**

Specifies the specified user’s user ID, which is used to identify the user’s permissions.

**user name gid <0-65535>**

Specifies the numeric group ID that identifies the primary group to which a user belongs. Use the group management commands to specify membership in other groups.
Deleting a User

Using the following command to delete an existing user.

```
delete user
    username
```

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.

```
Note
Only users with admin user permissions can change the user and admin passwords.
```

```
set user <admin | monitor> oldpasswd newpasswd passwd
```
Arguments

<admin | monitor> Specifies whether to change either the admin or the monitor password. Enter the existing password and then the new password. If you do not know the existing password, enter " " as the value for the existing password (oldpass).

oldpass passwd newpass passwd

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

user <admin | monitor> mode <disabled | allowed | required> Specifies whether to disable, allow, or require S/Key authentication for admin or monitor users.
3 Network Security and Access Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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

users
Displays all users, their user IDs, primary group IDs, user shells, home directories, and home pages.

user name
Displays information about the specified user, including the user ID, primary group ID, user shell, home directory and home page.

Arguments

skey all
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.

skey user
<admin | monitor>
Displays whether S/Key is enabled or disabled for the specified user and the configured sequence and seed values if S/Key is enabled.

skey user
<admin | monitor>
sequence
Displays the configured sequence value for the specified user.

skey user
<admin | monitor>
seed
Displays the configured seed value for the specified user.

skey user
<admin | monitor>
mode
Displays whether S/Key is enabled or disabled for the specified user.

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 alphanumeric 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.
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)
4 Routing Commands

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

BGP

When you do initial configuration, set the router ID. You can also use the following commands to change the router ID.

```
set router-id
default
ip_address
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</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. Nokia 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>Command</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. <strong>Caution:</strong> 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.</td>
</tr>
<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 \texttt{as\_number}  
\hspace{1em} \texttt{<on | off>}  
\hspace{1em} description \texttt{text}  
\hspace{1em} local-address \texttt{ip\_address} \texttt{<on | off>}  
\hspace{1em} virtual-address \texttt{<on | off>}  
\hspace{1em} outdelay \texttt{<0-65535>}  
\hspace{1em} outdelay \texttt{off}  
\hspace{1em} peer \texttt{ip\_address} \texttt{<on | off>}  
\hspace{1em} peer \texttt{ip\_address} \texttt{med-out \texttt{<0-4294967294>}  
\hspace{1em} peer \texttt{ip\_address} \texttt{med-out default}  
\hspace{1em} peer \texttt{ip\_address} \texttt{accept-med \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{multihop \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{no-aggregator-id \texttt{<on | off>}}  
\hspace{1em} aspath-prepend-count \texttt{<1-25>}  
\hspace{1em} aspath-prepend-count \texttt{default}  
\hspace{1em} peer \texttt{ip\_address} \texttt{holdtime \texttt{<6-65535>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{holdtime default}  
\hspace{1em} peer \texttt{ip\_address} \texttt{keepalive \texttt{<2-21845>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{keepalive default}  
\hspace{1em} peer \texttt{ip\_address} \texttt{ignore-first-ashop \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{send-keepalives \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{send-keepalives \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{accept-routers all}  
\hspace{1em} peer \texttt{ip\_address} \texttt{accept-routes none}  
\hspace{1em} peer \texttt{ip\_address} \texttt{passive-tcp \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{authtype none}  
\hspace{1em} peer \texttt{ip\_address} \texttt{authtype md5 secret secret}  
\hspace{1em} peer \texttt{ip\_address} \texttt{throttle-count \texttt{<0-65535>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{throttle-count \texttt{off}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{ttl default}  
\hspace{1em} peer \texttt{ip\_address} \texttt{ttl \texttt{<1-255>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{suppress-default-originate \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{log-state-transitions \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{log-warnings \texttt{<on | off>}}  
\hspace{1em} peer \texttt{ip\_address} \texttt{trace bgp_traceoption \texttt{<on | off>}}  

\textit{Arguments}

\texttt{as\_number \texttt{<on | off>}} \hspace{0.5em} Specifies the autonomous system number of the external peer group. Enter an integer from 1-65535.
### 4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>description text</code></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>
<tr>
<td>`virtual-address &lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><code>outdelay &lt;0-65535&gt;</code></td>
<td>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. The value zero (0) disables this feature. Default: <code>0</code></td>
</tr>
<tr>
<td><code>outdelay off</code></td>
<td>Disables outdelay.</td>
</tr>
<tr>
<td>`peer 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>peer ip_address med-out &lt;0-4294967294&gt;</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 use 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.</td>
</tr>
<tr>
<td>peer ip_address med-out default</td>
<td>Specifies a metric value of 4294967294</td>
</tr>
<tr>
<td>peer ip_address accept-med &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>peer ip_address multihop &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>peer ip_address no-aggregator-id &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
peer ip_address aspath-prepend-count <1-25>
Specifies the number of times this router adds to the autonomous system path on external BGP sessions. Use this option to bias the degree of preference some downstream routers have for the routes originated by this router. Some implementations prefer to select paths with shorter autonomous system paths.

peer ip_address aspath-prepend-count default
Specifies a value of 1.

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.

peer ip_address keepalive <2-21945>
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.

peer ip_address keepalive default
 Specifies a keepalive interval of 60 seconds.
peer ip_address
ignore-first-ashop
<on | off>

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.

**Default:** off

peer ip_address
send-keepalives
<on | off>

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.

**Default:** off

peer ip_address
accept-routes all

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.

peer ip_address
accept-routes none

Specifies an inbound BGP policy route if one is not already configured. Enter `none` to delete routes learned from a peer. This option saves memory overhead when many routes are rejected because no inbound policy exists.

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.

**Default:** off
### 4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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.  
**Default:** none |
| **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 ttl default** | Specifies of value of 64 as 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. |
| **peer ip-address ttl <1-255>** | Specifies a value for 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 multiop option is enabled.  
**Default:** 64 |
| **peer ip_address suppress-default-originate <on | off>** | Specifies NOT to generate a default route when the peer receives a valid update from its peer.  
**Default:** off |
BGP Confederations

Use the following commands to configure BGP confederations. You can configure a BGP confederation in conjunction with external BGP.

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.  
Default: off

peer ip_address
log-warnings <on | off>

Specifies for the rouer to log a message whenever a warning scenario is encountered in the codepath.  
Default: off

peer ip_address trace
bgp_traceoption
<on | off>

Specifies tracing options for your BGP implemention. Log messages are saved in the var/log/isprd directory. Enter the following words to set each trace option. Enter packets to trace all BGP packets to this peer. Enter open to trace all the BGP open messages to this peer. Enter update to trace all the BGP update messages to this peer. Enter keepalive to trace all the keepalive messages to this peer. Enter all to trace all the message types. Enter general to trace message related to Route and Normal. Enter route to trace routing table changes for routes installed by this peer. Enter normal to trace normal protocol occurrences. Abnormal protocol occurrences are always traced. Enter state to trace state machine transitions in the protocol. Enter policy to trace application of the protocol and user-specified policy to routes being imported and exported.
Routing Commands

```
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
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>confederation identifier as_number</code></td>
<td>Specifies the identifier for the entire confederation.</td>
</tr>
<tr>
<td><code>confederation identifier off</code></td>
<td>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><code>confederation aspath-loops-permitted &lt;1-10&gt;</code></td>
<td>Enables the confideration identifier.</td>
</tr>
<tr>
<td><code>confederation aspath-loops-permitted default</code></td>
<td>Specifies the number of times the local autonomous system can appear in an autonomous system path for BGP-learned routes. If this number is higher than the number of times the local autonomous system appears in an autonomous system path, the corresponding routes are discarded or rejected.</td>
</tr>
<tr>
<td><code>routing-domain identifier as_number</code></td>
<td>Specifies a value of 1.</td>
</tr>
</tbody>
</table>
**BGP Route Reflection**

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

cluster-id ip_address  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.

cluster-id off  Disables the cluster ID.

default-med <0-65535>  Specifies the multi-exit discriminator (MED) metric used to advertise routes through BGP.

default-med off  Disables the specified MED metric.

default-route-gateway ip_address  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 <ip_address> suppress-default-originate on command.

default-route-gateway off  Disables the configured default BGP route.

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>Option</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>
</tbody>
</table>
Internal BGP

Use the following commands to configure internal BGP sessions, that is, between routers within the same autonomous system.
BGP

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 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>

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>
med default
outdelay <0-65535>
\hspace{10pt} 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.
\hspace{10pt} **Default:** 0
outdelay off
\hspace{10pt} Disables outdelay.
next-hop-self <on | off>
\hspace{10pt} Specifies for this router to send one of its own IP addresses as the BGP next hop.
\hspace{10pt} **Default:** off
local-address ip_address <on | off>
\hspace{10pt} 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>
\hspace{10pt} 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.
\hspace{10pt} **Default:** off.
interface [all | if_name] <on | off>
\hspace{10pt} Specifies whether to enable the specified internal peer group on all interfaces or a specific interface.
protocol [all | bgp_internal_protocol] <on | off>
\hspace{10pt} 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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer ip_address</td>
<td>Specifies an internal peer address and peer type.</td>
</tr>
<tr>
<td>peer_type &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>peer ip_address</td>
<td>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 re-establish a session upon reconfiguration if import route policy is changed.</td>
</tr>
<tr>
<td>weight &lt;0-65535&gt;</td>
<td></td>
</tr>
<tr>
<td>peer ip_address</td>
<td>Enables or disables the weight associated with the specified peer.</td>
</tr>
<tr>
<td>weight off</td>
<td></td>
</tr>
<tr>
<td>peer ip_address</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. <strong>Default:</strong> off</td>
</tr>
<tr>
<td>aggregator id &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer ip_address</td>
<td>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.</td>
</tr>
<tr>
<td>holdtime &lt;6-65535&gt;</td>
<td></td>
</tr>
<tr>
<td>peer ip_address</td>
<td>Specifies a holdtime of 180 seconds.</td>
</tr>
<tr>
<td>holdtime default</td>
<td></td>
</tr>
<tr>
<td>peer ip_address</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>keepalive &lt;2-21845&gt;</td>
<td></td>
</tr>
<tr>
<td>peer ip_address</td>
<td>Specifies a keepalive interval of 60 seconds.</td>
</tr>
<tr>
<td>ip_address_keepalive</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td></td>
</tr>
<tr>
<td>peer ip_address</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. Default: off</td>
</tr>
<tr>
<td>ignore-first-ashop</td>
<td></td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>peer ip_address</code></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. <strong>Default</strong>: off</td>
</tr>
<tr>
<td><code>send-keepalives</code></td>
<td>Specifies an inbound BGP policy route if one is not already configured. Enter <strong>all</strong> 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><code>accept-routes all</code></td>
<td>Specifies for the router to wait for the specified peer to issue an open message. No TCP connections are initiated by the router. <strong>Default</strong>: off</td>
</tr>
<tr>
<td><code>accept-routes none</code></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>`passive-tcp &lt;on</td>
<td>off&gt;`</td>
</tr>
</tbody>
</table>
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.

Default: off

peer ip_address log-warnings <on | off>

Specifies for the router to log a message whenever a warning scenario is encountered in the codepath.

Default: off

peer ip_address 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. Enter packets to trace all BGP packets to this peer. Enter open to trace all the BGP open messages to this peer. Enter update to trace all the BGP update messages to this peer. Enter keepalive to trace all the keepalive messages to this peer. Enter all to trace all the message types. Enter general to trace message related to Route and Normal. Enter route to trace routing table changes for routes installed by this peer. Enter normal to trace normal protocol occurrences. Abnormal protocol occurrences are always traced. Enter state to trace state machine transitions in the protocol. Enter policy to trace application of the protocol and user-specified policy to routes being imported and exported.
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.

Note
IPSO 3.8 does not support route filtering and redistribution CLI commands. You must configure inbound routing policies and redistribution of routes through Voyager. Go to the Inbound Route Filters and Route Redistribution links on the Voyager Configuration page.

```
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
```
4 Routing Commands

```
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.

---

**Note**
IPSO 3.8 does not support route filtering and redistribution CLI commands. You must configure inbound routing policies and redistribution of routes through Voyager. Go to the *Inbound Route Filters* and *Route Redistribution* links on the Voyager Configuration page. You can configure route aggregation using CLI commands. See "Route Aggregation" on page 254.

---

**Note**
Builds of IPSO 3.8 prior to Build 039 do not support interoperability with Cisco routers that implement link-local signaling (LLS) when running
This issue is fixed in IPSO 3.8 Build 039, and you no longer have to disable LLS on a Cisco router that is running OSPF.

When you do initial configuration, set the router ID. You can also use the following commands to change the router ID.

```bash
set router-id
default
ip_address
```

**Arguments**

- `router-id default`: Selects the highest interface address when OSPF is enabled.
- `router-id ip_address`: Specifies a specific IP address to assign as the router ID. Do not use 0.0.0.0 as the router ID address. Nokia 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.

**OSPF Areas**

Use the following commands to configure OSPF areas, including the backbone and stub areas.

For OSPFv2 use the following commands:

```bash
set ospf area
  backbone <on | off>
  ospf_area <on | off>
  ospf_area stub <on | off>
  ospf_area stub default-cost <1-677215>
  ospf_area stub summary <on | off>
```
For OSPFv3 use the following with the same arguments as for OSPFv2:

```
set ipv6 ospf3 area
```

### Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backbone &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>ospf_area &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>ospf_area stub &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>ospf_area 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>ospf_area stub summary &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

### OSPF Interfaces

Use the following commands to configure a backbone and other areas, such as stub areas, for specified interfaces.
For OSPFv2 use the following commands:

```bash
set 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 <1-4294967295>
  interface if_name dead-interval default
  interface if_name retransmit-interval <1-4294967295>
  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 <on | off>
  interface if_name authtype none
  interface if_name simple password
  interface if_name md5 key authorization key id secret md5 secret
  interface if_name md5 key authorization key id
```

For OSPFv3 use the following with the same arguments as for OSPFv2:

```bash
set ipv6 ospf3
```
**Arguments**

- `area`<br>`<backbone | ospf_area>`<br>`range ip_prefix`<br>`<on | off>`<br>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`<br>`<backbone | ospf_area>`<br>`range ip_prefix`<br>`restrict <on | off>`<br>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.
### 4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface if_name</code> <code>hello-interval</code> <code>&lt;1-65535&gt;</code></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><code>interface if_name</code> <code>hello-interval default</code></td>
<td>Specifies the default value for the hello interval, which is 10 seconds.</td>
</tr>
<tr>
<td><code>interface if_name</code> <code>dead-interval</code> <code>&lt;1-4294967295&gt;</code></td>
<td>Specifies the number of seconds after which a router stops receiving hello packets that it declares the peer 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><code>interface if_name</code> <code>dead-interval default</code></td>
<td>Specifies the default value for the dead interval, which is 40 seconds.</td>
</tr>
<tr>
<td><code>interface if_name</code> <code>retransmit-interval</code> <code>&lt;1-4294967295&gt;</code></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><code>interface if_name</code> <code>retransmit-interval default</code></td>
<td>Specifies the default default for the retransmit interval, which is 5 seconds.</td>
</tr>
<tr>
<td><code>interface if_name</code> <code>cost</code> <code>&lt;1-65535&gt;</code></td>
<td>Specifies the weight of the given path in a route. The higher the cost, the less preferred the link. To use one interface over another for routing paths, assign one a higher cost.</td>
</tr>
</tbody>
</table>
interface if_name
priority <0-255>

Specifies the priority for becoming the designated router (DR) on the specified link. When two routers attached to a network attempt to become a designated router, the one with the highest priority wins. This option prevents the DR from changing too often. The DR option applies only to a share-media interface, such as Ethernet or FDDI; a DR is not elected on a point-to-point type interface. A router with a priority of 0 is not eligible to become the DR.

interface if_name
passive <on | off>

Enabling this option puts the specified interface into passive mode; that is, hello packets are not sent from the interface. Putting an interface into passive mode means that no adjacencies are formed on the link. This mode enables the network associated with the specified interface to be included in intra-area route calculation rather than redistributing the network into OSPF and having it function as an autonomous system external.

Default: off

interface if_name
virtual <on | off>

Enables OSPF on the virtual IP address associated with this interface. This option functions only if this router is a VRRP master. You must also configure VRRP to accept connections to VRRP IPs. See “VRRP” for more information.

Default: off

Note
You must use Monitored Circuit mode when configuring virtual IP support for OSPF or any other dynamic routing protocol. Do not use VRRPv2 when configuring virtual IP support for OSPF.
4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface if_name authtype none</td>
<td>Specifies not to use an authentication scheme for the specified interface.</td>
</tr>
<tr>
<td>interface if_name authtype simple password</td>
<td>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 peer adjacencies. Use an authentication scheme to guarantee that routing information is accepted only from trusted peers.</td>
</tr>
<tr>
<td>interface if_name authtype md5 key authorization key id secret md5 secret</td>
<td>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 peer adjacencies. Use an authentication scheme to guarantee that routing information is accepted only from trusted peers.</td>
</tr>
</tbody>
</table>

**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:

```bash
set 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:

```bash
set ipv6 ospf3 area backbone virtual-link
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>Specifies the IP address of the remote endpoint of the virtual link.</td>
</tr>
<tr>
<td>transit-area</td>
<td>Specifies the IP address of the remote endpoint of the virtual link.</td>
</tr>
<tr>
<td>ospf_area &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

Specifies the IP address of the remote endpoint of the virtual link and transit area, which is a specified ospf area you configure using the set ospf area command. Configure the ospf area you are using as the transit area before you configure the virtual link. The transit area is the area shared by the border router on which you configure the virtual link and the router with an interface in the backbone area. Traffic between the endpoints of the virtual link flow through this area. The virtual link IP address functions as the router ID of the remote endpoint of the virtual link.
### 4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_address transit-area ospf_area hello-interval &lt;1-65535&gt;</code></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><code>ip_address transit-area ospf_area hello-interval default</code></td>
<td>Specifies an interval of 10 seconds.</td>
</tr>
<tr>
<td><code>ip_address transit-area ospf_area dead-interval &lt;1-4294967295&gt;</code></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><code>ip_address transit-area ospf_area dead-interval default</code></td>
<td>Specifies a value of 40 seconds.</td>
</tr>
<tr>
<td><code>ip_address transit-area ospf_area retransmit-interval &lt;1-4294967295&gt;</code></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><code>ip_address transit-area ospf_area retransmit-interval default</code></td>
<td>Specifies a value of 5 seconds.</td>
</tr>
<tr>
<td><code>ip_address transit-area ospf_area authtype none</code></td>
<td>Specifies not to use an authentication scheme for the specified interface.</td>
</tr>
</tbody>
</table>
**OSPF Global Settings**

Use the following commands to configure setting that apply to all configured OSPF areas, including the backbone and stub areas.

For OSPFv2 use the following commands:

```
set ospf
   rfc1583-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>
```

```
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.

```
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.
4 Routing Commands

For OSPFv3 use the following commands:

```
set ipv6 ospf3
  spf-delay <1-60>
  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><code>rfc1583-compatibility</code></td>
<td>The Nokia implementation of OSPF is based on RFC 2178, which fixed some looping problems in an earlier specification of OSPF. If your implementation runs in an environment with OSPF implementations based on RFC 1583 or earlier, enable this option, which is on by default. Setting compatibility with RFC 1583 ensures backward compatibility. This argument is not used with OSPFv3. <strong>Default:</strong> on</td>
</tr>
<tr>
<td><code>spf-delay &lt;1-60&gt;</code></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><code>spf-delay default</code></td>
<td>Specifies an spf-delay time of 2 seconds.</td>
</tr>
<tr>
<td><code>spf-holdtime &lt;1-60&gt;</code></td>
<td>Specifies the minimum time, in seconds, between recalculations of the OSPF routing table.</td>
</tr>
<tr>
<td><code>spf-holdtime default</code></td>
<td>Specifies an spf-holdtime of 5 seconds.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>default-ase-cost</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</td>
<td>Specifies the type assigned to routes from other protocols that are redistributed into OSPF as autonomous systems external. If the route has a type already specified, that type takes precedent.</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 ospf` (for OSPFv2) or `show ipv6 ospf3` (for OSPFv3).
For OSPFv2 use the following commands:

```
show ospf
    neighbors
    neighbor ip_address
    interfaces
    interfaces stats
    interfaces detailed
    interface ifname
    interface ifname stats
    interface ifname detailed
    packets
    errors
    errors dd
    errors hello
    errors ip
    errors lsack
    errors lsr
    errors lsu
    errors protocol
    events
    border-routers
    database
    database areas
    database area ospf area
    database asbr-summary-lsa
    database checksum
    database database-summary
    database detailed
    database external-lsa
    database network-lsa
    database router-lsa
    database summary-lsa
    database type <1-5>
    summary
```
For OSPFv3 use the following commands:

```
show ipv6 ospf
   neighbors
   neighbor ip_address
   interfaces
   interfaces stats
   interfaces detailed
   interface ifname
   interface ifname stats
   interface ifname detailed
   packets
   errors
   errors dd
   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>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 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>
</tbody>
</table>
### interface if_name detailed
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.

### packets
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.

### errors
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.

### errors dd
Displays the number of each type of database-description error messages only.

### errors hello
Displays the number of each type of hello-error message only.

### errors ip
Displays the number of each type of IP-errors message only.

### errors lsack
Displays the number of each type of link-state acknowledgment error message only.

### errors lsu
Displays the number of each type of link-state update error message only.

### errors lsr
Displays the number of each type of link-state request error messages only.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>database areas</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>database area ospfarea</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>database asbr-summary</td>
<td>Displays a summary of AS-border-router link state statistics for each OSPF area. For OSPFv2 only.</td>
</tr>
<tr>
<td>database inter-area-router-lsa</td>
<td>Displays a summary of AS-border-router link state statistics for each OSPF area. For OSPFv3 only.</td>
</tr>
<tr>
<td>database external</td>
<td>Displays AS-external-link state statistics for each OSPF area.</td>
</tr>
<tr>
<td>database database-summary</td>
<td>Displays a summary of router-link-state, network-link state, summary-link-state , and AS-border-router-link state statistics.</td>
</tr>
</tbody>
</table>

OSPF CLI Reference Guide for Nokia IPSO 3.9
### Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 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>
<tr>
<td><code>database intra-area-prefix-lsa</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>link lsa</code></td>
<td>Describes a router's link-local address and the IPv6 address prefixes associated with a link. For OSPFv3 only.</td>
</tr>
<tr>
<td><code>database type &lt;1-5&gt;</code></td>
<td>Displays link-state statistics associated with the specified number:</td>
</tr>
<tr>
<td></td>
<td>• 1—router-link-state statistics.</td>
</tr>
<tr>
<td></td>
<td>• 2—network-link-state statistics.</td>
</tr>
<tr>
<td></td>
<td>• 3—summary-link-state statistics.</td>
</tr>
<tr>
<td></td>
<td>• 4—AS-border-router-link-state statistics.</td>
</tr>
<tr>
<td></td>
<td>• 5—AS-external-link-state statistics.</td>
</tr>
</tbody>
</table>
RIP

Use this group of commands to set and view parameters for RIP.

**Note**
IPSO 3.8 does not support route filtering and redistribution CLI commands. You must configure inbound routing policies and redistribution of routes through Voyager. Go to the **Inbound Route Filters** and **Route Redistribution** links on the Voyager Configuration page. You can configure route aggregation using CLI commands. See "Route Aggregation" on page 254.

Use these commands to configure RIP properties for specific interfaces.
4 Routing Commands

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.

Default: 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.
interface if_name virtual <on | off>
Enables RIP on the virtual IP address associated with this interface. This option functions only if this router is a VRRP master. You must also configure VRRP to accept connections to VRRP IPs. See “VRRP” for more information.

Default: off

Note
You must use Monitored Circuit mode when configuring virtual IP support for any dynamic routing protocol, including RIP. Do not use VRRPv2 when configuring virtual IP support for RIP or any dynamic routing protocol.

cisco-compatibility <on | off>
Specifies whether to interoperate with Cisco routers also using the MD5 authentication scheme.

Default: off

auto-summary <on | off>
Specifies whether to aggregate and distribute non-classful routes when using RIP version 1.

Default: on

update-interval <1-65535>
Specifies the amount of time, in seconds, between RIP updates.

update-interval default
Specifies a value of 30 seconds.

expire-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. This value should be 6 times the update interval in order to allow for the possibility that packets containing an update could be dropped by the network.

expire-interval default
Specifies a value of 180 seconds.
RIP Show Commands

Use these commands to monitor and troubleshoot RIP.

```
show rip
  interfaces
  interface <if_name>
  packets
  errors
  neighbors
  summary
```

IGRP

Use these commands to set and view parameters for the Interior Gateway Routing Protocol.

**Note**

IPSO 3.8 does not support route filtering and redistribution CLI commands. You must configure inbound routing policies and redistribution of routes through Voyager. Go to the Inbound Route Filters and Route Redistribution links on the Voyager Configuration page. You can configure route aggregation using CLI commands. See “Route Aggregation” on page 254.
General IGRP Properties

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
    update-interval <1-65535>
    update-interval default
    invalid-interval <1-65535>
    invalid-interval default
    hold-interval <1-65535>
    hold-interval default
    flush-interval <1-65535>
    flush-interval default
    validate fields <on | off>

IGRP Interfaces

Use these commands to configure IGRP properties for specific interfaces.
set igrp interface if_name
  <on | off>
  delay <1-16777215>
  bandwidth <1-65535>
  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.
## 4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-mtu &lt;0-65535&gt;</td>
<td>Specifies the IGRP maximum transmission unit. Set this option if you are exporting routes into IGRP.</td>
</tr>
<tr>
<td>k1 &lt;0-1677215&gt;</td>
<td>Specifies the IGRP bandwidth multiplier constant used in the composite metric computation.</td>
</tr>
<tr>
<td>k1 default</td>
<td>Specifies a value of 1.</td>
</tr>
<tr>
<td>k2 &lt;0-1677215&gt;</td>
<td>Specifies the IGRP delay multiplier constant used in the composite metric computation.</td>
</tr>
<tr>
<td>k2 default</td>
<td>Specifies a value of 1.</td>
</tr>
<tr>
<td>holddown &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>max-hop-count &lt;1-255&gt;</td>
<td>Specifies the maximum allowable &quot;hop count&quot; an incoming route must have in order to be accepted. For a route to be marked as &quot;reachable&quot; in an update, its “hop count” must not exceed this value.</td>
</tr>
<tr>
<td>max-hop-count default</td>
<td>Specifies a value of 100.</td>
</tr>
<tr>
<td>update-interval &lt;1-65535&gt;</td>
<td>Specifies the amount of time, in seconds, between regularly scheduled updates</td>
</tr>
<tr>
<td>update-interval default</td>
<td>Specifies a value of 90.</td>
</tr>
<tr>
<td>invalid-interval &lt;1-65535&gt;</td>
<td>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</td>
</tr>
<tr>
<td>invalid-interval default</td>
<td>Specifies a value of 3 times the update interval value.</td>
</tr>
</tbody>
</table>
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.
4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface if_name</code> &lt;on</td>
<td>Specifies whether to enable or disable IGRP on the specified interface.</td>
</tr>
<tr>
<td>on</td>
<td>off&gt;</td>
</tr>
<tr>
<td><code>interface if_name delay</code> &lt;1-16777215&gt;</td>
<td>Specifies the IGRP delay metric in units of 10 microseconds.</td>
</tr>
<tr>
<td><code>interface if_name bandwidth</code> &lt;1-16777215&gt;</td>
<td>Specifies the IGRP bandwidth metric in units of inverted bits/second scaled by a factor of 10,000,000.</td>
</tr>
<tr>
<td><code>interface if_name accept-updates</code> &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>Default: on</td>
<td></td>
</tr>
</tbody>
</table>

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 Interfaces

Use these commands to configure IGMP for specific interfaces.

```
set igmp interface if_name
   version <1 | 2>
   loss-robustness <1-255>
   loss-robustness default
   query-interval <1-3600>
   query-interval default
   query-response-interval <1-25>
   query-response-interval default
   last-member-query-interval <1-25>
   last-member-query-interval default
   router-alert <on | off>
```

Arguments.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version &lt;1</td>
<td>2&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></td>
</tr>
<tr>
<td>query-response-interval &lt;1-25&gt;</td>
<td></td>
</tr>
<tr>
<td>query-response-interval default</td>
<td></td>
</tr>
<tr>
<td>last-member-query-interval &lt;1-25&gt;</td>
<td></td>
</tr>
<tr>
<td>last-member-query-interval default</td>
<td></td>
</tr>
<tr>
<td>router-alert &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
Use the following commands when IP clustering is enabled. You must be logged in as cadmin. These commands are not available unless IP clustering is enabled. For more information about how to configure IP Clustering, see “IP Clustering Commands” or the Clustering Configuration Guide for IPSO 3.8.1.

```bash
set igmp network ip_address/mask length
version <1 | 2>
loss-robustness <1-255>
loss-robustness default
query-interval <1-3600>
query-interval default
query-response-interval <1-25>
query-response-interval default
last-member-query-interval <1-25>
last-member-query-interval default
router-alert <on | off>
```

### IGMP with IP Clustering

Use the following commands when IP clustering is enabled. You must be logged in as cadmin. These commands are not available unless IP clustering is enabled. For more information about how to configure IP Clustering, see “IP Clustering Commands” or the Clustering Configuration Guide for IPSO 3.8.1.

```bash
set igmp network ip_address/mask length
version <1 | 2>
loss-robustness <1-255>
loss-robustness default
query-interval <1-3600>
query-interval default
query-response-interval <1-25>
query-response-interval default
last-member-query-interval <1-25>
last-member-query-interval default
router-alert <on | off>
```
**Arguments.**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version &lt;1</td>
<td>2&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>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>router-alert &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>


IGMP Show Commands

Use these commands to monitor and troubleshoot IGMP.

```plaintext
show igmp
  stats
  stats receive
  stats transmit
  stats error
  interfaces
  interfaces if_address
  groups
  group if_address
  if-stats
  if-stat if_address
  summary
```

Use the following commands to monitor and troubleshoot IGMP when IP clustering is enabled.

```plaintext
show igmp
  networks
  network ip_address/mask length
  show igmp net-stats
  show igmp net-stat ip_address/masklength
  stats
  show igmp stats receive
  show igmp stats transmit
  stats summary
  summary
```

PIM

Use this group of commands to configure parameters for PIM.

```plaintext
set pim mode
  <dense | sparse>
```
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>

**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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;dense</td>
<td>sparse&gt;</td>
</tr>
<tr>
<td>interface if_name &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>virtual-address &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

**Note**

You must use Monitored Circuit mode when configuring virtual IP support for any dynamic routing protocol, including PIM, either sparse-mode or dense-mode. Do not use VRRPv2 when configuring virtual IP support for any dynamic routing protocol.
**local-address**<br>\*ip_address*  

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.
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.

**Default:** 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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr-priority default</td>
<td>Specifies a value of 1.</td>
</tr>
<tr>
<td>bootstrap-candidate</td>
<td>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. <strong>Default:</strong> off</td>
</tr>
<tr>
<td>local-address</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>priority &lt;0-255&gt;</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 default</td>
<td>Specifies a value of 0.</td>
</tr>
<tr>
<td>candidate-rp &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>local-address</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>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>candidate-rp priority</code></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><code>candidate-rp priority default</code></td>
<td>Specifies a value of 0.</td>
</tr>
<tr>
<td><code>candidate-rp multicast-group mcast_ip_prefix</code></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><code>static-rp off</code></td>
<td>Disables the static rendezvous point option.</td>
</tr>
<tr>
<td>`static-rp rp-address ip_address &lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><code>static-rp rp-address ip_address multicast-group mcast_ip_prefix</code></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><code>register-suppress-inter val &lt;60-3600&gt;</code></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><code>register-suppress-inter val default</code></td>
<td>Specifies a value of 60.</td>
</tr>
</tbody>
</table>
candidate-rp advertise-interval <1-3600>
Specifies the interval between which candidate-rendezvous point routers send candidate-rendezvous point advertisements.

candidate-rp advertise-interval default
Specifies a value of 60.

cisco-compatibility <on | off>
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 Nokia appliance being accepted by a Cisco router that is the elected rendezvous point (RP), configure this option. A Nokia 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.

Default: off

spt-threshold multicast mcast_ip_prefix threshold <0-1000000>
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.

spt-threshold multicast mcast_ip_prefix threshold infinity <on | off>
Specifies the data rate in kibts/sec to trigger the spt switch over as infinity.

hello interval <1-21845>
Specifies the interval, in seconds, at which PIM hello messages are sent on the LAN.

hello interval default
Specifies a value of 30.
### 4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>data-interval &lt;11-3600&gt;</code></td>
<td>Specifies the interval, in seconds, after which multicast (S,G) state for a silent source is deleted.</td>
</tr>
<tr>
<td><code>data-interval default</code></td>
<td>Specifies a value of 210.</td>
</tr>
<tr>
<td><code>assert-interval &lt;1-3600&gt;</code></td>
<td>Specifies the interval between the last time an assert is received and the assert is timed out.</td>
</tr>
<tr>
<td><code>assert-interval default</code></td>
<td>Specifies a value of 180.</td>
</tr>
<tr>
<td><code>assert-limit &lt;10-10000&gt;</code></td>
<td>Specifies the number of asserts to send per second.</td>
</tr>
<tr>
<td><code>assert-limit default</code></td>
<td>Specifies a value of 10.</td>
</tr>
<tr>
<td><code>assert-limit &lt;0&gt;</code></td>
<td>Disables the limit placed on the number of asserts that can be sent per second.</td>
</tr>
<tr>
<td><code>jp-interval &lt;1-3600&gt;</code></td>
<td>Specifies the interval, in seconds, between which join/prune messages are sent.</td>
</tr>
<tr>
<td><code>jp-interval default</code></td>
<td>Specifies a value of 60.</td>
</tr>
<tr>
<td><code>jp-delay-interval &lt;1-3600&gt;</code></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><code>jp-delay-interval default</code></td>
<td>Specifies a value of 5.</td>
</tr>
<tr>
<td><code>jp-suppress-interval &lt;2-3600&gt;</code></td>
<td>Specifies the mean interval between receiving a Join/Prune with a higher “holdtime” and allowing duplicate Join/Prunes to be sent again. Nokia recommends that you set the join/prune suppress interval 1.25 times that of the join/prune interval.</td>
</tr>
<tr>
<td><code>jp-suppress-interval default</code></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
  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
```

## 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 aggregate

    ip_prefix contributing protocol protocol contributing-route
    <all | ip_prefix> <on | off>
    ip_prefix contributing protocol protocol contributing-route
    <ip_prefix> exact on
    ip_prefix contributing protocol protocol contributing-route
    ip_prefix refines on
    ip_prefix off
    ip_prefix contributing protocol <protocol> off
    ip_prefix rank default
    ip_prefix rank <0-255>
    ip_prefix weight default
    ip_prefix aspath-truncate <on | off>

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_prefix contributing protocol protocol contributing-route &lt;all</td>
<td>ip_prefix&gt; &lt;on</td>
</tr>
<tr>
<td>ip_prefix contributing protocol protocol contributing-route ip_prefix exact on</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 exact on means that the contributing route is limited to the specified IP address and mask length only.</td>
</tr>
</tbody>
</table>
### 4 Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip_prefix contributing protocol protocol</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 refines on 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 exact on and refines on at the same time. If you enable refines on when exact on is enabled, exact on is automatically disabled.</td>
</tr>
<tr>
<td><strong>ip_prefix 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>ip_prefix 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>
<tr>
<td><strong>ip_prefix weight default</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
**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
```

| `ip_prefix 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. |
| `ip_prefix 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. **Default:** off |
arguments

primary ip_address
wait-time <0-65535> on

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.

relay-to ip_address
<on | off>

Specifies the server to which BOOTP requests are forwarded. You can specify more than one server.

off

Disables BOOTP on the specified interface.

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**

- `<on | off>` Specifies whether to run DVMRP on the specified interface.
- `threshold <1-255>` 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 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.
- `threshold default` Specifies a value of 1.
- `metric <1-32>` 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.
- `metric default` Specifies a value of 1.
DVMRP Timers

Use the following commands to configure values for DVMRP timers. Nokia 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.

```
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**

- `neighbor-probe-interval <5-30>`: Specifies the interval, in seconds, at which probe messages are sent on each DVMRP interface.  
  **Default**: 10

- `neighbor-probe-interval default`: Specifies a value of 10 seconds

- `neighbor-timeout-interval <35-8000>`: Specifies the interval, in seconds, after which a silent neighbor is timed out.  
  For DVMRPv3 neighbors, the default is 35, and for non-DVMRPv3 neighbors, the default is 140.

- `neighbor-timeout-interval default`: For DVMRPv3 neighbors, the default is 35, and for non-DVMRPv3 neighbors, the default is 140.
DVMRP

route-report-interval <10-2000>
Specifies the interval, in seconds, at which routing updates are sent on each DVMRP interface. Default: 60.

route-report-interval default
Specifies a value of 60 seconds.

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.

DVMRP Show Commands

Use the following commands to monitor and troubleshoot your DVMRP implementation.
4 Routing Commands

show dvmrp
   interfaces
   interfaces if_name
   neighbors
   neighbor ip_address
   stats
   mfc
   reports
   route
   neighbor-routes
   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> static-route
   ip_prefix nexthop gateway address gateway_address priority <1-8>
   on
   ip_prefix nexthop gateway logical gateway_address priority <1-8>
   on
   ip_prefix nexthop gateway address gateway_address off
   ip_prefix nexthop gateway logical gateway_address off
   ip_prefix nexthop reject
   ip_prefix nexthop blackhole
   ip_prefix off
   ip_prefix rank default
   ip_prefix rank <0-255>
### Arguments

<table>
<thead>
<tr>
<th>ip_prefix</th>
<th>nexthop</th>
<th>gateway address</th>
<th>gateway_address</th>
<th>priority &lt;1-8&gt; on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address and mask length of 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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ip_prefix</th>
<th>nexthop</th>
<th>logical_if_name</th>
<th>priority &lt;1-8&gt; on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address and mask length of 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>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_prefix nexthop gateway_address</code></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><code>ip_prefix nexthop gateway_logical if_name off</code></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>
<tr>
<td><code>ip_prefix nexthop reject</code></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><code>ip_prefix nexthop blackhole</code></td>
<td>Specifies for packets to be dropped rather than forwarded. Unlike reject option, however, the blackhole option does not result in unreachable messages being sent to the packet originators.</td>
</tr>
<tr>
<td><code>ip_prefix off</code></td>
<td>Deletes the specified static route and deletes any next hops associated with the route.</td>
</tr>
<tr>
<td><code>ip_prefix rank default</code></td>
<td>Specifies the rank for the specified static route the routing system uses to determine which route to use when there are routes from different protocols to the same destination. For each route, the route from the protocol with the lowest rank number is used. The default rank for static routes is 60.</td>
</tr>
<tr>
<td><code>ip_prefix rank &lt;0-255&gt;</code></td>
<td>Specifies the rank for the specified static route the routing system uses to determine which route to use when there are routes from different protocols to the same destination. For each route, the route from the protocol with the lowest rank number is used.</td>
</tr>
</tbody>
</table>
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>
```

**VRRP**

You can configure 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*.

---

**Note**

Beginning with IPSO 3.8.1, Nokia also supports VRRP for IPv6 addresses. For more information about the CLI commands for this implementation, see “VRRP for IPv6” page 447.

---

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

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
    monitor-firewall <on | off>
    accept-connections <on | off>

Arguments

accept-connections <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. Nokia recommends setting this option to on when deploying highly available applications whose service is tied to a VRRP backup address.

Default: off

monitor-firewall <on | off>  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 will be forwarded.

NOTE: Beginning with IPSO 3.8, the Enabling Coldstart Delay option is no longer available. This option is superseded by the Monitoring the Firewall State option.

Default: on
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_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
  hello-interval
  password
  priority
  priority-delta

show mcvr vrids

delete mcvr
  old-mc-config
  vrid <1-255>
    backup-address ip_address

**Arguments**

```
  mcvr vrid <1-255>  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.

  priority <1-254>    Specifies or shows this (physical) router's priority
                      during contention for a failed router's addresses.
                      **Default:** 100

  priority-delta <1-254>  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.
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authtype</code></td>
<td>Specifies or shows whether to use authentication.</td>
</tr>
<tr>
<td>`&lt;none</td>
<td>simple&gt;`</td>
</tr>
<tr>
<td><code>[password passwd]</code></td>
<td></td>
</tr>
</tbody>
</table>

**Default:** none

<table>
<thead>
<tr>
<th><code>hello-interval &lt;1-255&gt;</code></th>
<th>Specifies or shows the interval in seconds between VRRP advertisements. This value must be the same on all routers participating in the virtual router.</th>
</tr>
</thead>
</table>

**Default:** 1 second

<table>
<thead>
<tr>
<th><code>backup-address ip_address</code></th>
<th>Specifies or shows an IP address for the virtual router. This address must be on the same network as one of the interfaces in the physical router but must not match a real IP address of any device on this network. You must configure the same backup address on each physical router participating in the virtual router.</th>
</tr>
</thead>
</table>

| `vmac-mode <default-vmac|extended-vmac|interface-vmac|static-vmac>` | Specifies or shows how the virtual MAC address for the backup address is created. For more information on the options, refer to the Network Voyager Reference Guide. |
|------------------------|-----------------------------------------------------------------------------|

**Default:** default-vmac

<table>
<thead>
<tr>
<th><code>mcvr vrids</code></th>
<th>Shows all attributes of all the virtual routers configured on the system.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><code>all</code></th>
<th>Shows all the attributes of the specified virtual router.</th>
</tr>
</thead>
</table>
Full Method Monitored-Circuit VRRP

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>
   vmac-mode <default-vmac|extended-vmac|interface-vmac|static-vmac mac_address>
   backup-address ip_address <on | off>
   preempt-mode <on | off>
```

The following section explains the use and meaning of VRRP monitored circuit commands.

**Arguments**

- **monitored-interface if_name <on | off>**
  Specifies the ID for a virtual router with monitored circuit dependencies and the associated interface.

- **monitored-interface if_name priority-delta <1-254>**
  Specifies the priority delta associated with the interface with a dependency on the virtual router.

- **old-mc-config**
  Deletes any monitored-circuit configuration that was created using the full method of VRRP configuration. You must delete these configuration before you create a monitored-circuit configuration using the simplified method.
monitored interface if_name
auto-deactivation <on | off>

Specifies to allow the effective priority to go to 0 and for the virtual router to be removed from the network. In the typical implementation, if the effective priority goes to 0, the protocol reestablishes a value of 1.

Default: off

priority <1-254>

Specifies the priority assigned to the virtual router during contention for a fail router’s addresses.

hello-interval <1-255>

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

Default: 1 second

vmac-mode <default-vmac| extended-vmac| interface-vmac| static-vmac| mac_address>

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.

backup-address <ip_address> <on | off>

Specifies for the user to enter a backup IP address and enable or disable it.

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.

VRRP Show Commands

Use the following commands to monitor and troubleshoot your legacy VRRP implementation.
4 Routing Commands

```
show vrrp
    interfaces
    interface if_name
    stats
    summary

VRRPv2

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

VRRPv2 Interfaces

Use the following commands to configure properties for specific interfaces for VRRPv2 protocol specification.

```
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>
    vmac-mode <default-vmac|extended-vmac|interface-vmac|static-vmac mac_address>
```
The following section explains the use and meaning of VRRP version 2 commands.

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Specifies to disable VRRP on the specified interface.</td>
</tr>
<tr>
<td>!on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>hello-interval &lt;1-255&gt;</td>
<td>Specifies the interval in seconds between VRRP advertisements. This value must be the same on all the routers participating in the virtual router. <strong>Default:</strong> 1 second</td>
</tr>
<tr>
<td>authtype &lt;none</td>
<td>simple password&gt;</td>
</tr>
<tr>
<td>vmac-mode &lt;default-vmac</td>
<td>extended-vmac</td>
</tr>
<tr>
<td>backup-address ip_address &lt;on</td>
<td>off&gt;</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

<on | off> Specifies whether to run ICMP router
discovery on a specified interface

min-adv-interval <3-1800> Specifies the minimum time (in seconds)
allowed between sending unsolicited
broadcast or multicast ICMP router
advertisements on the interface.

min-adv-interval default Specifies a value of 450 seconds.

max-adv-interval <4-1800> Specifies the maximum time (in seconds)
allowed between sending unsolicited
broadcast or multicast ICMP router
advertisements on the interface.

max-adv-interval default Specifies a value of 600 seconds

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.
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
```

IP Broadcast Helper

Use the following group of commands to set and view parameters for IP Broadcast Helper.

```
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 Forwarding

Use the following commands to control whether to forward packets that are not locally originated by a source directly on the receiving interface.

```
set iphelper
  forward-nonlocal <on | off>
```

IP Broadcast Helper Interfaces

Use the following commands configure IP Broadcast Helper properties for specific interfaces.

```
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</td>
<td>Enter <strong>on</strong> to specify that packets be forwarded even if the source is not directly on the receiving interface. Enter <strong>off</strong> to require that packets for relay be generated by a source that is directly on the receiving interface. <strong>Default:</strong> off</td>
</tr>
<tr>
<td>interface if_name</td>
<td>Specifies to disable the interface configured for iphelper</td>
</tr>
<tr>
<td>udp-port &lt;1-65535&gt;</td>
<td>Specifies to disable the UDP services configured for this interface.</td>
</tr>
</tbody>
</table>
IP Broadcast Helper Show Commands

Use these commands to monitor and troubleshoot your IP Helper implementation.

```
show iphelper
   services
   stats
```

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>
```

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 for the associated interface and UDP service.
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
```

Arguments

- **server ip_address version <1-3>**
  - 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. Nokia recommends that you run version 3.
  - **Default:** 3

- **prefer server ip_address**
  - Specifies to prefer the specified time server if more than one configured time server is functioning.

- **peer ip_address version <1-3>**
  - 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. Nokia recommends that you run version 3.
  - **Default:** 3
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
```

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.

add ddrlist name

show ddrlist

delete ddrlist name

add ddrlist name interface log_if_name

delete ddrlist name interface log_if_name

Arguments

name 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.

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.

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.
4 Routing Commands

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

add ddrlist name rule
    rule_num is the number of an existing rule. The new rule being created will be positioned and numbered before the existing rule (and the number of the existing rule will be incremented by one). The default rule’s number is 1 until you create additional rules.

set ddrlist name rule
    rule_num is the number of the rule you want to modify.

delete ddrlist name rule rule_num
    Deletes the rule with the number of rule_num.
If `action` is set to `accept`, the system will set up a connection when it encounters packets that match the rules’ criteria. If `action` is set to `ignore`, matching packets will be passed over an existing connection but will not trigger the initiation of a connection. If `action` is set to `skip`, the system will not use compare packets against the rule—the rule is turned off.

**Default:** skip

- **src-address**: Specifies a source IP address to match against this rule.
- **src-masklen <0–32>**: Specifies a mask length for the source IP address. **Default:** 0
- **dest-address**: Specifies a destination IP address to match against the rule.
- **dest-masklen <0–32>**: Specifies a mask length for the destination IP address. **Default:** 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 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></td>
<td><strong>Default:</strong> 8</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 nexthop-selection
    src-dest-hash
    dest-hash
    src-hash
    rr
```
Routing Option Commands

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src-dest-hash</td>
<td>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.</td>
</tr>
<tr>
<td>dest-hash</td>
<td>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 &quot;next hop&quot;.</td>
</tr>
<tr>
<td>src-hash</td>
<td>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 &quot;next hop&quot;.</td>
</tr>
<tr>
<td>rr</td>
<td>Round robin: Each time a set of &quot;next hop&quot;s is used for forwarding, a different &quot;next hop&quot; 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.</td>
</tr>
</tbody>
</table>

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
```
4 Routing Commands

set protocol-rank protocol
  ospf rank <0–255>
  ospf rank default
  ospfase rank <0–255>
  ospfase rank default

Arguments

protocol rank <0–255> Specifies the protocol rank value.
bgp rank default The default rank value for BGP is 170.
igrp rank default The default rank value for IGRP is 80.
rip rank default The default rank value for RIP is 100.
ospf rank default The default rank value for OSPF is 10.
ospfase rank default The default rank value for OSPF ASE routes is 150.

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 are saved in /var/log/ipsrd.log.

Configuring the Trace Log File

Use the following commands to configure the log file options for trace routing.

set 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>
<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>
</tbody>
</table>
4 Routing Commands

**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 bgp**
- keepalive <on | off>
- open <on | off>
- update <on | off>
- packets <on | off>
- traceoptions <on | off>
Trace Routing Commands

set trace dvmrp
   graft <on | off>
   mfc <on | off>
   mapper <on | off>
   neighbor <on | off>
   probe <on | off>
   prune <on | off>
   report <on | off>
   packets <on | off>
   traceoptions <on | off>

Arguments

`graft`     Trace DVMRP graft and graftack packets.
`mfc`       Trace DVMRP multicast forwarding cache packets
`mapper`   Trace DVMRP neighbor and neighbor2 packets.
`neighbor` Trace DVMRP neighbor packets.
`probe`    Trace DVMRP probe packets.
`prune`    Trace DVMRP prune packets.
`report`   Trace DVMRP route report packets.
`packet`   Trace all DVMRP packets.
`traceoptions` <all | general | normal | policy | route | state | task | timer>

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>
4 Routing Commands

**Arguments**

- **error**  
  Trace only ICMP error packets, which include:
  - time exceeded
  - parameter problem
  - unreachable
  - source quench

- **info**  
  Trace only ICMP informational packets, which include:
  - mask request/response
  - info request/response
  - echo request/response
  - time stamp request/response

- **routerdiscovery**  
  Trace only ICMP router discovery packets.

- **packets**  
  Trace all ICMP packets.

- **traceoptions**  
  <all | general | normal | policy | route | state | task | timer>

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.
Trace Routing Commands

set trace igmp
  group <on | off>
  leave <on | off>
  mtrace <on | off>
  query <on | off>
  report <on | off>
  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.
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>
  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.
Trace Routing Commands

---

**set trace pim**
- **assert** <on | off>
- **bootstrap** <on | off>
- **crp** <on | off>
- **graft** <on | off>
- **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**

- **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**

---

**Arguments**

- **assert** Trace PIM assert messages.
- **bootstrap** Trace bootstrap messages (sparse-mode only).
- **crp** Trace candidate-RP-advertisements (sparse-mode only).
- **graft** Trace graft and graft acknowledgment packets.
- **hello** Trace PIM router hello packets.
- **join** Trace PIM join/prune messages.
Use the following command to turn BGP trace options on or off.

```
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>`
Trace Routing Commands

```
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.

```
set trace kernel
  iflist <on | off>
  interface <on | off>
  packets <on | off>
  remnants <on | off>
  request <on | off>
  routes <on | off>
  traceoptions <on | off>
```
4 Routing Commands

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iflist</td>
<td>Trace iflist, the interface list scan.</td>
</tr>
<tr>
<td>interface</td>
<td>Trace interface status messages that are received from the kernel.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace packets that are read from the kernel</td>
</tr>
<tr>
<td>remnants</td>
<td>Trace remnants, which specify routes read from the kernel when the routing daemon starts.</td>
</tr>
<tr>
<td>request</td>
<td>Trace requests, which specify to add, delete, or change routes in the kernel forwarding table.</td>
</tr>
<tr>
<td>routes</td>
<td>Trace routes that are exchanged with the kernel, including add, delete, or change messages and add, delete, or change messages received from other processes.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

Use the following command to turn OSPF trace options on or off.

```
set trace ospf
    ack <on | off>
    dd <on | off>
    dr <on | off>
    hello <on | off>
    lsa <on | off>
    packets <on | off>
    request <on | off>
    spf <on | off>
    trap <on | off>
    update <on | off>
    traceoptions <on | off>
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ack</td>
<td>Trace link-state acknowledgment packets.</td>
</tr>
<tr>
<td>dd</td>
<td>Trace all database description packets.</td>
</tr>
</tbody>
</table>
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>
```

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr</td>
<td>Trace designated router packets.</td>
</tr>
<tr>
<td>hello</td>
<td>Trace hello packets.</td>
</tr>
<tr>
<td>lsa</td>
<td>Trace link-state announcement packets.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace OSPF packets.</td>
</tr>
<tr>
<td>request</td>
<td>Trace link-state request packets.</td>
</tr>
<tr>
<td>spf</td>
<td>Trace shortest-path-first (SPF) calculations.</td>
</tr>
<tr>
<td>trap</td>
<td>Traces OSPF trap packets.</td>
</tr>
<tr>
<td>update</td>
<td>Trace link-state updates packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>
Use the following command to show information about active, inactive, or all routes on your system for the OSPF protocol.

```
show route
    ospf
    inactive ospf
    all ospf
```

Use the following command to show information about active, inactive and all aggregate routes on your system.

```
show route
    aggregate
    inactive aggregate
    all aggregate
```

Use the following command to show additional information about routes on your system.

```
show [slot <1-15>] route
    all
    all direct
    all static
    direct
    inactive
    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 reclaims
  - File system writes
  - File system reads
  - Message writes
  - Message reads
  - Signals received
  - Total swaps
  - Voluntary context switches
  - Involuntary context switches
Show MFC Commands

Use the following commands to view information about multicast forwarding cache (MFC) on your system.

```plaintext
show mfc
  cache
  summary
  interface
  orphans
  stats
```
**Arguments**

- **cache**: Displays MFC state information.
- **summary**: Displays the following MFC state information:
  - Number of interfaces enabled
  - Number of cache entries
  - Kernel forwarding entry limit
  - Number of kernel forwarding entries
  - Cache entry average lifetime
  - Prune average lifetime
  - Cache age cycle
  - Data rate update interval
  - Multicast protocol (instance)
- **interface**: Displays MFC interface state information.
- **orphans**: Displays MFC orphan state information.
- **stats**: Displays various information about the following MFC properties:
  - Resolve task summary
  - Resolve requests
  - RPF failure notifications
  - MFC maintenance
5 Traffic Management Commands

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

IP Clustering Commands

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.

See the Voyager Reference Guide for information about how to configure and manage an IPSO cluster.

Note
The IP2250 appliance does not support IP clustering.

General Clustering Commands

Use the following commands to create a cluster configuration.
5 Traffic Management Commands

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.</td>
</tr>
<tr>
<td></td>
<td>If you enter this command without specifying a password, the system responds with</td>
</tr>
<tr>
<td></td>
<td>Enter password for cadmin:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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>
network network/mask

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.

cluster-address
ip_address

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.

ip-pool network network/mask
member ip_address

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.
Use the following commands to configure properties for an existing cluster:

```plaintext
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>
interface log_if_name cluster-address ip_address
join-remote ip_address
mode <mcast | mcast-group | forwarding>
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>
```

**vpn-tunnel network**

*network/mask*

*destination ip_address*

Creates one end of a VPN tunnel. 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.

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.
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

id <0-65535> Specifies the unique identification number of an existing cluster.

cadmin passwd oldpass
    passwd newpass passwd 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.

change <0-65535> Specifies the new cluster identification number.

coldstart-delay <20-200> 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.

VPN-1/FireWall-1 NG_AI does not require this delay.

Default: 30
failure-interval <500-10000>  
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. 
**Default:** 500

firewall-check-required <yes | no>  
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. If VPN-1/FireWall-1 is not running at the time you change the cluster state to up, set this option to no temporarily. In this case, be sure to set the option to yes before you put the cluster into service (assuming that you are using FireWall-1). If VPN-1/FireWall-1 is not running and you do not disable firewall monitoring, the member cannot be part of a cluster (even if it is the only member). Be sure to enable firewall monitoring before you put the cluster into service.

interface log_if_name  
Specifies a logical interface name.

cluster-address cluster-address ip_address  
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.
### IP 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>

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.
5 Traffic Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary-interface log_if_name</td>
<td>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.</td>
</tr>
<tr>
<td>primary-network network/mask</td>
<td>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.</td>
</tr>
<tr>
<td>remote-node ip_address performance-rating integer</td>
<td>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.</td>
</tr>
<tr>
<td>secondary-interface log_if_name</td>
<td>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.</td>
</tr>
<tr>
<td>secondary-network network/mask</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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.

### work-assign <static | dynamic>

Specifies whether the cluster can rebalance the load of active connections by moving them between nodes.
- **static** 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.
- **dynamic** allows the cluster to periodically rebalance the load by moving active connections between nodes. Use for optimum load balancing.
Use the following commands to delete a cluster or to turn off specified features:

```
delete cluster id <0–65535>
```

### ip-pool network network/mask member ip_address
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.

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.

- `securemote <yes | no>`
  Specifies whether SecuRemote clients can connect to the system.
  **Default:** no

- `vpn-clients <yes | no>`
  Specifies whether the cluster supports VPNs with non-Check Point clients.

- `vpn-interop <yes | no>`
  Specifies whether the cluster supports VPNs with non-Check Point gateways.

- `vpn-tunnel network network/mask destination ip_address`
  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).
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**

- **id <0—65535>**
  Specifies the unique identification number of the cluster.

- **feature feature**
  Specifies a feature to remove from the list of join-time shared features.

- **interface log_if_name**
  Specifies the logical name of an interface to disassociate from the cluster. You cannot delete the primary cluster protocol interface.

- **network network/mask**
  Specifies a network to disassociate from the cluster. You cannot delete the primary cluster protocol network.

- **secondary-interface log_if_name**
  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.

- **secondary-network network/mask**
  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.

- **ip-pool network network/mask**
  Deletes the specified IP pool.
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
    secureremote
    secureremote clients
    vpn-clients
    vpn-interop
    vpn-tunnels
```

**vpn-tunnel network**

```
deletes the specified VPN tunnel.
```

```
vpn-tunnel network network/mask
```

```
 network/mask
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clusters</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>coldstart-delay</td>
<td>Shows the number of seconds the system waits before starting the cluster protocol.</td>
</tr>
<tr>
<td>failure-delay</td>
<td>Shows the number of milliseconds the system waits before assuming the cluster has dissolved.</td>
</tr>
<tr>
<td>info</td>
<td>Shows all the configuration and monitoring information for the specified cluster.</td>
</tr>
<tr>
<td>features</td>
<td>Shows the join-time shared features.</td>
</tr>
<tr>
<td>firewall-check-required</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>interfaces</td>
<td>Shows the logical names of all the cluster interfaces.</td>
</tr>
<tr>
<td>interface log_if_name</td>
<td>Shows the cluster IP address for the specified interface.</td>
</tr>
<tr>
<td>cluster-address</td>
<td></td>
</tr>
</tbody>
</table>
### Traffic Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>member info</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>mode</td>
<td>Shows the clustering mode.</td>
</tr>
<tr>
<td>network network/mask</td>
<td>Shows the cluster IP address for the specified network.</td>
</tr>
<tr>
<td>cluster-address</td>
<td></td>
</tr>
<tr>
<td>networks</td>
<td>Shows all the networks in which this cluster is participating.</td>
</tr>
<tr>
<td>performance-rating</td>
<td>Shows the performance rating of this member.</td>
</tr>
<tr>
<td>primary-interface</td>
<td>Shows logical name of the primary cluster protocol interface for the cluster.</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>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>
</tbody>
</table>
**ip-pools**  Shows the configuration of any IP pools used with VPN tunnels formed with non-Check Point gateways or clients.

**securemote**  Shows whether SecuRemote client access is enabled.

**securemote clients**  Shows whether there are any SecuRemote clients connected.

**vpn-clients**  Shows whether the cluster supports VPNs with non-Check Point clients.

**vpn-interop**  Shows whether the cluster supports VPNs with non-Check Point gateways.

**vpn-tunnels**  Shows the configuration of any VPN tunnels formed with non-Check Point gateways or clients.

---

**Clustering Administration**

**Note**
See the *Voyager Reference Guide* for information about how to configure and manage an IPSO cluster.

If you log into command-line session with 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.

**Note**
While logged in as cadmin, you can use all the clustering CLI commands. Instead of being applied to one member, the commands are applied to all the members.

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

```plaintext
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.

**Note**
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**

**Note**
See the *Voyager Reference Guide* for complete information about 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
```

The default list of features is

```
aaa
arp
autosupport
cron
dns
hosts
http
mailrelay
monitor
services
snmp
ssh
static
syslog
time
ntp
```

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. Nokia 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**

- `reboot` Reboots each of the cluster members members in a staggered manner so that only one member is out of service at a time. Used by itself, `reboot` will reboot the cluster members with the image they are running prior to the reboot.
5 Traffic Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>image &lt;name</td>
<td>last-download&gt;</td>
</tr>
<tr>
<td>cluster-all</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>cluster-force</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>save</td>
<td>Saves any unsaved configuration changes prior to booting.</td>
</tr>
</tbody>
</table>

Access List Commands

Access lists 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
```

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.

```
```
5 Traffic Management Commands

```plaintext
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.
  - **Default**: `ip4`
- `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). Traffic with existing type of service (TOS) settings will be prioritized according to the following three queue specifiers: Internetwork Control, Expedited Forwarding, or Best Effort.

```plaintext
set acl name bypass <on | off>
```
ACL Ruleset Commands

Use the following command to show information about all existing ACL rule sets.

`show aclrules`

**Note**
Every ACL has a default ruleset that is originally in position 1. When you use the `show` command, the default ruleset will be marked as such. You cannot delete the default ruleset. This ruleset 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**

- `aclrule name` Specifies the name of the ACL for which to display ruleset information. Use alphanumeric characters.

Use the following command to add an ACL ruleset for an existing ACL.

`add aclrule name position integer`
**Arguments**

`aclrule name`  
Specifies the name of the ACL where the new ruleset will be added. The ACL must already exist. Use alphanumeric characters.

`position integer`  
Specifies the ruleset position number within the ACL. Position number specifies ruleset priority within the ACL. The highest ruleset priority is `position_num = 1`.

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 action  
<accept | drop | reject | prioritize | skip | 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>
```

**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.
action <accept | drop | reject | prioritize | skip | shape>

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** - Expedited forwarding. See “Queue Class Commands” on page 332
- **skip** - Skip the specified rule. It does not apply.
- **shape** - Rate shaping. See “Aggregation Class Commands” on page 331.

**Default:** skip
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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>srcport &lt;0–65535&gt;</td>
<td>Specifies the source port number or port range. The default is the entire range, 0–65535.</td>
</tr>
<tr>
<td>destport &lt;0–65535&gt;</td>
<td>Specifies the destination port number or port range. The default is the entire range, 0–65535.</td>
</tr>
<tr>
<td>protocol</td>
<td>Specifies the IP protocol to be used for matching this rule. <strong>Default:</strong> any</td>
</tr>
<tr>
<td>tcp-estab &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td>tos &lt;any</td>
<td>0x0–0xff&gt;</td>
</tr>
<tr>
<td>dsfield &lt;none&gt;</td>
<td>Specifies the DiffServ codepoint with which to mark traffic that matches this rule. <strong>Note:</strong> This field is inactive and accepts “none” as its only value. <strong>Default:</strong> none</td>
</tr>
</tbody>
</table>
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 331.

```
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**

- **aclrule name** Specifies the name of the ACL. Use alphanumeric characters.
- **position integer** Specifies the ruleset position number within the ACL.
- **aggrclass name** Specifies the name of the aggregation class. Use alphanumeric characters.

**qspec <none | 0–7>** Specifies the logical queue specifier value to be used by the output scheduler for traffic matching this rule.

**Note:** This field is inactive when the rule action is set to anything other than prioritize.

**Note:** When the DSfield is set to one of the predefined codepoints (e.g., Internetwork Control, EF, or best effort), then the QueueSpec field is not used, and the parameter value is “none”.

**Default:** none
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**

```
aggrclass name
```

Specifies the name of the aggregation class to display. Use alphanumeric characters.

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>
```
5 Traffic Management Commands

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggrclass name</td>
<td>Specifies the name of the aggregation class. Use alphanumeric characters.</td>
</tr>
<tr>
<td>meanrate &lt;10–10000000&gt;</td>
<td>Specifies the packet stream mean rate in kilobytes. Range 10-10000000 Kbps</td>
</tr>
<tr>
<td>burstsize &lt;1500–150000&gt;</td>
<td>Specifies the burst value of the packet stream in bytes. Range 1500 - 150000 bytes</td>
</tr>
</tbody>
</table>

Use the following command to delete an existing aggregation class.

delete aggrclass name

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggrclass name</td>
<td>Specifies the name of the aggregation class to delete. Use alphanumeric characters.</td>
</tr>
</tbody>
</table>

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.
Queue Class Commands

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 set values for one or multiple queue class properties. The specified queue class must exist before you use this command. 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>

**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>
</tbody>
</table>
5 Traffic Management Commands

**priority <0–7>**

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.

**name name**

Specifies the logical name for a priority level. It is used to help identify the use of a queue.

- 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

**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

**Default:** For queues 3 to 7 the default is 0
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**
  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
```
5 Traffic Management Commands

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

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.

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:
add atmqos qosd name pcr <64–146000>

Use the following command to delete the specified ATM QoS descriptor:

delete atmqos qosd name

Use the following command to show all ATM QoS descriptors:

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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>direction on a CBR channel. Peak cell rate is rounded down to a multiple of</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Example: atm-s3p1</td>
</tr>
</tbody>
</table>
5 Traffic Management Commands

vc <vpc/vci | vci> Specifies the VC to associate or disassociate with the ATM QoS descriptor. Use non-negative integers in a VPI/VCI format (for example, 1/3) or a single integer to represent the VCI. The VPI value defaults to zero if not specified.

qosd name Specifies the name of the ATM QoS descriptor to associate with the VC.

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
```

**Arguments**
6 System Configuration Commands

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

System Configuration Summary

Use the following command to view the configuration summary:

```plaintext
show
summary
```

Arguments

<table>
<thead>
<tr>
<th>show</th>
<th>summary</th>
<th>Displays the configuration of the platform.</th>
</tr>
</thead>
</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

Use the following command to show the type of service.

show dhcp service

Use the following command to view all DHCP configurations.

show dhcp server all

**Arguments**

- **server**: Specifies that the server process will be configured on the appliance.
- **client**: Specifies that the client process will be configured on the appliance.
- **none**: No DHCP process is specified. None is the default.

---

**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.
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>
    router 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
```

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

reboot <0-4294967295, 10>  Specifies the time, in seconds, after the client first tries to reacquire an IP address and the time the client tries to discover a new IP address.

interfaces  When used with the show command, displays all client DHCP interfaces.

enable  Enables the DHCP client process.

disable  Disables the DHCP client process.
add dhcp server subnet ip_address
    pool start ip_address end ip_address

Use the following commands to change subnet configurations.

set dhcp server subnet ip_address netmask <1-32>
    router 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.

router ip_address  Specifies the default router clients will use.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-lease</td>
<td>Specifies the IP address lease time, in seconds, that clients will be given if clients do not request</td>
</tr>
<tr>
<td></td>
<td>a specific lease time. The default is 43200 seconds.</td>
</tr>
<tr>
<td>max-lease</td>
<td>Specifies the maximum IP address lease time, in seconds, that clients will be given regardless of</td>
</tr>
<tr>
<td></td>
<td>client requests. The default is 43200 seconds.</td>
</tr>
<tr>
<td>domain name</td>
<td>Specifies the domain name clients will be given, for example, client_name.nokia.com.</td>
</tr>
<tr>
<td>dns ip_address</td>
<td>Specifies the Domain Name Server (DNS) servers for clients, in order of precedents. Use commas to</td>
</tr>
<tr>
<td></td>
<td>separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.</td>
</tr>
<tr>
<td>ntp ip_address</td>
<td>Specifies the Network Time Protocol (NTP) servers for clients, in order of precedents. Use commas to</td>
</tr>
<tr>
<td></td>
<td>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></td>
<td>valid hostname.</td>
</tr>
<tr>
<td>wins ip_address</td>
<td>When configuring NetBIOS, specifies the Windows Internet Naming Server (WINS) servers for clients,</td>
</tr>
<tr>
<td></td>
<td>in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1,</td>
</tr>
<tr>
<td></td>
<td>195.163.23.5, etc.</td>
</tr>
<tr>
<td>ddserver ip_address</td>
<td>When configuring NetBIOS, specifies the Datagram Distribution (DD) servers for clients, in order of</td>
</tr>
<tr>
<td></td>
<td>precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5,</td>
</tr>
<tr>
<td></td>
<td>etc.</td>
</tr>
</tbody>
</table>
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.

scope name

When configuring NetBIOS, specifies the scope for the client.

zone name

swap name | ip_address

 specifies the server which provides a swap space for clients. Use a dotted-quad address or valid hostname.

enable | disable

Enables or disables the subnet for DHCP service.

add dhcp server subnet
ip_address
pool start ip_address
end ip_address

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.

subnets

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.

subnet ip_address

When used with the show command, displays the DHCP subnet specified. When used with the delete command, deletes the DHCP subnet specified.
6 System Configuration Commands

Configuring Fixed-IP Addresses

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

```bash
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.

```bash
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>
<tr>
<td>clientid name</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>mac-address mac_address</td>
<td>Specifies the MAC address of the client. If clientid is configured, the clientid will take precedence.</td>
</tr>
<tr>
<td>address ip_address</td>
<td>Specifies the IP address to be assigned to the client.</td>
</tr>
<tr>
<td>domain name</td>
<td>Specifies the domain name for the client will be given, for example, client_name.nokia.com.</td>
</tr>
<tr>
<td>file file_name</td>
<td>Specifies the bootfile name for the client.</td>
</tr>
<tr>
<td>dns ip_address</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>ntp ip_address</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>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>smtp ip_address</code></td>
<td>Specifies the Simple Mail Transfer Protocol (SMTP) servers 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><code>root file_name</code></td>
<td>Specifies the full path name to be used as the root disk partition for the client.</td>
</tr>
<tr>
<td><code>extension file_name</code></td>
<td>Specifies the full path name of the file that contains additional options for the client.</td>
</tr>
<tr>
<td><code>time &lt;-43200 to 43200&gt;</code></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>
<tr>
<td><code>wins ip_address</code></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><code>ddserver ip_address</code></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>
</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.

```
set dhcp server ddns
  update-style <none | interm>
  ttl <0-255>
  enable | disable
```

Use the following commands to create a DDNS key configuration.

```
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.

```
scope name
```

When configuring NetBIOS, specifies the scope for the client.

```
swap name | ip_address
```

Specifies the server which provides a swap space for clients. Use a dotted-quad address or valid hostname.

```
hosts
```

All hosts with fixed-ip addresses.

```
host name
```

Specific host named in the variable.
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

update-style
    Specifies the update style for DDNS.

ttl <0-255)
    Specifies the time to live value, in seconds, for DNS update messages.

enable | disable
    Enables or disable DDNS service.

dhcp server ddns key name
    Specifies the key name identifier when used with the add command.

algorithm HMAC-MD5-SIG-ALG.REG.INT | none
    Specifies the algorithm used by the associated key.

secret value
    Secret to be matched by DNS server for this key.

keys
    Shows all keys.

key name
    Shows specified key.
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
                secondary ip_address
```

Use the following commands to change DDNS zone configurations.

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

Use the following commands to delete DDNS zones.

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

Use the following commands to view DDNS key configurations.

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

Arguments

- `dhcp server zone name` specifies zone name, associates a key and the primary DNS server. Optionally you can specify a secondary DNS server.
- `key name primary ip_address secondary ip_address` Enables or disables DDNS zones.
- `zones` All configured zones.
- `zone name` Specified zone.
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. The archives created by a manual backup reside in the var/backup/ directory.

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

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Specifies 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>
<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 manual backup.</td>
</tr>
<tr>
<td>homedirs &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>logfiles &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

**Default:**
- homedirs: off
- logfiles: off
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 time-stamped.

Use the following commands to create and manage scheduled backups.

Note

The command set below allows you to add a scheduled backup one-time only. To schedule a new regularly scheduled backup, delete the existing scheduled backup and use the set backup scheduled command set to configure a new regularly scheduled backup.

```
gplcfiles <on | off>  Specifies whether to include all GPLC files in the backup file.
package name <on | off> Specifies whether to include a specific package file in the backup file. Package files are not automatically included in a backup file. Enter the filename for the package you want to include in the backup.
```

```
add backup scheduled
    filename name
    dayofmonth <1-31>
    minute <0-59>
    dayofweek <1-7>
    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>

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

delele backup scheduled
  dayofmonth <1-31> dayofweek <1-7>

**Arguments**

**on**  
Specifies to perform a regularly scheduled 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.

**filename name**  
Specifies the name of the file that includes all the backed up files. You must specify this name to configure a regularly scheduled backup.

**homedirs <on | off>**  
Specifies whether to include all home directories in the backup file.  
**Default:** off

**logfiles <on | off>**  
Specifies whether to include all logfiles in the backup file.  
**Default:** off
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 355 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 359.
6 System Configuration Commands

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**

- **ipaddr ip_address**: Specifies or deletes the IP address of the system to which application core dumps should be sent.
- **protocol ftp ftp-dir path_name**: Specifies to use FTP when sending application core dumps 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.
- **protocol tftp**: Specifies to use TFTP when sending application core dumps. Because TFTP does not work with TFTP servers running on many Unix-based operating systems, Nokia 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.
Transferring Backup Files Manually

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

```
set backup remote
  ftp-site ip_address
  ftp-dir path_name
  ftp-user name
  manual filename [ftp-passwd password]
  scheduled filename [ftp-passwd password]
```

To run an interactive session enter:
```
set backup remote <manual | scheduled> filename
```

To run a machine to machine (MMI) session, enter:
```
set backup remote <manual | scheduled> filename ftp-passwd password
```

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.


6 System Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ftp-user name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>manual filename</strong></td>
<td>Specifies the name of the manual backup file you want to transfer to the remote server and the optional password to use when connecting to the FTP site.</td>
</tr>
<tr>
<td><strong>scheduled filename</strong></td>
<td>Specifies the name of the scheduled backup file you want to transfer to the remote server and the optional password to use when connecting to the FTP site.</td>
</tr>
</tbody>
</table>

### Restore Files from Locally Stored Backup Files

```bash
set restore
  manual filename
  scheduled filename
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>manual filename</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>scheduled filename</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Caution**

Restoring from a backup file overwrites your existing files.
**Caution**
Make sure that you have enough disk space available on your Nokia 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).

### Restore Files from Backup Files Stored on Remote Server

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 357 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**
- `filename name` Specifies to restore your files from the filename stored on the remote server.
- `ftp-site ip_addr` Specifies the IP address of the remote server on which the backup files are stored.
6 System Configuration Commands

**ftp-dir path_name**  Specifies the Unix path to the directory on which the backup files are stored.

**ftp-user user_name**  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*.

**ftp-passwd password**  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.

---

**Caution**
Restoring from a backup file overwrites your existing files.

**Caution**
Make sure that you have enough disk space available on your Nokia 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).

---

**Show Backup Commands**

Use the following commands to monitor and troubleshoot your backup and restore configuration.
show backup
  auto-transfer
    all
    ftp-dir
    ipaddr
    protocol
  manual
    filename
    homedirs
    logfiles
    package name
    packages
  remote ftp-site
    ftp-dir
    ftp-user
    manual filenames
    scheduled filenames
  scheduled filename
    package name
    packages
    homedirs
    dayofmonth
    dayofweek
    hour
    minute
    status

Arguments

- **auto-transfer all**: Shows all the auto-transfer settings.
- **auto-transfer ftp-dir**: Shows the path name of the directory on the remote server where backed up files are stored.
- **auto-transfer ipaddr**: Shows the IP address of the remote server that backed up files are stored on.
- **auto-transfer protocol**: Shows the protocol used to transfer files automatically.
## System Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>manual filename</td>
<td>Shows the names of the files that have been manually backed up and are stored in the <code>/var/backup/</code> 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 <code>/var/backup/</code> directory.</td>
</tr>
<tr>
<td>remote ftp-site</td>
<td>Shows the IP address of the remote server that backed up files are stored on.</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 <code>/var/backup/sched/</code> directory.</td>
</tr>
<tr>
<td>scheduled homedirs</td>
<td>Shows whether home directories are backed up.</td>
</tr>
<tr>
<td>scheduled gplcfiles</td>
<td>Shows whether GPLC files are scheduled for backup.</td>
</tr>
<tr>
<td>scheduled logfiles</td>
<td>Shows whether log files are scheduled for backup.</td>
</tr>
<tr>
<td>scheduled package</td>
<td>Shows whether a specified package is scheduled for back up.</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td></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>

**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
timezone <local | utc>
dayofmonth <1-31>
dayofweek <0-7>
hour <0-23>
minute <0-59>
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
   job name
timezone <local | utc>
dayofmonth <1-31>
dayofweek <0-7>
mailto email_addr
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>job name</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>command name</code></td>
<td>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.</td>
</tr>
<tr>
<td>`timezone &lt;local</td>
<td>utc&gt;`</td>
</tr>
<tr>
<td><code>dayofmonth &lt;1-31&gt;</code></td>
<td>Specifies the day of the month for the cron daemon to execute the scheduled job. Use this argument only to schedule monthly jobs.</td>
</tr>
<tr>
<td><code>dayofweek &lt;0-7&gt;</code></td>
<td>Specifies the day of the week for the cron daemon to execute the scheduled job. Use this argument only to schedule weekly jobs.</td>
</tr>
<tr>
<td><code>hour &lt;0-23&gt;</code></td>
<td>Specifies the hour of the day for the cron daemon to execute the scheduled job.</td>
</tr>
<tr>
<td><code>minute &lt;0-59&gt;</code></td>
<td>Specifies the minute of the day for the cron daemon to execute the scheduled job.</td>
</tr>
<tr>
<td><code>job name on</code></td>
<td>Enables the specified job name</td>
</tr>
<tr>
<td><code>mailto email_addr</code></td>
<td>Specifies the email address for the system to send mail regarding your scheduled jobs.</td>
</tr>
</tbody>
</table>
Show Cron Commands

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

show cron
    job name command
    job name dayofmonth
    job name dayofweek
    job name hour
    job name minute
    jobs
    mailto

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>job name command</td>
<td>Shows the Unix command associated with the specified job name.</td>
</tr>
<tr>
<td>job name dayofmonth</td>
<td>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.</td>
</tr>
<tr>
<td>job name dayofweek</td>
<td>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.</td>
</tr>
<tr>
<td>job name hour</td>
<td>Shows the hour of the day on which the job associated with the specified job name is executed by the cron daemon.</td>
</tr>
<tr>
<td>job name minute</td>
<td>Shows the minute of the day on which the job associated with the specified job name is executed by the cron daemon.</td>
</tr>
<tr>
<td>jobs</td>
<td>Shows only the names of jobs are scheduled for the cron daemon to execute.</td>
</tr>
</tbody>
</table>
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 e-mail address for notification of a system failure:

```
add notify onfail
  recipient name
```

Use the following command to delete a user name or e-mail 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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>onfail name</code></td>
<td>Specifies an e-mail 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. If you have purchased a support contract, you are encouraged to set this field to <code>system-failure@iprg.nokia.com</code>. This will allow Nokia Support to track more easily and respond to system failures.</td>
</tr>
</tbody>
</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:

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

Deleting DNS

Use the following commands to delete DNS configurations:

```plaintext
delete dns slot <1-15>
do
domaintname
dns primary
dns secondary
dns tertiary
```

Arguments

- **domainname <name>**
  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.

- **primary <IPv4 address>**
  Specifies the IP address of the first server to use when resolving hostnames. This address should be a host running a DNS server.
6 System Configuration Commands

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

show
  hostname
  hostname slot <1-15>

set
  hostname name
  hostname name slot <1-15>

Arguments

hostname name 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 <1-15>
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
<1-15>, the command changes the host name of the slot
specified in the slot variable.

Managing IPSO Images

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

Note
IP2250 systems can store a maximum of two IPSO images
Managing IPSO Images

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 select an IPSO image for the next boot for a particular slot:

```
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

- **images**: The IPSO images on your platform.
- **image current**: The currently running IPSO image on your platform
- **image testboot**: Displays the image being executed while the in test boot mode.
- **delete image <name | last-download>**: Deletes the specified image name. The last-download argument deletes the image last downloaded.
testboot image <name | last-download> Reboots your system for a test of an IPSO image. The testboot command works on all platforms except for the IP400 series. If you do not execute a testboot keep command within five minutes of a test boot, the platform will reboot with the previous image. The last-download argument specifies to use the image most recently downloaded.

reboot image <name | last-download> Reboots your system with the specified IPSO image. The last-download argument specifies to use the image most recently downloaded.

halt image <name | last-download> Halts the system and specifies the image to use the next time the system is started.

save Saves any unsaved configuration changes prior to booting.

keep Accepts the IPSO image being tested as the default image. You do not have to reboot.

cancel Immediately cancels the test boot and reboots your platform with the previous image.

url name 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.

http-realm name Specifies the HTTP realm to which authentication is needed. The name must be printable characters, for example, download.

user name Specifies a login name if one is required to access the ftp or http server. The format must be printable characters.
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:

```
show
cfgfiles
config-state
```

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

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

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

```
load
cfgfile name
```

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

```
disable-packages
Specifies to deactivate installed packages after the next reboot. The default is for installed packages to remain active after a reboot.
```

```
passwd name
Specifies a password if one is required to access the ftp or http server. The format can be any characters.
```
Managing Configuration Sets

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

Use the following command to delete a configuration database file:

```
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:

```
cfgfile active.prev
active initial
cfgfile initial_3.6v13
cfgfile initial_3.6v15
```

**config-state**
Specifies the current state of the active configuration, which can be either unsaved or saved:

- **unsaved**—a change has been made to the configuration which has not been written to the configuration database file.
- **saved**—the configuration of the system matches the current configuration file.
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. Default: root</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 (Diskless Systems)” on page 385 for information about the commands for diskless 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>
    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
  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.
  Default: 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 the set syslog command.
  • disable: Disables audit log.
  • 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.
  • permanent: Log transient changes and changes that have been saved and will persist after a reboot.
  Default: disable

filename name
  Specifies destination log file when you enable auditlog.
  Default: /var/log/messages
voyager-auditlog <on | off>

Specifies to set the system to log all Apply and Save actions to the Voyager pages. If you enable this option, each time Apply or Save is pressed on a Voyager page, the log records the name of the user, the name of the Voyager page, and the name of the button that was pressed. 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 that 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.
System Logging Configuration

logging trap <0-7> Specifies the severity level for each system log message sent to a remote host. The severity levels are as follows:
0    emerg
1    alert
2    crit
3    err
4    warning
5    notice
6    info
7    debug
Default: 6

logging Any command using this argument is a Cisco-like command.

Logging Commands (Diskless Systems)

Use the following commands to configure logging on diskless 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
```
# System Configuration Commands

## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auditlog</strong></td>
<td>Specifies whether the diskless system logs configuration changes. If you enable the auditlog, the messages are saved to <code>/var/log/messages</code>.</td>
</tr>
<tr>
<td>&lt;disable</td>
<td>transient</td>
</tr>
<tr>
<td></td>
<td>- <strong>transient</strong>: 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>- <strong>permanent</strong>: Log transient changes and changes that have been saved and will persist after a reboot.</td>
</tr>
<tr>
<td><strong>Default</strong>: disable</td>
<td></td>
</tr>
<tr>
<td><strong>flush-frequency &lt;1-24&gt;</strong></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 <strong>threshold</strong> for saving messages.</td>
</tr>
<tr>
<td><strong>Default</strong>: 4</td>
<td></td>
</tr>
<tr>
<td>**local-log &lt;on</td>
<td>off&gt;**</td>
</tr>
<tr>
<td><strong>Default</strong>: off</td>
<td></td>
</tr>
</tbody>
</table>
### System Logging Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-log &lt;on</td>
<td>off&gt;</td>
<td>off</td>
</tr>
<tr>
<td>primary-log-server &lt;ip_address&gt;</td>
<td>Specifies or deletes the IP address of a remote log server to which the diskless system will send system log messages.</td>
<td></td>
</tr>
<tr>
<td>secondary-log-server &lt;ip_address&gt;</td>
<td>Specifies or deletes the IP address of a remote log server to which the diskless system will send system log messages if the primary log server is not reachable.</td>
<td></td>
</tr>
<tr>
<td>threshold &lt;percent&gt;</td>
<td>Sets the threshold level for saving log messages to the remote server. IP2250 (diskless) systems can hold 512 log messages in a specific memory buffer. Use this option to control when the messages are saved to the remote server and the buffer is cleared. For example, assume that the threshold percentage is 50 percent. When there are 256 messages in the buffer, the messages are transferred to the remote server and the buffer is cleared. Setting the option to 0 causes the messages to be transferred immediately and not stored in the buffer. Do not use a percent symbol.</td>
<td>0</td>
</tr>
</tbody>
</table>

Use the following commands to view system log configurations:
show syslog
    all
    auditlog
    flush-frequency
    local-log
    network-log
    primary-log-server
    secondary-log-server
    threshold

**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>auditlog</td>
<td>Shows whether the system logs configuration changes.</td>
</tr>
<tr>
<td>flush-frequency</td>
<td>Shows the frequency (in hours) at which log messages are saved to the remote server.</td>
</tr>
<tr>
<td>local-log</td>
<td>Shows whether the system is configured to save log messages to a PC flash memory card (optional disk).</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 (IP2250 Systems)

You can add PC card flash memory in IP2250 systems so that you can store log files locally. When you install a PC card (optional disk) for logging, you must reboot the system to make it available for use.

Note
PC card memory smaller than 512 megabytes is not recognized by the IP2250. Use a card that has at least this much storage capacity.

Configuring an Optional Disk

Use the following command to enable or disable an optional disk:

```
set optional-disk device-id <1 | 2> <on | off>
```

Use the following command to see whether an optional disk is present and enabled:

```
show optional-disks
```

Arguments

device-id <1 | 2> Specifies whether the PC card is in slot 1 or 2.
<on | off> Specifies whether to enable or disable the PC card as an optional disk. After enabling or disabling an optional disk, you must reboot the system.
Core-Dump Server Configuration (Diskless Systems)

Application core files are stored in memory in the directory `/var/tmp/`. When the file system is 95 percent filled, diskless systems delete older core files to make room for newer ones. You can configure diskless systems to transfer the core files to a remote server so that older files can be retained. After application core files are transferred to a remote server, they are deleted from memory. The core files are transferred on a predetermined schedule that is not configurable by users.

This feature does not apply to IPSO kernel core files. To transfer these files to a remote system, you must use the command

```
savecore -r ftp://user:passwd@host-ip-address/directory/
```

Diskless systems store kernel core files on the internal compact flash memory card and can store a maximum of two at a time. If necessary, older core files are deleted to make room for newer files. If a kernel core file is created, this is indicated in the log file the next time the system boots.

Configuring an Application Core-Dump Server

Use the following commands to configure the system to send application core dumps to a remote server:

```
set dumpserver
    ipaddr ip_address
    protocol
        ftp ftp-dir path_name
tftp

delete dumpserver ipaddr
```
Date and Time Configuration

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

**Setting Date and Time from Server**

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

---

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipaddr ip_address</code></td>
<td>Specifies or deletes the IP address of the system to which application core dumps should be sent.</td>
</tr>
<tr>
<td><code>protocol ftp ftp-dir path_name</code></td>
<td>Specifies to use FTP when sending application core dumps 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><code>protocol tftp</code></td>
<td>Specifies to use TFTP when sending application core dumps. Because TFTP does not work with TFTP servers running on many Unix-based operating systems, Nokia 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>
Note
To display a complete list of timezone values, press tab after timezone-city.
The default value is Greenwich(GMT).

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

Setting Date and Time Manually

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

set clock time month date year

set clock time date month year

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>once-from ntpserver</td>
<td>Specifies to set the local time by contacting the NTP server. Enter either</td>
</tr>
<tr>
<td></td>
<td>the NTP server’s IP address or fully qualified domain name.</td>
</tr>
<tr>
<td>timezone-city value</td>
<td>Specifies a time based on the time zone of a particular place. The default</td>
</tr>
<tr>
<td></td>
<td>is Greenwich Mean Time (GMT). To display the complete list of values, press</td>
</tr>
<tr>
<td></td>
<td>tab after timezone-city.</td>
</tr>
<tr>
<td>day &lt;1-31&gt;</td>
<td>Specifies which day of the month to use to set the initial time.</td>
</tr>
<tr>
<td>hour &lt;0-23&gt;</td>
<td>Specifies which hour of the day to use to set the initial time.</td>
</tr>
</tbody>
</table>
The following table explains the arguments for the `set clock` command set.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>minute</code></td>
<td>Specifies which minute of the hour to use to set the initial time.</td>
</tr>
<tr>
<td><code>second</code></td>
<td>Specifies which second of the minute to use to set the initial time.</td>
</tr>
<tr>
<td><code>month</code></td>
<td>Specifies which month of the year to use to set the initial time.</td>
</tr>
<tr>
<td><code>year</code></td>
<td>Specifies the year to use to set the initial time. For example, enter 2002.</td>
</tr>
<tr>
<td><code>time</code></td>
<td>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</td>
</tr>
<tr>
<td><code>month</code></td>
<td>Specifies the month of the year. Enter one of the following: jan; feb; mar; apr; may; jun; jul; aug; sep; oct; nov; dec.</td>
</tr>
<tr>
<td><code>date</code></td>
<td>Specifies the date. Enter 1-31.</td>
</tr>
<tr>
<td><code>year</code></td>
<td>Specifies the year. Enter a 4 digit value.</td>
</tr>
</tbody>
</table>

**Show Date and Clock Commands**

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

```
show date
show date timezone-city
show clock
```
Arguments

**date**
Displays the system’s configured date and time in the following format: day of the week; month; date time year; timezone. For example: Mon Mar 18 22:16:51 2002 GMT

**date timezone-city**
Displays the system’s configured time only. For example: Greenwich (GMT).

**clock**
Displays the system’s configure date and time in the following format: day of the week; month; date time year; timezone. For example: Mon Mar 18 22:16:51 2002 GMT

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**

- `disk id` 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.
- `model` Specifies the model of the drive that IPSO detects.
- `type` Specifies whether the disk is a Bootmgr or IPSO disk.
- `capacity` Specifies the disk capacity in megabytes.
- `geometry` Specifies the logical block address geometry of the drive in CHS format: cylinders x heads x sectors per track detected for each drive.
- `location` Specifies the physical location of the drive on the chasis.

---

**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 394 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
```
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
    server ip_address version <1-3> [prefer <yes | no>]
    peer ip_address version <1-3> [prefer <yes | no>]
```

<table>
<thead>
<tr>
<th><strong>Arguments</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server ip_address</code></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><code>peer ip_address</code></td>
<td></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> [prefer <yes | no>] 
  peer ip_address version <1–3> [prefer <yes | no>] 
  master <yes | no>
  stratum <1–15> source local-clock
```

**Arguments**

- **active <on | off>**
  Specifies whether the time service is active or inactive. When NTP is active, the local clock will be synchronized as configured and other systems will be able to set their time from this system.

- **server ip_address**
  Specifies the NTP server that you want to configure.

- **peer ip_address version**
  Specifies the NTP peer that you want to configure.
Use the following commands to stop this 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:

```
version <1–3>  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.

prefer <yes | no>  Specifies whether this system should be selected as the time source if more than one server or peer is available to another system that requests a time source. This setting is used as a tie-breaker.
    **Default:** no

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 be.
    **Default:** 0

source local-clock
```
show ntp
  active
  servers
  peers
  <server | peer> ip_address version [prefer]
  master

Arguments

active Shows whether or not NTP is active.

servers Lists any systems configured as NTP servers and shows the appropriate NTP version and prefer settings.

peers Lists any systems configured as NTP peers and shows the appropriate NTP version and prefer settings.

<server | peer> ip_address version [prefer] Shows the NTP version (and prefer setting if specified) of the specified server or peer.

master Shows whether this system has been configured as an NTP master server. If it has, this command also shows the appropriate stratum setting.

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 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>addr ip_address</strong></td>
<td>Specifies the IPv4 address of the remote machine containing the package.</td>
</tr>
<tr>
<td>Example:</td>
<td>192.168.10.10</td>
</tr>
<tr>
<td><strong>user name</strong></td>
<td>Specifies the login name for FTP.</td>
</tr>
<tr>
<td><strong>password password</strong></td>
<td>Specifies the password associated with the username parameter for the FTP login.</td>
</tr>
<tr>
<td><strong>name name</strong></td>
<td>Specifies the file name of the package to install. Use the complete path.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>/opt/packages/IPSO-3.7.tgz</code></td>
</tr>
</tbody>
</table>
Use the following commands to upgrade the existing package (*.tgz) by specifying a different package located on a remote or local system:

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

**Arguments**

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

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

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

Use the following command to uninstall a specified package:

```
delete package name name
```

**Arguments**

- `name name`: Specifies the name of the package. Use the complete path.
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.

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 commands 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 commands to view the configured setting:

```plaintext
show advanced-tuning ip-options stripra
```
7 SNMP Commands

This chapter describes the SNMP configuration commands that you can enter from the initial CLI prompt, called Command mode.

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 Nokia 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 Nokia implementation supports, see the online Voyager documentation that comes with the system. You can also download a pdf version of the online documentation from the Nokia support site at https://support.nokia.com. To view detailed information about each supported MIB, go to the /etc/snmp/mibs directory.

The Nokia implementation also supports the User-based Security model (USM) portion of SNMPv3. The SNMPv3 message encapsulates a protocol data unit (PDU) compatible with earlier versions of SNMP. SNMPv3 defines a user-based security mechanism that enables per-message authentication and encryption. See RFC 3414 for more information.
SNMP Command Set

Use the following commands for configuring SNMP parameters.

```
set snmp
    daemon <on | off>
    snmp snmp-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-diskmirror-create status <on | off>
    sys-diskmirror-delete status <on | off>
    sys-diskmirror-syncfail status <on | off>
    sys-diskmirror-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>
```
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 408.

For more detailed information about SNMP traps, see “Enabling and Disabling SNMP Traps” on page 411.

For more detailed information about SNMPv3 and USM Users, see “Enabling/Disabling and Changing SNMPv3 USM Users” on page 415.
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>
```

⚠️ **Caution**
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

daemon <on | off> Specifies whether to enable or disable SNMP.  
**Default:** on

snmp-version <v1/v2/v3 | v3-Only> Specifies which version of SNMP to implement. Selecting access limits community access. Only requests from users with enabled v3 access are allowed. All other requests are rejected. v1/v2/v3 allows the use of community names.  
**Default:** v1/v2/v3

snmp address ip_address 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.

snmp community string read-only 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.

snmp community string read-write 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.
trapreceiver ip_address  community string  version <v1 | v2>

Specifies the IP address of a new receiver to accept traps from this system and the receiver’s corresponding string. For the string, use alphanumeric characters with no spaces. You can add multiple receivers. The Nokia implementation supports using version 1 or version 2.

The string for a receiver has no relationship with the read-only or read-write community strings. If you do not configure a string for the receiver, the string defaults to public

Default: v1

trapPduAgent ip_address

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.

location string

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
Enabling and Disabling SNMP Traps

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

```
contact string
```

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

**Note**
Only the cold start and authorization traps are enabled by default. You must enable all other 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-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>

Arguments

status <on | off>  Specifies whether to enable or disable the specified trap.

coldstart  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
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>systemTrapConfigurationFileChange 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>
</tbody>
</table>
### sys-nodiskspace

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%.

### sys-diskfailure

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.

### sys-diskmirr-create

systemTrapDiskMirrorSetCreate is sent when a particular mirror set has been created on the system.

### sys-diskmirr-delete

systemTrapDiskMirrorSetDelete is sent when a particular mirror set has been deleted from the system.

### sys-diskmirr-syncfail

systemTrapDiskMirrorSyncFailure is sent when a particular mirror set fails during syncing.

### sys-diskmirr-syncsuccess

systemTrapDiskMirrorSyncSuccess is sent when a particular mirror set has been successfully synced.

### cluster-member-join

ipsoLBClusterMemberJoin trap is sent when a member node joins the cluster by the master.

### cluster-member-left

ipsoLBClusterMemberLeft trap is sent when a member node leaves the cluster by the master.
Enabling/Disabling and Changing SNMPv3 USM Users

Use the following commands to add users who are authorized to use SNMPv3.

```
add user
    username uid <0-65535> homedir string
```
After you add the new user’s account, use the following command to set the user’s password. Note that an SNMPv3 USM user’s password must be at least 8 characters long. Use alphanumeric characters only.

```
set user
  username passwd
```

You are then prompted for an old password. If this user is new, press enter and then type in the new password.

Use the following commands to add or change a user’s homepage, shell, or password.

```
set user
  username shell string
  username homepage string
  username oldpass string newpass string
```

Use the following command to change user permissions. The default is read-only. You can change the SNMP user permissions to read-write.

```
set usm users info <readonly | readwrite>
```

Use the following command to delete an existing SNMPv3 USM user

```
delete user
  username
```

**Note**

You can remove a user’s SNMPv3 functionality but keep that user as an IPSO user by changing the user’s password to one that has fewer than 8 characters.
Arguments

username uid <0-65535> homedir string
Specifies the user’s name, the user’s id and the user’s home directory. For the home directory, enter the full Unix path name where the user is placed after he/she logs in. If the home directory does not exist, the system creates it.

username passwd
Specify the user name and press enter. The system prompts you to enter the new password and to verify it. You must enter a password for the user to have SNMPv3 functionality.

username shell string
Specifies the user’s shell. 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.

username homepage string
Specifies the user’s homepage, which appears when the user logs in.

username oldpass string newpass string
Specifies to change the user’s existing password. Enter the old password first and then the new password. The system then prompts you to reenter the new password to verify it.

username info <readonly | readwrite>
Specifies whether to set the user’s SNMPv3 permissions as read-only or read-write.

Default: readonly
Show SNMP Implementation and Trap Commands

show snmp
  daemon
  community
  trapreceiver
  traps
  snmp trapPduAgent
  snmp location
  snmp contact
Show SNMPv3 Users Commands

```
show snmp
  usm users

show user
  username
  username uid
  username homedir
  username shell
  username homepage
  username info
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon</td>
<td>shows whether or not snmp is enabled on your system.</td>
</tr>
<tr>
<td>community</td>
<td>shows which community strings are enabled and their names.</td>
</tr>
<tr>
<td>trapreceiver</td>
<td>shows the IP address, community string, and version assigned to each configured trapreceiver.</td>
</tr>
<tr>
<td>traps</td>
<td>shows which traps are enabled on your system.</td>
</tr>
<tr>
<td>TrapPduAgent</td>
<td>shows the IP address assigned as the Trap PDU Agent</td>
</tr>
<tr>
<td>location</td>
<td>shows the location specified for the system.</td>
</tr>
<tr>
<td>contact</td>
<td>shows the contact specified for the system.</td>
</tr>
<tr>
<td>usm users</td>
<td>shows the names of each SNMPv3 USM user and each user’s permissions.</td>
</tr>
</tbody>
</table>
SNMP Commands

---

user username shows the User id, group id, home directory, shell, default page, and permission of the specified user.

user username uid shows the user id of the specified user.

user username homedir shows the location of the home directory of the specified user.

user username shell shows the default shell specified for the specified user.

user username homepage shows the homepage that comes up when the specified user logs in.

user username info shows the permissions of the specified user.

---

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>
</tbody>
</table>

---
### Error Status Code

<table>
<thead>
<tr>
<th>Error Status Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<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 Bindings element</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><strong>noSuchObject</strong></td>
<td>If a variable does not have an OBJECT IDENTIFIER prefix that exactly matches the prefix of any variable accessible by this request, then its value field is set to noSuchObject.</td>
</tr>
<tr>
<td><strong>noSuchInstance</strong></td>
<td>If the variable’s name does not exactly match the name of a variable, then its value field is set to noSuchInstance.</td>
</tr>
<tr>
<td><strong>genErr</strong></td>
<td>If the processing of a variable fails for any other reason, the responding entity returns genErr 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><strong>tooBig</strong></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 tooBig, 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.
8 IPv6 Commands

Use the commands in this chapter to configure most IPv6 settings for your system. To configure IPsec for IPv6, see “IPsec Commands” on page 121. To configure traffic management for IPv6, see “Clustering Administration” on page 317.

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

**interface if_name**  
Specifies the name of an existing logical interface.

**Note**  
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.

**ipv6prefix ip6_address/mask**  
Specifies the IPv6 address and mask length. The mask length range is <8–126>.
- Format: IPv6 Prefix/<8–126>
- Example: 1000:50:32::3/64

**anycast ip6_address**  
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.

**family inet6**  
Add an IPv6 address family to the specified logical interface.
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
```
Use the following commands to configure global NDP properties:

```plaintext
set neighbor
duplicate-detection <1-100>
multicast-limit <1-100>
queue-limit <1-3>
unicast-limit <1-100>
```

### Arguments

- **address ip6_address**
  - Specifies the IPv6 address of the static NDP entry to add or delete.
  - Format: IPv6 address
  - Example: 1000:50:32::2

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

- **duplicate-detection <1–100>**
  - Specifies the number of times to retry Duplicate Address Detection NDP requests.
  - Default: 3

- **multicast-limit <1–100>**
  - Specifies the number of times to retry Multicast NDP requests.
  - Default: 3

- **queue-limit <1–3>**
  - Specifies the maximum number of output packets to be queued while resolving link-layer destination address.
  - **Default:** 3
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>
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>]
v4inv6 address ip6_address remote ip6_address
```

**Arguments**

- **interface phys_if_name** Specifies the physical tunnel interface name. The value must be a tunnel that exists on the system.
  - Example: tun0

- **gre** Specifies a GRE tunnel.

- **dvmrp** Specifies a DVMRP tunnel.

- **v6inv4** 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.
v4inv6

Specifies a tunnel that encapsulates IPv4 packets in IPv6 packets. This argument allows you to connect IPv4 enabled systems over existing IPv6 connections.

address

<ip_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

<ip_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
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> <enable | disable>
  destination <ip_address | ip6_address> remote-endpoint
  <ip_address | ip6_address> remote-endpoint
```

**Arguments**

- **interface if_name**
  - Specifies the logical tunnel interface name. The value must be a tunnel that exists on the system:
    - Example: tun0c3

- **interface-binding <on | off>**
  - Specifies whether to bind a tunnel to an outgoing interface.
    - on: Bind the tunnel to the interface.
    - off: Do not bind the tunnel to the interface.
  - Default: on

**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.
Use the following command to delete a specified logical tunnel:

```
delete interface if_name
```
**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>]
   disable
```

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

```
set ipv6toipv4 active <on | off>
```

**Arguments**

- `interface if_name` Specifies the logical interface name of the tunnel to delete:
  - Example: tun0c3

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

```
show ipv6 tunnels
```
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>]
    disable
```

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

```
set ipv6overIPv4 active <on | off>
```
**IPv6 Commands**

### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active on address</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>ip_address</td>
<td>Specifies the time to live (TTL) of packets sent on the tunnel. This argument is optional. Default: 255</td>
</tr>
<tr>
<td>ttl &lt;1–255&gt;</td>
<td>Deletes the settings.</td>
</tr>
<tr>
<td>disable</td>
<td>Activates or deactivates existing IPv6 over IPv4 settings. If you use active off, you will not lose the current settings.</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 3.8.1 does not support route filtering and redistribution CLI commands. You must configure inbound routing policies and
redistribution of routes through Voyager. Go to the Inbound Route Filters and Route Redistribution links on the Voyager Configuration page. You can configure route aggregation using CLI commands. See “Route Aggregation” on page 438.

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**

<on | off> Specifies whether to run RIPng on the specified interface.

metric <0–16> Specifies the RIP metric added to routes that use the specified interface.

metric default Specifies a value of 0.

Show Commands

Use the following commands to monitor and troubleshoot RIPng:

```
show ipv6 ripng
   interfaces
      interface if_name
      packets
      errors
      neighbors
      summary
```
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 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>
```

**Arguments**

- `ip6_prefix`: Specifies the IPv6 address and mask length of the new aggregate route and the contributing protocol or interface route:
  - Example: 1000:50:32::/64
IPv6 Routing Configuration

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.

off

Deactivates the specified aggregate route.

ccontributing-protocol
<all | direct | static
| aggregate | ripng>
off

Specifies the contributing route source type or protocol to turn off:

- all — Use all routes.
- direct — Use only direct routes.
- static — Use only static routes.
- aggregate — Use only aggregate routes.
- ripng — Use only routes that use ripng protocol.

contributing-route
<all | ip6_prefix>
<on | off>

Specifies the contributing route to turn on or off for the specific contributing protocol. You must use this argument after specifying a contributing protocol.

- all — Contribute all the routes for a specific source type or protocol.
- ip6_prefix — Contribute a specific route.
Use the following group of commands to configure specific static routes:

```
set slot <1-15> 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**

- `static-route ip6_prefix` 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.
  Address example: 1000:50.32::/64

- `static-route default` 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.

- `nexthop gateway ip6_address <on | off>` Specifies the gateway address and enables or disables it for the IP address configured as the endpoint of the static route from your system. Disabling the gateway address does not delete the route itself.
  Address example: 1000:50:32::1
### nexthop gateway

**ip6_address interface if_name <on | off>**

Specifies the gateway address for a specified interface and enables or disables it for the IP address configured as the endpoint of the static route from your system. Disabling the gateway address does not delete the route itself.

Address example: 1000:50:32::1

Interface example: eth-s1p1c0

### priority <1-8>

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.

**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.

### ip6_prefix nexthop reject

Specifies for packets to be dropped rather than forwarded and for unreachable messages to be sent to the packet originators. Specifying this option causes this route to be installed as a reject route.

### ip6_prefix nexthop backhole

Specifies for packets to be dropped rather than forwarded but does **not** specify for unreachable messages to be sent to the packet originator.

### ip6_prefix off

Deletes the specified static route and deletes any next hops associated with the route.
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:

```
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>
   hop-limit default
   managed-config <on | off>
   other-config <on | off>
   reachable-time <0-3600000>
   reachable-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:

```
default off
```

Deletes the default route and deletes any next hops associated with the route.
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 447.

min-adv-interval default  Specifies a value of 450 seconds.
max-adv-interval 4-1800>  Specifies the maximum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMPv6 router advertisements on the interface.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
IPv6 Routing Configuration

reachable-time
<0–3600000>
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).

reachable-time default
Specifies a value of zero (0).

retransmit-timer integer
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).

retransmit-timer default
Specifies a value of zero (0).

router-lifetime integer
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.

router-lifetime default
Specifies a value of 1800 seconds.

send-mtu <on | off>
Specifies whether the router advertisement packet includes MTU options.
Default: off
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autonomous &lt;on</td>
<td>off&gt;</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>
<tr>
<td>prefix-pref-lifetime integer</td>
<td>Specifies the length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix through stateless address autoconfiguration remain preferred. This value is placed in the Preferred Lifetime field in the Prefix Information option. The designated value of all 1s (0xffffffff) represents infinity, which means that the node can use the prefix in existing connections, but it is not valid for new connections.</td>
</tr>
<tr>
<td>prefix-pref-lifetime default</td>
<td>Specifies a value of 604800 seconds (7 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

Beginning with IPSO 3.8.1, Nokia supports VRRP for IPv6 interfaces. Nokia supports 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.

Default: on

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
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>off</strong></td>
<td>Specifies to disable VRRPv3 on the specified IPv6 interface</td>
</tr>
<tr>
<td><strong>virtual router vrid &lt;1-255&gt; address ip_address on</strong></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><strong>virtual-router backup-vrid &lt;1-255&gt; address ip_address on</strong></td>
<td>Specifies the virtual router ID for the virtual router used the 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><strong>vrid &lt;1-255&gt; off</strong></td>
<td>Specifies to remove the specified virtual router.</td>
</tr>
</tbody>
</table>
vrid <1-255> address ip_address <on | off>

Specifies to add or remove the IP address for the specified local or backup virtual router. Unlike the VRRP for IPv4 implementation, where a virtual router used to back up the IP addresses of the local interface automatically picks up those addresses, you must manually configure the IP addresses for the virtual router to back up. For both a local virtual router and a virtual router used to back up the IPv6 addresses of a remote system, when a new subnet is added to the interface, you must manually configure any IPv6 addresses you want to include in the 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.

Default: 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.

Default: 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.

Default: 100
Monitored Circuit for IPv6 Interfaces

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

```
vrld <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.

**Default:** on

```
vrld <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:** default-vmac
8 IPv6 Commands

```
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Specifies to disable monitored circuit on the specified IPv6 interface</td>
</tr>
<tr>
<td>monitored-circuit vrid &lt;1-255&gt; address ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>vrid &lt;1-255&gt; off</td>
<td>Specifies to remove the specified virtual router with monitored circuit dependencies.</td>
</tr>
<tr>
<td>vrid &lt;1-255&gt; address ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
vrid <1-255> accept-mode <on | off>
Specifies for the virtual router in a master state to accept packets addressed to virtual IP addresses.
**Default:** 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.
**Default:** 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 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 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.
**Default:** 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.

**Default:** off

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:** default-vmac
**VRRP for IPv6 Show Commands**

```
show ipv6 vrrp6
    interface if_name
    interfaces
    stats
    summary
```

**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 ipv6 route
    aggregate
    inactive aggregate
    all aggregate
```

Use the following command to show additional information about routes on your system:
show [slot <1-15>] 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
   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

localhost Adds or deletes an IPv6 local host. The associated address is ::1.
IPv6 Routing Configuration

ipv6host name name
   Specifies a logical host name. Use alphanumeric characters, dashes (-), and periods (.)
   however, periods must be followed by a letter or a digit. The host name cannot end in a dash or a period.

ipv6 ip6_address
   Specifies the IPv6 address to associate with the host name:
   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
9 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

Use the commands in the following sections to configure various network reports.

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
```
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
    cpuutilization state <on | off>
    cpuutilization 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
    cpuutilization state
    cpuutilization interval

Use the following command to specify a start time and 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 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
    summary <hourly | daily | weekly | monthly> memoryutilization

Arguments

state <on | off>  Turns data collection on or off.
    Default: on
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.
show monitor summary <hourly | daily | weekly | monthly> linkstate
   interface-type <logical | physical>
   interface <name>

**Configuring Rate Shaping Bandwidth Reports**

Use the following commands to turn data collection on or off and to set the data collection time interval.

```bash
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.

```bash
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.

```bash
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.

```bash
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.

```plaintext
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.

```plaintext
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.

```plaintext
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.

```plaintext
show monitor summary <hourly | daily | weekly | monthly> throughput
    type <bytes | packets | multicast | broadcast> interface-type
    <logical | physical> interface <name>
```

Arguments

| aggregate <name> | Specifies information for a given aggregation class. The name is case-sensitive. |
Useful System Information

Use the following commands to view various information about your system.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>endtime &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>interface &lt;name&gt;</code></td>
<td>Specifies the name of a given interface of which you want to collect data.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>Specifies whether you want to collect data from the logical or physical interface.</td>
</tr>
<tr>
<td>`&lt;logical</td>
<td>physical&gt;`</td>
</tr>
<tr>
<td><code>interval &lt;60-2100000&gt;</code></td>
<td>Specifies the data collection time in seconds. Default: 60</td>
</tr>
<tr>
<td><code>rateshape type</code></td>
<td>Specifies the type of rate shaping data.</td>
</tr>
<tr>
<td>`&lt;bytesdelayed</td>
<td>packetdelayed&gt;`</td>
</tr>
<tr>
<td>`state &lt;on</td>
<td>off&gt;`</td>
</tr>
<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>
Displaying Useful System Statistics

Use the following commands to display useful system statistics.

```plaintext
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.

```plaintext
show interfacemonitor
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interfacemonitor</td>
<td>Displays the interface settings.</td>
</tr>
</tbody>
</table>

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
  log messagelog
      type name date name keyword name case-sensitive
      include-zipped name

Arguments

logging Displays the system log configuration.
logininfo all Displays the login/logout activity for all users.
logininfo name Displays the login/logout activity for the named user.
log auditlog Displays a log that shows configuration changes made by users.
log httpd-access-log 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.
log httpd-error-log Displays the log file generated by the web server showing errors that the web server detects.
log messagelog 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 be case-sensitive or case-insensitive. Archived log files can be included in the search.
<table>
<thead>
<tr>
<th>type name date name</th>
<th>Specifies the type of log messages to be displayed. The type is the severity of the log message, from least sever to most sever, and can be specified by one of the following keywords:</th>
</tr>
</thead>
</table>
| keyword name        | - emerg  
|                     | - alert  
|                     | - crit  
|                     | - error  
|                     | - warning  
|                     | - notice  
|                     | - info  
|                     | - debug  |
| case-sensitive      | To include all kinds of log message either specify the keyword "all" or skip this part of the command. |
| include-zipped name | 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.
**Displaying Interface Traffic Statistics**

Use the following commands to display interface traffic statistics.

```
show iftrafficstats
```

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.

**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
- Signals received
- Total swaps
- Voluntary context switches
- Involuntary context switches
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:

**Code** | **Flag**
--- | ---
1 | RTF_PROTO1: Protocol specific routing flag 1
2 | RTF_PROTO2: Protocol specific routing flag 2
3 | RTF_PROTO3: Protocol specific routing flag 3
B | RTF_BLACKHOLE: Just discard packets during updates
C | RTF_CLONING: Generate new routes on use
c | RTF_PRCLONING: Protocol-specified generate new routes on use
D | RTF_DYNAMIC: Created dynamically by redirect
G | RTF_GATEWAY: Destination requires forwarding by intermediary
H | RTF_HOST: Host entry net otherwise
L | RTF_LLINFO: Valid protocol to link address translation
M | RTF_MODIFIED: Modified dynamically by redirect
R | RTF_REJECT: Host or net unreachable
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays information about all of the temperature sensors.</td>
</tr>
<tr>
<td>sensor sensor-number</td>
<td>Displays information about the temperature sensor specified by sensor-number.</td>
</tr>
<tr>
<td>all</td>
<td>Displays all information about the sensor specified by sensor-number.</td>
</tr>
<tr>
<td>location</td>
<td>location displays the location (for example, lm79_temp) of the sensor specified by sensor-number.</td>
</tr>
<tr>
<td>status</td>
<td>status displays the status (for example, good) for the sensor specified by sensor-number.</td>
</tr>
<tr>
<td>current</td>
<td>current displays the current value of the sensor specified by sensor-number.</td>
</tr>
<tr>
<td>limit</td>
<td>limit displays the limit value for the sensor specified by sensor-number.</td>
</tr>
<tr>
<td>hysteresis</td>
<td>hysteresis displays the hysteresis value for the sensor specified by sensor-number.</td>
</tr>
</tbody>
</table>

### Displaying a Watchdog Timer Information

Use the following commands to display watchdog timer information.

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all watchdog timer information.</td>
</tr>
<tr>
<td>status</td>
<td>Displays the watchdog timer status.</td>
</tr>
<tr>
<td>mode</td>
<td>Displays the watchdog timer mode.</td>
</tr>
<tr>
<td>tickles</td>
<td>Displays watchdog timer tickle information.</td>
</tr>
<tr>
<td>last-reboot</td>
<td>Displays the watchdog timer last-reboot time.</td>
</tr>
</tbody>
</table>

**Displaying Voltage Sensor Information**

Use the following commands to display voltage sensor information.

```
show sysenv voltage
  all
  all
    sensor sensor-number
      <all | location | status | nominal | measured | error | lo-limit | hi-limit>
```
9 Monitoring Commands

Voltage sensor information includes the following:

- Location
- Status
- Nominal
- Measured
- Error
- Low Limit
- High Limit

**Arguments**

- `all` Displays all voltage sensor information.

```plaintext
sensor sensor-number
<all | location | status | nominal | measured | error | lo-limit | hi-limit>
```

- `sensor sensor-number` Displays information about the voltage sensor specified by `sensor-number`.
- `all` displays all information about the sensor specified by `sensor-number`.
- `location` displays the location (for example, lm79_IN0) of the sensor specified by `sensor-number`.
- `status` displays the status of the sensor specified by `sensor-number`.
- `nominal` displays the nominal value for the sensor specified by `sensor-number`.
- `measured` displays the measurement for the sensor specified by `sensor-number`.
- `error` displays error information as a numerical value for the sensor specified by `sensor-number`.
- `lo-limit` displays the low-limit for the sensor specified by `sensor-number`.
- `hi-limit` displays the high-limit for the sensor specified by `sensor-number`.
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

Hyphens are displayed where no information is available for an information field.
9 Monitoring Commands

Arguments

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all voltage sensor information</td>
</tr>
<tr>
<td>id pwr-supply-id</td>
<td>all displays all information about the power supply specified by pwr-supply-id.</td>
</tr>
<tr>
<td>&lt;all</td>
<td>present</td>
</tr>
</tbody>
</table>

Displaying Fan Sensor Information

Use the following commands to display fan sensor information.

show sysenv fan
   all
   sensor sensor-number
       <all | location | status | current | normal | limit>

Fan sensor information includes the following:

- Location (for example, lm79_FAN1)
- Status (for example, Normal)
- Current Value
- Normal Value
- Fan limit
Displaying Hardware Monitors

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all fan sensor information</td>
</tr>
<tr>
<td>sensor sensor-number</td>
<td>all displays all information about the fan sensor specified by sensor-number.</td>
</tr>
<tr>
<td>&lt;all</td>
<td>location</td>
</tr>
<tr>
<td></td>
<td>status displays status information (for example, Normal) for the fan sensor specified by sensor-number.</td>
</tr>
<tr>
<td></td>
<td>current displays current information for the fan sensor specified by sensor-number.</td>
</tr>
<tr>
<td></td>
<td>normal displays normal information for the fan sensor specified by sensor-number.</td>
</tr>
<tr>
<td></td>
<td>limit displays limit information for the fan sensor specified by sensor-number.</td>
</tr>
</tbody>
</table>

### Displaying a Network Interface Card Slot Status

Use the following commands to display the network interface card (NIC) slot status for each slot in the system.

```bash
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)
9 Monitoring Commands
10 Command-Line Utilities

This chapter contains information on a selected list of command-line utilities. On the whole, these command-line utility descriptions are similar to the man pages you would access with the man command on a typical Unix-based system.
apcssd

Name

apcssd - the command interface to the APC Simple Signaling Daemon, SSD.

Synopsis

/etc/apcssd start
/etc/apcssd stop
/etc/apcssd restart

Description

The APC Simple Signaling Daemon, SSD, provides basic shutdown and notification services for systems powered by an APC UPS in simple signaling mode. When an extended power failure occurs, SSD sends notifications to logged-in users and shuts down the appliance cleanly.

The options for apcssd are as follows:

- **start**: Starts the SSD daemon.
- **stop**: Stops the SSD daemon.
- **restart**: Stops the running daemon and then starts a new one.
Configuration File

The configuration file for SSD is /etc/ssd.conf, which contains two parameters:

TTY The serial port used to connect the simple signaling cable to the UPS. The default is /dev/ttyd1.

MaxBatRT The number of seconds the system should run after power fails. The default is 180 seconds (3 minutes). To allow the system to run as long as possible before the battery discharges, set this to a large number.

Notes

• To start the SSD daemon automatically on reboot, enter the apssd start command into /var/etc/rc.local.

• Make sure you use the 940-0020B simple signaling cable to connect the UPS to your appliance. Do not use a standard RS-232 cable or a smart signaling cable.

• A Smart UPS, such as SU420NET, must be in simple mode. If it is in smart mode:
  1 Reattach the 940-0024C smart signaling cable and use a terminal program to communicate with the UPS.
  2 Make sure the settings are 2400 baud, 8 bits, no parity, and no hardware or software flow control.
  3 Type the Y character, which should return "SM". Now type a capital R (case matters). The UPS should respond with "BYE." It is now in simple signaling mode.
  4 Reattach the 940-0020B cable.
cst

Name

cst - configuration summary tool

Synopsis

cst [-small]

Description

The Nokia IPSO Configuration Summary Tool (CST) is a troubleshooting tool that displays a summary of the current configuration of your system. It also creates a compressed file (in /admin) that you can move to a workstation and uncompres to produce various HTML and image files that make it easy to view the current configuration.

CST replaces ipsoinfo, and its HTML output is easier to read than a typical ipsoinfo output file.

CST reports the MD5 of key files on the system. This is important if vmcores exist on the system and an analysis is to be performed. The MD5 information reported by CST ensures the correct kernel and loadable modules are used during the analysis.

CST generates historical reports for cpu utilization, memory utilization, and traffic throughput for all interfaces. These reports contain pie and chart graphs as well as the raw data collected. CST also gathers debug information on VRRP, RIP, OSPF, BGP, and DVMRP.
The following option is available:

- **small**  Do not gather core files. If you do not specify this option, CST gathers core files produced in the last four weeks.
df

Name

df - display free disk space

Synopsis

df [-ikn] [-t fstype] [file | filesystem ...]

Description

df displays statistics about the amount of free disk space on the specified filesystem or on the filesystem of which file is a part. Values are displayed in 512-byte per block counts. If neither a file or a filesystem operand is specified, statistics for all mounted filesystems are displayed (subject to the -t option below).

The following options are available:

-i Include statistics on the number of free inodes.

-k Use 1024-byte (1-Kbyte) blocks rather than the default. Note that this overrides the BLOCKSIZE specification from the environment.

-n Print out the previously obtained statistics from the filesystems. This option should be used if it is possible that one or more filesystems are in a state such that they will not be able to provide statistics without a long delay. When this option is specified, df will not request new statistics from the filesystems, but will respond with the possibly stale statistics that were previously obtained.
Environment

Blocksize

If the environment variable BLOCKSIZE is set, the block counts will be displayed in units of that size block.

Bugs

The -n and -t flags are ignored if a file or filesystem is specified.

See Also

lsvfs(1), quota(1), fstatfs(2), getfsstat(2), statfs(2), getmntinfo(3), fstat(5), mount(8), quot(8)

History

A df command appeared in Version 1 AT&T UNIX.
ipsoinfo

This utility is replaced by the CST utility. Executing the command `ipsoinfo` invokes CST.
netstat

Name

netstat - show network status

Synopsis

netstat [-Aan] [-f address_family] [-M core] [-N system]
netstat [-bdghimns] [-f address_family] [-M core] [-N system]
netstat [-p protocol] [-M core] [-N system] netstat [-F]

Description

The netstat command symbolically displays the contents of various network-related data structures. There are a number of output formats, depending on the options for the information presented. The first form of the command displays a list of active sockets for each protocol. The second form presents the contents of one of the other network data structures according to the option selected. Using the third form, with a wait interval specified, netstat will continuously display the information regarding packet traffic on the configured network interfaces. The fourth form displays statistics about the named protocol.

The options have the following meaning:

-A
With the default display, show the address of any protocol control blocks associated with sockets; used for debugging.

-a
With the default display, show the state of all sockets; normally sockets used by server processes are not shown.
-b  With either interface display (option -i or an interval, as described below), show the number of bytes in and out.

-d  With either interface display (option -i or an interval, as described below), show the number of dropped packets.

-f  *address_family* Limit statistics or address control block reports to those of the specified address family. The following address families are recognized: inet, for AF_INET, ns, for AF_NS, iso, for AF_ISO, and unix, for AF_UNIX.

-F  Show the state of the flows table.

-g  Show information related to multicast (group address) routing. By default, show the IP Multicast virtual-interface and routing tables. If the -s option is also present, show multicast routing statistics.

-h  Show the state of the IMP host table (obsolete).

-I  *interface* Show information about the specified interface; used with a wait interval as described below.

-i  Show the state of interfaces which have been auto-configured (interfaces statically configured into a system, but not located at boot time are not shown). If the -a options is also present, multicast addresses currently in use are shown for each Ethernet interface and for each IP interface address. Multicast addresses are shown on separate lines following the interface address with which they are associated.

-M  Extract values associated with the name list from the specified core instead of the default /dev/kmem.

-m  Show statistics recorded by the memory management routines (the network manages a private pool of memory buffers).
The default display, for active sockets, shows the local and remote addresses, send and receive queue sizes (in bytes), protocol, and the internal state of the protocol. Address formats are of the form "host.port" or "network.port" if a socket’s address specifies a network but no specific host address. When known the host and network addresses are displayed symbolically according to the data bases /etc/hosts and /etc/networks, respectively. If a symbolic name for an address is unknown, or if the -n option is specified, the address is printed numerically, according to the address family. For more information regarding the Internet “dot format,” refer to inet(3)). Unspecified, or “wildcard”, addresses and ports appear as “*”.

-N
Extract the name list from the specified system instead of the default /kernel.

-n
Show network addresses as numbers (normally netstat interprets addresses and attempts to display them symbolically). This option may be used with any of the display formats.

-p
protocol Show statistics about protocol, which is either a well-known name for a protocol or an alias for it. Some protocol names and aliases are listed in the file /etc/protocols. A null response typically means that there are no interesting numbers to report. The program will complain if protocol is unknown or if there is no statistics routine for it.

-s
Show per-protocol statistics. If this option is repeated, counters with a value of zero are suppressed.

-r
Show the routing tables. When -s is also present, show routing statistics instead.

-w wait
Show network interface statistics at intervals of wait seconds.
The interface display provides a table of cumulative statistics regarding packets transferred, errors, and collisions. The network addresses of the interface and the maximum transmission unit (“mtu”) are also displayed.

The routing table display indicates the available routes and their status. Each route consists of a destination host or network and a gateway to use in forwarding packets. The flags field shows a collection of information about the route stored as binary choices. The individual flags are discussed in more detail in the route(8) and route(4) manual pages. The mapping between letters and flags is:

1  RTF_PROTO2  Protocol specific routing flag #1
2  RTF_PROTO1  Protocol specific routing flag #2
3  RTF_PROTO3  Protocol specific routing flag #3
B  RTF_BLACKHOLE  Just discard pkts (during updates)
C  RTF_CLONING  Generate new routes on use
c  RTF_PRCLONING  Protocol-specified generate new routes on use
D  RTF_DYNAMIC  Created dynamically (by redirect)
G  RTF_GATEWAY  Destination requires forwarding by intermediary
H  RTF_HOST  Host entry (net otherwise)
L  RTF_LLINFO  Valid protocol to link address translation
M  RTF_MODIFIED  Modified dynamically (by redirect)
R  RTF_REJECT  Host or net unreachable
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

Direct routes are created for each interface attached to the local host; the gateway field for such entries shows the address of the outgoing interface. The refcnt field gives the current number of active uses of the route. Connection oriented protocols normally hold on to a single route for the duration of a connection while connectionless protocols obtain a route while sending to the same destination. The use field provides a count of the number of packets sent using that route. The interface entry indicates the network interface utilized for the route.

When netstat is invoked with the -w option and a wait interval argument, it displays a
running count of statistics related to network interfaces. An obsolescent version of this option used a numeric parameter with no option, and is currently supported for backward compatibility. This display consists of a column for the primary interface (the first interface found during autoconfiguration) and a column summarizing information for all interfaces. The primary interface may be replaced with another interface with the -I option. The first line of each screen of information contains a summary since the system was last rebooted. Subsequent lines of output show values accumulated over the preceding interval.

See Also

iostat(1), nfsstat(1), ps(1), vmstat(1), hosts(5), networks(5), protocols(5), services(5), trpt(8), trsp(8)

History

The netstat command appeared in 4.2BSD.

Bugs

The notion of errors is ill-defined.
ping

Name

`ping` - send ICMP ECHO_REQUEST packets to network hosts

Synopsis

```
ping [ -CFILNORudfjmnruv ] [ -c count ] [ -K count ] [ -g | -G gateway ] [ -t timeout ] [ -l preload ] [ -o type ] [ -p pattern ] [ -s length ] [ -T ttl ] [ -S tos ] host
default_multicast_interface
```

Description

The DARPA Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking a single-point hardware or software failure can often be difficult. Ping utilizes the ICMP protocol’s mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (“pings”) have an IP and ICMP header, followed by a struct timeval, and then an arbitrary number of “pad” bytes used to fill out the packet. Default datagram length is 64 bytes, but this may be changed using the command-line option.

The default mode is to send a packet every timeout seconds and display the response, including sequence number and round-trip time if the packet size allows. Two other modes are available and are mutually exclusive:
Use cisco style packet sending; that is, spew packets as fast as possible, but don’t send packet N+1 until an reply or timeout has been registered for packet N. A ‘!’ is printed for every response received and a ‘.’ is printed when a packet is not received during the timeout period. Also, a ‘*’ is printed whenever a duplicate response is received.

Floodping style packet sending; send packets as fast as possible, attempting to send at at least 100 packets per second. A ‘.’ is printed for every response that is missed and a ‘*’ is printed whenever a duplicate packet is received. Only users in group zero (0) are allowed to use this option.

Specify strict source routing via this gateway. Multiple gateways may be specified by repeating the option. This option only works on BSD 4.3 based systems that allow setting of IP options.

On systems where setting the TTL of outbound ICMP packets is supported, this option sets the initial TTL to 1 and increments it each time an ECHO_REQUEST packet is sent, until an ECHO_REPLY is received or the TTL wraps to zero.

Count Terminate after receiving responses for count packets. This is subtly different from -c. If you use this option to ping a host that is down, the command might not terminate.

On systems supporting IP multicasting, disable multicast loopback.

Always lookup the returned IP addresses. By default the IP source address of packets received is printed in numeric form. Use of this option can adversely affect the round trip statistics.

Print Options. The contents of the IP Options on packets sent and received are listed.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-R</code></td>
<td>Insert “record route” IP option in outgoing packets, summarizing routes taken when program exits. This option only works on BSD 4.3 based systems that allow setting of IP options.</td>
</tr>
<tr>
<td><code>-S tos</code></td>
<td>On systems where setting the TOS of outbound ICMP packets is supported, this option sets the TOS field of all outbound ICMP ECHO REQUEST packets.</td>
</tr>
<tr>
<td><code>-T ttl</code></td>
<td>On systems where setting the TTL of outbound ICMP packets is supported, this option sets the initial TTL of all outbound ICMP ECHO REQUEST packets.</td>
</tr>
<tr>
<td><code>-U</code></td>
<td>Print round trip times and accumulate statistics with millisecond precision.</td>
</tr>
<tr>
<td><code>-c count</code></td>
<td>Terminate after count packets have been sent or received.</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Enable socket level debugging with the SO_DEBUG option.</td>
</tr>
<tr>
<td><code>-f Fast</code></td>
<td>ping, send a packet as soon as a response is received.</td>
</tr>
<tr>
<td><code>-g</code></td>
<td>Specify loose source routing via this gateway. Multiple gateways may be specified by repeating the option. This option only works on BSD 4.3 based systems that allow setting of IP options.</td>
</tr>
<tr>
<td><code>-j</code></td>
<td>When the destination host is really an IP multicast group on systems supporting IP multicasting, join the specified group.</td>
</tr>
<tr>
<td><code>-l</code></td>
<td>Specifies the number of packets to preload; packets which are sent at startup before listening for a response. The default is not to send any preload packets.</td>
</tr>
<tr>
<td><code>-m</code></td>
<td>Enable printing of a summary of missed responses.</td>
</tr>
<tr>
<td><code>-n</code></td>
<td>Disable hostname lookup of the returned IP addresses. By default the hostname and IP address of the destination host is displayed in the header, summary and “record route” summary. If the hostname lookup fails, just the IP address is displayed.</td>
</tr>
</tbody>
</table>
-o Specifies the type of ICMP packet to send. The default is an ECHO_REQUEST. The type may be abreviated down to one character.

Supported types are:

- **echo** Send an ECHO_REQUEST, expect and ECHO_RESPONSE. If at least eight bytes of data are available, round trip timing is done. This is the default.

- **info** Send an INFO_REQUEST, expect and INFO_RESPONSE. Roundtrip timing and additional data are not possible with this type.

- **mask** Send a MASK_REQUEST, expect a MASK_REPLY. Round trip timing and additional data are not possible with this type.

- **router** Send a ROUTER_SOLICITATION, expect a ROUTER_ADVERTISEMENT. Round trip timing and additional data are not possible with this type.

- **timestamp** Send a TIMESTAMP_REQUEST, expect a TIMESTAMP_REPLY. Route trip and additional timing is always done. Additional data may be carried.

-p Specifies the pattern to fill unused data in the packets. The default is to fill with the data position modulo 256. A pattern Is a string of hex digit pairs used to specify the contents of the bytes of the packet. Multiple patterns are concatenated. The pattern(s) are replicated until they fill the packet.

-q Disable displaying of ping response messages, only display the summary.
When using ping for fault isolation, it should first be run on the local host, to verify that the local network interface is up and running. Then, hosts and gateways further and further away should be “pinged.” Ping sends one datagram per second, and prints one line of output for every ECHO_RESPONSE returned. No output is produced if there is no response. If an optional length is specified, it is used as the length of the data portion of the ICMP ECHO_REQUEST packet. The default length is 56 data bytes. If an optional count is given, only that number of requests is sent. Round-trip times and packet loss statistics are computed. When all responses have been received or the program times out (with a count specified), or if the program is terminated with a SIGINT, a brief summary is displayed.

This program is intended for use in network testing, measurement and management. It should be used primarily for manual fault isolation. Because of the load it could impose on the network, it is unwise to use ping during normal operations or from automated scripts.

- **-r**  Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it (e.g., after the interface was dropped by routed(8C)).

- **-t**  Specify the timeout between pings in normal and cisco style modes as a floating point number. The default is one second. Only users in group zero (0) are allowed to specify a value less than one second.

- **-u**  Print round trip times and accumulate statistics with microsecond precision.

- **-v**  Verbose output. ICMP packets other than ECHO_RESPONSE that are received are listed.
Return Values

An exit status of zero is returned if at least one response was heard from the specified host; a status of two if the transmission was successful but no responses were received; or another value if an error occurred.

Author

Mike Muuss

Co-conspirators

Ron Natalie, David Paul Zimmerman, Jeffrey C Honig, Vernon Schryver, Dennis Ferguson.

Bugs

More options than ls(1).

See Also

netstat(1), ifconfig(8C)
ps

Name

ps - process status

Synopsis

[-p pid] [-t tty] [-W swap] ps [-L]

Description

Ps displays a header line followed by lines containing information about your processes that have controlling terminals. This information is sorted by controlling terminal, then by process ID.

The information displayed is selected based on a set of keywords (see the -L -O and -o options). The default output format includes, for each process, the process’ ID, controlling terminal, CPU time (including both user and system time), state, and associated command.

The process file system (see procfs(5)) should be mounted when ps is executed, otherwise not all information will be available.

The options are as follows:

- `-a` Display information about other users’ processes as well as your own.
- `-C` Change the way the cpu percentage is calculated by using a “raw” cpu calculation that ignores “resident” time (this normally has no effect).
-e  Display the environment as well.
-h  Repeat the information header as often as necessary to guarantee one header per page of information.
-j  Print information associated with the following keywords: user, pid, ppid, pgid, sess, jobc, state, tt, time and command.
-L  List the set of available keywords.
-l  Display information associated with the following keywords: uid, pid, ppid, cpu, pri, nice, vsz, rss, wchan, state, tt, time and command.
-M  Extract values associated with the name list from the specified core instead of the default /dev/kmem.
-m  Sort by memory usage, instead of by process ID.
-N  Extract the name list from the specified system instead of the default /kernel.
-O  Add the information associated with the space or comma separated list of keywords specified, after the process ID, in the default information display. Keywords may be appended with an equals ("=") sign and a string. This causes the printed header to use the specified string instead of the standard header.
-o  Display information associated with the space or comma separated list of keywords specified. Keywords may be appended with an equals ("=") sign and a string. This causes the printed header to use the specified string instead of the standard header.
-p  Display information associated with the specified process ID.
-r  Sort by current cpu usage, instead of by process ID.
-S  Change the way the process time is calculated by summing all excited children to their parent process.
Display information about processes attached to the device associated with the standard input.

Display information about processes attached to the specified terminal device.

Display information associated with the following keywords: user, pid, %cpu, %mem, vsz, rss, tt, state, start, time and command. The -u option implies the -r option.

Display information associated with the following keywords: pid, state, time, sl, re, pagein, vsz, rss, lim, tsiz, %cpu, %mem and command. The -v option implies the -m option.

Extract swap information from the specified file instead of the default /dev/drum.

Use 132 columns to display information, instead of the default which is your window size. If the -w option is specified more than once, ps will use as many columns as necessary without regard for your window size.

Display information about processes without controlling terminals.

A complete list of the available keywords are listed below. Some of these keywords are further specified as follows:

%cpu The cpu utilization of the process; this is a decaying average over up to a minute of previous (real) time. Since the time base over which this is computed varies (since processes may be very young) it is possible for the sum of all %CPU fields to exceed 100%.

%mem The percentage of real memory used by this process.

flags The flags associated with the process as in the include file <sys/proc.h>:

P_ADVLOCK 0x00001 Process may hold a POSIX advisory lock
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_CONTROLT</td>
<td>0x00002</td>
<td>Has a controlling terminal</td>
</tr>
<tr>
<td>P_INMEM</td>
<td>0x00004</td>
<td>Loaded into memory</td>
</tr>
<tr>
<td>P_NOCLDSTOP</td>
<td>0x00008</td>
<td>No SIGCHLD when children stop</td>
</tr>
<tr>
<td>P_PPWAIT</td>
<td>0x00010</td>
<td>Parent is waiting for child to exec/exit</td>
</tr>
<tr>
<td>P_PROFIL</td>
<td>0x00020</td>
<td>Has started profiling</td>
</tr>
<tr>
<td>P_SELECT</td>
<td>0x00040</td>
<td>Selecting; wakeup/waiting danger</td>
</tr>
<tr>
<td>P_SINTR</td>
<td>0x00080</td>
<td>Sleep is interruptible</td>
</tr>
<tr>
<td>P_SUGID</td>
<td>0x00100</td>
<td>Had set id privileges since last exec</td>
</tr>
<tr>
<td>P_SYSTEM</td>
<td>0x00200</td>
<td>System proc: no sigs, stats or swapping</td>
</tr>
<tr>
<td>P_TIMEOUT</td>
<td>0x00400</td>
<td>Timing out during sleep</td>
</tr>
<tr>
<td>P_TRACED</td>
<td>0x00800</td>
<td>Debugged process being traced</td>
</tr>
<tr>
<td>P_WAITED</td>
<td>0x01000</td>
<td>Debugging process has waited for child</td>
</tr>
<tr>
<td>P_WEXIT</td>
<td>0x02000</td>
<td>Working on exiting</td>
</tr>
<tr>
<td>P_EXEC</td>
<td>0x04000</td>
<td>Process called exec</td>
</tr>
<tr>
<td>P_NOSWAP</td>
<td>0x08000</td>
<td>Another flag to prevent swap out</td>
</tr>
<tr>
<td>P_PHYSIO</td>
<td>0x10000</td>
<td>Doing physical I/O</td>
</tr>
<tr>
<td>P_OWEUPC</td>
<td>0x20000</td>
<td>Owe process an addupc() call at next ast</td>
</tr>
<tr>
<td>P_SWAPPING</td>
<td>0x40000</td>
<td>Process is being swapped</td>
</tr>
</tbody>
</table>

**lim**
The soft limit on memory used, specified via a call to setrlimit(2).

**lstart**
The exact time the command started, using the “%c” format described in strftime(3).
nice The process scheduling increment (see setpriority(2)).

rss The real memory (resident set) size of the process (in 1024 byte units).

start The time the command started. If the command started less than 24 hours ago, the start time is displayed using the “%l:ps.1p” format described in strftime(3). If the command started less than 7 days ago, the start time is displayed using the “%a6.15p” format. Otherwise, the start time is displayed using the “%e%b%y” format.

state The state is given by a sequence of letters, for example, “RWNA”.
The first letter indicates the run state of the process:

D Marks a process in disk (or other short term, uninterruptible) wait.
I Marks a process that is idle (sleeping for longer than about 20 seconds).
R Marks a runnable process.
S Marks a process that is sleeping for less than about 20 seconds.
T Marks a stopped process.
Z Marks a dead process (a “zombie”).

Additional characters after these, if any, indicate additional state information:
+
The process is in the foreground process group of its control terminal.
< The process has raised CPU scheduling priority.
> The process has specified a soft limit on memory requirements and is currently exceeding that limit; such a process is (necessarily) not swapped.
A  The process has asked for random page replacement (MADV_RANDOM, from madvise(2), for example, lisp(1) in a garbage collect).

E  The process is trying to exit.

L  The process has pages locked in core (for example, for raw I/O).

N  The process has reduced CPU scheduling priority (see setpriority(2)).

S  The process has asked for FIFO page replacement (MADV_SEQUENTIAL, from madvise(2), for example, a large image processing program using virtual memory to sequentially address voluminous data).

s  The process is a session leader.

V  The process is suspended during a vfork.

W  The process is swapped out.

X  The process is being traced or debugged.

tt  An abbreviation for the pathname of the controlling terminal, if any. The abbreviation consists of the three letters following /dev/tty, or, for the console, “con”. This is followed by a “-” if the process can no longer reach that controlling terminal (i.e., it has been revoked).

wchan  The event (an address in the system) on which a process waits. When printed numerically, the initial part of the address is trimmed off and the result is printed in hex, for example, 0x80324000 prints as 324000.
When printing using the command keyword, a process that has exited and has a parent that has not yet waited for the process (in other words, a zombie) is listed as “<defunct>”, and a process which is blocked while trying to exit is listed as “<exiting>". Ps makes an educated guess as to the file name and arguments given when the process was created by examining memory or the swap area. The method is inherently somewhat unreliable and in any event a process is entitled to destroy this information, so the names cannot be depended on too much. The ucomm (accounting) keyword can, however, be depended on.

**Keywords**

The following is a complete list of the available keywords and their meanings. Several of them have aliases (keywords which are synonyms).

- **%cpu**: percentage cpu usage (alias pcpu)
- **%mem**: percentage memory usage (alias pmem)
- **acflag**: accounting flag (alias acflg)
- **command**: command and arguments
- **cpu**: short-term cpu usage factor (for scheduling)
- **flags**: the process flags, in hexadecimal (alias f)
- **inblk**: total blocks read (alias inblock)
- **jobc**: job control count
- **ktrace**: tracing flags
- **ktracep**: tracing vnode
- **lim**: memory use limit
- **logname**: login name of user who started the process
- **lstart**: time started
- **majflt**: total page faults
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minflt</td>
<td>total page reclaims</td>
</tr>
<tr>
<td>msgrcv</td>
<td>total messages received (reads from pipes/sockets)</td>
</tr>
<tr>
<td>msgsnd</td>
<td>total messages sent (writes on pipes/sockets)</td>
</tr>
<tr>
<td>nice</td>
<td>nice value (alias ni)</td>
</tr>
<tr>
<td>nivcsw</td>
<td>total involuntary context switches</td>
</tr>
<tr>
<td>nsigs</td>
<td>total signals taken (alias nsignals)</td>
</tr>
<tr>
<td>nswap</td>
<td>total swaps in/out</td>
</tr>
<tr>
<td>nvcsw</td>
<td>total voluntary context switches</td>
</tr>
<tr>
<td>nwchar</td>
<td>wait channel (as an address)</td>
</tr>
<tr>
<td>oublk</td>
<td>total blocks written (alias oublock)</td>
</tr>
<tr>
<td>p_ru</td>
<td>resource usage (valid only for zombie)</td>
</tr>
<tr>
<td>paddr</td>
<td>swap address</td>
</tr>
<tr>
<td>pagein</td>
<td>pageins (same as majflt)</td>
</tr>
<tr>
<td>pgid</td>
<td>process group number</td>
</tr>
<tr>
<td>pid</td>
<td>process ID</td>
</tr>
<tr>
<td>poip</td>
<td>pageouts in progress</td>
</tr>
<tr>
<td>ppid</td>
<td>parent process ID</td>
</tr>
<tr>
<td>pri</td>
<td>scheduling priority</td>
</tr>
<tr>
<td>re</td>
<td>core residency time (in seconds; 127 = infinity)</td>
</tr>
<tr>
<td>rgid</td>
<td>real group ID</td>
</tr>
<tr>
<td>rlink</td>
<td>reverse link on run queue, or 0</td>
</tr>
<tr>
<td>rss</td>
<td>resident set size</td>
</tr>
</tbody>
</table>
rsz  resident set size + (text size / text use count) (alias rssize)
rt prio  realtime priority (101 = not a realtime process)
ruid  real user ID
ruser  user name (from ruid)
sess  session pointer
sig  pending signals (alias pending)
sigcatch  caught signals (alias caught)
signore  ignored signals (alias ignored)
sigmask  blocked signals (alias blocked)
sl  sleep time (in seconds; 127 = infinity)
start  time started
state  symbolic process state (alias stat)
svgid  saved gid from a setgid executable
svuid  saved uid from a setuid executable
tdev  control terminal device number
time  accumulated cpu time, user + system (alias cputime)
tpgid  control terminal process group ID
tsess  control terminal session pointer
tsz  text size (in Kbytes)
tt  control terminal name (two letter abbreviation)
tty  full name of control terminal
uprocp  process pointer
ucomm name to be used for accounting
uid effective user ID
upr scheduling priority on return from system call (alias usrpri)
user user name (from uid)
vsz virtual size in Kbytes (alias vsize)
wchan wait channel (as a symbolic name)
xstat exit or stop status (valid only for stopped or zombie process)

Files

/dev special files and device names
/dev/drum default swap device
/dev/kmem default kernel memory
/var/run/dev.db /dev name database
/var/db/kvm_kernel.db system namelist database
/kernel default system namelist
/proc the mount point of procfs(5)

See Also

kill(1), w(1), kvm(3), strftime(3), procfs(5), pstat(8)
10 Command-Line Utilities

Bugs

Since `ps` cannot run faster than the system and is run as any other scheduled process, the information it displays can never be exact.
tcpdump

Name
tcpdump - dump traffic on a network

Synopsis
tcpdump [ -defglnNOpqStvxX ] [ -c count ] [ -F file ]
[-i interface ] [ -r file ] [ -s snaplen ] [ -T type ]
[ -w file ] [ expression ]

Description
Tcpdump prints out the headers of packets on a network interface that match the boolean expression.

Under SunOS with nit or bpf: To run tcpdump you must have read access to /dev/net or /dev/bpf*. Under Solaris with dlpi: You must have read access to the network pseudo device, e.g. /dev/le. Under HP-UX with dlpi: You must be root or it must be installed setuid to root. Under IRIX with snoop: You must be root or it must be installed setuid to root. Under Linux: You must be root or it must be installed setuid to root. Under Ultrix and Digital UNIX: Once the super-user has enabled promiscuous-mode operation using pfconfig(8), any user may run tcpdump. Under BSD: You must have read access to /dev/bpf*.

Options

-c Exit after receiving count packets.
-d  Dump the compiled packet-matching code in a human readable form to standard output and stop.
-dd  Dump packet-matching code as a C program fragment.
-ddd  Dump packet-matching code as decimal numbers (preceded with a count).
-e  Print the link-level header on each dump line.
-f  Print ‘foreign’ internet addresses numerically rather than symbolically (this option is intended to get around serious brain damage in Sun’s yp server -- usually it hangs forever translating nonlocal internet numbers).
-g  Should be used with -r and -w flags to convert an IPSO formatted dump that was written earlier using tcpdump, to more portable generic format.
-F  Use file as input for the filter expression. An additional expression given on the command line is ignored.
-i  Listen on interface. If unspecified, tcpdump searches the system interface list for the lowest numbered, configured up interface (excluding loopback). Ties are broken by choosing the earliest match.
-l  Make stdout line buffered. Useful if you want to see the data while capturing it. E.g., “tcpdump -l | tee dat” or “tcpdump -l> dat & tail -f dat”.
-n  Don’t convert addresses (i.e., host addresses, port numbers, etc.) to names.
-N  Don’t print domain name qualification of host names. E.g., if you give this flag then tcpdump will print “nic” instead of “nic.ddn.mil”.
-O  Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer.

-p  Don’t put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, ‘-p’ cannot be used as an abbreviation for ‘ether host {local-hw-addr} or ether broadcast’.

-q  Quick (quiet?) output. Print less protocol information so output lines are shorter.

-r  Read packets from file (which was created with the -w option). Standard input is used if file is “-”.

-s  Snarf snaplen bytes of data from each packet rather than the default of 68 (with SunOS’s NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of a limited snapshot are indicated in the output with “[ proto]”, where proto is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit snaplen to the smallest number that will capture the protocol information you’re interested in.

-T  Force packets selected by “expression” to be interpreted the specified type. Currently known types are rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), vat (Visual Audio Tool), and wb (distributed White Board).

-S  Print absolute, rather than relative, TCP sequence numbers.

-t  Don’t print a timestamp on each dump line.

-tt  Print an unformatted timestamp on each dump line.
Expression

Expression selects which packets will be dumped. If no expression is given, all packets on the net will be dumped. Otherwise, only packets for which expression is ‘true’ will be dumped.

The expression consists of one or more primitives. Primitives usually consist of an id (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

type qualifiers say what kind of thing the id name or number refers to. Possible types are host, net and port. E.g., ‘host foo’, ‘net 128.3’, ‘port 20’. If there is no type qualifier, host is assumed.

dir qualifiers specify a particular transfer direction to and/or from id. Possible directions are src, dst, src or dst and src and dst. E.g., ‘src foo’, ‘dst net 128.3’, ‘src or dst port ftp-data’. If there is no dir qualifier, src or dst is assumed. For ‘null’ link layers (i.e. point to point protocols such as slip) the inbound and outbound qualifiers can be used to specify a desired direction.

- \texttt{v} (Slightly more) verbose output. For example, the time to live and type of service information in an IP packet is printed.

- \texttt{vv} Even more verbose output. For example, additional fields are printed from NFS reply packets.

- \texttt{w} Write the raw packets to file rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if file is ‘-’. Use -g flag if the file will be read on some other platform.

- \texttt{x} Print each packet (minus its link level header) in hex. The smaller of the entire packet or snaplen bytes will be printed.

- \texttt{X} Print each packet (minus its link level header) in hex and ascii. The smaller of the entire packet or snaplen bytes will be printed.
proto qualifiers restrict the match to a particular protocol. Possible protos are: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp. E.g., ‘ether src foo’, ‘arp net 128.3’, ‘tcp port 21’. If there is no proto qualifier, all protocols consistent with the type are assumed. E.g., ‘src foo’ means ‘(ip or arp or rarp) src foo’ (except the latter is not legal syntax), ‘net bar’ means ‘(ip or arp or rarp) net bar’ and ‘port 53’ means ‘(tcp or udp) port 53’.

[‘fddi’ is actually an alias for ‘ether’; the parser treats them identically as meaning “the data link level used on the specified network interface.” FDDI headers contain Ethernet-like source and destination addresses, and often contain Ethernet-like packet types, so you can filter on these FDDI fields just as with the analogous Ethernet fields. FDDI headers also contain other fields, but you cannot name them explicitly in a filter expression.]

In addition to the above, there are some special primitive keywords that don’t follow the pattern: gateway, broadcast, less, greater and arithmetic expressions. All of these are described below.

More complex filter expressions are built up by using the words and, or and not to combine primitives, for example, ‘host foo and not port ftp and not port ftp-data’. To save typing, identical qualifier lists can be omitted, for example, ‘tcp dst port ftp or ftp-data or domain’ is exactly the same as ‘tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain’.

Allowable primitives are:

- **dst host host**  True if the IP destination field of the packet is host, which may be either an address or a name.
- **src host host**  True if the IP source field of the packet is host.
host host

True if either the IP source or destination of the packet is host. Any of the above host expressions can be prepended with the keywords, ip, arp, or rarp as in: ip host host which is equivalent to: ether proto \ip and host host If host is a name with multiple IP addresses, each address will be checked for a match.

ether dst ehost

True if the ethernet destination address is ehost. Ehost may be either a name from /etc/ethers or a number (see ethers(3N) for numeric format).

ether src ehost

True if the ethernet source address is ehost.

ether host ehost

True if either the ethernet source or destination address is ehost.

gateway host

True if the packet used host as a gateway. I.e., the ethernet source or destination address was host but neither the IP source nor the IP destination was host. Host must be a name and must be found in both /etc/hosts and /etc/ethers. (An equivalent expression is ether host ehost and not host host which can be used with either names or numbers for host / ehost.)

dst net net

True if the IP destination address of the packet has a network number of net. Net may be either a name from /etc/networks or a network number (see networks(4) for details).

src net net

True if the IP source address of the packet has a network number of net.

net net

True if either the IP source or destination address of the packet has a network number of net.

net net mask mask

True if the IP address matches net with the specific netmask. May be qualified with src or dst.
net net/len

True if the IP address matches net a netmask len bits wide. May be qualified with src or dst.

dst port port

True if the packet is ip/tcp or ip/udp and has a destination port value of port. The port can be a number or a name used in /etc/services (see tcp(4P) and udp(4P)). If a name is used, both the port number and protocol are checked. If a number or ambiguous name is used, only the port number is checked (e.g., dst port 513 will print both tcp/login traffic and udp/who traffic, and port domain will print both tcp/domain and udp/domain traffic).

src port port

True if the packet has a source port value of port.

port port

True if either the source or destination port of the packet is port. Any of the above port expressions can be prepended with the keywords, tcp or udp, as in: tcp src port port which matches only tcp packets whose source port is port.

less length

True if the packet has a length less than or equal to length. This is equivalent to: len <= length.

greater length

True if the packet has a length greater than or equal to length. This is equivalent to: len >= length.

ip proto protocol

True if the packet is an ip packet (see ip(4P)) of protocol type protocol. Protocol can be a number or one of the names icmp, igrp, udp, nd, or tcp. Note that the identifiers tcp, udp, and icmp are also keywords and must be escaped via backslash (\), which is \ in the C-shell.

ether broadcast

True if the packet is an ethernet broadcast packet. The ether keyword is optional.
ip broadcast  True if the packet is an IP broadcast packet. It checks for both the all-zeroes and all-ones broadcast conventions, and looks up the local subnet mask.

ether multicast  True if the packet is an ethernet multicast packet. The ether keyword is optional. This is shorthand for ‘ether[0] & 1 != 0’.

ip multicast  True if the packet is an IP multicast packet.

ether proto protocol  True if the packet is of ether type protocol. Protocol can be a number or a name like ip, arp, or rarp. Note these identifiers are also keywords and must be escaped via backslash (\). [In the case of FDDI (e.g., ‘fddi protocol arp’), the protocol identification comes from the 802.2 Logical Link Control (LLC) header, which is usually layered on top of the FDDI header. Tcpdump assumes, when filtering on the protocol identifier, that all FDDI packets include an LLC header, and that the LLC header is in so-called SNAP format.]

decnet src host  True if the DECNET source address is host, which may be an address of the form “10.123”, or a DECNET host name. [DECNET host name support is only available on Ultrix systems that are configured to run DECNET.]

decnet dst host  True if the DECNET destination address is host.

decnet host host  True if either the DECNET source or destination address is host.

ip, arp, rarp, decnet  Abbreviations for: ether proto p where p is one of the above protocols.
Primitives may be combined using:

- `lat, moprc, mopdl`  
  Abbreviations for: ether proto p where p is one of the above protocols. Note that tcpdump does not currently know how to parse these protocols.

- `tcp, udp, icmp`  
  Abbreviations for: ip proto p where p is one of the above protocols.

- `expr relop expr`  
  True if the relation holds, where relop is one of `>`, `<`, `>==`, `<=`, `=`, `!=`, and expr is an arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators `+`, `-`, `*`, `/`, `&`, `|`, a length operator, and special packet data accessors. To access data inside the packet, use the following syntax: proto [ expr : size ] Proto is one of ether, fddi, ip, arp, rarp, tcp, udp, or icmp, and indicates the protocol layer for the index operation. The byte offset, relative to the indicated protocol layer, is given by expr. Size is optional and indicates the number of bytes in the field of interest; it can be either one, two, or four, and defaults to one. The length operator, indicated by the keyword len, gives the length of the packet.

  For example, ‘ether[0] & 1 != 0’ catches all multicast traffic. The expression ‘ip[0] & 0xf != 5’ catches all IP packets with options. The expression ‘ip[6:2] & 0xff = 0’ catches only unfragmented datagrams and frag zero of fragmented datagrams. This check is implicitly applied to the tcp and udp index operations. For instance, tcp[0] always means the first byte of the TCP header, and never means the first byte of an intervening fragment.

Primitives may be combined using:
A parenthesized group of primitives and operators (parentheses are special to the Shell and must be escaped).

- Negation (‘!’ or ‘not’).
- Concatenation (‘&&’ or ‘and’).
- Alternation (‘||’ or ‘or’).

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right. Note that explicit and tokens, not juxtaposition, are now required for concatenation.

If an identifier is given without a keyword, the most recent keyword is assumed. For example, not host vs and ace is short for not host vs and host ace which should not be confused with not ( host vs or ace )

Expression arguments can be passed to tcpdump as either a single argument or as multiple arguments, whichever is more convenient. Generally, if the expression contains Shell metacharacters, it is easier to pass it as a single, quoted argument. Multiple arguments are concatenated with spaces before being parsed.

**Examples**

To print all packets arriving at or departing from sundown: tcpdump host sundown

To print traffic between helios and either hot or ace: tcpdump host helios and \( \text{hot or ace} \)

To print all IP packets between ace and any host except helios: tcpdump ip host ace and not helios

To print all traffic between local hosts and hosts at Berkeley: tcpdump net ucb-ether

To print all ftp traffic through internet gateway snup: (note that the expression is quoted to prevent the shell from (mis-)interpreting the parentheses): tcpdump ‘gateway snup and (port ftp or ftp-data)’
To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net): tcpdump ip and not net localnet

To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host: tcpdump ‘tcp[13] & 3 != 0 and not src and dst net localnet’

To print IP packets longer than 576 bytes sent through gateway snup: tcpdump ‘gateway snup and ip[2:2] > 576’

To print IP broadcast or multicast packets that were not sent via ethernet broadcast or multicast: tcpdump ‘ether[0] & 1 = 0 and ip[16] >= 224’

To print all ICMP packets that are not echo requests/replies (i.e., not ping packets): tcpdump ‘icmp[0] != 8 and icmp[0] != 0”

Output Format

The output of tcpdump is protocol dependent. The following gives a brief description and examples of most of the formats.

Link Level Headers

If the ‘-e’ option is given, the link level header is printed out. On Ethernet networks, the source and destination addresses, protocol, and packet length are printed.

On FDDI networks, the ‘-e’ option causes tcpdump to print the ‘frame control’ field, the source and destination addresses, and the packet length. (The ‘frame control’ field governs the interpretation of the rest of the packet. Normal packets (such as those containing IP datagrams) are ‘async’ packets, with a priority value between 0 and 7; for example, ‘async4’. Such packets are assumed to contain an 802.2 Logical Link Control (LLC) packet; the LLC header is printed if it is not an ISO datagram or a so-called SNAP packet.
(N.B.: The following description assumes familiarity with the SLIP compression algorithm described in RFC-1144.)

On SLIP links, a direction indicator (“I” for inbound, “O” for outbound), packet type, and compression information are printed out. The packet type is printed first. The three types are ip, utcp, and etcp. No further link information is printed for ip packets. For TCP packets, the connection identifier is printed following the type. If the packet is compressed, its encoded header is printed out. The special cases are printed out as *S+n and *SA+n, where n is the amount by which the sequence number (or sequence number and ack) has changed. If it is not a special case, zero or more changes are printed. A change is indicated by U (urgent pointer), W (window), A (ack), S (sequence number), and I (packet ID), followed by a delta (+n or -n), or a new value (=n). Finally, the amount of data in the packet and compressed header length are printed.

For example, the following line shows an outbound compressed TCP packet, with an implicit connection identifier; the ack has changed by 6, the sequence number by 49, and the packet ID by 6; there are 3 bytes of data and 6 bytes of compressed header: O etcp * A+6 S+49 I+6 3 (6)

ARP/RARP Packets

Arp/rarp output shows the type of request and its arguments. The format is intended to be self explanatory. Here is a short sample taken from the start of an ‘rlogin’ from host rtsg to host csam: arp who-has csam tell rtsg arp reply csam is-at CSAM The first line says that rtsg sent an arp packet asking for the ethernet address of internet host csam. Csam replies with its ethernet address (in this example, ethernet addresses are in caps and internet addresses in lower case).

This would look less redundant if we had done tcpdump -n: arp who-has 128.3.254.6 tell 128.3.254.68 arp reply 128.3.254.6 is-at 02:07:01:00:01:c4

If we had done tcpdump -e, the fact that the first packet is broadcast and the second is point-to-point would be visible: RTSG Broadcast 0806 64: arp who-has csam tell rtsg CSAM RTSG 0806 64: arp reply csam is-at CSAM For the first packet this says the
The ethernet source address is RTSG, the destination is the ethernet broadcast address, the type field contained hex 0806 (type ETHER_ARP) and the total length was 64 bytes.

**TCP Packets**

(N.B.: The following description assumes familiarity with the TCP protocol described in RFC-793. If you are not familiar with the protocol, neither this description nor tcpdump will be of much use to you.)

The general format of a tcp protocol line is: src > dst: flags data-seqno ack window urgent options Src and dst are the source and destination IP addresses and ports. Flags are some combination of S (SYN), F (FIN), P (PUSH) or R (RST) or a single `.` (no flags). Data-seqno describes the portion of sequence space covered by the data in this packet (see example below). Ack is sequence number of the next data expected the other direction on this connection. Window is the number of bytes of receive buffer space available the other direction on this connection. Urg indicates there is ‘urgent’ data in the packet. Options are tcp options enclosed in angle brackets (e.g., `<mss 1024>`).

Src, dst and flags are always present. The other fields depend on the contents of the packet’s tcp protocol header and are output only if appropriate.

Here is the opening portion of an rlogin from host rtsg to host csam.

```
rtsg.1023 > csam.login: S 768512:768512(0) win 4096 <mss 1024>
csam.login > rtsg.1023: S 947648:947648(0) ack 768513 win 4096 <mss1024>
rtsg.1023 > csam.login: .ack 1 win 4096
rtsg.1023 > csam.login: P 1:2(1) ack 1 win 4096
csam.login > rtsg.1023: .ack 2 win 4096
rtsg.1023 > csam.login: P 2:21(19) ack 1 win 4096
csam.login > rtsg.1023: P 1:2(1) ack 21 win 4077
csam.login > rtsg.1023: P 2:3(1) ack 21 win 4077 urg 1
csam.login > rtsg.1023: P 3:4(1) ack 21 win 4077 urg 1
```
The first line says that tcp port 1023 on rtsg sent a packet to port login on csam. The S indicates that the SYN flag was set. The packet sequence number was 768512 and it contained no data. (The notation is ‘first:last(nbytes)’ which means ‘sequence numbers first up to but not including last which is nbytes bytes of user data’.) There was no piggy-backed ack, the available receive window was 4096 bytes and there was a max-segment-size option requesting an mss of 1024 bytes.

Csam replies with a similar packet except it includes a piggy-backed ack for rtsg’s SYN. Rtsg then acks csam’s SYN. The ‘.’ means no flags were set. The packet contained no data so there is no data sequence number. Note that the ack sequence number is a small integer (1). The first time tcpdump sees a tcp ‘conversation’, it prints the sequence number from the packet. On subsequent packets of the conversation, the difference between the current packet’s sequence number and this initial sequence number is printed. This means that sequence numbers after the first can be interpreted as relative byte positions in the conversation’s data stream (with the first data byte each direction being ‘1’). ‘-S’ will override this feature, causing the original sequence numbers to be output.

On the 6th line, rtsg sends csam 19 bytes of data (bytes 2 through 20 in the rtsg -> csam side of the conversation). The PUSH flag is set in the packet. On the 7th line, csam says it’s received data sent by rtsg up to but not including byte 21. Most of this data is apparently sitting in the socket buffer since csam’s receive window has gotten 19 bytes smaller. Csam also sends one byte of data to rtsg in this packet. On the 8th and 9th lines, csam sends two bytes of urgent, pushed data to rtsg.

If the snapshot was small enough that tcpdump didn’t capture the full TCP header, it interprets as much of the header as it can and then reports “[tcp]” to indicate the remainder could not be interpreted. If the header contains a bogus option (one with a length that’s either too small or beyond the end of the header), tcpdump reports it as “[bad opt]” and does not interpret any further options (since it’s impossible to tell where they start). If the header length indicates options are present but the IP datagram length is not long enough for the options to actually be there, tcpdump reports it as “[bad hdr length].”
UDP Packets

UDP format is illustrated by this rwho packet: actinide.who > broadcast.who: udp 84
This says that port who on host actinide sent a udp datagram to port who on host
broadcast, the Internet broadcast address. The packet contained 84 bytes of user data.

Some UDP services are recognized (from the source or destination port number) and
the higher level protocol information printed. In particular, Domain Name service
requests (RFC-1034/1035) and Sun RPC calls (RFC-1050) to NFS.

UDP Name Server Requests

(N.B.: The following description assumes familiarity with the Domain Service
protocol described in RFC-1035. If you are not familiar with the protocol, the
following description will appear to be written in greek.)

Name server requests are formatted as src > dst: id op? flags qtype qclass name (len)
h2opolo.1538 > helios.domain: 3+ A? ucbvax.berkeley.edu. (37) Host h2opolo asked
the domain server on helios for an address record (qtype=A) associated with the name
ucb-vax.berkeley.edu. The query id was ‘3’. The ‘+’ indicates the recursion desired
flag was set. The query length was 37 bytes, not including the UDP and IP protocol
headers. The query operation was the normal one, Query, so the op field was omitted.
If the op had been anything else, it would have been printed between the ‘3’ and the
‘+’ . Similarly, the qclass was the normal one, C_IN, and omitted. Any other qclass
would have been printed immediately after the ‘A’.

A few anomalies are checked and may result in extra fields enclosed in square
brackets: If a query contains an answer, name server or authority section, ancount,
nscount, or arcount are printed as ‘[na]’, ‘[nn]’ or ‘[nau]’ where n is the appropriate
count. If any of the response bits are set (AA, RA or rcode) or any of the ‘must be
zero’ bits are set in bytes two and three, ‘[b2&3=x]’ is printed, where x is the hex value
of header bytes two and three.

UDP Name Server Responses

Name server responses are formatted as
src > dst: id op rcode flags a/n/au type class data (len)
helios.domain > h2opolo.1538: 3 3/3/7 A 128.32.137.3 (273)
helios.domain > h2opolo.1537: 2 NXDomain* 0/1/0 (97)

In the first example, helios responds to query id 3 from h2opolo with 3 answer records, 3 name server records and 7 authority records. The first answer record is type A (address) and its data is internet address 128.32.137.3. The total size of the response was 273 bytes, excluding UDP and IP headers. The op (Query) and response code (NoError) were omitted, as was the class (C_IN) of the A record.

In the second example, helios responds to query 2 with a response code of non-existent domain (NXDomain) with no answers, one name server and no authority records. The '*' indicates that the authoritative answer bit was set. Since there were no answers, no type, class or data were printed.

Other flag characters that might appear are ‘-’ (recursion available, RA, not set) and ‘|’ (truncated message, TC, set). If the ‘question’ section doesn’t contain exactly one entry, ‘[nq]’ is printed.

Note that name server requests and responses tend to be large and the default snaplen of 68 bytes may not capture enough of the packet to print. Use the -s flag to increase the snaplen if you need to seriously investigate name server traffic. ‘-s 128’ has worked well for me.

**NFS Requests and Replies**

Sun NFS (Network File System) requests and replies are printed as:

src.xid > dst.nfs: len op args
src.nfs > dst.xid: reply stat len op results
sushi.6709 > wrl.nfs: 112 readlink fh 21,24/10.73165
wrl.nfs > sushi.6709: reply ok 40 readlink “/var”
sushi.201b > wrl.nfs: 144 lookup fh 9,74/4096.6878 “xcolors”
wrl.nfs > sushi.201b: reply ok 128 lookup fh 9,74/4134.3150
In the first line, host sushi sends a transaction with id 6709 to wrl (note that the number following the src host is a transaction id, not the source port). The request was 112 bytes, excluding the UDP and IP headers. The operation was a readlink (read symbolic link) on file handle (fh) 21.24/10.731657119. (If one is lucky, as in this case, the file handle can be interpreted as a major and minor device number pair, followed by the inode number and generation number.) Wrl replies ‘ok’ with the contents of the link.

In the third line, sushi asks wrl to lookup the name ‘xcolors’ in directory file 9.74/4096.6878. Note that the data printed depends on the operation type. The format is intended to be self explanatory if read in conjunction with an NFS protocol spec.

If the -v (verbose) flag is given, additional information is printed. For example:
sushi.1372a > wrl.nfs: 148 read fh 21.11/12.195 8192 bytes @ 24576 wrl.nfs > sushi.1372a: reply ok 1472 read REG 100664 ids 417/0 sz 29388

(-v also prints the IP header TTL, ID, and fragmentation fields, which have been omitted from this example.) In the first line, sushi asks wrl to read 8192 bytes from file 21.11/12.195, at byte offset 24576. Wrl replies ‘ok’; the packet shown on the second line is the first fragment of the reply, and hence is only 1472 bytes long (the other bytes will follow in subsequent fragments, but these fragments do not have NFS or even UDP headers and so might not be printed, depending on the filter expression used). Because the -v flag is given, some of the file attributes (which are returned in addition to the file data) are printed: the file type (“REG”, for regular file), the file mode (in octal), the uid and gid, and the file size.

If the -v flag is given more than once, even more details are printed.

**NOTE:** that NFS requests are very large and much of the detail won’t be printed unless snaplen is increased. Try using ‘-s 192’ to watch NFS traffic.

NFS reply packets do not explicitly identify the RPC operation. Instead, tcpdump keeps track of “recent” requests, and matches them to the replies using the transaction ID. If a reply does not closely follow the corresponding request, it might not be parsable.
KIP Appletalk (DDP in UDP)

Appletalk DDP packets encapsulated in UDP datagrams are de-encapsulated and dumped as DDP packets (i.e., all the UDP header information is discarded). The file /etc/atalk.names is used to translate appletalk net and node numbers to names. Lines in this file have the form number name:

1.254 ether
16.1 icsd-net
1.254.110 ace

The first two lines give the names of appletalk networks. The third line gives the name of a particular host (a host is distinguished from a net by the 3rd octet in the number - a net number must have two octets and a host number must have three octets.) The number and name should be separated by whitespace (blanks or tabs). The /etc/atalk.names file may contain blank lines or comment lines (lines starting with a ‘#’).

Appletalk addresses are printed in the form net.host.port

144.1.209.2 > icsd-net.112.220
office.2 > icsd-net.112.220
jssmag.149.235 > icsd-net.2

(If the /etc/atalk.names doesn’t exist or doesn’t contain an entry for some appletalk host/net number, addresses are printed in numeric form.) In the first example, NBP (DDP port 2) on net 144.1 node 209 is sending to whatever is listening on port 220 of net icsd node 112. The second line is the same except the full name of the source node is known (‘office’). The third line is a send from port 235 on net jssmag node 149 to broadcast on the icsd-net NBP port (note that the broadcast address (255) is indicated by a net name with no host number - for this reason it’s a good idea to keep node names and net names distinct in /etc/atalk.names).

NBP (name binding protocol) and ATP (Appletalk transaction protocol) packets have their contents interpreted. Other protocols just dump the protocol name (or number if no name is registered for the protocol) and packet size.
NBP packets are formatted like the following examples:

icsd-net.112.220 > jssmag.2: nbp-lkup 190: “::LaserWriter@*”

The first line is a name lookup request for laserwriters sent by net icsd host 112 and broadcast on net jssmag. The nbp id for the lookup is 190. The second line shows a reply for this request (note that it has the same id) from host jssmag.209 saying that it has a laserwriter resource named “RM1140” registered on port 250. The third line is another reply to the same request saying host techpit has laserwriter “techpit” registered on port 186.

ATP packet formatting is demonstrated by the following example:

jssmag.209.165 > helios.132: atp-req 12266<0-7> 0xae030001
helios.132 > jssmag.209.165: atp-resp 12266:0 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:1 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:2 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:3 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:4 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:5 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:6 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp* 12266:7 (512) 0xae040000
jssmag.209.165 > helios.132: atp-req 12266<3,5> 0xae030001
helios.132 > jssmag.209.165: atp-resp 12266:3 (512) 0xae040000
helios.132 > jssmag.209.165: atp-resp 12266:5 (512) 0xae040000
jssmag.209.165 > helios.132: atp-rel 12266<0-7> 0xae030001
jssmag.209.133 > helios.132: atp-req* 12267<0-7> 0xae030002

Jssmag.209 initiates transaction id 12266 with host helios by requesting up to 8 packets (the ‘<0-7>‘). The hex number at the end of the line is the value of the ‘userdata’ field in the request.
Helios responds with 8 512-byte packets. The ‘:digit’ following the transaction id gives the packet sequence number in the transaction and the number in parentheses is the amount of data in the packet, excluding the atp header. The ‘*’ on packet 7 indicates that the EOM bit was set.

Jssmag.209 then requests that packets 3 & 5 be retransmitted. Helios resends them then jssmag.209 releases the transaction. Finally, jssmag.209 initiates the next request. The ‘*’ on the request indicates that XO (‘exactly once’) was not set.

**IP Fragmentation**

Fragmented Internet datagrams are printed as

(frag id:size@offset+)
(frag id:size@offset)

(The first form indicates there are more fragments. The second indicates this is the last fragment.)

Id is the fragment id. Size is the fragment size (in bytes) excluding the IP header. Offset is this fragment’s offset (in bytes) in the original datagram.

The fragment information is output for each fragment. The first fragment contains the higher level protocol header and the frag info is printed after the protocol info. Fragments after the first contain no higher level protocol header and the frag info is printed after the source and destination addresses. For example, here is part of an ftp from arizona.edu to lbl-rtsg.arpa over a CSNET connection that doesn’t appear to handle 576 byte datagrams:

arizona.ftp-data > rtsg.1170: . 1024:1332(308) ack 1 win 4096 (frag 595a:328@0+)
arizona > rtsg: (frag 595a:204@328)
rtsg.1170 > arizona.ftp-data: . ack 1536 win 2560

There are a couple of things to note here: First, addresses in the 2nd line don’t include port numbers. This is because the TCP protocol information is all in the first fragment and we have no idea what the port or sequence numbers are when we print the later
fragments. Second, the tcp sequence information in the first line is printed as if there were 308 bytes of user data when, in fact, there are 512 bytes (308 in the first frag and 204 in the second). If you are looking for holes in the sequence space or trying to match up acks with packets, this can fool you.

A packet with the IP don’t fragment flag is marked with a trailing (DF).

**Timestamps**

By default, all output lines are preceded by a timestamp. The timestamp is the current clock time in the form hh:mm:ss.frac and is as accurate as the kernel’s clock. The timestamp reflects the time the kernel first saw the packet. No attempt is made to account for the time lag between when the ethernet interface removed the packet from the wire and when the kernel serviced the ‘new packet’ interrupt.

**See Also**

traffic(1C), nit(4P), bpf(4), pcap(3)

**Authors**

Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA.

The current version is available via anonymous ftp:


**Bugs**

Please send bug reports to tcpdump@ee.lbl.gov.
NIT doesn’t let you watch your own outbound traffic, BPF will. We recommend that you use the latter.

Some attempt should be made to reassemble IP fragments or, at least to compute the right length for the higher level protocol.

Name server inverse queries are not dumped correctly: The (empty) question section is printed rather than real query in the answer section. Some believe that inverse queries are themselves a bug and prefer to fix the program generating them rather than tcpdump.

Apple Ethertalk DDP packets could be dumped as easily as KIP DDP packets but aren’t. Even if we were inclined to do anything to promote the use of Ethertalk (we aren’t), LBL doesn’t allow Ethertalk on any of its networks so we’d would have no way of testing this code.

A packet trace that crosses a daylight savings time change will give skewed time stamps (the time change is ignored).

Filters expressions that manipulate FDDI headers assume that all FDDI packets are encapsulated Ethernet packets. This is true for IP, ARP, and DECNET Phase IV, but is not true for protocols such as ISO CLNS. Therefore, the filter may inadvertently accept certain packets that do not properly match the filter expression.
traceroute

Name

traceroute - print the route packets take to network host

Synopsis

traceroute [ -dnrv ] [ -g gw_host ] [ -m max_ttl ] [ -p port ] [ -q nqueries ] [ -s src_addr ] [ -t tos ] [ -w waittime ] host [ packetlen ]

Description

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one’s packets follow (or finding the miscreant gateway that’s discarding your packets) can be difficult. Traceroute utilizes the IP protocol ‘time to live’ field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

The only mandatory parameter is the destination host name or IP number. The default probe datagram length is 40 bytes, but this may be increased by specifying a packet length (in bytes) after the destination host name.

Other options are:

- `g` Specify a loose source route gateway (8 maximum).
- `m` Set the max time-to-live (max number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).
-n
Print hop addresses numerically rather than symbolically and
numerically (saves a nameserver address-to-name lookup for each
gateway found on the path).

-p
Set the base UDP port number used in probes (default is 33434).
Traceroute hopes that nothing is listening on UDP ports base to base
+ nhops - 1 at the destination host (so an ICMP
PORT_UNREACHABLE message will be returned to terminate the
route tracing). If something is listening on a port in the default
range, this option can be used to pick an unused port range.

-r
Bypass the normal routing tables and send directly to a host on an
attached network. If the host is not on a directly-attached network,
an error is returned. This option can be used to ping a local host
through an interface that has no route through it (e.g., after the
interface was dropped by routed(8C)).

-s
Use the following IP address (which must be given as an IP number,
not a hostname) as the source address in outgoing probe packets. On
hosts with more than one IP address, this option can be used to force
the source address to be something other than the IP address of the
interface the probe packet is sent on. If the IP address is not one of
this machine’s interface addresses, an error is returned and nothing
is sent.

-t
Set the type-of-service in probe packets to the following value
(default zero). The value must be a decimal integer in the range 0 to
255. This option can be used to see if different types-of-service
result in different paths. (If you are not running 4.4bsd, this may be
academic since the normal network services like telnet and ftp don’t
let you control the TOS). Not all values of TOS are legal or
meaningful - see the IP spec for definitions. Useful values are
probably ‘-t 16’ (low delay) and ‘-t 8’ (high throughput).

-v
Verbose output. Received ICMP packets other than
TIME_EXCEEDED and UNREACHABLEs are listed.
This program attempts to trace the route an IP packet would follow to some internet host by launching UDP probe packets with a small ttl (time to live) then listening for an ICMP “time exceeded” reply from a gateway. We start our probes with a ttl of one and increase by one until we get an ICMP “port unreachable” (which means we got to “host”) or hit a max (which defaults to 30 hops & can be changed with the -m flag). Three probes (change with -q flag) are sent at each ttl setting and a line is printed showing the ttl, address of the gateway and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system will be printed. If there is no response within a 5 sec. timeout interval (changed with the -w flag), a “*” is printed for that probe.

We don’t want the destination host to process the UDP probe packets so the destination port is set to an unlikely value (if some clod on the destination system is using that value, it can be changed with the -p flag).

A sample use and output might be:

[yak 71]% traceroute nis.nsf.net.
traceroute to nis.nsf.net (35.1.1.48), 30 hops max, 38 byte packet
  1 helios.ee.lbl.gov (128.3.112.1) 19 ms 19 ms 0 ms
  2 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 39 ms 19 ms
  3 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 39 ms 19 ms
  4 ccngw-ner-cc.Berkeley.EDU (128.32.136.23) 39 ms 40 ms 39 ms
  5 ccn-nerif22.Berkeley.EDU (128.32.168.22) 39 ms 39 ms 39 ms
  6 128.32.197.4 (128.32.197.4) 40 ms 59 ms 59 ms
  7 131.119.2.5 (131.119.2.5) 59 ms 59 ms 59 ms
  8 129.140.70.13 (129.140.70.13) 99 ms 99 ms 80 ms
  9 129.140.71.6 (129.140.71.6) 139 ms 239 ms 319 ms
 10 129.140.81.7 (129.140.81.7) 220 ms 199 ms 199 ms
 11 nic.merit.edu (35.1.1.48) 239 ms 239 ms 239 ms

-w Set the time (in seconds) to wait for a response to a probe (default 5 sec.).
Note that lines 2 & 3 are the same. This is due to a buggy kernel on the 2nd hop system - lbl-csam.arpa - that forwards packets with a zero ttl (a bug in the distributed version of 4.3BSD). Note that you have to guess what path the packets are taking cross-country since the NSFNet (129.140) does not supply address-to-name translations for its NSSes.

A more interesting example is:

[yak 72]% traceroute allspice.lcs.mit.edu.
traceroute to allspice.lcs.mit.edu (18.26.0.115), 30 hops max
  1 helios.ee.lbl.gov (128.3.112.1) 0 ms 0 ms 0 ms
  2 lilac-dmc.Berkeley.EDU (128.32.216.1) 19 ms 19 ms 19 ms
  3 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 19 ms 19 ms
  4 ccngw-ner-ce.Berkeley.EDU (128.32.136.23) 19 ms 39 ms 39 ms
  5 ccn-nerif22.Berkeley.EDU (128.32.168.22) 20 ms 39 ms 39 ms
  6 128.32.197.4 (128.32.197.4) 59 ms 119 ms 39 ms
  7 131.119.2.5 (131.119.2.5) 59 ms 59 ms 39 ms
  8 129.140.70.13 (129.140.70.13) 80 ms 79 ms 99 ms
  9 129.140.71.6 (129.140.71.6) 139 ms 139 ms 159 ms
 10 129.140.81.7 (129.140.81.7) 199 ms 180 ms 300 ms
 11 129.140.72.17 (129.140.72.17) 300 ms 239 ms 239 ms
 12 ** *
 13 128.121.54.72 (128.121.54.72) 259 ms 499 ms 279 ms
 14 ** *
 15 ** *
 16 ** *
 17 ** *
 18 ALLSPICE.LCS.MIT.EDU (18.26.0.115) 339 ms 279 ms 279 ms

Note that the gateways 12, 14, 15, 16 & 17 hops away either do not send ICMP “time exceeded” messages or send them with a ttl too small to reach us. The 14 - 17 gateways are running the MIT C Gateway code that does not send time exceeded messages. It is unclear what happens with gateway 12.
The silent gateway 12 in the above example may be the result of a bug in the 4.[23]BSD network code (and its derivatives): 4.x (x<= 3) sends an unreachable message using whatever ttl remains in the original datagram. Since, for gateways, the remaining ttl is zero, the ICMP “time exceeded” is guaranteed to not make it back to us. The behavior of this bug is slightly more interesting when it appears on the destination system:

1 helios.ee.lbl.gov (128.3.112.1) 0 ms 0 ms 0 ms
2 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 19 ms 39 ms
3 lilac-dmc.Berkeley.EDU (128.32.216.1) 19 ms 39 ms 19 ms
4 ccngw-ner-cc.Berkeley.EDU (128.32.136.23) 39 ms 40 ms 19 ms
5 ccn-nerif35.Berkeley.EDU (128.32.168.35) 39 ms 39 ms 39 ms
6 csgw.Berkeley.EDU (128.32.133.254) 39 ms 59 ms 39 ms
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 rip.Berkeley.EDU (128.32.131.22) 59 ms ! 39 ms ! 39 ms !

Notice that there are 12 “gateways” (13 is the final destination) and exactly the last half of them are “missing”. What’s really happening is that rip (a Sun-3 running Sun OS3.5) is using the ttl from our arriving datagram as the ttl in its ICMP reply. So, the reply will time out on the return path (with no notice sent to anyone since ICMP’s aren’t sent for ICMP’s) until we probe with a ttl that’s at least twice the path length. I.e., rip is really only 7 hops away. A reply that returns with a ttl of 1 is a clue this problem exists. Traceroute prints a “!” after the time if the ttl is <= 1. Since vendors ship a lot of obsolete (DEC’s Ultrix, Sun 3.x) or non-standard (HPUX) software, expect to see this problem frequently and/or take care picking the target host of your probes.

Other possible annotations after the time are !H, !N, or !P (got a host, network or protocol unreachable, respectively), !S or !F (source route failed or fragmentation needed - neither of these should ever occur and the associated gateway is busted if you see one), !X (communication administratively prohibited), or !<N> (ICMP unreachable-
able code N). If almost all the probes result in some kind of unreachable, traceroute will give up and exit.

This program is intended for use in network testing, measurement and management. It should be used primarily for manual fault isolation. Because of the load it could impose on the network, it is unwise to use traceroute during normal operations or from automated scripts.

See Also

netstat(1), ping(8)

Author

Implemented by Van Jacobson from a suggestion by Steve Deering. Debugged by a cast of thousands with particularly cogent suggestions or fixes from C. Philip Wood, Tim Seaver and Ken Adelman.

The current version is available via anonymous ftp:


Bugs

Please send bug reports to traceroute@ee.lbl.gov.
uptime

Name

uptime - show how long system has been running

Synopsis

uptime

Description

The uptime utility displays the current time, the length of time the system has been up, the number of users, and the load average of the system over the last 1, 5, and 15 minutes.

Files

/kernel system name list

See Also

w(1)

History

The uptime command appeared in 3.0BSD.
vmstat

Name

vmstat - report virtual memory statistics

Synopsis

vmstat [-ims] [-c count] [-M core] [-N system] [-w wait] [if,pass] [disks]

Description

Vmstat reports certain kernel statistics kept about process, virtual memory, disk, trap and CPU activity.

The options are as follows:

- **c**: Repeat the display count times. The first display is for the time since a reboot and each subsequent report is for the time period since the last display. If no repeat count is specified, and -w is specified, the default is infinity, otherwise the default is one.

- **-i**: Report on the number of interrupts taken by each device since system startup.

- **-M**: Extract values associated with the name list from the specified core instead of the default /dev/kmem.

- **-N**: Extract the name list from the specified system instead of the default /kernel.
By default, `vmstat` displays the following information:

**procs** Information about the numbers of processes in various states.

- **r** in run queue
- **b** blocked for resources (i/o, paging, etc.)
- **w** runnable or short sleeper (< 20 secs) but swapped

**memory** Information about the usage of virtual and real memory. Virtual pages (reported in units of 1024 bytes) are considered active if they belong to processes which are running or have run in the last 20 seconds.

- **avm** active virtual pages
- **fre** size of the free list

**page** Information about page faults and paging activity. These are averaged each five seconds, and given in units per second.

- **-m** Report on the usage of kernel dynamic memory listed first by size of allocation and then by type of usage.

- **-s** Display the contents of the sum structure, giving the total number of several kinds of paging related events which have occurred since system startup.

- **-w** Pause wait seconds between each display. If no repeat wait interval is specified, the default is 1 second.
flt  total number of page faults
re  page reclaims (simulating reference bits)
pi  pages paged in
po  pages paged out
fr  pages freed per second
sr  pages scanned by clock algorithm, per-second

Disks
Disk operations per second (this field is system dependent). Typically paging will be split across the available drives. The header of the field is the first two characters of the disk name and the unit number. If more than three disk drives are configured in the system, vmstat displays only the first three drives, unless the user specifies the -n argument to increase the number of drives displayed. This will probably cause the display to exceed 80 columns, however. To force vmstat to display specific drives, their names may be supplied on the command line. vmstat defaults to show disks first, and then various other random devices in the system to add up to three devices, if there are that many devices in the system. If devices are specified on the command line, or if a device type matching pattern is specified (see above), vmstat will only display the given devices or the devices matching the pattern, and will not randomly select other devices in the system.

Faults
Trap/interrupt rate averages per second over last 5 seconds.

in  device interrupts per interval (including clock interrupts)
sy  system calls per interval
cs  cpu context switch rate (switches/interval)

CPU
Breakdown of percentage usage of CPU time.

us  user time for normal and low priority processes
sy  system time
id  cpu idle
Examples

The command: `vmstat -w 5` will print what the system is doing every five seconds; this is a good choice of printing interval since this is how often some of the statistics are sampled in the system. Others vary every second and running the output for a while will make it apparent which are recomputed every second.

The command: `vmstat -p da -p cd -w 1` will tell `vmstat` to select the first three direct access or CDROM devices and display statistics on those devices, as well as other systems statistics every second.

Files

/kernel default kernel namelist /dev/kmem default memory file

See Also

fstat(1), netstat(1), nfsstat(1), ps(1), systat(1), iostat(8), pstat(8)

The sections starting with “Interpreting system activity” in Installing and Operating 4.3BSD.

Bugs

The -c and -w options are only available with the default output.
List of Commands

Introducing the Command-Line Interface

Environment Commands

```plaintext
set clienv ......................................................... 23
  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 .................................................. 23

show clienv .................................................. 25
  debug
  echo-cmd
  output
  on-failure
  output
  rows
  syntax-check
```

Transaction Mode

```plaintext
start transaction ........................................... 26
commit ......................................................... 26
rollback ....................................................... 26
```
General CLI Features

- `set config-lock` .............................................. 36
  - `<on | off>`
  - `on timeout <5-900>`
  - `on override`
- `show fsinfo` .................................................. 36
- `show processes` .............................................. 36
- `show swapinfo` ............................................... 36
- `shell` .......................................................... 38
- `exit` .......................................................... 38

Saving Configuration Changes

- `clish -s -c "cli_command"` .................................. 38
- `clish -s -f filename` ......................................... 38

Interface Commands

General Commands

Viewing All Interfaces

- `show interfaces` ................................................ 39

Deleting Any Logical Interface

- `delete interface log_if_name` ............................... 41
- `delete interface log_if_name address ip_address` ....... 41

Viewing Tunnels

- `show tunnels` .................................................. 41

Viewing Status and Statistics

- `show interface if_name status` .............................. 42
show interface if_name statistics ................................. 42
show interface if_name all ................................. 42

ARP

ARP Commands

set arp......................................................... 42
  keep-time <60–86400>
  retry-limit <1–100>
  accept-multicast-replies <on | off>
show arp......................................................... 42
  keep-time
  retry-limit
  accept-multicast-replies
  all
add......................................................... 43
  arpproxy address ip_address <macaddress mac_address | interface log_if_name>
  arpstatic address ip_address macaddress mac_address
show arpproxy all.................................................... 44
show arpstatic all.................................................... 44
show arpdynamic all.................................................... 44
delete......................................................... 45
  arpproxy address ip_address
  arpstatic address ip_address

ATM Interfaces

Physical ATM Interfaces

set interface phys_if_name ........................................ 45
  active <on | off>
  framing <sonet | sdh>
  transmitclock <freerun | looptiming>
  atm-oam <on | off>
vc-max \texttt{maxVPI/ maxVCI}

\texttt{show interface phys\_if\_name} ........................................ 46
all
framing
transmitclock
atm-oam
vc-max
statistics
lb-status
status

\textbf{Logical ATM Interfaces}

\texttt{add interface phys\_if\_name [unit <1—255>] type} ............... 48
ipoa vcs \texttt{[VPI/]}VCI(s) \texttt{[logical-name log\_if\_name]}
p2p vc \texttt{[VPI/]}VCI \texttt{[logical-name log\_if\_name]}

\texttt{set interface log\_if\_name} ........................................ 49
mtu <768—9180>
address \texttt{ip\_address}[/\texttt{mask} <8—30>]
destination address
unnumbered \texttt{[yes | no]}
proxy-interface \texttt{log\_if\_name}
enable \texttt{| disable}
vcs \texttt{[VPI/]}VCI(s)

\texttt{show interface log\_if\_name} ........................................ 51
all
status
unnumbered
address
destination
mtu
proxy-interface
vcs
type
statistics

\texttt{show interface log\_if\_name atmarp}................................. 54
static
dynamic
delete interface log_if_name atmarp ....................... 54
    static vc VCI
    dynamic vc VCI

set inatmarp..................................................... 54
    keep-time <1–900>
    timeout <1–30>
    max-retries <1–100>
    holdoff-time <1–900>

show inatmarp..................................................... 55

Ethernet Interfaces

Physical Ethernet Interfaces

set interface phys_if_name ..................................... 56
    speed <10M | 100M | 1000M>
    duplex <full | half>
    auto-advertise <on | off>
    link-recog-delay <1–255>
    active <on | off>
    flow-control <on | off>

show interface phys_if_name ..................................... 56
    speed
    duplex
    auto-advertise
    link-recog-delay
    flow-control
    status

Logical Ethernet Interfaces

add interface log_if_name vlanid <2–4094> address ip_address/masklen <0–31>.................................................. 57

add interface log_if_name ......................................... 58
    address ip_address/mask

set interface log_if_name ......................................... 58
    vlanid <2–4094>
    logical-name new_log_if_name
enable | disable
MTU <1500–16,000>

show interface log_if_name vlanid............................... 58

### Transparent Mode

#### Configuring Transparent Mode

**add xmode................................................. 59**

- id <any integer greater than 0>
- interface logical_if_name

**delete xmode............................................. 59**

- id <any integer greater than 0>
- interface logical_if_name

**set xmode id <any integer greater than 0> ..................... 60**

- state <on | off>
- vrrp_enabled <on | off>

**show......................................................... 60**

- xmode id <any integer greater than 0> info
- xmode id <any integer greater than 0> interfaces
- xmode id <any integer greater than 0> stat
- xmode id <any integer greater than 0> state
- xmode id <any integer greater than 0> vrrp_enabled
- xmodes

### Link Aggregation

**add linkaggregation............................................ 62**

- group <1-1024>
  - port phys_if_name [type primary]

**delete linkaggregation........................................ 62**

- group <1-1024>
  - port phys_if_name

**show......................................................... 62**

- linkaggregation
Point-to-Point Over Ethernet

Configuring Profiles

add pppoe profile name profile_name interface phys_if_name mode <connect-on-demand | keep-alive> noauth

timeout <30-259200; 300, 60>

peernat name
description name
mss mss_value
mtu <136-1492>

add pppoe profile name profile_name interface phys_if_name mode mode_name

username name password password

authype PAP | CHAP CASE
timeout <30-259200; 300, 60>

peernat name
description name
mss mss_value
mtu <136-1492>

set pppoe profile name profile_name interface phys_if_name mode mode_name

noauth
timeout time_in_seconds

peernat name
description name
mtu mtu_value

set pppoe profile name profile_name interface phys_if_name mode mode_name

username name password password

authype PAP | CHAP CASE
timeout time_in_seconds

peernat name
description name
mtu mtu_value

delete pppoe profile name profile_name

show pppoe profile

}
all
name profile_name

Configuring PPPoE Logical Interface
add interface pppoe0 mode dynamic profile-name profile_name...
  interface-name log_if_name
  enable off | on
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
add interface pppoe0 mode unnumbered logical-interface log_if_name
  interface-name log_if_name
  enable off | on
set interface log_if_name ..............................
  admin-status enable | disable
  link_trap on | off

Configuring PPPoE Physical Interface
  admin-status enable | disable
  link_trap on | off

FDDI Interfaces

Physical FDDI Interfaces
  set interface phys_if_name ..............................
    active <on | off>
    duplex <half | full>
  show interface phys_if_name ..........................
    all
duplex
status
statistics
Logical FDDI Interfaces

add interface log_if_name address ip_address/mask <8-31> .......... 70

set interface default_log_if_name........................................ 70
  enable | disable
  logical-name log_if_name

show interface default_log_if_name................................. 70
  address
  status
  statistics
  logical-name
  all

ISDN Interfaces

Physical ISDN Interfaces

set interface phys_if_name ............................................ 71
  status <on | off>
  switch-type etsi
  line-topology [point-to-point | multi]
  tei-option [automatic | manual]
  tei-assignment [first-call | power-up]
  tei <0-63>
  local-number number
  local-sub-number number
  logging [warn | info | error]
  disconnect-channel <1 | 2>

show interface phys_if_name ....................................... 72
  all
  status
  switch-type
  line-topology
  tei-option
  tei-assignment
  tei
  local-number
  local-sub-number
logging
disconnect-channel
chan-state
chan-link
chan-call-info
chan-last-call-info

Logical ISDN Interfaces

add interface phys_if_name encapsulation <ppp | multilink-ppp> 74
add interface log_if_name incoming-number number............. 75
delete interface log_if_name incoming-number number........... 75
set interface log_if_name ........................................ 76
  enable | disable
description description
direction <outgoing | incoming | both>
rate <64kbps | 56kbps>
idle-time <0-999999>
minimum-call-time <0-999999>
remote-number number
remote-sub-number number
calling-number number
calling-sub-number number
local-name name
local-password password
remote-auth-method <pap | chap | none>
remote-name name
remote-password password
bandwidth-util-level <0-100>
bandwidth-util-period <0-999>
echo-interval <0-255>
max-echo-failures <0-255>
max-mrru <0-99999>
fragment-size <0-99999>
address ip_address
destination ip_address
unnumbered <yes | no>
proxy-interface if_name
connect-channel
lcp-options <magic-number | no-magic-number | mru | no-mru
|mrru| no-mrru
|short-seq-num | no-short-seq-num | endpoint-disc
|no-endpoint-disc>

show interface log_if_name ........................................... 77
encapsulation
status
description
direction
rate
idle-time
minimum-call-time
remote-number
remote-sub-number
calling-number
calling-sub-number
local-name
local-password
remote-auth-method
remote-name
remote-password
bandwidth-util-level
bandwidth-util-period
echo-interval
max-echo-failures
max-mrru
fragment-size
address
destination
unnumbered
proxy-interface
connect-channel
lcp-options
incoming-number number

Loopback Interfaces
Logical Loopback Interfaces

add interface log_if_name address ip_address ................. 84
delete interface log_if_name address ip_address ................. 84
set interface log_if_name logical-name log_name ............... 84
show interface log_if_name addresses........................... 84

Logical or Physical Loopback Interfaces

show interface if_name ........................................... 85
  status
  disabled,proto
  enabled,proto
  all

Modem Interfaces

set modem <com2 | com3 | com4> ................................. 86
  country-code <<0–99> | <00–FF>>
  enable | disable
  inactivity-timeout <0–5>
  poll-interval <0–59>
  enable-dialback | disable-dialback
  dialback-number phone_num
  type <5oC1 | 5oC2> [country-code <<0–99> | <00–FF>>]

show modem <com2 | com3 | com4> ................................. 86
  active
  inactivity-timeout
  poll-interval
dialback
  dialback-number
  country-code
  status
  all

Serial Interfaces
Physical Serial Interfaces

set interface phys_if_name ................................. 88
    active <on | off>
    encaps <chdlc | ppp | fr>
    keepalive <0-255>
    clocking <external | internal>
    queue-mode <disable | min-latency | max-bw>

show interface phys_if_name ................................. 88
    status
    encaps
    keepalive
    clocking
    speed
    queue-mode

set interface phys_if_name ................................. 90
    channel-mode <full-duplex | loopback>
    speed <1-45000000 | 1-20480000 | 1-10000000>

show interface phys_if_name ................................. 90
    channel-mode
    speed

set interface phys_if_name ................................. 92
    channel-mode <normal | llb | clb | rlb | plb>
    line-type <short-haul | long-haul>
    cable-length <0-655>
    transmit-loss <0 | -7.5 | -15 | -22>
    receiver-gain <-30 | -36>
    invert-data | noinvert-data
    timeslot channel(s)
    encoding <ami | b8zs>
    framing <sf | esf>
    channel-speed <64Kbps | 56Kbps>
    jitter-attenuator <off | rx | tx>
    jabuffer-depth <32 | 128>
    fdl-type <ansi | none>
    density-enforcer <on | off>
    speed
show interface phys_if_name ............................... 92
  channel-mode
  line-type
  cable-length
  transmit-loss
  receiver-gain
  invert-data
  timeslot
  encoding
  framing
  channel-speed
  jitter-attenuator
  jabuffer-depth
  fd1-type
  density-enforcer
  speed

set interface phys_if_name ............................... 99
  channel-mode <normal | llb | clb | rlb | plb>
  encoding <ami | hdb3>
  framing <e1 | e1-noframe>
  crc4-framing | no-crc4-framing
  timeslot-16-framing | no-timeslot-16-framing
  timeslot channel(s)
  line-type <short-haul | long-haul>
  invert-data | noinvert-data

show interface phys_if_name ............................... 100
  channel-mode
  encoding
  framing
  crc4-framing
  timeslot-16-framing
  timeslot
  line-type
  invert-data

set interface phys_if_name ............................... 105
  dte | dce
  active-status-monitor <on | off>
lmi-type <ansi | ccitt | fr-consortium>
n391 <1-255>
n392 <1-10>
n393 <1-10>
dlci-length <10 | 11 | 13>

add interface phys_if_name ................................. 105
dlci <16-1007>

show interface phys_if_name ................................. 105
dte | dce
active-status-monitor
lmi-type
n391
n392
n393
dlci-length

set interface phys_if_name ................................. 108
keepalive-failures <1-255>
magic-number | no-magic-number
mru | no-mru

show interface phys_if_name ................................. 108
keepalive-failures
magic-number
mru

Logical Serial Interfaces

set slot <1-15> interface log_if_name ........................ 109
logical-name log_if_name
address ip_address
destination ip_address
unnumbered <yes | no>
proxy-interface log_if_name
enable | disable
mtu <128-65535>

show slot <1-15> interface log_if_name ........................ 109
all
logical-name
address
VPP Interfaces

Create Appropriate Static Routes

VPP Interface Commands

set interface log_if_name ................................. 112
   enable | disable
   address ip_address
   destination ip_address
   unnumbered <yes | no>
   proxy-interface log_if_name
   logical-name log_if_name

show interface log_if_name ............................... 113
   all
   status
   address
   destination
   unnumbered
   proxy-interface
   logical-name

Network Security and Access Commands

Network Access and Services

set net-access........................................... 115
   ftp <yes | no>
      port <1-65535>
tftp <yes | no>
telnet <yes | no>
admin-net-login <yes | no>
cli-http <yes | no>
cli-https <yes | no>
com2-login <yes | no>
com3-login <yes | no>
com4-login <yes | no>
set modem com4 <country code>

show................................................................. 116
net-access
net-access ftp
net-access tftp
net-access telnet
net-access admin-net-login
net-access cli-http
net-access cli-https
net-access com2-login
net-access com3-login
net-access com4-login

set services.......................................................... 116
echo <yes | no>
discard <yes | no>
chargen <yes | no>
daytime <yes | no>
time <yes | no>

show................................................................. 116
services
services echo
services discard
services chargen
services daytime
services time

Licenses
Configuring Software Licenses

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

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

show licensing
  licensing
  licensing bgp-key
  licensing dvmrp-rip-key
  licensing dvmrp-ospf-key
  licensing igrp-key
  licensing dvmrp-key

IPsec Commands

General IPsec Commands

set ipsec clear
show ipsec all

Proposal Commands

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

set ipsec proposal name
  auth <sha1 | md5>
  crypto <des | 3des | blowfish | null>
show ipsec proposal .................. 123
  all
  name
delete ipsec proposal .................. 124
  all
  name

Filter Commands
add ipsec filter name .................. 124
  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 .................. 125
  address ip_address mask <0-128>
  address6 ip6_address mask6 <0-128>
  proto tcp | udp | icmp | any
  port <0-65535>
show ipsec filter .................. 125
  all
  name
delete ipsec filter .................. 126
  all
  name

Certificate Commands
add ipsec x509cert name type <dev | ca> source ............ 127
  pem_file name
  url url url
     realm name [user username password password]
set ipsec x509cert name source .................. 127
  pem file name
  url url url
     realm name [user username password password]
show ipsec x509cert................................. 128
  all
    options <attrs | content | decoded>
  name
    options <attrs | content | decoded>
delete ipsec x509cert................................. 129
  all
  name
add ipsec x509certreq name key-len <512 | 768 | 1024> sig-algo <dsa | rsa> pass-phrase phrase country country state state locality org org-unit name dns-name name................. 130
  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 org-unit name dns-name name................. 130
  ip-address ip_address email email_address
  ip-address6 ip6_address email email_address
show ipsec x509certreq................................. 131
  all
    options <attrs | content | decoded>
  name
    options <attrs | content | decoded>
delete ipsec x509certreq................................. 132
  all
  name

Policy Commands
add ipsec policy name proposal name priority integer ........ 133
  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 ................................. 133
   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>

show ipsec policy ................................. 135
   all
   name

delete ipsec policy .............................. 135
   all
   name
   proposal name

Rule Commands

add ipsec rule name mode tunnel ................. 136
   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 ................................. 137
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>

add ipsec rule name mode transport ................. 137
policy name
src-filter name
dst-filter name

set ipsec rule name................................. 137
policy name
src-filter name
dst-filter name

show ipsec rule................................. 139
all [mode <tunnel | transport>]
name

delete ipsec rule................................. 140
all [mode <tunnel | transport>]
name
policy name
src-filter name
dst-filter name

Miscellaneous IPsec Commands
set ipsec...................................... 141
log-level <error | debug | info>
hardware-accl <on | off>
allow-interfaceless-tunnels <on | off>

add ipsec ldap url.............................. 141

delete ldap url .................................. 141
show ipsec................................. 142
  log-level
  ldap
  hardware-accl
  allow-interfaceless-tunnels

AAA

Viewing AAA Configuration

show aaa all............................. 142

Configuring Service Modules

add aaa service name profile name............... 142
delete aaa service name.......................... 142
set aaa service name profile name............... 142
show aaa.................................... 143
  services
  service name

Configuring Service Profiles

add aaa profile name.......................... 143
  authprofile name acctprofile name sessprofile name
  authprofile name
  acctprofile name
  sessprofile name

delete aaa.................................. 144
  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

set aaa profile name......................... 144
  authprofile name auth-priority integer
  acctprofile name acct-priority integer
```
sessprofile name sess-priority integer

show aaa.......................................................... 144
  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

Configuring Authentication Profiles

add aaa authprofile name [authtype name authcontrol name]...... 146
delete aaa authprofile name ...................................... 146
set aaa authprofile name ........................................... 146
  authtype name
  authcontrol name

show aaa.......................................................... 147
  authprofiles
  authprofile name
  authtype name
  authcontrol name

Configuring Account Profiles

add aaa acctprofile name accttype name acctcontrol name...... 148
delete aaa acctprofile name ...................................... 149
set aaa acctprofile name .......................................... 149
  authtype name
  authcontrol name

show aaa.......................................................... 149
  acctprofiles
  acctprofile name
  accttype name
```
acctprofile name acctcontrol

Configuring Session Profiles

add aaa sessprofile name sesstype name sesscontrol name .......... 151
delete aaa sessprofile name ........................................ 151
set aaa sessprofile name .......................................... 152
   sesstype name
   sesscontrol name
show aaa.............................................................. 152
   sessprofiles
   sessprofile name
   sessprofile name sesstype
   sessprofile name sesscontrol

Configuring RADIUS

add aaa radius-servers authprofile name priority integer host IPv4 address
   port integer <secret name | prompt-secret> timeout integer maxtries integer 153
delete aaa radius-servers authprofile name priority integer 153
set aaa radius-servers authprofile name priority integer...
   host IPv4 address
   port integer
   secret name
   prompt-secret
   timeout integer
   maxtries integer
   new-priority integer
show aaa radius-servers authprofile name list................. 154
show aaa radius-servers authprofile name priority integer..
   host
   port
   timeout
   maxtries
   new-priority

Configuring TACPLUS

add aaa tacplus-servers authprofile name priority integer host IPv4 address
port integer <secret name | prompt-secret> timeout integer maxtries integer

delete aaa tacplus-servers authprofile name
priority integer

set aaa tacplus-servers authprofile name priority integer
host IPv4 address
port integer
secret name
prompt-secret
timeout integer
new-priority integer

show aaa radius-servers authprofile name list

show aaa tacplus-servers authprofile name priority integer
host
port
timeout

**SSH**

**Enabling/Disabling SSH Service**

set ssh server
enable <0 | 1>

show ssh server
enable

**Configuring Server Options**

set ssh server
allow-groups name
allow-users name
deny-groups name
deny-users name
permit-root-login <yes | no | without-password>

show ssh server
allow-groups
allow-users
deny-groups
deny-users
permit-root-login

set ssh server........................................ 161
  pubkey-authentication <0 | 1>
  password-authentication <0 | 1>
  rhosts-authentication <0 | 1>
  rhosts-rsa-authentication <0 | 1>
  rsa-authentication <0 | 1>

show ssh server....................................... 161
  pubkey-authentication
  password-authentication
  rhosts-authentication
  rhosts-rsa-authentication
  rsa-authentication

set ssh server........................................ 162
  print-motd <0 | 1>
  use-login <0 | 1>

show ssh server....................................... 162
  print-motd
  use-login

set ssh server........................................ 163
  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>

show ssh server....................................... 163
  ciphers
  keepalives
  listen-addr
  listen-addr2
  port
  protocol
  server-key-bits


set ssh server.................................................. 164
  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
show ssh server................................................ 165
  gateway-ports
  ignore-rhosts
  ignore-user-known-hosts
  key-regeneration-time
  login-grace-time
  max-starups
set ssh server.................................................. 166
  log-level name
  strict-modes <0 | 1>
show ssh server................................................ 166
  log-level
  strict-modes

Configuring and Managing SSH Key Pairs
set ssh hostkey.................................................. 167
  v1 size integer
  v2 dsa size integer
show ssh hostkey................................................ 167
  v1
  v2 dsa
  v2 dsa ssh2-format
set ssh identity.................................................. 168
  v1 user name size integer <passphrase
  name | prompt-passphrase>
  v2 user name size integer <passphrase
  name | prompt-passphrase>
show ssh identity................................................ 168
  v1 user name
v2 dsa user name
v2 dsa user name ssh2-format

add ssh authkeys .................................................. 170
v1 user name bits integer exponent integer modulus name
comment name
v2 dsa user name <openssh-format name | ssh2-format file
name> comment name

delete ssh authkeys ............................................... 170
v1 user name id id number
v2 dsa user name id id number

show ssh authkeys .................................................. 170
v1 user name list
v1 user name id id number
v2 dsa user name list
v2 dsa user name id id number

Voyager Web Access (SSL)

Enabling SSL Voyager Web Access

set voyager.......................................................... 172
daemon-enable <0 | 1>
port <1-65535>
ssl-port <1-65535>
ssl-level <0-168>

show voyager........................................................ 172
port
ssl-port
ssl-level
daemon-enable

Generating a Certificate and Private Key

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 .......... 174
Installing a Certificate and Private Key

set voyager ssl-certificate ................. 177
   cert-file path key-file path <passphrase
   name | prompt-passphrase>

User Management

Adding New Users

set user........................................... 178
   name passwd
   name oldpass passwd newpass passwd
   name info string
   name uid <0-65535>
   name gid <0-65535>
The default gid value is 10.
   name homedir Unix path name
   name shell string
   name homepage Tcl script name

add user........................................... 178
   name uid <0-65535> homedir Unix path name

Deleting a User

delete user........................................ 180
   username

Changing the Admin and Monitor Password

set user <admin | monitor> oldpass passwd newpass passwd... 180

Configuring S/Key for Admin and Monitor

set skey........................................... 181
   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
Show Commands

show users ................................................................. 182
show user name .......................................................... 182
show skey ................................................................. 182
  all
  user <admin | monitor>
  user <admin | monitor> sequence
  user <admin | monitor> seed
  user <admin | monitor> mode

Group Management

Managing Groups

set group string gid <100-65530> ............................... 184
add group string gid <100-65530> ............................... 184
delete group string .................................................. 184
add group string member username ......................... 184
delete group string member username ...................... 184

Show Commands

show groups ............................................................. 185
show group string ..................................................... 185

VPN Acceleration

Configuring VPN Acceleration

set cryptaccel <disable | enable> ............................... 185

Displaying VPN Accelerator Information

show cryptaccel <status | statistics> ....................... 185
Routing Commands

BGP

set router-id ......................................................... 187
  default
  ip_address

set as ................................................................. 188
  as_number
  off

External BGP

set bgp external remote-as as_number ....................... 189
  <on | off>
  description text
  local-address ip_address <on | off>
  virtual-address <on | off>
  outdelay <0-65535>
  outdelay off
  peer ip_address <on | off>
  peer ip_address med-out <0-4294967294>
  peer ip_address med-out default
  peer ip_address accept-med <on | off>
  peer ip_address multihop <on | off>
  peer ip_address no-aggregator-id <on | off>
  aspath-prepend-count <1-25>
  aspath-prepend-count default
  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-keepalives <on | off>
  peer ip_address accept-routers all
  peer ip_address accept-routes none
  peer ip_address passive-tcp <on | off>
  peer ip_address authype none
peer ip_address authtype md5 secret secret
peer ip_address throttle-count <0–65535>
peer ip_address throttle-count off
peer ip_address ttl default
peer ip_address ttl <1–255>
peer ip_address suppress-default-originate <on | off>
peer ip_address log-state-transitions <on | off>
peer ip_address log-warnings <on | off>
peer ip_address trace bgp_traceoption <on | off>

**BGP Confederations**

set bgp................................................................. 196
  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

**BGP Route Reflection**

set bgp................................................................. 197
  cluster-id ip_address
  cluster-id off
  default-med <0–65535>
  default-med off
  default-route-gateway ip_address
  default-route-gateway off

**BGP Route Dampening**

set bgp dampening.................................................. 199
  <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

Internal BGP

set bgp internal ........................................ 201
    <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 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>

BGP Communities
set bgp communities ......................................................... 207
<on | off>

BGP Show Commands
show bgp ................................................................. 207
show bgp ................................................................. 208
groups
memory
errors
paths
stats
peers
peers detailed
peer ip_address detailed
peers established
peer ip_address advertise
peer ip_address received
summary

OSPF
set router-id ......................................................... 209
default
ip_address

OSPF Areas
set ospf area ......................................................... 209
backbone <on | off>
ospf_area <on | off>
ospf_area stub <on | off>
ospf_area stub default-cost <1-677215>
ospf_area stub summary <on | off>
set ipv6 ospf3 area .................................................. 210
**OSPF Interfaces**

```plaintext
set ospf ........................................... 211
    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 <1-4294967295>
    interface if_name dead-interval default
    interface if_name retransmit-interval <1-4294967295>
    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 <on | off>
    interface if_name simple password
    interface if_name md5 key authorization key id secret md5 secret
    interface if_name md5 key authorization key

set ipv6 ospf3 ....................................... 211
```

**OSPF Virtual Links**

```plaintext
set ospf area backbone virtual-link ....................... 217
    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

set ipv6 ospf3 area backbone virtual-link ............... 217

**OSPF Global Settings**

set ospf.......................................................... 219
  rfc1583-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>

set ipv6 ospf3.................................................. 220
  spf-delay <1-60>
  spf-delay default
  spf-holdtime <1-60>
  spf-holdtime default
  default-ase-cost <1-677215>
  default-ase-type <1 | 2>

**OSPF Show Commands**

show ospf.......................................................... 223
  neighbors
  neighbor ip_address
  interfaces
  interfaces stats
  interfaces detailed
  interface ifname
  interface ifname stats
  interface ifname detailed
  packets
  errors
  errors dd
  errors hello
  errors ip
  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 <1-5>
summary

show ipv6 ospf3
neighbors
neighbor ip_address
interfaces
interfaces stats
interfaces detailed
interface ifname
interface ifname stats
interface ifname detailed
packets
errors
errors dd
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

RIP

RIP Interfaces

set rip interface if_name ................................................ 230
  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

set rip ................................................................. 230
  auto-summary <on | off>
  update-interval <1-65535>
  update-interval default
  expire-interval <1-65535>
expire-interval default

RIP Show Commands
show rip......................................................... 233
   interfaces
   interface <if_name>
   packets
   errors
   neighbors
   summary

IGRP
General IGRP Properties
set igrp......................................................... 234
   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
   update-interval <1-65535>
   update-interval default
   invalid-interval <1-65535>
   invalid-interval default
hold-interval <1-65535>
hold-interval default
flush-interval <1-65535>
flush-interval default
validate fields <on | off>

IGRP Interfaces

set igrp interface if_name ................................. 235
  <on | off>
  delay <1-16777215>
  bandwidth <1-6777215>
  accept-updates <on | off>

IGRP Show Commands

show igrp....................................................... 238
  errors
  interfaces
  interface if_address
  neighbors
  packets
  policy
  route-stats

IGMP

IGMP Interfaces

set igmp interface if_name ................................. 239
  version <1 | 2>
  loss-robustness <1-255>
  loss-robustness default
  query-interval <1-3600>
  query-interval default
  query-response-interval <1-25>
  query-response-interval default
  last-member-query-interval <1-25>
  last-member-query-interval default
  router-alert <on | off>
IGMP with IP Clustering

set igmp network ip_address/mask length ............................. 240
  version <1 | 2>
  loss-robustness <1-255>
  loss-robustness default
  query-interval <1-3600>
  query-interval default
  query-response-interval <1-25>
  query-response-interval default
  last-member-query-interval <1-25>
  last-member=query-interval default
  router-alert <on | off>

IGMP Show Commands

show igmp ................................................................. 242
  stats
  stats receive
  stats transmit
  stats error
  interfaces
  interfaces if_address
  groups
  group if_address
  if-stats
  if-stat if_address
  summary

show igmp ................................................................. 242
  networks
  network ip_address/mask length
  show igmp net-stats
  show igmp net-stat ip_address/masklength
  stats
  show igmp stats receive
  show igmp stats transmit
  stats summary
  summary
PIM

set pim mode ........................................................................ 242
<dense | sparse>

PIM Interfaces

set pim interface if_name ...................................................... 243
<on | off>
    virtual-address <on | off>
    local-address ip_address
    dr-priority <0-4294967295>
    dr-priority default

PIM With IP Clustering

set pim network ip_address/mask length............................... 243
<on | off>
    dr-priority <0-4294967295>
    dr-priority default

Sparse Mode PIM

set pim ................................................................................. 244
    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>

Timer and Assert Rank Parameters for Dense Mode and Sparse Mode

```plaintext
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
```

Show PIM Commands

```plaintext
show pim
interfaces
interfaces if_address
neighbors
neighbor ip_address
memory
timers
stats
summary
show pim bootstrap
```

245
253
254
candidate-rp
joins
rps
sparse-mode-stats
group-rp-mapping <mcast_address>

show pim..................................................... 254
    networks
    network ip_address

Route Aggregation

set aggregate............................................. 255
    ip_prefix contributing protocol protocol contributing-route
        <all | ip_prefix> <on | off>
    ip_prefix contributing protocol protocol contributing-route
        <ip_prefix> exact on
    ip_prefix contributing protocol protocol contributing-route
        ip_prefix refines on
    ip_prefix refines on
    ip_prefix refines on
    ip_prefix off
    ip_prefix contributing protocol <protocol> off
    ip_prefix rank default
    ip_prefix rank <0-255>
    ip_prefix weight default
    ip_prefix aspath-truncate <on | off>

BOOPT

BOOPT Interfaces

set bootp interface if_name............................... 257
    primary ip_address wait-time <0-65535> on
    relay-to ip_address <on | off>
    off

BOOPT Show commands

show bootp............................................... 258
    interfaces
    interface if_name
**stats**
**stats receive**
**stats request**
**stats reply**

**DVMRP**

**DVMRP Interfaces**

```plaintext
set dvmrp interface if_name ................................. 259
  <on | off>
  threshold <1-255>
  threshold default
  metric <1-32>
  metric default
```

**DVMRP Timers**

```plaintext
set dvmrp ...................................................... 260
  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
```

**DVMRP Show Commands**

```plaintext
show dvmrp ...................................................... 262
  interfaces
  interfaces if_name
  neighbors
  neighbor ip_address
  stats
  mfc
  reports
```
route
neighbor-routes
summary

Static Routes

Configuring Static Routes

set slot <1-15> static-route ......................... 262
    ip_prefix nexthop gateway address gateway_address priority <1-8> on
    ip_prefix nexthop gateway logical gateway_address priority <1-8> on
    ip_prefix nexthop gateway address gateway_address off
    ip_prefix nexthop gateway logical gateway_address off
    ip_prefix nexthop reject
    ip_prefix off
    ip_prefix rank default
    ip_prefix rank <0-255>

set static-route default ......................... 265
    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>

VRRP

All Implementations

set vrrp.............................................. 266
    monitor-firewall <on | off>
    accept-connections <on | off>
Simplified Method Monitored-Circuit VRRP

add mcvr vrid <1-255> priority <1-254> priority-delta <1-254> 267
   authtype <none|simple> [password passwd]
   hello-interval <1-255>
add mcvr vrid <1-255> backup-address ip_address ............... 267
   vmac-mode <default-vmac|extended-vmac|interface-vmac|static-vmac|static_VMAC>
set mcvr vrid <1-255> ............................................. 267
   authtype <none|simple> [password passwd]
   hello-interval <1-255>
   priority <1-254>
   priority-delta <1-254>
show mcvr vrid <1-255> ............................................. 268
   all
   authtype
   backup-addresses
   hello-interval
   password
   priority
   priority-delta
show mcvr vrids....................................................... 268
delete mcvr......................................................... 268
   old-mc-config
   vrid <1-255>
     backup-address ip_address

Full Method Monitored-Circuit VRRP

set vrrp interface if_name monitored-circuit vrid <1-255> ... 270
   monitored-interface if_name <on | off>
   auto-deactivation <on | off>
   priority <1-254>
   hello-interval <1-255|default>
   vmac-mode <default-vmac|extended-vmac|interface-vmac|static-vmac mac_address>
   backup-address ip_address <on | off>
preempt-mode <on | off>

show vrrp............................... 272
  interfaces
  interface if_name
  stats
  summary

VRRPv2

set vrrp interface if_name ....................... 272
  off
    authtype <none|simple password>
  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 vrid <1-255> .... 272
  <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> 272
  <on | off>
    backup-address ip_address <on | off>
    hello-interval <1-255|default>
    preempt-mode <on | off>
    priority <1-254>
    vmac-mode <default-vmac|extended-vmac|interface-vmac|static-vmac mac_address>

ICMP Router Discovery

ICMP Router Discovery Interfaces

set rdisc interface if_name.................. 275
  <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

ICMP Router Discovery Show Commands
show rdisc
  interfaces
  interface if_name
  stats
  summary

IP Broadcast Helper
IP Broadcast Helper Forwarding
set iphelper
  forward-nonlocal <on | off>

IP Broadcast Helper Interfaces
set iphelper interface if_name
  off
  udp-port <1-65535> off
  udp-port <1-65535> relay-to ip_address <on | off>

IP Broadcast Helper Show Commands
show iphelper
  services
  stats

Network Time Protocol
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

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

delete ntp
server ip_address
peer ip_address

NTP Show Commands

show ntp
active
ntp master
ntp peer ip_address
ntp peers
ntp server ip_address
ntp servers

Dial on Demand Routing

Dial on Demand Routing Commands

add ddrlist name
show ddrlist
delete ddrlist name
add ddrlist name interface log_if_name
delete ddrlist name interface log_if_name
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

set ddrlist name rule rule_num................................. 282
  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............................... 282

Routing Option Commands

Equal-cost Path Splitting (Load Sharing)
set max-path-splits <1–8>............................... 284
set nexthop-selection................................. 284
  src-dest-hash
  dest-hash
  src-hash
  rr

Protocol Rank

set protocol-rank protocol................................. 285
  bgp rank <0–255>
  bgp rank default
  igrp rank <0–255>
  igrp rank default
  rip rank <0–255>
  rip rank default

set protocol-rank protocol................................. 286
  ospf rank <0–255>
  ospf rank default
  ospfase rank <0–255>
ospfase rank default

Trace Routing Commands

Configuring the Trace Log File

set tracefile....................................................... 286
  size <1-4095>
  size default
  maxnum <1-4294967295>
  maxnum default

Trace Option Variables

set trace bgp.................................................. 288
  keepalive <on | off>
  open <on | off>
  update <on | off>
  packets <on | off>
  traceoptions <on | off>

set trace dvmrp............................................... 289
  graft <on | off>
  mfc <on | off>
  mapper <on | off>
  neighbor <on | off>
  probe <on | off>
  prune <on | off>
  report <on | off>
  packets <on | off>
  traceoptions <on | off>

set trace icmp............................................... 289
  error <on | off>
  info <on | off>
  routerdiscovery <on | off>
  packets <on | off>
  traceoptions <on | off>

set trace igrp............................................... 290
  packets <on | off>
  traceoptions <on | off>
set trace igmp................................................. 291
  group <on | off>
  leave <on | off>
  mtrace <on | off>
  query <on | off>
  report <on | off>
  request <on | off>
  packets <on | off>
  traceoptions <on | off>

set trace iphelper........................................ 291
  packets <on | off>
  traceoptions <on | off>

set trace mfc............................................. 292
  alerts <on | off>
  cache <on | off>
  interface <on | off>
  mcastdist <on | off>
  packets <on | off>
  resolve <on | off>
  wrongif <on | off>
  traceoptions <on | off>

set trace pim............................................. 293
  assert <on | off>
  bootstrap <on | off>
  crp <on | off>
  graft <on | off>
  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>

set trace rip............................................. 294
  packets <on | off>
traceoptions <on | off>

set trace vrrp .................................................... 294
   advertise <on | off>
   traceoptions <on | off>

set trace router-discovery option <on | off>.............. 295
   traceoptions

set trace global ............................................... 295
   adv <on | off>
   parse <on | off>
   traceoptions <on | off>

set trace kernel .............................................. 295
   iflist <on | off>
   interface <on | off>
   packets <on | off>
   remnants <on | off>
   request <on | off>
   routes <on | off>
   traceoptions <on | off>

set trace ospf ................................................. 296
   ack <on | off>
   dd <on | off>
   dr <on | off>
   hello <on | off>
   lsa <on | off>
   packets <on | off>
   request <on | off>
   spf <on | off>
   trap <on | off>
   update <on | off>
   traceoptions <on | off>

Show Route Summary Commands

Route Summary Commands

show route ..................................................... 297
   igrp
rip
bgp <aspath | communities | detailed | metrics | suppressed>
inactive <bgp | igrp | rip>
all <bgp | igrp | rip>

show route................................................................. 298
  ospf
  inactive ospf
  all ospf

show route................................................................. 298
  aggregate
  inactive aggregate
  all aggregate

show [slot <1-15>] route.................................................. 298
  all
  all direct
  all static
  direct
  inactive
  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

show ipsrd................................................................. 299
  memory
  resources
  krt
  version

Show MFC Commands
show mfc

IP Clustering Commands

General Clustering Commands

add cluster id <0—65535> [passwd passwd]................. 304
add cluster id <0—65535> ........................................ 304
   feature name
      interface log_if_name cluster-address ip_address
      network network/mask cluster-address ip_address

add cluster.......................................................... 304
   ip-pool network network/mask member ip_address
   vpn-tunnel network ip_address/mask destination ip_address

set cluster id <0—65535> ........................................... 306
   cadmin passwd oldpass passwd newpass passwd
   change <0—65535>
   coldstart-delay integer
   failure-interval integer
   firewall-check-required <yes | no>
   interface log_if_name cluster-address ip_address
   join-remote ip_address
   mode <mcast | mcast-group | forwarding>
   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

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

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................................. 314
  ip-pools
  securemote
  securemote clients
  vpn-clients
  vpn-interop
  vpn-tunnels

**Clustering Administration**

set cluster id 10 coldstart-delay 40 ................. 318
show cluster id integer features...................... 319
delete cluster id integer feature feature............. 319
reboot........................................... 321
reboot........................................... 321
  image <name | last-download>
    cluster-all
    cluster-force
    save

**Access List Commands**

**ACL Node Commands**

show acl.......................................... 323
add acl........................................... 323
  name
    name version <ip | ip6>
    name outinterface if_name
    name ininterface if_name

set acl name..................................... 323
  outinterface if_name
ACL Ruleset Commands

Set, Change, and View Aggregation Classes

Queue Class Commands
Set, Change, and View Queue Classes

show qclasses ....................................................... 332
show qclass name ............................................. 333
add qclass name ................................................. 333
set qclass name priority <0-7> ............................... 333
    name name
    qspec <0-5>
    qlength <0-256>

set qclass name interface if_name qmode
    <disabled | maxthroughput | minlatency> ................... 335

delete qclass name ............................................ 335
show qclass-statistics ......................................... 336

ATM QoS

Configuring ATM QoS Descriptors

add atmqos qosd name pcr <64-146000> ....................... 337
delete atmqos qosd name ..................................... 337
show atmqos qosd .............................................. 337
set atmqos interface if_name vc integer qosd name ........ 337
delete atmqos interface if_name vc <vpc/vci | vci> .......... 337
show atmqos interface if_name settings ...................... 338
show atmqos interface if_name bandwidth
    <available | reserved> ...................................... 338

DSCP to VLAN Priority Commands

Configuring DSCP to VLAN Mapping

set custom dscp-to-vlanprio on | off ......................... 339
show custom dscp-to-vlanprio .................................. 339
System Configuration Commands

System Configuration Summary

show................................................................. 341
summary........................................................... 341

Configuring DHCP

DHCP Service Commands

server
client
relay
none

show dhcp service.................................................... 342
show dhcp server all.................................................. 342

Configuring DHCP Clients

add dhcp client interface logical_name......................... 342

clientid name
hostname name
timeout <0-4294967295, 60>
retry <0-4294967295, 300>
leasetime <0-4294967295>
reboot <0-4294967295, 10>

set dhcp client interface logical_name......................... 343

clientid name
hostname name
timeout <0-4294967295, 60>
retry <0-4294967295, 300>
leasetime <0-4294967295>
reboot <0-4294967295, 10>
enable
disable

delete dhcp client interface logical_name...................... 343
show dhcp client .............................................. 343
    interface logical_name
    interfaces

Configuring DHCP Servers

add dhcp server subnet ip_address netmask <1-32> .......... 344
    router 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

add dhcp server subnet ip_address ............................ 345
    pool start ip_address end ip_address

set dhcp server subnet ip_address netmask <1-32> .......... 345
    router 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

show dhcp server .............................................. 345
subnets
  subnet ip_address

delete dhcp server........................................... 345
  subnets
  subnet ip_address

add dhcp server host name.................................... 348
  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

set dhcp server host name.................................... 348
  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

delete dhcp server........................................... 349
  hosts
  host hostname
show dhcp server .......................... 349
hosts
host hostname
set dhcp server ddns .............................. 351
  update-style <none | interm>
  ttl <0-255>
  enable | disable
add dhcp server ddns key name ................. 352
  algorithm HMAC-MD5-SIG-ALG.REG.INT | none
  secret value
set dhcp server ddns key name ...................... 352
  algorithm HMAC-MD5-SIG-ALG.REG.INT | none
  secret name
delete dhcp server key name ..................... 352
show dhcp server .............................. 352
keys
  key name
add dhcp server zone name key name primary ip_address .......... 353
  secondary ip_address
set dhcp server zone name key name primary ip_address .......... 353
  secondary ip_address
  enable | disable
delete dhcp server ............................. 353
  zones
  zones name
show dhcp server .............................. 353
  zones
  zone name

Backup and Restore Files

Manually Backing Up
set backup manual .............................. 354
  on
filename name
homedirs <on | off>
logfiles <on | off>
package name <on | off>

Scheduling Backups

add backup scheduled ........................................ 355
filename name
dayofmonth <1-31>
minute <0-59>
dayofweek <1-7>
hour <0-23>

set backup scheduled ........................................ 356
on
filename name
hour <0-23>
minute <0-59>
homedirs <on | off>
logfiles <on | off>
package name <on | off>

delete backup scheduled ........................................ 356
dayofmonth <1-31> dayofweek <1-7>

Transferring Backup Files to a Remote Server

set backup auto-transfer ........................................ 358
ipaddr ip_address
protocol
    ftp ftp-dir path_name
tftp
delete backup auto-transfer ipaddr ip_address ............... 358

set backup remote .............................................. 359
ftp-site ip_address
ftp-dir path_name
ftp-user name
manual filename [ftp-passwd password]
scheduled filename [ftp-passwd password]
set backup remote <manual | scheduled> filename .................. 359
set backup remote <manual | scheduled> filename ftp-passwd password 359
delete backup remote ................................................. 359
    ftp-site
    ftp-dir
    ftp-user

**Restore Files from Locally Stored Backup Files**

set restore............................................................. 360
    manual filename
    scheduled filename

**Restore Files from Backup Files Stored on Remote Server**

set restore remote..................................................... 361
    filename name
    ftp-site ip_addr
    ftp-dir path_name
    ftp-user user_name
    ftp-passwd password

**Show Backup Commands**

show backup............................................................. 363
    auto-transfer
        all
        ftp-dir
        ipaddr
        protocol
    manual
        filename
        homedirs
        logfiles
        package name
        packages
    remote ftp-site
        ftp-dir
        ftp-user
        manual filenames
        scheduled filenames
scheduled filename
package name
packages
homedirs
dayofmonth
dayofweek
hour
minute
status

Schedule Jobs Through Crontab File

Scheduling Jobs

set cron.................................................... 366
  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

add cron job name command name timezone <local | utc> ....... 366
dayofmonth <1-31>
  hour <0-23>
  minute <0-59>
dayofweek <0-7>
  hour <0-23>
  minute <0-59>
  mailto email_addr

Deleting Jobs

delete cron............................................... 366
  job name
  job name dayofmonth <1-31>
  job name dayofweek <0-7>
  mailto email_addr
Show Cron Commands

```
show cron................................. 368
   job name command
   job name dayofmonth
   job name dayofweek
   job name hour
   job name minute
   jobs
   mailto
```

System Failure Notification Configuration

Enabling System Failure Notification

```
set notify............................... 369
   onfail <on | off>
add notify onfail...................... 369
   recipient name
delete notify onfail................... 369
   recipient name
```

Show System Failure Notification

```
show notify onfail..................... 370
   all
```

DNS

Setting DNS

```
set dns slot <1-15>..................... 370
   domainname name
   primary ip_address
   secondary ip_address
   tertiary ip_address
```

Show DNS

```
show slot <1-15>....................... 371
   dns
```
dns domainname
dns primary
dns secondary
dns tertiary

Deleting DNS
delete dns slot <1-15> ........................................ 371
domainname
primary
secondary
tertiary

Static Host Address Assignment Configuration

Adding New Host Names
add host.......................................................... 372
  name name ipv4 ip_address

Modifying Host Names
set host.......................................................... 372
  name name ipv4 ip_address

Deleting Host Names
delete host.......................................................... 373
  name name

Showing Host Names
show host.......................................................... 373
  names
  name name ipv4

Host Name Configuration

show................................................................. 374
  hostname
  hostname slot <1-15>
set................................................................. 374
Managing IPSO Images

Show IPSO Images

show slot <1-15> ................................................. 375
images
image current
image testboot

Deleting IPSO Images

delete image <name | last-download> ....................... 375

Test Boot, Reboot, and Halt IPSO Images

testboot .......................................................... 375
image <name | last-download>
save
keep
cancel
reboot .............................................................. 375
image <name | last-download>
save
halt ............................................................... 376
image <name | last-download>
save

Downloading IPSO Images

download image .................................................. 376
url name <disable-packages>
  http-realm name user name passwd name <disable-packages>

Managing Configuration Sets
Configuration Set Commands

```plaintext
show
  cfgfiles
  config-state

copy running-config startup-config

load
  cfgfile name

save
  config
  cfgfile name
  factory-cfg name

delete
  cfgfile name
```

Mail Relay Configuration

Mail Relay Commands

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

show mail-relay
  server
  username
```

System Logging Configuration

Logging Commands (Systems with Disks)

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

add
  syslog log-remote-address ip_address
```
level <emerg | alert | crit | err | warning | notice
info | debug | all>
logging ip_address
set logging trap <0-7> ................................. 382
delete..................................................... 382
logging ip_address
syslog log-remote-address ip_address
    level <emerg | alert | crit | err | warning | notice
    info | debug | all>
show.................................................... 383
logging
syslog all
syslog log-remote-address ip_address
syslog log-remote-addresses
syslog auditlog
syslog filename
syslog voyager-auditlog

Logging Commands (Diskless Systems)

set syslog............................................. 385
    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

delete syslog........................................ 385
    primary-log-server ip_address
    secondary-log-server ip_address

show syslog........................................... 388
    all
    auditlog
    flush-frequency
    local-log
    network-log
    primary-log-server
Optional Disk Configuration (IP2250 Systems)

Configuring an Optional Disk

set optional-disk device-id <1 | 2> <on | off>............ 389
show optional-disks........................................... 389

Core-Dump Server Configuration (Diskless Systems)

Configuring an Application Core-Dump Server

set dumpserver.................................................... 390
  ipaddr ip_address
  protocol
    ftp ftp-dir path_name
tftp
delete dumpserver ipaddr...................................... 390
show dumpserver............................................... 391
  all
  ftp-dir
  ipaddr
  protocol

Date and Time Configuration

Setting Date and Time from Server

set date.......................................................... 391
  once-from-ntpserver <ip_address | fully qualified domain name>
timezone-city value
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

set clock time month date year................................. 392
set clock time date month year................................. 392

Show Date and Clock Commands

show date............................................................. 393
show date timezone-city............................................. 393
show clock.......................................................... 393

Disk Commands

Viewing Disk Information

show disks............................................................ 394
show disk.............................................................. 395
  id
  id model
  id type
  id capacity
  id geometry
  id location

Disk Mirroring Commands

Configuring Disk Mirroring

add diskmirror..................................................... 396
delete diskmirror id................................................ 396
show diskmirrors.................................................. 396
show diskmirror..................................................... 396
  id
  id mrdrive
  id srcdrive
  id syncpercent
NTP

Configuring NTP

add ntp................................................................. 397
  server ip_address version <1-3> [prefer <yes | no>]
  peer ip_address version <1-3> [prefer <yes | no>]

set ntp............................................................... 398
  active <on | off>
  server ip_address version <1-3> [prefer <yes | no>]
  peer ip_address version <1-3> [prefer <yes | no>]
  master <yes | no>
  stratum <1-15> source local-clock

delete ntp........................................................... 399
  server ip_address
  peer ip_address

show ntp............................................................ 400
  active
  servers
  peers
  <server | peer> ip_address version [prefer]
  master

Package Commands

Managing Packages

show package....................................................... 401
  all
  active
  inactive

show package media.............................................. 401
  ftp addr ip_address user name password password dir name
  anonftp addr ip_address dir name
  cdrom dir name
  local dir name

add package media............................................... 402
  ftp addr ip_address user name password password name name
anonftp addr ip_address name name

cdrom name name

local name name

upgrade package media ........................................ 403

ftp addr ip_address user name password old name new name

anonftp addr ip_address old name new name

cdrom old name new name

local old name new name

set package name name <on | off> ............................... 403

delete package name name .......................... 403

Advanced System Tuning Commands

Tuning the TCP/IP Stack

set advanced-tuning tcp-ip tcp-mss <512-1500> ............ 404

show advanced-tuning tcp-ip tcp-mss .......................... 404

set advanced-tuning ip-options stripra <1 | 0> ............ 404

show advanced-tuning ip-options stripra ........................ 404

SNMP Commands

SNMP Description

SNMP Command Set

set snmp .......................................................... 406

  daemon <on | off>

  snmp smv-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

set snmp traps .................................................. 406
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>

add snmp................................................................. 407
    address ipaddress
    community string read-only
    community string read-write
    trapreceiver ip_addr community string version <v1 | v2>

delete snmp............................................................ 407
    address ipaddress
    community string read-only
    community string read-write
    trapreceiver ip_address

Enabling/Disabling and Setting SNMP

set snmp............................................................... 408
    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

add snmp............................................. 408
  address ip_address
  community string read-only
  community string read-write
  trapreceiver ip_addr community string version <v1 | v2>

delete snmp....................................... 408
  address ip_address
  community string read-only
  community string read-write
  trapreceiver ip_address

Enabling and Disabling SNMP Traps

set snmp traps..................................... 412
  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-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>

Enabling/Disabling and Changing SNMPv3 USM Users

add user.................................................. 415
  username uid <0-65535> homedir string

set user.................................................. 416
  username passwd

set user.................................................. 416
  username shell string
  username homepage string
  username oldpass string newpass string

set usm users info <readonly | readwrite> .............. 416

delete user............................................. 416
  username

Show SNMP Implementation and Trap Commands

show snmp............................................... 418
  daemon
  community
  trapreceiver
  traps
  snmp trapPduAgent
  snmp location
  snmp contact

Show SNMPv3 Users Commands

show snmp............................................... 419
  usm users

show user............................................... 419
  username
  username uid
  username homedir
  username shell
  username homepage
IPv6 Commands

Configuration Summary

show ipv6 config .................................................. 425

Interface Commands

add interface if_name ............................................. 425
ipv6prefix ip6_address/mask
anycast ip6_address
family inet6
delete interface if_name ........................................ 426
ipv6prefix ip6_address/mask
anycast ip6_address
family inet6
show ipv6 ................................................................. 427
interfaces
interface if_name
show interface if_name ipv6prefix............................... 427

Neighbor Discovery Protocol

add neighbor-entry address ip6_address macaddress mac_address.. 427
set neighbor ............................................................. 428
duplicate-detection <1-100>
multicast-limit <1-100>
queue-limit <1-3>
unicast-limit <1-100>
show neighbor ........................................................ 429
dynamic-table
interface-table
parameters
static-table
table
Tunnels

add interface phys_if_name encapsulation.................... 430
dvmrp
gre
v6inv4 address ip_address remote ip_address [local-link-local linklocal_address] [remote-link-local linklocal_address] [ttl <1–255>]
v4inv6 address ip6_address remote ip6_address

set interface if_name ............................................ 432
interface-binding <on | off>
local-endpoint <ip_address | ip6_address> <enable | disable>
address <ip_address | ip6_address> destination
<iip_address | ip6_address> remote-endpoint
<iip_address | ip6_address>

delete interface if_name ........................................ 433
show ipv6 tunnels................................................... 434

IPv6 to IPv4

set ipv6toipv4....................................................... 434
active on address ip_address enable [ttl <1–255>]
disable

set ipv6toipv4 active <on | off> .............................. 434

IPv6 Over IPv4

set ipv6overipv4.................................................... 435
active on address ip_address enable [ttl <1–255>]
disable

set ipv6overIPv4 active <on | off> ...................... 435

IPv6 Routing Configuration

RIPng

set ipv6 ripng interface if_name............................... 437
<on | off >
metric <0-16>
metric default

show ipv6 ripng

interfaces
interface if_name
packets
errors
neighbors
summary

Route Aggregation

set 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

set slot <1-15> 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

ICMP Router Discovery

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>
hop-limit default
managed-config <on | off>
other-config <on | off>
reachable-time <0–3600000>
reachable-time default
retransmit-timer integer
retransmit-timer default
router-lifetime integer
router-lifetime default
send-mtu <on | off>

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

show ipv6 rdisc6
interfaces
interface if_name
stats
summary

VRRP for IPv6

set ipv6 vrrp6
monitor-firewall <on | off>

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
vird <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

set ipv6 vrrp6 interface if_name......................... 452
  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

show ipv6 vrrp6............................................. 455
  interface if_name
  interfaces
  stats
  summary

Show Routing Summary Commands

show ipv6 route............................................. 455
  ripng
  inactive ripng
  all ripng
show ipv6 route............................................. 455
  aggregate
  inactive aggregate
all aggregate
show [slot <1–15>] ipv6 route ......................... 456
   all
da all direct
da all static
direct
inactive
inactive direct
inactive static
static
summary
destination ipv6_address
eexact ipv6_prefix
less-specific ipv6_prefix
more-specific ipv6_prefix

Host Name Configuration
add ipv6host........................................... 456
   localhost
      name name ipv6 ip6_address
delete ipv6host.................................... 456
   localhost
      name name
set ipv6host name name ipv6 ip6_address .............. 456
show ipv6host names................................. 457
show ipv6host name name ipv6....................... 457

Network Access and Services
set.................................................... 457
   ipv6ftpaccess <enable | disable>
   ipv6tftpaccess <enable | disable>
   ipv6telnetaccess <enable | disable>
show.................................................. 457
   ipv6ftpaccess
   ipv6tftpaccess
   ipv6telnetaccess
Monitoring Commands

Current and Historical Network Reports

Configuring How Much Data is Stored

set monitor config maxhour <24-167> ......................... 459
show monitor config maxhour ............................. 459

Configuring CPU Utilization Reports

set monitor config ............................................ 460
cpuutilization state <on | off>
cpuutilization interval <60-2100000>
show monitor config ....................................... 460
cpuutilization state
cpuutilization interval

show monitor ................................................. 461
starttime <date time year> endtime <date time year>
cpuutilization
summary <hourly | daily | weekly | monthly> cpuutilization

Configuring Memory Utilization Reports

set monitor config ............................................ 461
maxhour
memoryutilization state <on | off>
memoryutilization interval <60-2100000>
show monitor config ....................................... 461
maxhour
memoryutilization state
memoryutilization interval

show monitor ................................................. 461
starttime <date time year> endtime <date time year>
memoryutilization
summary <hourly | daily | weekly | monthly> memoryutilization
Configuring Interface Linkstate Reports

set monitor config.................................................. 462
    linkstate state <on | off>
    linkstate interval <60-2100000 seconds>

show monitor config.............................................. 462
    linkstate state
    linkstate interval

show monitor..................................................... 462
    starttime <date time year> endtime <date time year>
    interface-type <logical | physical>
    interface <name>

show monitor summary <hourly | daily | weekly | monthly>
    interface-type <logical | physical>
    interface <name>........................................... 463

Configuring Rate Shaping Bandwidth Reports

set monitor config.............................................. 463
    rateshape type <bytesdelayed | packetdelayed> state
        <on | off>
    rateshape interval <60-2100000 seconds>

show monitor config............................................ 463
    rateshape type <bytesdelayed | packetdelayed> state
    rateshape interval

show monitor starttime <date time year> endtime <date time year>
    rateshape type <bytesdelayed | packetdelayed>
    aggregate <name>........................................... 463

show monitor summary <hourly | daily | weekly | monthly>
    rateshape type <bytesdelayed | packetdelayed>
    aggregate <name>........................................... 463

Configuring Interface Throughput Reports

set monitor config.............................................. 464
    throughput type <bytes | packets | multicast | broadcast>
        state <on | off>
    throughput interval <60-2100000 seconds>
show monitor config
throughput type <bytes | packets | multicast | broadcast>
state
throughput interval

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>

show monitor summary <hourly | daily | weekly | monthly> throughput type <bytes | packets | multicast | broadcast>
interface-type <logical | physical> interface <name>

Useful System Information

Displaying Useful System Statistics
show useful-stats

Displaying Interface Settings
show interfacemonitor

Displaying System Logs
show logging
logging
logininfo all
logininfo user
log auditlog
log httpd-access-log
log httpd-error-log
log messagelog
type name date name keyword name case-sensitive
include-zipped name

Displaying Interface Traffic Statistics
show iftrafficstats

Displaying the Interface Monitor
show interfacemonitor
Displaying Resource Statistics
show resource-statistics ............................................. 470

Displaying the Forwarding Table
show forwarding-table .................................................. 471

Displaying Hardware Monitors
show sysenv all.......................................................... 473

Displaying a Temperature Sensor Information
show sysenv temperature .............................................. 473
  all
  sensor sensor-number
  <all | location | status | current | limit | hysteresis>

Displaying a Watchdog Timer Information
show sysenv watchdog-timer
  <all | status | mode | tickles | last-reboot> ............... 474

Displaying Voltage Sensor Information
show sysenv voltage .................................................. 475
  all
  sensor sensor-number
  <all | location | status | nominal | measured | error | lo-limit | hi-limit>

Displaying Power Supply Information
show sysenv power-supply ........................................... 477
  all
  id pwr-supply-id
  <all | present | volts | amps | status | revision>

Displaying Fan Sensor Information
show sysenv fan ...................................................... 478
  all
  sensor sensor-number
  <all | location | status | current | normal | limit>
Displaying a Network Interface Card Slot Status

show sysenv slot-status ........................................ 479

Command-Line Utilities

apcssd ................................................................. 482
cst. ................................................................. 484
df ................................................................. 486
ipsoinfo .......................................................... 488
netstat. .......................................................... 489
ping ............................................................. 494
ps ................................................................. 500
tcpdump .......................................................... 511
traceroute ......................................................... 533
uptime ............................................................ 539
vmstat ............................................................. 540
Index

A
AAA 142
    Account Profiles, Configuring 148
    Authentication Profiles, Configuring 146
    Configuration, Viewing 142
    Radius 153
    Service Modules, Configuring 142
    Service Profiles, Configuring 143
    Session Profiles, Configuring 151
    TACAS+ 156
Access Control, SSH Server 159
Access List 322
Access, IPv6 457
Access, Network 115
Account Profiles, AAA 148
ACL
    Bypass Mode 324
    Node 323
    Rule and Aggregation Class, Associating 330
    Ruleset 325
    Viewing 323
Aggregation Class 331
    Configuring 331
    Viewing 331
Aggregation, Routes 254
Alert, System Failure 369
All 447
APC UPS utility 482
apcswd Command 482
Area Backbone, OSPF 217
Areas, OSPF 209
ARP 42
    Proxy, Adding 43
ARP For IPoA 53
ATM
    Configuring Interfaces 45
    Interfaces, Logical 47
    Interfaces, Physical 45
ATM QoS
    Descriptors 336
    Viewing 338
Authentication Profiles, AAA 146
Authorized Keys, SSH 170

B
Backup
    Monitoring and Troubleshooting 362
Backup Files 354
    Transferring to a Remote Server 357
Backups
    Manual 354
    Scheduling 355
Bandwidth, Rate Shaping 463
BGP 187
    Communities 207
    Confederations 195
    External 188
    Internal 200
    Route Dampening 198
Route Reflection 197
Trace 288
Viewing Configurations 207
BOOTP 257
Interfaces 257
Monitoring and Troubleshooting 258

C
Certificates
IPsec 126
SSL 176
Certificates, SSL 174
CLI
Editing 34
Environment, Configuring 23
Features 28
Formats, Output 27
Invoking 22
Mode, Transaction 26
Modes 22
Movement 34
Operations 28
Utilities 481
Clock, Setting 392
Cluster
Administration 317
Commands 303
Configuring an Existing Cluster 306
Creating 304
Installing Images 321
IP-Pool 304
Join-Time Shared Features 318
Join-Time Shared Features,
 Configuring 320
Reboot 321
Shared Features 319
Viewing 314
VPN-Tunnel 304

Clustering 303
Clustering Administration 317
Command
 Completion 29
Default Values 31
Executing Previous 33
Expanding 29
Help 32
Loading from a File 37
Recall 32
Reusing 33
Syntax Conventions 18
Command File 37
Command-Line
 Utilities 481
Commit 26
Communities, BGP 207
Confederations, BGP 195
Configuration
 Copy Running to Startup 378
Load 378
Save 38
Configuration Files
 Managing Sets 378
Saving 379
Viewing 378
Configuration Locks, Setting 35
Copy Configurations 378
CPU Utilization Reports 460
Cron, Monitoring and Troubleshooting 368
Crontab File 365
cst Command 484

D
Dampening, BGP 199
Date, Configuring 391
DDR 280
Default Values 31
Deleting 366
df Command 486
Dial On Demand Routing 280
Disk Mirroring 395
Disk Space, Display 486
Disks, Viewing 394
DNS 370
   Deleting 371
   Setting 370
   Viewing Configurations 371
Download, IPSO Image 376
DSCP To VLAN Priority
   Mapping 339
DSCP to VLAN Priority 338
DVMRP 258
   Interfaces 259
   Monitoring and Troubleshooting 262
   Trace 289
Dynamic ARP 42

E
E1 Interfaces 99
E1, Configure a Physical Interface 99
Environment Commands 23
Equal-Cost Path Splitting 284
Escape Key 30
Ethernet
   Configure a Physical Interface 56
   Interfaces 55
   Logical Interfaces 57
   Physical Interfaces 56
Exiting An Output Screen 35
Expand Commands 29
External BGP 188

F
Failure, System 369
Fan Sensor 478

FDDI
   Interfaces 68
   Logical Interfaces, 70
   Physical Interfaces 69
File System And Processes, Monitoring 36
File Systems 36
Files, Backup and Restore 354
Filter, IPsec 124
Format, Command 31
Formats, Output 27
Forwarding Table 471
Frame Relay
   Configuring an Interface 105
   Encapsulation 105
FTP
   Access 115
   IPv6 Access 457

G
Global, Trace 295
Group Management 183

H
Halt, IPSO 375
Hardware Acceleration, IPsec 140
Hardware Monitors 473
Health, System 466
Help With Commands 32
History, Command 33
Host Address Assignment, Static 372
Host Keys, SSH 167
Host Name
   Adding 372
   Configuring 373
   Deleting 373
   IPv6 456
   Modifying 372
   Viewing 373
Troubleshooting 437
Route Aggregation 438
Routing Configuration 436
Routing Summary 455
Static Routes 439
Tunnels 430
VRRP for IPv6 447
VRRP, All Implementations 447
VRRPv3 448
IPv6 Over IPv4, Configuring 435
IPv6 To IPv4, Configuring 434
ISDN
  Adding Incoming Numbers 75
  Deleting Incoming Numbers 75
  Interfaces 71
  Logical Interfaces, 74
  Physical Interfaces 71

Logical Interface, Deleting 40
Login, SSH 162
Logs, System 466
Load Sharing 284
Loading Commands 37
Local Server, Restore Files 360
Logging, System 381

M
Mail Relay, Configuring 380
Memory Utilization, Reports 461
Memory, Viewing 36
MFC
  Commands, Viewing Information 300
  Trace 292
Modem Interfaces 85
Monitored 451
Monitoring 459

N
netstat Command 489
Network Access 115
Network Access, IPv6 457
Network Interface Card, Status 479
Network Security And Access 115
Network Services 115, 457
Network Status 489
Network Time Protocol 278
Network Time Protocol, Configuring 397
NIC Slot, Status 479
Notification, Failure 369
NTP
  Adding a Server 279
  Configuring 397
  Configuring a Server 278
  Deleting a Server 279
  Monitoring and Troubleshooting 280

K
Kernel, Trace 295
Keys, User Identity 168

L
LDAP, IPsec 141
Licenses 119
Link Aggregation 61
Linkstate Reports 462
Load Sharing 284
Loading Commands 37
Local Server, Restore Files 360
Logging, System 381
Index - 643

Router Discovery Protocol 275
Routes, Static 262
Routing 187
Routing Daemon 299
Routing Summary, IPv6 455
Routing, Miscellaneous Commands 284
Rule, IPsec 135

S
S/Key, Configuring 181
Saving Configuration Changes 38
Scheduling Jobs 366
Security, Network 115
Serial Interfaces 88
 Logical 109
 Physical 88
Server Authentication Of Users 160
Services, IPv6 457
Session Profiles, AAA 151
Shell Options 23
 set 112
 show 113
SNMP
 Commands 405
 Configuring 406
 Enabling and Disabling 408
 Nokia Implementation 405
 Traps, Enabling And Disabling 411
 Viewing Implementation And Traps 418
SNMPv3
 Users, Viewing 419
 Usm Users 415
Sparse Mode PIM 243
SSH 158
 Authorized Keys 170
 Configuring Server Options 159
 Host Keys 167
 Key Pairs 167
Login Environment 162
Service Details, Configuring 164
Service, Enabling and Disabling 158
User Identity Keys 168
SSH Server
 Access Control 159
 Authentication 160
 Implementation 166
 Protocol Details 162
SSL
 Private Key and Certificate 174
 Voyager Web Access 172
Static ARP 42
Static Host Address Assignment 372
Static Routes 262
Static Routes, IPv6 439
Statistics
 Interface 469
 Interface Traffic 469
 Resource 470
 System 466
 Statistics, System 41
 Status 41
 Swapping, Viewing Memory 36
 Syntax, Command 18
 System Configuration 341
 Summary 341
 System Environment, Viewing 473
 System Failure Notification 369
 System Health 465
 System Logging, Configuring 381
 System Logs, Viewing 466
 System Monitoring 459
 System Statistics 41, 466
 System Status 41
 System Summary, cst 484
 System Summary, ipsoinfo 488
 System Tuning 404
 System Uptime 539
T
T1
Configure a Physical Interface 92
T1 Interfaces 91
Tab Key 29
TACAS+, AAA 156
TCP/IP Stack, Tuning 404
tcpdump Command 511
TELNET
  Access 115
  IPv6 Access 457
Temperature Sensor 473
Test Boot, IPSO 375
TFTP
  Access 115
  IPv6 Access 457
Throughput Reports 464
Time, Configuring 391
Trace Routing 286
Trace, Global Options 295
traceroute Command 533
Traffic Management 303
Traffic Statistics 469
Transaction Mode 26
Transparent Mode 59
Troubleshooting with tcpdump 511
Tune, TCP/IP Stack 404
Tunnels 41
  IPv6 430
System 178
Utilities, Command-Line 481

V
V.35 90
Virtual Links, OSPF 216
Virtual Memory Statistics 540
vmstat Command 540
Voltage Sensor 475
Voyager SSL Certificate 174
Voyager Web Access, SSL 172
VPN Accelerator
  Configuring 185
  Displaying Information 185
  Set 185
VRRP 265
  Monitored Circuit, Full 270
  Monitored Circuit, Legacy 274
  Monitored Circuit, Simplified 267
  version 2 272
  VRRP Version 2 272

W
Watchdog Timer 474

X
X.21 90
X509 Certificate Request 130
X509 Certificate, IPsec 127

U
Upgrading Packages 403
UPS utility 482
uptime Command 539
User Identity Keys 168
User Management 177
Users
  SNMPv3 419