Nokia Network Voyager for IPSO 3.9 Reference Guide

Part No. N451628001 Rev A
Published June 2005
### 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>
<tr>
<td>Mail Address</td>
<td>Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA</td>
</tr>
</tbody>
</table>

#### Regional Contact Information

<table>
<thead>
<tr>
<th>Americas</th>
<th>Corporate Headquarters (Nokia Inc.) 313 Fairchild Drive Mountain View, CA 94043-2215 USA Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: <a href="mailto:info.ipnetworking_americas@nokia.com">info.ipnetworking_americas@nokia.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe, Middle East, and Africa</td>
<td>Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK Tel: UK: +44 161 601 8908 Tel: France: +33 170 708 166 email: <a href="mailto:info.ipnetworking_emea@nokia.com">info.ipnetworking_emea@nokia.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968 Tel: +65 6588 3364 email: <a href="mailto:info.ipnetworking_apac@nokia.com">info.ipnetworking_apac@nokia.com</a></td>
</tr>
</tbody>
</table>

#### Nokia Customer Support

| Web Site:         | https://support.nokia.com/ |
| Email:            | tac.support@nokia.com |

<table>
<thead>
<tr>
<th>Americas</th>
<th>Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice:</td>
<td>Voice: +44 (0) 125-286-8900</td>
</tr>
<tr>
<td>1-888-361-5030 or 1-613-271-6721</td>
<td>1-613-271-8782</td>
</tr>
<tr>
<td>Fax:</td>
<td>Fax: +44 (0) 125-286-5666</td>
</tr>
<tr>
<td>1-613-271-8782</td>
<td>1-613-271-6721</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td></td>
</tr>
<tr>
<td>Voice:</td>
<td>Voice: +65-67232999</td>
</tr>
<tr>
<td>Fax:</td>
<td>Fax: +65-67232897</td>
</tr>
</tbody>
</table>

050602
Contents

Overview ................................................................. 9

Command-Line Utility Files ................................. 13

Monitoring and Configuring System Resources ................. 15
  Dynamic Monitoring .................................................. 16
  Static Monitoring .................................................... 26

Configuring Interfaces ................................................ 39
  Ethernet Interfaces .................................................. 47
  Gigabit Ethernet Interfaces .......................................... 56
  Point-to-Point Over Ethernet ......................................... 59
  Virtual LAN Interfaces ................................................ 62
  FDDI Interfaces ...................................................... 65
  ISDN Interfaces ........................................................ 69
  Token Ring Interfaces ................................................ 90
  Point-to-Point Link over ATM ......................................... 95
  IP over ATM (IPoA) .................................................... 100
  Serial (V.35 and X.21) Interfaces ..................................... 104
  T1 (with Built-In CSU/DSU) Interfaces .............................. 110
  E1 (with Built-In CSU/DSU) Interfaces ............................ 118
  HSSI Interfaces ........................................................ 125
  Unnumbered Interfaces ............................................... 130
  Cisco HDLC Protocol ................................................ 134
  Point-to-Point Protocol ............................................... 136
  Frame Relay Protocol ................................................. 137
  Loopback Interfaces .................................................. 141
  GRE Tunnels .......................................................... 142
  DVMRP Tunnels ....................................................... 149
  ARP Table Entries ................................................... 152
  Configuring ARP for the ATM Interface ...................... 155
  Configuring Transparent Mode .................................... 157
## Configuring Routing .............................................................. 165

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>171</td>
</tr>
<tr>
<td>RIP</td>
<td>179</td>
</tr>
<tr>
<td>Protocol-Independent Multicast</td>
<td>184</td>
</tr>
<tr>
<td>IGRP</td>
<td>199</td>
</tr>
<tr>
<td>DVMRP</td>
<td>205</td>
</tr>
<tr>
<td>IGMP</td>
<td>207</td>
</tr>
<tr>
<td>Static Routes</td>
<td>210</td>
</tr>
<tr>
<td>Backup Static Routes</td>
<td>214</td>
</tr>
<tr>
<td>Route Aggregation</td>
<td>215</td>
</tr>
<tr>
<td>Route Rank</td>
<td>218</td>
</tr>
<tr>
<td>BGP</td>
<td>220</td>
</tr>
<tr>
<td>Route Redistribution</td>
<td>254</td>
</tr>
</tbody>
</table>

## Configuring Router Services ............................................. 265

<table>
<thead>
<tr>
<th>Service</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootp Relay</td>
<td>266</td>
</tr>
<tr>
<td>IP Broadcast Helper</td>
<td>267</td>
</tr>
<tr>
<td>Router Discovery</td>
<td>269</td>
</tr>
<tr>
<td>VRRP</td>
<td>271</td>
</tr>
<tr>
<td>NTP</td>
<td>293</td>
</tr>
</tbody>
</table>

## Configuring Security and Access ........................................ 297

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Procedures</td>
<td>299</td>
</tr>
<tr>
<td>Group Procedures</td>
<td>302</td>
</tr>
<tr>
<td>Network Access Procedures</td>
<td>303</td>
</tr>
<tr>
<td>Services</td>
<td>309</td>
</tr>
<tr>
<td>Secure Shell (SSH)</td>
<td>311</td>
</tr>
<tr>
<td>Secure Socket Layer (SSL)</td>
<td>318</td>
</tr>
<tr>
<td>Authentication, Authorization, and Accounting (AAA)</td>
<td>322</td>
</tr>
<tr>
<td>Encryption Acceleration</td>
<td>337</td>
</tr>
<tr>
<td>IPSec Tunnels</td>
<td>338</td>
</tr>
<tr>
<td>Miscellaneous Security Settings</td>
<td>359</td>
</tr>
<tr>
<td>Network Voyager Session Management</td>
<td>359</td>
</tr>
<tr>
<td>Virtual Tunnel Interfaces for Check Point Route-Based VPN</td>
<td>362</td>
</tr>
</tbody>
</table>

## Configuring Traffic Management ......................................... 367

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring IP Clustering in IPSO</td>
<td>368</td>
</tr>
<tr>
<td>Configuring Access Control Lists (ACL)</td>
<td>405</td>
</tr>
<tr>
<td>Configuring Access Control List Rules</td>
<td>408</td>
</tr>
<tr>
<td>Configuring Aggregation Classes</td>
<td>412</td>
</tr>
<tr>
<td>Configuring Queue Classes</td>
<td>414</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring ATM QoS</td>
<td>417</td>
</tr>
<tr>
<td>Configuring Common Open Policy Server</td>
<td>420</td>
</tr>
<tr>
<td>Configuring SNMP</td>
<td>429</td>
</tr>
<tr>
<td>Overview</td>
<td>430</td>
</tr>
<tr>
<td>Configuring SNMP v1 and v2</td>
<td>434</td>
</tr>
<tr>
<td>Interpreting SNMP Messages</td>
<td>440</td>
</tr>
<tr>
<td>Configuring SNMP v3</td>
<td>443</td>
</tr>
<tr>
<td>Configuring System Functions</td>
<td>447</td>
</tr>
<tr>
<td>Configuring DHCP</td>
<td>449</td>
</tr>
<tr>
<td>DNS Hostname Procedures</td>
<td>458</td>
</tr>
<tr>
<td>Configuring Disk Mirroring</td>
<td>459</td>
</tr>
<tr>
<td>Using an Optional Disk (Diskless Systems Only)</td>
<td>460</td>
</tr>
<tr>
<td>Mail Relay</td>
<td>462</td>
</tr>
<tr>
<td>Failure Notification</td>
<td>463</td>
</tr>
<tr>
<td>Time and Date Procedures</td>
<td>464</td>
</tr>
<tr>
<td>Static Host Procedures</td>
<td>464</td>
</tr>
<tr>
<td>System Logging Procedures</td>
<td>465</td>
</tr>
<tr>
<td>Remote Core-Dump Server (Diskless Systems Only)</td>
<td>469</td>
</tr>
<tr>
<td>Hostname Procedure</td>
<td>470</td>
</tr>
<tr>
<td>Managing Configuration Sets</td>
<td>471</td>
</tr>
<tr>
<td>Backing Up and Restoring Files</td>
<td>472</td>
</tr>
<tr>
<td>Scheduling Jobs Through the Crontab File</td>
<td>477</td>
</tr>
<tr>
<td>Managing Nokia IPSO Images</td>
<td>478</td>
</tr>
<tr>
<td>Installing New Nokia IPSO Images</td>
<td>479</td>
</tr>
<tr>
<td>Managing Packages</td>
<td>483</td>
</tr>
<tr>
<td>Advanced System Tuning</td>
<td>484</td>
</tr>
<tr>
<td>Configuring IPv6</td>
<td>487</td>
</tr>
<tr>
<td>Overview</td>
<td>488</td>
</tr>
<tr>
<td>Interfaces</td>
<td>489</td>
</tr>
<tr>
<td>IPv6 and IPv4 Compatibility</td>
<td>491</td>
</tr>
<tr>
<td>Routing Configuration</td>
<td>494</td>
</tr>
<tr>
<td>Router Discovery</td>
<td>497</td>
</tr>
<tr>
<td>VRRP for IPv6</td>
<td>499</td>
</tr>
<tr>
<td>Traffic Management</td>
<td>506</td>
</tr>
<tr>
<td>Security and Access Configuration</td>
<td>507</td>
</tr>
<tr>
<td>Configuring Asset Management</td>
<td>509</td>
</tr>
<tr>
<td>Asset Management Summary</td>
<td>509</td>
</tr>
</tbody>
</table>
Chapter Contents

- About Nokia Network Voyager
- Software Overview
- Navigating in Network Voyager
- Accessing Documentation and Help

1 Overview

About Nokia Network Voyager

Nokia Network Voyager is a Web-based interface that you can use to manage IPSO-SX systems from any authorized location. Network Voyager comes packaged with the IPSO-SX operating system software and is accessed from a client using a browser.

You can also use the command-line interface (CLI) to perform all of the tasks that you can perform when you use Network Voyager, which allows you to choose the interface you are most comfortable with. For information about the CLI, see the CLI Reference Guide.

Software Overview

This section gives you an overview of the Nokia software configured and maintained by Nokia Voyager software.

Nokia firewalls function with the help of several software components:

- **Operating System**—Nokia firewalls run Nokia IPSO, a UNIX-like operating system based on FreeBSD. IPSO is customized to support Nokia’s enhanced routing capabilities and Check Point’s FireWall-1 firewall functionality, and to "harden" network security. Unnecessary features have been removed to minimize the need for UNIX system administration.

- **Ipsilon Routing Daemon (IPSRD)**—IPSRD is Nokia’s routing software. The routing policy implemented by IPSRD resides in a database. Voyager (see below) configures and maintains the routing software and database.

- **Check Point FireWall-1**—FireWall-1 consists of two major components: (1) the Firewall module, which runs on the Nokia firewall and implements the security policy, and (2) the
Management module, which runs either on the Nokia firewall or on another workstation. Use the Management Module to define and maintain the security policy.

- **Voyager**—Voyager communicates with the routing software to configure interfaces and routing protocols, to manage routing policy for the firewall, and to monitor network traffic and protocol performance. Voyager also provides online documentation. Voyager itself runs on a remote machine as a client application of the Nokia routing software and is HTML based.

## Navigating in Network Voyager

The following table explains the functions of the blue buttons in Network Voyager. Other buttons are described in the inline help for each page.

### Note
You can click buttons to produce a result when they have a dark shadow behind them. Buttons without shadows, such as those found in the Voyager Online Help instructions, do not function; they are only for display.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply</td>
<td>Applies the settings on the current page (and any deferred applies from other pages) to the current (running) configuration file in memory.</td>
</tr>
<tr>
<td>Config</td>
<td>Takes you to the configuration page main menu.</td>
</tr>
<tr>
<td>Contents</td>
<td>Takes you to the online help table of contents.</td>
</tr>
<tr>
<td>Doc</td>
<td>Takes you to the online help table of contents.</td>
</tr>
<tr>
<td>Feedback</td>
<td>Takes you to the documentation or Technical Assistance Center (TAC) feedback page.</td>
</tr>
<tr>
<td>Help</td>
<td>Turns on contextual inline help for all elements of the page.</td>
</tr>
<tr>
<td>H</td>
<td>Turns on contextual inline help for a specific element of the page.</td>
</tr>
<tr>
<td>Home</td>
<td>Takes you to the home page.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Takes you to the monitor page main menu.</td>
</tr>
<tr>
<td>Reset Routing</td>
<td>Restarts the routing daemon.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the current (running) configuration file to disk.</td>
</tr>
<tr>
<td>Support</td>
<td>Takes you to contact information for the Technical Assistance Center (TAC).</td>
</tr>
<tr>
<td>Top</td>
<td>Takes you to the top-level configuration page.</td>
</tr>
<tr>
<td>Up</td>
<td>Takes you one level up from the current page.</td>
</tr>
</tbody>
</table>
Avoid using your browser’s Back and Forward buttons while in Network Voyager. The browser caches the HTML page information; therefore, using Back and Forward may not display the latest configuration and diagnostic information as you move from page to page. Use the Config, Monitor, Home, Top, and Up buttons to get the most current data.

**Reloading Pages**

If the pages seem to have outdated information, you can use the Reload button on the browser to update it. You can also clear memory and disk cache with the following procedure.

**To clear the memory and disk cache**

1. Select Network Preferences from the Options menu in Netscape.
2. Select Cache in the Preferences window.
3. Click the Clear Memory Cache Now button, then click OK.
4. Click Clear Disk Cache Now, then click OK.
5. Click OK or close the Preferences window.

**Accessing Documentation and Help**

You can access the *Nokia Network Voyager Reference Guide for IPSO*, the *CLI Reference Guide*, and Network Voyager online help from links within the Network Voyager interface.

This guide, the *Nokia Network Voyager Reference Guide for IPSO*, is the comprehensive reference source for IPSO-SX administration and using the Network Voyager interface. You can access this guide and the *CLI Reference Guide* from the following locations:

- Network Voyager interface—Click the Doc button located at the top of each Network Voyager page.
- Nokia support site ([https://support.nokia.com](https://support.nokia.com)).
- On the software CD that might have been delivered with your appliance. If you have a CD, the documentation is located in the doc folder.

Inline help supplies context sensitive information for Network Voyager. To access inline help for a Network Voyager page, navigate to that page and click Help. Text-only definitions and related information on fields, buttons, and sections appear in a separate window.

To view inline help for a specific section or field on a Network Voyager page, click the **H** button next to the field or section. Text-only definitions and related information related to that specific field or section appear in a separate window.

Inline and online help use the following text conventions.

<table>
<thead>
<tr>
<th>Type of Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>italic text</em></td>
<td>Introduces a word or phrase, highlights an important term, phrase, or hypertext link, indicates a field name, system message, or document title.</td>
</tr>
</tbody>
</table>
### Type of Text

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>typewriter text</td>
</tr>
<tr>
<td>Indicates a UNIX command, program, file name, or path name.</td>
</tr>
<tr>
<td>bold typewriter text</td>
</tr>
<tr>
<td>Indicates text to be entered verbatim by you.</td>
</tr>
<tr>
<td>Represents the name of a key on the keyboard, of a button displayed on your</td>
</tr>
<tr>
<td>screen, or of a button or switch on the hardware. For example, press the</td>
</tr>
<tr>
<td>RETURN key.</td>
</tr>
<tr>
<td>&lt;bracketed&gt;</td>
</tr>
<tr>
<td>Indicates an argument that you or the software replaces with an appropriate</td>
</tr>
<tr>
<td>value. For example, the command <code>rm &lt;filename&gt;</code> indicates that you should</td>
</tr>
<tr>
<td>type <code>rm</code> followed by the filename of the file to be removed.</td>
</tr>
<tr>
<td>LinkText</td>
</tr>
<tr>
<td>Indicates a hypertext link.</td>
</tr>
<tr>
<td>- OR -</td>
</tr>
<tr>
<td>Indicates an exclusive choice between two items.</td>
</tr>
</tbody>
</table>

You can preserve the current page content in your browser and start another browser window to display the inline or online help text by using the following procedure.

**To open a new window to view help**

1. Right-click the Doc button.
2. Click Open Link in New Browser Window.
   Displays the online help in a new window.
3. Right-click the Help On button.
4. Click Open Link in New Browser Window.
   Displays the inline (text-only) help in a new window.
2 Command-Line Utility Files

Chapter Contents

- CAMCONTROL
- FTP
- ID
- MAIL
- MTRACE
- NETSTAT
- PCCARDD
- PING
- SCP
- SSH
- SSHD
- SSH-ADD
- SSH-AGENT
- SSH-KEYGEN
- TCPDUMP
- TELNET
- TFTP
- TRACEROUTE
Chapter Contents

- Dynamic Monitoring
  - Dynamic and Static Monitoring Described
  - Displaying System Utilization Statistics
  - Configuring Data Collection Events
  - Displaying the Rate Shaping Bandwidth Report
  - Displaying Historical Rate Shaping Bandwidth Statistics
  - Displaying Interface Throughput Statistics
  - Displaying Historical Interface Throughput Statistics
  - Displaying Interface Linkstate Statistics
  - Displaying Historical Interface Linkstate Statistics
  - Displaying CPU Utilization Statistics
  - Displaying Historical CPU Utilization Statistics
  - Displaying Memory Utilization Statistics
  - Displaying Historical Memory Utilization Statistics
  - Monitoring System Health
  - Monitoring System Logs

- Static Monitoring
  - Displaying Cluster Status and Members
  - Displaying Routing Protocol Information
  - Displaying Resource Settings
  - Displaying the Kernel Forwarding Table
  - Displaying Route Settings
  - Displaying Interface Settings
  - Displaying System Status
  - Displaying Slot Statistics
  - Displaying Cryptographic Acceleration States
Dynamic Monitoring

Dynamic and Static Monitoring Described

The monitoring features in Network Voyager give you the ability to better maintain system performance and security. You can also customize certain types of data collection to better help you manage and maintain system availability. The following are some of the key features available to you:
- Displaying rate-shaping bandwidth, throughput and linkstate data for each interface
- Monitoring core values associated with different protocols
- Accessing system logs, forwarding tables, and other interface information

Displaying System Utilization Statistics

The system utilization links display statistical information for the following:
- CPU and memory
- Disk and swap space
- Processes

To display the statistical information
1. Click Monitor on the home page.
2. Click the link under System Utilization for which you want to obtain statistics.

Configuring Data Collection Events

To configure data collection events
1. Click Monitor on the home page.
2. Click the Monitor Report Configuration link.
3. (Optional) Click On to enable a particular data collection event.
   The default is set to on.
4. (Optional) Click Off to disable a particular data collection event.
5. (Optional) Enter the collection interval, in seconds, in the Collection Interval text box for each data collection event. The default is 60 seconds.

6. Click Apply.

7. Click Save.

8. In the Data Available for Hours field, specify how many hours of collected data is stored on the system.

   Data that is older than the specified number of hours is deleted.

   The setting for this option controls how much data is available when you use the Detailed Search option on any of the pages available under Current and Historical Network Reports. It does not affect how much data is available when you use the Hourly, Weekly, Daily, or Monthly options on these pages.

**Caution**

Nokia recommends that you set this option to 24 hours (the default value) on diskless systems to avoid exhausting the available storage space.

---

### Displaying the Rate Shaping Bandwidth Report

**To display rate shaping bandwidth statistics**

1. Click Monitor on the home page.

2. Click the Rate Shaping Bandwidth link.

3. In the Select Report Type field, click the button next to Hourly, Daily, Weekly, or Monthly.

4. In the Select Aggregates field, click on the name of the Aggregation class for which you want to display a report or click on ALL AGGREGATES to display data for all configured aggregation classes.

**Note**

You must configure an aggregation class and associate it with an access control list for the name to appear as a choice in the Aggregation Class list. (put link here)

For more information, see Traffic Management, "Creating an Aggregation Class" and "Creating an Access Control List" in Network Voyager.

5. In the Type of RateShaping Data field, check the check box either next to Packets Delayed or Bytes Delayed.

6. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text.
   
   If you select Delimited Text, click the Delimiter drop-down list and select either SEMI-COLON(;) COMMA(,) or TAB.
Note
The Graphical View option displays information at the bottom of the page in a table. The Delimited Text option displays the report in a new page from which you can download the information.

7. Click View Report or Apply to view current rate-shaping bandwidth data.

Displaying Historical Rate Shaping Bandwidth Statistics

To display Rate Shaping Bandwidth for a specific period of time
1. Click Monitor on the home page.
2. Click the Rate Shaping Bandwidth link.
3. In the Select Report Type field, click the button next to Detailed Search.
4. Enter a value for the date and time in the Start Date text box.
   The date defaults to the current date and time minus 10 minutes.
5. Enter a value for the date and time in the End Date text box.
   The date defaults to the current date and time.

Note
Data for the previous seven days is available.

6. In the Select Aggregates field, click the name of the Aggregation class to display a report or click on All Aggregates to display data for all configured aggregation classes.

Note
You must configure an aggregation class and associate it with an access control list for the name to appear as a choice in the Aggregation Class list. (put link here)For more information, see Traffic Management, “Creating an Aggregation Class” and “Creating an Access Control List” in Network Voyager.

7. In the Type of RateShaping Data field, check either the Packets Delayed or Bytes Delayed check box.
8. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text. If you select Delimited Text, click on the Delimiter drop-down list and select either SEMI-COLON(;) COMMA(,) or TAB.
Note
The Graphical View option displays information at the bottom of the page in a table. The Delimited Text option displays the report in a new page from which you can download the information.

9. Click View Report or Apply to view rate-shaping bandwidth data for the period of time selected.

Displaying Interface Throughput Statistics

To display interface throughput statistics
1. Click Monitor on the home page.
2. Click the Interface Throughput link.
3. In the Select Report Type field, click the button next to Hourly, Daily, Weekly, or Monthly. The default is set to Daily.
4. Select an interface name from the Select Interface list or select All Logical to display throughput data for all logical interfaces.
5. In the Type of Throughput field, check the check box next to Packet Throughput, Byte Throughput, Broadcast Throughput, or Multicast Throughput to select the type of throughput data to view.
6. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text.
   If you select Delimited Text from the Delimiter drop-down list, select either SEMI-COLON(;) COMMA(,) or TAB.

Note
The Graphical View option displays information at the bottom of the page in a table. The Delimited Text option displays the report in a new page from which you can download the information.

7. Click View Report or Apply to view current interface throughput data.

Displaying Historical Interface Throughput Statistics

To display interface throughput statistics for a specific period of time
1. Click Monitor on the home page.
2. Click the Interface Throughput link.
3. In the Select Report Type field, click the button next to Detailed Search.
4. Enter a value for the date and time in the Start Date text box.  
The date defaults to the current date and time minus 10 minutes.
5. Enter a value for the date and time in the End Date text box.  
The date defaults to the current date and time.

Note  
Data for the previous seven days is available.

6. Select an interface name from the Select Interface list or select All Logical to display  
throughput data for all logical interfaces.
7. In the Type of Throughput field, click the check box next to Packet Throughput, Byte  
Throughput, Broadcast Throughput, or Multicast Throughput to select the type of  
throughput data you want to view.
8. To select a format type for displaying the report, in the Select Format field, click the button  
next to Graphical View or Delimited Text.  
If you select Delimited Text, click on the Delimiter drop-down list and select either Semi-  
Colon(;) Comma(,) or Tab.

Note  
The Graphical View displays information at the bottom of the page in a table and graph.  
Delimited Text format displays the report as text in a new page from which you can  
download the information.

9. Click **VIEW REPORT** or **APPLY** to view interface throughput data for the period of time  
selected.

**Displaying Interface Linkstate Statistics**

**To display interface linkstate statistics**

1. Click Monitor on the home page.
2. Click the Interface Linkstate link.
3. In the Select Report Type field, click the button next to Hourly, Daily, Weekly, or Monthly.  
The default is set to Daily.
4. Select an interface name from the Select Interfaces for Query list or select All Logical to  
display linkstate data for all logical interfaces.
5. To select a format type for displaying the report, in the Select Format field, click the button  
next to Graphical View or Delimited Text. If you select Delimited Text, click on the  
Delimiter drop-down list and select either Semi-Colon(;) Comma(,) or Tab.
Note
The Graphical View displays information at the bottom of the page in a table. Delimited Text format displays the report as text in a new page from which you can download the information.

6. Click **VIEW REPORT** or **APPLY** to view current interface linkstate data

**Displaying Historical Interface Linkstate Statistics**

To display interface linkstate statistics for a specific period of time, follow these instructions:

1. Click Monitor on the home page.
2. Click the Interface Linkstate link.
3. In the Select Report Type field, click the button next to Detailed Search.
4. Enter a value for the date and time in the Start Date text box.
   The date defaults to the current date and time minus 10 minutes.
5. Enter a value for the date and time in the End Date text box.
   The date defaults to the current date and time.

Note
Data for the previous seven days is available.

6. Select an interface name from the Select Interfaces for Query list or select All Logical to display link state data for all logical interfaces.
7. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text.
   If you select Delimited Text, click on the Delimiter drop-down list and select either Semi-Colon(;) Comma(,) or Tab.

Note
The Graphical View displays information at the bottom of the page in a table. Delimited Text format displays the report as text in a new page from which you can download the information.

8. Click **View Report** or **Apply** to view interface linkstate data for the period of time selected.
Displaying CPU Utilization Statistics

To display CPU utilization statistics
1. Click Monitor on the home page.
2. Click the CPU Utilization link.
3. In the Select Report Type field, click the button next to Hourly, Daily, Weekly, or Monthly. The default is set to Hourly.
4. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text.
   If you select Delimited Text, click on the Delimiter drop-down list and select either Semi-Colon(;) Comma(,) or Tab.

Note
The Graphical View displays information at the bottom of the page in a table and graph. Delimited Text format displays the report as text in a new page from which you can download the information.

5. Click View Report or Apply to view current CPU utilization data.

Displaying Historical CPU Utilization Statistics

To display CPU utilization statistics for a specific period of time
1. Click Monitor on the home page.
2. Click the CPU Utilization link.
3. In the Select Report Type field, click the button next to Detailed Search.
4. Enter a value for the date and time in the Start Date text box.
   The date defaults to the current date and time minus 10 minutes.
5. Enter a value for the date and time in the End Date text box.
   The date defaults to the current date and time.

Note
Data for the previous seven days is available.

6. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text.
   If you select Delimited Text, click on the Delimiter drop-down list and select either Semi-Colon(;) Comma(,) or Tab.
7. Click View Report or Apply to view interface throughput data for the period of time selected.

Displaying Memory Utilization Statistics

To display memory utilization statistics
1. Click Monitor on the home page.
2. Click the Memory Utilization link.
3. In the Select Report Type field, click the button next to Hourly, Daily, Weekly, or Monthly. The default is set to Hourly.
4. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text.
   - If you select Delimited Text, click on the Delimiter drop-down list and select either Semi-Colon(;) Comma(,) or Tab.

5. Click View Report or Apply to view current memory utilization data.

Displaying Historical Memory Utilization Statistics

To display memory utilization statistics for a specific period of time
1. Click Monitor on the home page.
2. Click the Memory Utilization link.
3. In the Select Report Type field, click the button next to Detailed Search.
4. Enter a value for the date and time in the Start Date text box.
   - The date defaults to the current date and time minus 10 minutes.
5. Enter a value for the date and time in the End Date text box.
   - The date defaults to the current date and time.
6. To select a format type for displaying the report, in the Select Format field, click the button next to Graphical View or Delimited Text.
   If you select Delimited Text, click on the Delimiter drop-down list and select either Semi-Colon(;) Comma(,) or Tab.

   **Note**
   Data for the previous seven days is available.

   The Graphical View displays information at the bottom of the page in a table and graph.
   Delimited Text format displays the report as text in a new page from which you can download the information.

7. Click View Report or Apply to view memory utilization data for the period of time selected.

**Monitoring System Health**

The system health links allow you to display statistics to help you monitor the health of your system.

- Useful System Statistics
- Interface Traffic Statistics
- Interface Queue Statistics
- VRRP Service Statistics

**To display the statistical information**

1. Click Monitor on the home page.
2. Click the Link under *System Health* for which you want to obtain statistics.

**Monitoring System Logs**

The system logs links allow you to display updated system logs:

- System Message Log
- Web Server access Log
- Web Server error Log
- User Login/Logout Activity
- Management Activity Log
To display the statistical information

1. Click Monitor on the home page.
2. Click the Link under System Logs for which you want to obtain log activity.

Note
You do not need to configure the Web Server Access log or the Web Server Error log. For more information on configuring the System Message Log, User Login/Logout Activity, and Management Activity Log, see the appropriate section.

To refresh the information in a log, reload the Web page.

System Message log
The system message log lets you view the message log file either in its entirety or to select search criteria to view specific system log activity.

To view a particular type or types of log activity, click one or more items in the Log Type list. On a management console running a Windows operating system, hold down the Ctrl key while you select multiple items. Click Apply to view messages. The default is to display all types of system messages.

To select a month for which to display messages, click on the Select Month drop-down list and select a particular month. Click Apply. The default is to display all messages available.

To select a particular date for which to display messages, click on the Select Date drop-down list and select a particular date. You must also select a month from the Select Month drop-down list to activate this option. Click Apply.

You can also display system messages based on a keyword. Enter a keyword to search for in the system messages in the Keyword text box. To make the keyword search case-sensitive, click the Case Sensitive check box. Click Apply.

You can also include certain zipped files in your search. Click the appropriate check box in the Include Zipped Files in Search section. Click Apply.

The system log also displays messages generated by the Voyager AuditLog. For more information on how to configure the Voyager AuditLog, see “Setting the Nokia Network Voyager AuditLog.”

User Login/Logout Activity
The user login/logout activity log lets you view login and logout activity for users. The default is to display activity for all users. To view activity for a particular user only, click the Login/Logout info for user drop-down list and select the user for whom you want to view login and logout activity. Click Apply.

Management Activity Log
The management activity log lets you view configuration changes. The log includes a time stamp, which provides the date and time when a configuration change occurred; the hostname or
IP address from which the user logged in; and the config entry, which displays the entry changed in the configuration database.

To activate the management activity log feature, click the System Logging link in the System Configuration section. For more information, see “Disabling the System Configuration Auditlog.”

Static Monitoring

Displaying Cluster Status and Members

Displaying cluster status and members provides information about a configured IPSO cluster, including information about cluster status and load sharing among members of the cluster. The information summary is refreshed every 30 seconds.

The Cluster Status table contains the following information:

- **Cluster ID**: ID number of the cluster.
- **Cluster Uptime**: Time since the cluster was formed.
- **Number of Members**: Current number of members in the cluster.
- **Number Of Interfaces**: Number of interfaces on which clustering is enabled.
- **Network**: Networks on which clustering is enabled.
- **Cluster IP Address**: Cluster IP Address on each network.

The Cluster Member table contains the following information:

- **Member Id**: Node ID in the cluster.
- **IP Addr**: Primary IP address of the member.
- **Hostname**: Hostname of the node.
- **Platform**: Type of platform.
- **OS Release**: Operating system version node is running.
- **Rating**: Node performance rating.
- **Time since join**: Time since node joined the cluster.
- **Work Assigned (%)**: Percentage of work load assigned to this node.

**To display the information**

1. Click Monitor on the home page.
2. Click the Cluster Monitor link to view cluster information.

**Note**

If your cluster is not initialized, the Cluster Monitor page contains a link to the Cluster Configuration page, which enables you to configure cluster parameters for this node.
Displaying Routing Protocol Information

The routing protocol link displays statistical information on the following routing protocols:
- OSPF
- BGP
- RIP
- IGRP
- VRRP
- PIM
- DVMRP
- IGMP

It also presents routing daemon information regarding the routing table (through the Route link) and interfaces (through the Interfaces link).

To display routing information
1. Click Monitor on the home page.
2. Click the Routing Protocol link for which you want to obtain statistics.

Displaying Resource Settings

To display resource statistics
1. Click Monitor on the home page.
2. Click the Resource Statistics link to display system resource statistics.

Displaying the Kernel Forwarding Table

The forwarding table link displays information in the kernel forwarding table.

To display forwarding table information
1. Click Monitor on the home page.
2. Click the Forwarding Table link.
   The IP forwarding table that the kernel is using to make its forwarding decisions appears.

Displaying Route Settings

To display route settings
1. Click Monitor on the home page.
2. Click the Route Settings link for the interface for which you want to obtain statistics.
Displaying Interface Settings

To display interface statistics
1. Click Monitor on the home page.
2. Click the Interface Settings link for the interface for which you want to obtain statistics.

Displaying System Status

To display system status information
1. Click Monitor on the home page.
2. Click the System Status link.

Displaying Slot Statistics

To display the statistical information
1. Click Monitor on the home page.
2. Click the Slot Status link.

Displaying Cryptographic Acceleration States

To monitor the Nokia Cryptographic Acceleration Card
1. Click Monitor on the home page.
2. Click the Cryptographic Accelerator Statistics link in the Hardware Monitoring section.

Displaying IPv6 Running States

To monitor the IPv6 running state
1. Click Monitor on the home page.
2. Click the IPv6 Monitor link to display the IPv6 running state.

Displaying Routing Daemon Status (iclid)

Obtain routing diagnostic information by creating a telnet session on the IP security platform and running iclid (IPSRD command-line interface daemon).
To display routing daemon status using iclid

1. Create a Telnet session and log into the firewall.
2. Type iclid

The prompt changes (to `<node-name>`) to indicate that you can now enter iclid commands.

**iclid Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>? or &lt;tab&gt;</td>
<td>Shows all possible command completions.</td>
</tr>
<tr>
<td>help</td>
<td>Displays help information.</td>
</tr>
<tr>
<td>quit or exit</td>
<td>Quits iclid.</td>
</tr>
<tr>
<td>show</td>
<td>Shows formatted, categorized system information.</td>
</tr>
</tbody>
</table>

Some commands might produce more output than can fit on a single screen; iclid pages the output of such commands for you, that is, stops the output after one screen and indicates that there is more output with a MORE prompt. You can see the next screenful of output by selecting any key except the q key; you can abort the command and any further output by typing q at the MORE prompt. If you do not enter anything within about 30 seconds, the system automatically pages to the next screenful of information. You can temporarily defeat this automatic paging by typing ctl-S, although when you resume scrolling (by selecting any key) you might lose a page of information.

At any point in iclid, you can type ? to display possible command completions. You can also abbreviate commands when an abbreviation is not ambiguous.

The help command takes as arguments iclid commands and top-level iclid categories; it displays a brief summary of what the specified command displays.

The quit command returns control to the firewall shell. The exit command is the same as the quit command.

The show command provides many kinds of information, displayed in useful formats. The following table shows examples of the top-level iclid element that can be displayed by the show command as applied to each parameter, along with any selected categories and subcategories, and a description of the information the command displays.

<table>
<thead>
<tr>
<th>Element</th>
<th>Category</th>
<th>Subcategory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Subcategory</td>
<td>errors</td>
<td>Provides a BGP summary.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A table of BGP errors.</td>
</tr>
<tr>
<td>Element</td>
<td>Category</td>
<td>Subcategory</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>bootpgw</td>
<td>interface</td>
<td>&lt;interface&gt;</td>
<td>BOOTP relay state of interfaces enabled for BOOT protocols.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BOOTP relay state of specified interface.</td>
</tr>
<tr>
<td>stats</td>
<td></td>
<td>rec</td>
<td>Summary of BOOTP relay requests received.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>req</td>
<td>Summary of BOOTP relay requests made.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rep</td>
<td>Summary of BOOTP relay replies made.</td>
</tr>
</tbody>
</table>

groups

- **detailed**: Detailed statistics on BGP groups.
- **summary**: A summary of statistics on BGP groups.

memory

- **<peerid> advertise**: Shows BGP neighbor statistics.
- **detailed**: Provides detailed information about BGP neighbors and is organized by neighbor address. In the event of an excessively long list, type `q`.

paths

- **List of BGP paths; in the event of an excessively long list, type `q`.**

peers

- **detailed**: Detailed information about each peer firewall; in the event of an excessively long list, type `q`.
- **summary**: Summary table about peer firewalls.

redistribution

- **to AS <as number>**: Shows detailed redistribution data from BGP to the designated AS.
- **from <proto> to AS <as number>**: Shows detailed redistribution data to the designated AS from the specified protocol.

statistics

- **A table of peer parameters and statistics.**
<table>
<thead>
<tr>
<th>Element</th>
<th>Category</th>
<th>Subcategory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dvmrp</td>
<td></td>
<td></td>
<td>Summary of DVMRP state.</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
<td>Interface-specific state of DVMRP for each DVMRP-enabled interface.</td>
</tr>
<tr>
<td>neighbor routes</td>
<td></td>
<td></td>
<td>State of DVMRP neighbor route.</td>
</tr>
<tr>
<td>neighbors</td>
<td></td>
<td></td>
<td>Interface state of DVMRP neighbor parameters.</td>
</tr>
<tr>
<td>route</td>
<td></td>
<td></td>
<td>Shows state of DVMRP route parameters.</td>
</tr>
<tr>
<td>stats</td>
<td></td>
<td></td>
<td>Statistical information about DVMRP packets sent and received, including an error summary.</td>
</tr>
<tr>
<td>receive</td>
<td></td>
<td></td>
<td>A summary of statistical information about received DVMRP packets.</td>
</tr>
<tr>
<td>transmit</td>
<td></td>
<td></td>
<td>A summary of statistical information about transmitted DVMRP packets.</td>
</tr>
<tr>
<td>error</td>
<td></td>
<td></td>
<td>A summary of DVMRP packets with errors.</td>
</tr>
<tr>
<td>Element</td>
<td>Category</td>
<td>Subcategory</td>
<td>Description</td>
</tr>
<tr>
<td>igmp</td>
<td></td>
<td></td>
<td>State of IGMP.</td>
</tr>
<tr>
<td>groups</td>
<td></td>
<td></td>
<td>State of the IGMP groups maintained for each network interface.</td>
</tr>
<tr>
<td>if stats</td>
<td></td>
<td></td>
<td>Summary of information about IGMP interface packets transmitted and received for each network interface.</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
<td>IGMP settings for each network interface.</td>
</tr>
<tr>
<td>stats</td>
<td></td>
<td></td>
<td>Statistical information about IGMP packets sent and received as well as an error summary.</td>
</tr>
<tr>
<td>Element</td>
<td>Category</td>
<td>Subcategory</td>
<td>Description</td>
</tr>
<tr>
<td>inbound filter</td>
<td></td>
<td></td>
<td>Lists inbound filters and data for all protocols.</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
<td>Status and addresses of all configured interfaces.</td>
</tr>
<tr>
<td>krt</td>
<td></td>
<td></td>
<td>Displays IPSRD core information.</td>
</tr>
<tr>
<td>memory</td>
<td></td>
<td></td>
<td>Total memory usage in kilobytes.</td>
</tr>
<tr>
<td>Element</td>
<td>Category</td>
<td>Subcategory</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ospf</td>
<td>border routers</td>
<td></td>
<td>Lists OSPF border routers and associated codes.</td>
</tr>
<tr>
<td>database</td>
<td>area</td>
<td></td>
<td>Provides statistical data on OSPF database area.</td>
</tr>
<tr>
<td>database summary</td>
<td></td>
<td>A database summary of the OSPF firewall.</td>
<td></td>
</tr>
<tr>
<td>router</td>
<td></td>
<td></td>
<td>Statistical data on firewall link states as well as link connections.</td>
</tr>
<tr>
<td>asbr summary</td>
<td></td>
<td>A summary of the OSPF firewall.</td>
<td></td>
</tr>
<tr>
<td>external</td>
<td></td>
<td></td>
<td>Information on the OSPF external database.</td>
</tr>
<tr>
<td>summary</td>
<td></td>
<td></td>
<td>Summary of OSPF database.</td>
</tr>
<tr>
<td>checksum</td>
<td></td>
<td></td>
<td>Statistical data on the OSPF checksum database.</td>
</tr>
<tr>
<td>network</td>
<td></td>
<td></td>
<td>Data on OSPF database network.</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td></td>
<td>Data on the state of firewall link parameters.</td>
</tr>
<tr>
<td>errors</td>
<td>brief</td>
<td></td>
<td>Provides basic data on OSPF errors.</td>
</tr>
<tr>
<td></td>
<td>dd</td>
<td></td>
<td>OSPF dd errors.</td>
</tr>
<tr>
<td></td>
<td>hello</td>
<td></td>
<td>OSPF hello errors.</td>
</tr>
<tr>
<td></td>
<td>ip</td>
<td></td>
<td>OSPF interface protocol errors.</td>
</tr>
<tr>
<td></td>
<td>lsack</td>
<td></td>
<td>OSPF ls acknowledge errors.</td>
</tr>
<tr>
<td></td>
<td>lsr</td>
<td></td>
<td>OSPF lsr errors.</td>
</tr>
<tr>
<td></td>
<td>lsu</td>
<td></td>
<td>A list of OSPF lsu errors.</td>
</tr>
<tr>
<td></td>
<td>proto</td>
<td></td>
<td>OSPF protocol errors.</td>
</tr>
<tr>
<td>events</td>
<td></td>
<td></td>
<td>OSPF events and event occurrences.</td>
</tr>
<tr>
<td>interface</td>
<td>detail</td>
<td></td>
<td>A comprehensive presentation of detailed OSPF interface data.</td>
</tr>
<tr>
<td>stats</td>
<td></td>
<td></td>
<td>A comprehensive list of OSPF interface statistics.</td>
</tr>
<tr>
<td>Element</td>
<td>Category</td>
<td>Subcategory</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>neighbor</td>
<td></td>
<td></td>
<td>Lists OSPF neighbors and associated parameters.</td>
</tr>
<tr>
<td>packets</td>
<td></td>
<td></td>
<td>Lists received and transmitted OSPF packets.</td>
</tr>
<tr>
<td>&lt;proto&gt;</td>
<td>inbound</td>
<td>filter</td>
<td>Lists inbound filter data for the specified protocol.</td>
</tr>
<tr>
<td></td>
<td>redistribution</td>
<td></td>
<td>Lists redistributions from all sources to the designated protocol.</td>
</tr>
<tr>
<td></td>
<td>redistribution from &lt;proto&gt;</td>
<td></td>
<td>Lists redistributions from a specified protocol to another specified protocol.</td>
</tr>
<tr>
<td>Element</td>
<td>Category</td>
<td>Subcategory</td>
<td>Description</td>
</tr>
<tr>
<td>redistribution</td>
<td></td>
<td></td>
<td>Shows a comprehensive list of redistributions to various protocols and autonomous systems, and includes detailed distribution data.</td>
</tr>
<tr>
<td>resource</td>
<td></td>
<td></td>
<td>A comprehensive listing of resource statistics.</td>
</tr>
<tr>
<td>rip</td>
<td></td>
<td></td>
<td>A summary of information on the RIP routing process.</td>
</tr>
<tr>
<td>errors</td>
<td></td>
<td></td>
<td>A list of various RIP errors.</td>
</tr>
<tr>
<td>packets</td>
<td></td>
<td></td>
<td>Statistics on various RIP packets transmitted and received.</td>
</tr>
<tr>
<td>route</td>
<td></td>
<td></td>
<td>Lists data on static and directly connected routes.</td>
</tr>
<tr>
<td>aggregate</td>
<td></td>
<td></td>
<td>Data on aggregate routes by code letter.</td>
</tr>
<tr>
<td>all</td>
<td></td>
<td></td>
<td>List of all routes and status data. In the event of a long list type q.</td>
</tr>
<tr>
<td>aggregate</td>
<td></td>
<td></td>
<td>Data on all aggregate routes by code letter.</td>
</tr>
<tr>
<td>bgp</td>
<td></td>
<td></td>
<td>Data on BGP routes.</td>
</tr>
<tr>
<td>direct</td>
<td></td>
<td></td>
<td>Data on direct routes.</td>
</tr>
<tr>
<td>igrp</td>
<td></td>
<td></td>
<td>Data on IGRP routes.</td>
</tr>
</tbody>
</table>
### Data Description

<table>
<thead>
<tr>
<th>Element</th>
<th>Category</th>
<th>Subcategory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospf</td>
<td></td>
<td></td>
<td>Data on OSPF routes.</td>
</tr>
<tr>
<td>rip</td>
<td></td>
<td></td>
<td>Data on RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td></td>
<td></td>
<td>Data on static routes.</td>
</tr>
<tr>
<td>bgp</td>
<td></td>
<td></td>
<td>Statistics on BGP routes.</td>
</tr>
<tr>
<td>aspath</td>
<td></td>
<td></td>
<td>List of parameters and status of BGP AS path.</td>
</tr>
<tr>
<td>communities</td>
<td></td>
<td></td>
<td>Status of BGP communities.</td>
</tr>
<tr>
<td>detailed</td>
<td></td>
<td></td>
<td>Details of BGP routes.</td>
</tr>
<tr>
<td>metrics</td>
<td></td>
<td></td>
<td>Status of BGP metrics.</td>
</tr>
<tr>
<td>suppressed</td>
<td></td>
<td></td>
<td>List and status of suppressed BGP routes.</td>
</tr>
<tr>
<td>direct</td>
<td></td>
<td></td>
<td>Directly connected routes and their status.</td>
</tr>
<tr>
<td>igrp</td>
<td></td>
<td></td>
<td>Displays IGRP routes.</td>
</tr>
<tr>
<td>inactive</td>
<td></td>
<td></td>
<td>Inactive routes.</td>
</tr>
<tr>
<td>aggregate</td>
<td></td>
<td></td>
<td>Inactive aggregate routes.</td>
</tr>
<tr>
<td>bgp</td>
<td></td>
<td></td>
<td>Inactive BGP routes.</td>
</tr>
<tr>
<td>direct</td>
<td></td>
<td></td>
<td>Inactive direct routes.</td>
</tr>
<tr>
<td>igrp</td>
<td></td>
<td></td>
<td>Inactive IGRP routes.</td>
</tr>
<tr>
<td>ospf</td>
<td></td>
<td></td>
<td>Inactive OSPF routes.</td>
</tr>
<tr>
<td>rip</td>
<td></td>
<td></td>
<td>Inactive RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td></td>
<td></td>
<td>Inactive static routes.</td>
</tr>
<tr>
<td>ospf</td>
<td></td>
<td></td>
<td>OSPF route data.</td>
</tr>
<tr>
<td>rip</td>
<td></td>
<td></td>
<td>RIP route data.</td>
</tr>
<tr>
<td>static</td>
<td></td>
<td></td>
<td>Static route data.</td>
</tr>
<tr>
<td>summary</td>
<td></td>
<td></td>
<td>Displays the number of routes for each protocol.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Element</th>
<th>Category</th>
<th>Subcategory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td></td>
<td></td>
<td>Operating system version information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Element</th>
<th>Category</th>
<th>Subcategory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp</td>
<td></td>
<td></td>
<td>VRRP state information.</td>
</tr>
</tbody>
</table>
The following table shows examples of the iclid show command.

<table>
<thead>
<tr>
<th>iclid show command</th>
<th>Shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ospf</td>
<td>OSPF summary information.</td>
</tr>
<tr>
<td>show ospf neighbor (s o n)</td>
<td>OSPF neighbor information.</td>
</tr>
<tr>
<td>show route</td>
<td>All routes</td>
</tr>
<tr>
<td>show route bgp 127</td>
<td>Only BGP routes that start with 127.</td>
</tr>
<tr>
<td>show b?</td>
<td>All possible command completions for show b</td>
</tr>
</tbody>
</table>

### Resolving and Preventing Full Log Buffers and Related Console Messages

When a significant amount of your traffic is using fast path for delay-critical, real-time routing through the firewall, the console might display one of the following error messages:

```
[LOG-CRIT] kernel: FW-1: Log Buffer is full
[LOG-CRIT] kernel: FW-1: lost 500 log/trap messages
```

The kernel module maintains a buffer of waiting log messages that it forwards through `fwd` to the management module. The buffer is circular, so that high logging volumes can cause buffer entries to be overwritten before they are sent to `fwd`. When this happens, the system log displays the following message:

```
log records lost
```

The lost records are those that should have been recorded in the FW-1 log message file (typically located in the `$FWDIR/log` directory).

You can use one or both of the following solutions to resolve this issue:

- Reduce the number of rules that are logged by:
  - Disabling as many accounting rules as possible
  - Changing as many long logging rules to short logging as possible
  - Eliminating logging entirely if it is practical to do so
- Increase the size of the kernel module buffer
Note
To perform the following procedures, use the zap or modzap utility (which you can obtain from the Nokia Technical Assistance Center (TAC); refer to Resolution 1261).

If you are using FireWall-1 4.1

1. Set the execute permissions by issuing an `fwstop` command.

2. To confirm that you have sufficient resources to increase the buffer size, issue the following command:
   
   ```bash
   # ./modzap -n _fw_logalloc $FWDIR/boot/modules/fwmod.o 0x20000
   ```
   
   where `0x20000` indicates a buffer size of 2MB, and the `-n` option causes `modzap` to check the value at the symbol reported.

3. A console message is displayed confirming the change that will take place when you issue the `modzap` command in the next step.
   You can safely ignore this message.

Note
If the message indicates that you have insufficient resources to accommodate a larger buffer size, take appropriate actions and try this procedure again. For further information, contact Nokia Technical Assistance Center (TAC).

4. After you verify that the change is appropriate, issue the same command without the `-n` option:
   
   ```bash
   # ./modzap _fw_logalloc $FWDIR/boot/modules/fwmod.o 0x20000
   ```
   
   A confirmation message is displayed, which you can safely ignore.

5. Reboot the system.

If you are using FireWall-1 NG

1. Set the execute permissions by issuing a `cpstop` command.

2. To confirm that you have sufficient resources to increase the buffer size, issue the following command:
   
   ```bash
   modzap -n _fw_logbufsize $FWDIR/boot/modules/fwmod.o 0x200000
   ```
   
   where `0x20000` indicates a buffer size of 2 MB, and the `-n` option causes `modzap` to check the value at the symbol reported.

3. A console message is displayed confirming the change that will take place when you issue the `modzap` command in the next step.
   You can safely ignore this message.
Note
If the message indicates that you have insufficient resources to accommodate a larger buffer size, take appropriate actions and try this procedure again. For further information, contact Nokia Technical Assistance Center (TAC).

4. After you verify that the change is appropriate, issue the same command without the -n option:
   
   modzap _fw_log_bufsize $FWDIR/boot/modules/fwmod.o 0x200000
   
   A confirmation message is displayed, which you can safely ignore.

5. Reboot the system.

Because these console messages are also written to the FW-1 log message file, Nokia recommends that you do the following to prevent depleting the disk space allocated for the FW-1 log message file:

1. Move your log files from the system hard drive to a server.
2. Configure the relocated files by using the Check Point management client GUI (Smart Dashboard) as follows:
   a. Select the Check Point gateway object you are configuring.
   b. Under Gateway Object Configuration, select the Logs and Masters section and do the following:
      ■ Specify the amount of free disk space required for local logging.
      ■ Specify to stop logging when the free disk space drops below x MB and to start logging to a new file.

   Once a new file is being used, the previously used log files are deleted until the required free disk space is restored.
4 Configuring Interfaces

Chapter Contents

- Interface Overview
- Ethernet Interfaces
  - Configuring Ethernet Interfaces
  - Ethernet Example
  - Link Aggregation
- Gigabit Ethernet Interfaces
  - Configuring Gigabit Ethernet Interfaces
  - Gigabit Ethernet Example
- Point-to-Point Over Ethernet
  - Introduction to Point-to-Point Over Ethernet
  - Configuring PPPoE
  - Creating PPPoE Logical Interfaces
  - Deleting PPPoE Logical Interfaces
  - Changing Configuration Profiles
  - Deleting Configuration Profiles
- Virtual LAN Interfaces
  - Virtual LAN Description
  - Configuring a VLAN Interface
  - Defining the Maximum number of VLANs
  - VLAN Example Topology
- FDDI Interfaces
  - Configuring an FDDI Interface
  - Changing the Duplex Setting of an FDDI Interface
  - Changing the IP Address of an FDDI Interface
  - FDDI Example
- ISDN Interfaces
  - Features
  - Configuring a Physical Interface
- Creating a Logical Interface
- Dial-on-Demand Routing Lists
- ISDN Network Configuration Example
- ISDN Troubleshooting

Token Ring Interfaces
- Configuring a Token Ring Interface
- Deactivating a Token Ring Interface
- Changing a Token Ring Interface
- Token Ring Example

Point-to-Point Link over ATM
- Configuring an ATM Interface
- Changing the VPI/VCI of an ATM Interface
- Changing the IP Address of an ATM Interface
- Changing the IP MTU of an ATM Interface
- Removing an ATM Interface
- ATM Example

Logical IP Subnets (LIS) over ATM
- Configuring an ATM Logical IP Subnet (LIS) Interface
- Changing the VPI/VCIs of an ATM LIS Interface
- Changing the IP Address of an ATM LIS Interface
- Changing the IP MTU of an ATM Interface
- Removing an ATM Interface

Serial (V.35 and X.21) Interfaces
- Configuring a Serial Interface for Cisco HDLC
- Configuring a Serial Interface for PPP
- Configuring a Serial Interface for Frame Relay
- Serial Interface Example

T1 (with built-in CSU/DSU) Interfaces
- Configuring a T1 Interface for Cisco HDLC
- Configuring a T1 Interface for PPP
- Configuring a T1 Interface for Frame Relay
- T1 Interface Example

E1 (with built-in CSU/DSU) Interfaces
- Configuring an E1 Interface for Cisco HDLC
- Configuring an E1 Interface for PPP
- Configuring an E1 Interface for Frame Relay

HSSI Interfaces
- Configuring an HSSI Interface for Cisco HDLC
- Configuring an HSSI Interface for PPP
- Configuring an HSSI Interface for Frame Relay

- Unnumbered Interfaces
  - Unnumbered Interfaces Description
  - Configuring an Unnumbered Interface
  - Changing an Unnumbered Interface to a Numbered Interface
  - Configuring a Static Route over an Unnumbered Interface
  - Configuring OSPF over an Unnumbered Interface
  - Configuring OSPF over an Unnumbered Interface Using Virtual Links

- Cisco HDLC Protocol
  - Changing the Keepalive Interval for Cisco HDLC
  - Changing the IP Address in Cisco HDLC

- Point-to-Point Protocol
  - Changing the Keepalive Interval in PPP
  - Changing the Keepalive Maximum Failures in PPP
  - Changing the IP Address in PPP

- Frame Relay Protocol
  - Changing the Keepalive Interval in Frame Relay
  - Changing the DLCI in Frame Relay
  - Changing the LMI Parameters in Frame Relay
  - Changing the Interface Type in Frame Relay
  - Changing the Active Status Monitor Setting in Frame Relay
  - Changing the IP Address in Frame Relay
  - Removing a Frame Relay Interface

- Loopback Interfaces
  - Adding an IP Address to a Loopback Interface
  - Changing the IP Address of a Loopback Interface

- GRE Tunnels
  - Creating a GRE Tunnel
  - Changing the Local and/or Remote Address or Local/Remote Endpoint of a GRE Tunnel
  - Changing IP TOS Value of a GRE Tunnel
  - Removing a GRE Tunnel
  - GRE Tunnel Example
  - HA GRE Tunnels Description
  - HA GRE Tunnel Example

- DVMRP Tunnels
  - Creating a DVMRP Tunnel
  - Changing the Local or Remote Addresses of a DVMRP Tunnel
- Removing a DVMRP Tunnel
- DVMRP Tunnel Example

- ARP Table Entries
  - Changing ARP Global Parameters
  - Adding a Static ARP Entry
  - Adding a Proxy ARP Entry
  - Deleting a Static ARP Entry
  - Viewing Dynamic ARP Entries
  - Deleting Dynamic ARP Entries
  - Flushing All Dynamic ARP Entries

- Configuring ARP for the ATM Interface
  - Changing Global Parameters
  - Adding a Static ATM ARP Entry
  - Deleting a Static ATM ARP Entry
  - Viewing and Deleting Dynamic ATM ARP Entries

- Configuring Transparent Mode
  - Transparent Mode Description
  - Creating a Transparent Mode Group
  - Deleting a Transparent Mode Group
  - Adding or Removing Interfaces to/from Transparent Mode Groups
  - Enabling or Disabling a Transparent Mode Group
  - Enabling or Disabling VRRP for a Transparent Mode Group
  - Transparent Mode and Check Point NGX SmartDashboard
  - Monitoring Transparent Mode Groups

Interface Overview

Interface Types

Nokia NAPs support the following interface types.

- Ethernet/Fast Ethernet
- Gigabit Ethernet
- FDDI
- ATM (RFC1483 PVCs only)
- Serial (V.35 and X.21) running PPP, point-to-point Frame Relay, or Cisco HDLC
- T1/E1 running PPP, Frame Relay, or Cisco HDLC
- HSSI running PPP, point-to-point Frame Relay, or Cisco HDLC
- VPN Tunneling
- Token Ring
- Unnumbered Interface
- ISDN

**Note**
Consult the appropriate hardware installation guide to find out what interfaces your unit supports.

You can configure these interfaces with IP addresses. You also can assign additional IP addresses to the loopback, FDDI, and Ethernet interfaces. All interface types support IP multicast.

**Configuring Network Devices**

Network Voyager displays network devices as physical interfaces. A physical interface exists for each physical port on a network interface card (NIC) installed in the unit. Physical interface names have the form:

```
<type>-s<slot>p<port>
```

where:

- `<type>` is a prefix indicating the device type.
- `<slot>` is the number of the slot the device occupies in the unit.
- `<port>` is the port number of the card. The first port on a NIC is port one. For example, a two-port Ethernet NIC in slot 2 is represented by two physical interfaces: `eth-s2p1` and `eth-s2p2`.

The following table lists the interface-name prefixes for each type.

<table>
<thead>
<tr>
<th>Type</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>eth</td>
</tr>
<tr>
<td>FDDI</td>
<td>fddi</td>
</tr>
<tr>
<td>ATM</td>
<td>atm</td>
</tr>
<tr>
<td>Serial</td>
<td>ser</td>
</tr>
<tr>
<td>T1/E1</td>
<td>ser</td>
</tr>
<tr>
<td>HSSI</td>
<td>ser</td>
</tr>
<tr>
<td>Token Ring</td>
<td>tok</td>
</tr>
<tr>
<td>ISDN</td>
<td>isdn</td>
</tr>
</tbody>
</table>
The loopback interface also has a physical interface named loop0. Use Network Voyager to set the attributes of the device. For example, line speed and duplex mode are attributes of an Ethernet physical interface. Each communications port has exactly one physical interface.

**Configuring IP Addresses**

Logical interfaces are created for a device's physical interface. You assign an IP address to logical interfaces and then route to the IP address. Ethernet, FDDI, and Token Ring devices have one logical interface.

For ATM devices, you create a new logical interface each time you configure an RFC1483 PVC for the device. Serial, T1/E1, and HSSI devices have one logical interface when they are running PPP or Cisco HDLC. Serial, T1/E1, and HSSI devices running point-to-point Frame Relay have a logical interface for each PVC configured on the port. You also have the option of configuring an unnumbered interface for point-to-point interfaces. Tunnels, however, cannot be configured as unnumbered interfaces.

Logical interfaces, by default, are named after the physical interface for which they are created. If you wish, you can override this default name with a more descriptive or familiar name. You can also associate a comment with the logical interface as a further way to define its relationship in the network. Default logical interface names have the form:

\(<\text{type}>-s<\text{slot}>p<\text{port}>c<\text{chan}>\)

where

\(<\text{type}>,<\text{slot}>\) and \(<\text{port}>\) have the same values as the corresponding physical interface.

\(<\text{chan}>\) is the channel number of the logical interface.

For logical interfaces created automatically, the channel number is always zero. For logical interfaces created manually, the channel number is the identifier of the virtual circuit (VC) for which the interface is created (for example, the ATM VCI or the Frame Relay DLCI).

<table>
<thead>
<tr>
<th>Physical Interface</th>
<th>Logical Interface</th>
<th>Default</th>
<th>Cisco HDLC</th>
<th>PPP</th>
<th>Frame Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>One (c0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDDI</td>
<td>One (c0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>One per VCI (c#)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial (X.21 or V.35)</td>
<td>One (c0)</td>
<td>One (c0)</td>
<td>One (c0)</td>
<td>One per DLCI (c#)</td>
<td></td>
</tr>
<tr>
<td>T1/E1</td>
<td>One (c0)</td>
<td>One (c0)</td>
<td>One (c0)</td>
<td>One per DLCI (c#)</td>
<td></td>
</tr>
<tr>
<td>HSSI</td>
<td>One (c0)</td>
<td>One (c0)</td>
<td>One (c0)</td>
<td>One per DLCI (c#)</td>
<td></td>
</tr>
</tbody>
</table>
For example, the logical interface of a physical interface `eth-s2p1` is called `eth-s2p1c0`. The logical interfaces for PVCs 17 and 24 on an ATM NIC in slot 3 are called `atm-s3p1c17` and `atm-s3p1c24` respectively.

Once a logical interface exists for a device, you can assign an IP address to it. For Ethernet, FDDI, and Token Ring, you must specify the interface's local IP address and the length (in bits) of the subnet mask for the subnet to which the device connects.

If you are running multiple subnets on the same physical network, you can configure additional addresses and subnet masks on the single logical interface connected to that network. You do not need to create additional logical interfaces to run multiple subnets on a single physical network.

For point-to-point media, such as ATM, serial, or HSSI, you can either assign IP addresses or configure an unnumbered interface. When assigning IP addresses you must specify the IP address of the local interface and the IP address of the remote system's point-to-point interface. You can add only one local/destination IP address pair to a point-to-point logical interface. To assign IP addresses to multiple VCs, you must create a logical interface for each VC. IP subnets are not supported on point-to-point interfaces.

Whenever an unnumbered interface generates a packet, it uses the address of the interface that the user has specified as the source address of the IP packet. Thus, for a router to have an unnumbered interface, it must have at least one IP address assigned to it. The Nokia implementation of unnumbered interfaces does not support virtual links.

**Note**
If you make changes to IP addresses or delete interfaces, the firewall sometimes does not learn of the changes when you get the topology. If you get the topology and your changes to interfaces are not shown, stop and restart the firewall.

### Indicators and Interface Status

The configuration and status of removable-interface devices are displayed. Interfaces can be changed while they are offline. Indicators include the following:

- **None**: If no color indication is displayed, the physical interface is disabled. To enable the interface, click on the physical interface name to go to its configuration page.

- **Blue**: The device corresponding to this physical interface has been removed from the system, but its configuration remains. To delete its configuration, click on the physical interface name to go to its configuration page.
Red: The physical interface is enabled, but the device does not detect a connection to the network.

Green: The physical interface is ready for use. It is enabled and connected to the network.

Events that can affect the status of interfaces include the following:

- If you hot-insert a device (not power down the unit first), it appears in the lists of interfaces immediately (after a page refresh) on the configuration pages.
- If you hot-pull a device, and no configuration exists for it, it disappears from the lists of interfaces immediately.
- If you hot-pull a device, and it had a configuration, its configuration details continue to be displayed and can be changed even after a reboot.
- Hotswapped interfaces that are fully seated in a router’s chassis are represented in the ifTable (MIB-II), ipsoCardTable (IP440-IPSO-System-MIB), and the hrNetworkTable (Host-Resources-MIB).
- Unwanted configurations of absent devices can be deleted, which removes the physical and logical interfaces from all interface lists.

**Address Resolution Protocol (ARP)**

ARP allows a host to find the physical address of a target host on the same physical network using only the target’s IP address. ARP is a low-level protocol that hides the underlying network physical addressing and permits assignment of an arbitrary IP address to every machine. ARP is considered part of the physical network system and not as part of the internet protocols.

**Using the Loopback Interface**

By default, the loopback interface has 127.0.0.1 configured as its IP address. Locally originated packets sent to this interface are sent back to the originating process.

You might want to assign an address to the loopback interface that is the same as the OSPF firewall ID, or is the termination point of a BGP session. This allows firewall adjacencies to stay up even if the outbound interface is down. Do not specify an IP subnet mask length when you add addresses to the loopback interface.

**Configuring Tunnel Interfaces**

Tunnel interfaces are used to encapsulate protocols inside IP packets. Use tunneling to:

- Send network protocols over IP networks that don’t support them.
- Encapsulate and encrypt private data to send over a public IP network.

Create a tunnel logical interface by specifying an encapsulation type. Use Network Voyager to set the encapsulation type. Network Voyager supports two encapsulation types, DVMRP and GRE.

The tunnel logical interface name has the form:
tun0c<chan>

where:

<chan> (channel number) is an instantiation identifier.

**DVMRP Tunnels**

DVMRP (Distance Vector Multicast Routing Protocol) tunnels encapsulate multicast packets using IP-in-IP encapsulation. The encapsulated packets appear as unicast IP packets. This technique allows two multicast routers to exchange multicast packets even when they are separated by routers that cannot forward multicast packets. For each DVMRP tunnel you create, you must provide the IP address of the interface that forms the local endpoint of the tunnel and the IP address of the multicast router that is at the remote end of the tunnel forming the remote endpoint of the tunnel.

**Note**
The remote multicast router must support IP-in-IP encapsulation and must be configured with a tunnel interface to the local router.

When you have created the DVMRP tunnel interface, set all other DVMRP multicast configuration parameters from the DVMRP configuration page.

**VPN Tunnels**

VPN (Virtual Private Networking) tunnels encapsulate IP packets using Generic Routing Encapsulation (GRE) without options. The encapsulated packets appear as unicast IP packets. For each VPN tunnel you create, you must assign a local and remote IP address. You also must provide the local and remote endpoint addresses of the interface to which this tunnel is bound. VPN tunnels provide redundant configuration between two sites for high availability. The remote router must also support VPN encapsulation and must be configured with a tunnel interface to the local router.

**Ethernet Interfaces**

**Configuring Ethernet Interfaces**

You can configure a number of parameters for each Ethernet interface, including the following:

- Enable (make active) or disable the interface.
- Change the IP address for the interface.
- Change the speed and duplex mode.

For information on how to complete the initial configuration of an Ethernet interface or to change some of the parameters, see “To configure an Ethernet interface” on page 48.

Table 1 describes the configuration settings for an Ethernet interface.
To configure an Ethernet interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the name of the physical interface you want to configure.
   Example: eth-s2p1
4. Specify the configuration parameters for speed add duplex mode.

---

Table 1 Physical Interface Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select On to enable the interface, select Off to disable the interface. These selections appear on both the main Interface Configuration page and the pages for each individual interface.</td>
</tr>
<tr>
<td>Link Trap</td>
<td>Click On or Off to enable or disable the linkup/linkdown traps for the interface. Default is On for all physical interfaces.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Select 100 Mbit/sec or 10 Mbit/sec. This setting must be the same for all hosts on the network to which the device connects.</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Select Full or Half. This setting must be the same for all hosts on the network to which the device connects.</td>
</tr>
<tr>
<td>Autoadvertise</td>
<td>Click on or off to enable or disable autoadvertise. If turned on, the device advertises its configured speed and duplicity by using Ethernet negotiation.</td>
</tr>
<tr>
<td>Link recognition delay</td>
<td>Specify how many seconds a link must be stable before the interface is declared up. Default is 6; range is 1-255.</td>
</tr>
<tr>
<td>Queue mode</td>
<td>For more information, see &quot;Queue Class Description&quot; on page 414.</td>
</tr>
<tr>
<td>IP address &amp; Mask length</td>
<td>You can add multiple IP addresses.</td>
</tr>
</tbody>
</table>

**Note**
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security appliance with your Network browser.

Logical name | Use this to enter a more meaningful name for the interface.
Comments      | (Optional) This field is displayed on the main Interface Configuration and the Logical Interface pages. Use it to add a description that you might find useful in identifying the logical interface.
Click Apply.

5. Click the logical interface name in the Logical Interfaces table.
   The Logical Interface page is displayed.

6. Enter the IP address and mask length.
   Click Apply.
   Each IP addresses and mask length that you add are added to the table when you click Apply. The entry fields return to blank to allow you to add more IP addresses.
   Use the delete check box to delete IP addresses from the table.

7. (Optional) Change the interface logical name to a more meaningful name by typing the preferred name in the Logical name text box.
   Click Apply.

8. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   Click Apply.

9. Click Up to go to the Interface Configuration page.

10. Click On button that corresponds to the logical interface you configured.
    Click Apply.
    The Ethernet interface is now available for IP traffic and routing.

11. To make your changes permanent, click Save.

**Ethernet Example**

This section describes how you might configure the interfaces of your IP security appliance in an example network using Network Voyager.

Before you can configure the device by using Network Voyager, you must configure an IP address on one of the interfaces. You can do this through device console port during installation or by using the Lynx browser. This allows a graphical browser such as Microsoft Internet Explorer or Netscape Navigator to access the device through that interface. You can use any graphical web browser to configure the other interfaces on the device by entering the IP address of the device in the location field of the browser.
The following figure shows the network configuration for this example.

In a company main office, Nokia Platform A terminates a serial line to an Internet service provider, running PPP with a keepalive value of 10.

Nokia Platform A also provides internet access for a FDDI ring and a remote branch office connected through ATM PVC 93.

The branch office contains Nokia Platform B, which routes traffic between a local Fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. This example configures the Ethernet interface on Nokia Platform B.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click eth-s2p1 in the Physical column of the table.
4. Click 100 Mbit/sec.
5. Click Apply.
6. Click eth-s2p1c0 in the logical interfaces table to go to the Interface page.
7. Enter 192.168.4.1 in the New IP address text box.
8. Enter 24 in the New mask length text box.
9. Click Apply.
10. Click Up to go the Interfaces page.
11. Click On for eth-s2p1c0.
12. Click Apply.
13. Click Save

**Link Aggregation**

Nokia IPSO appliances allow you to aggregate (combine) Ethernet ports so that they function as one logical port. You get the benefits of greater bandwidth per logical interface and load balancing across the ports. For example, you can aggregate two 10/100 mbps ports so they function like a single port with a theoretical bandwidth of 200 mbps, and you can aggregate two Gigabit Ethernet ports so they function like a single port with a theoretical bandwidth of 2000 mbps. If you have only 10/100 interfaces and need a faster link but can’t or don’t want to use Gigabit Ethernet, you can use link aggregation to achieve faster throughput with the interfaces you already have.

Another benefit of link aggregation is redundancy—if one of the physical links in an aggregation group fails, the traffic is redistributed to the remaining physical links and the aggregation group continues to function. IPSO distributes the outbound IP traffic across the physical links using the source and destination IP addresses. It uses the source and destination MAC addresses to distribute non-IP traffic.

You can aggregate as many as four ports in one aggregation group, and you can have as many as eight aggregation groups on one appliance.

You can hot swap NICs that have ports participating in an aggregation group. If the group has ports on other NICs, the traffic is distributed to those ports and the aggregation group continues to function when you remove a NIC in this manner. If you reinser the NIC, the appropriate ports rejoin the aggregation group and resume forwarding traffic automatically.

**Managing with SNMP**

Nokia has implemented a proprietary SNMP MIB to use in managing link aggregation. To incorporate link aggregation into your SNMP-based management, perform the following tasks:

- Copy the file NOKIA-IPSO-LINKAGGREGATION-MIB.txt to your management system. This file is located at /etc/snmp/mibs/.
- In Network Voyager or the IPSO CLI, enable the following traps:
  - Enable lamemberActive traps
  - Enable lamemberInactive traps

IPSO does not use the standard IEEE8023-LAG-MIB to support link aggregation.

**Configuring Switches for Link Aggregation**

Observe the following considerations when you configure a switch to support link aggregation in combination with a Nokia appliance:

- You must configure the appropriate switch ports to use static link aggregation. (On Cisco switches, this means you must enable EtherChannel.) That is, if you aggregate four ports...
into one group on your Nokia appliance, the four switch ports that they connect to must
static link aggregation.

- When you assign switch ports to an EtherChannel group, set the channel mode to **on** to
  force the ports to form a channel without using the Link Aggregation Control Protocol
  (LACP) or Port Aggregation Protocol (PAgP).

- If your switch supports it, configure the aggregated ports to distribute the traffic using
  source and destination IP addresses.

- If your switch can only distribute traffic based on source or destination MAC addresses,
  configure it to use the source MAC addresses. If it uses the destination MAC address to
  distribute the load, all the traffic flowing from the switch to the IPSO system over the
  aggregated link is sent to the primary port of the aggregation group.

- You must configure the switch ports to have the same physical characteristics (link speed,
  duplicity, autoadvertise/autonegotiation setting, and so on) as the corresponding aggregated
  ports on the Nokia system.

- On Cisco switches, trunking must be enabled if you create more than one tagged VLAN on
  an aggregated link. (You can configure as many as 1015 VLANs for an IPSO system.).

- If you use IOS on a Cisco switch, trunking is enabled automatically.

- If you run CatOS on a Cisco switch, use the following command to configure VLAN
  trunking on the EtherChannel:

  ```
  set trunk ports nonegotiate dot1q vlans
  ```

**Static Link Aggregation**

The IPSO implementation of link aggregation complies with the IEEE 802.3ad standard for
static link aggregation. Nokia has also tested IPSO link aggregation with the following Cisco
Catalyst switches:

- 6500 Series
- 3550 Series
- 2950 Series

IPSO does not support LACP, which is used for dynamic link aggregation.

**Link Aggregation on the IP2250**

This section describes aspects of link aggregation that are specific to the IP2250 appliance.

**Firewall Synchronization Traffic**

If you configure two IP2250 appliances in a VRRP pair and run VPN-1 NG on them, Nokia
recommends that you aggregate two of the built-in 10/100 Ethernet management ports to create
a 200 mbps logical link and configure VPN-1 NG to use this network for firewall
synchronization traffic. If you use a single 100 mbps connection for synchronization, connection
information might not be properly synchronized when the appliance is handles a large number of
connections.
**Note**

Use Ethernet crossover cables to connect the built-in 10/100 ports that you aggregate. Using a switch or a hub can result in incomplete synchronization.

Because you should use crossover cables for these connections, you should not configure more than two IP2250 appliances in a VRRP group. (You can use a switch or hub to connect the built-in 10/100 mbps ports that you do not aggregate.)

You should use the built-in Ethernet management ports that you do not aggregate for your management connections and to connect to log servers.

If you use aggregated built-in ports for firewall synchronization traffic and delete a port from the aggregation group but do not delete the group itself, be sure to delete the corresponding port on the other IP2250 system. If you delete a port on one system only and that port remains physically and logically enabled, the other system will continue to send traffic to the deleted port. This traffic will not be received, and firewall synchronization will therefore be incomplete.

**Caution**

Do not use ports on IP2250 I/O cards for firewall synchronization traffic. Doing so can cause connections to be dropped in the event that there is a failover to a backup router.

**Production Traffic**

You can aggregate the ports on IP2250 I/O cards and use the aggregated links for traffic other than firewall synchronization. If you aggregate ports on IP2250 I/O cards, observe the following constraints:

- Do not include ports on different I/O cards in the same aggregation group.
- Do not combine any of the built-in 10/100 Ethernet management ports with ports on an I/O card to form an aggregation group.

These configurations are not supported.

**Configuring Link Aggregation**

Setting up link aggregation in Network Voyager comprises three processes:

1. Physically configuring the interfaces.
2. Creating the aggregation group.
3. Logically configuring the aggregation group.

**Physical Interface Configuration**

To set up link aggregation in Network Voyager, you first configure the physical interfaces that you will aggregate.
Note
Make sure that the physical configurations (link speed, duplicity, autoadvertise setting, and so on) are identical for all the interfaces that will participate in a given group. These settings must match the settings for the switch ports that the interfaces are connected to.

When you aggregate an interface, any logical configuration information is deleted. Be careful not to aggregate the interface that you use for your management connection because doing so breaks your HTTP connection to the appliance. Should this occur, you can restore HTTP connectivity by using one of the following approaches:

- Connect to another configured port and use Network Voyager to reconfigure the management port.
- Use the IPSO CLI over a console connection to reconfigure the management port.

Because the management port is now part of an aggregation group, Network Voyager and the CLI identify it using the format \texttt{ae\text{xxx}}, in which \texttt{xxx} is the group ID.

To physically configure the interfaces you will aggregate, follow these steps:

1. On the Network Voyager home page, click Interface Configuration.
2. Click a link for one of the physical interfaces that you will aggregate.
   Be careful not to select a port that you are using for a management connection.
3. Configure the physical configuration to the settings you want.
4. Click Apply
5. Click Save to make the changes permanent.
6. Perform step 2 through step 5 again to configure the other interfaces identically.

Group Configuration
Once the physical interfaces are configured, you need to create and configure link aggregation groups.

On appliances other than the IP2250, you can put ports on different LAN interface cards in the same aggregation group. For example, you can include a port on a card in slot 1 and a port on a card in slot 2 in the same group. On the IP2250, do not include ports on different IO cards in the same aggregation group.

If you use VRRP and VPN-1 NG with appliances other than the IP2250, you can run firewall synchronization traffic over an aggregated link, regardless of which ports participate in the link. On the IP2250, do not run this traffic over an aggregated link that is made up of ports on an interface card.

To configure link aggregation groups, follow these steps:

1. On the Network Voyager home page, click Interface Configuration.
2. Click Link Aggregation.
3. In the New Group ID field, enter a numeric value that will identify the group of aggregated interfaces.

4. Click Apply.
   An entry for the new group appears under Existing Link Aggregation Groups.

5. Use the Primary Port pull-down menu to select a port for the aggregation group.
   The menu shows the physical names of the interfaces that correspond to the available Ethernet ports. For example, eth1 corresponds to the first built-in ethernet port, and eth-s5p1 corresponds to port 1 on the NIC in slot 5. Be careful not to select a port that you are using for a management connection.

6. Click Apply.
   The entry for the aggregation group indicates that the MAC address for the interface you selected is used as the MAC address for all the interfaces in the group.

7. Add a port to the group by selecting another interface from the Add Port menu.

   **Caution**
   Do not include ports on different IP2250 I/O cards in the same aggregation group. This configuration is not supported.

8. Click Apply.
   Note that Network Voyager’s display of the aggregated bandwidth does not reflect whether any of the ports are physically up or logically active.

**Logical Configuration**

When you have completed the aggregation group, you must configure it with an IP address and so on. Navigate to the Interfaces Configuration page and click the logical name of the group. Network Voyager shows the logical name in the format aexxx:c0. For example, the logical name of a group with the ID 100 is ae100c0.

If you create a link aggregation group but do not add any interfaces to it, the logical name of the group does not appear on the Interfaces Configuration page. You cannot configure an aggregation group with logical information until you have added an interface to the group.

**Deleting aggregation groups**

To delete an aggregation group, you must first remove all the ports from the group. To remove a port from an aggregation group, simply click the Delete checkbox next to the appropriate port and click Apply. Click Save to make the change permanent.

You cannot remove the primary port from an aggregation group unless the other ports have been removed, but you can remove all the ports simultaneously. You can simultaneously remove all the ports and delete the group by clicking all the Delete checkboxes and then clicking Apply. Click Save to make the change permanent.
Gigabit Ethernet Interfaces

Configuring Gigabit Ethernet Interfaces

You can configure the parameters listed in Table 2 for each Gigabit Ethernet interface.

For information on how to complete the configuration of an Gigabit Ethernet interface, see “To configure an Ethernet interface” on page 48.

Table 2 Gigabit Ethernet Interface Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select On to enable the interface, select Off to disable the interface. These selections appear on both the main Interface Configuration page and the pages for each individual interface.</td>
</tr>
<tr>
<td>Link trap</td>
<td>Click On or Off to enable or disable the linkup/linkdown traps for the interface. Default is On for all physical interfaces.</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control can be implemented to reduce receiving-buffer overflows, which can cause received packets to be dropped, and to allow local control of network congestion levels. With the flow control On, the Gigabit Ethernet card can send flow-control packets and respond to received packets. Default is Off.</td>
</tr>
<tr>
<td>Link recognition delay</td>
<td>Specify how many seconds a link must be stable before the interface is declared up. Default is 6; range is 1-255.</td>
</tr>
<tr>
<td>MTU</td>
<td>The maximum length of frames, in bytes, that can be transmitted over this device. This value limits the MTU of any network protocols that use this device. This option appears only for NICs that have the capability of transmitting jumbo frames. Default is 1500; range is 1500-16,000.</td>
</tr>
</tbody>
</table>

**Note**
On the IP2250, the range is 1500-9600.

<table>
<thead>
<tr>
<th>IP address &amp; Mask length</th>
<th>You can add multiple IP addresses.</th>
</tr>
</thead>
</table>

**Note**
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security appliance with your Network browser.
To configure a Gigabit ethernet interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. (Optional) Set flow control to On.
   Click Apply.
4. Click the name of the logical interface in the Logical interfaces table.
   The Logical Interface page is displayed.
5. (Optional) To increase the maximum length of frames, in bytes, that can be transmitted over this device, enter a value for MTU. The default is 1500.
6. Enter the IP address and subnet mask length for the device in the appropriate text fields.
7. Enter the IP address and mask length.
   Click Apply.
   Each IP addresses and mask length that you add are added to the table when you click Apply. The entry fields return to blank to allow you to add more IP addresses.
   Use the delete check box to delete IP addresses from the table.
8. (Optional) Change the interface logical name to a more meaningful name by typing the preferred name in the Logical name text box.
   Click Apply.
9. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   Click Apply.
10. Click Up to go to the Interface Configuration page.
11. Click On button that corresponds to the logical interface you configured.
   Click Apply.
   The Gigabit Ethernet interface is now available for IP traffic and routing.

---

Table 2  Gigabit Ethernet Interface Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical name</td>
<td>Use this to enter a more meaningful name for the interface.</td>
</tr>
<tr>
<td>Comments</td>
<td>(Optional) This field is displayed on the main Interface Configuration and the Logical Interface pages. Use it to add a description that you might find useful in identifying the logical interface.</td>
</tr>
</tbody>
</table>

---

Note
Link speed is fixed and duplex mode is set to full at all times for Gigabit Ethernet interfaces.
12. To make your changes permanent, click Save.

**Gigabit Ethernet Example**

This section describes how you might configure the interfaces of your IP security platform device in an example network, by using Network Voyager.

Before you can configure the device by using Network Voyager, you must configure an IP address on one of the interfaces. You can do this through the device console port during installation or by using the Lynx browser. This allows a graphical browser such as Microsoft Internet Explorer or Netscape Navigator to access the device through that interface. You can use any graphical web browser to configure the other interfaces on the unit by entering the IP address of the device in the location field of the browser.

The following figure below shows the network configuration for this example.

In a company main office, Nokia Platform A terminates a serial line to an Internet service provider.

Nokia Platform A also provides internet access for an FDDI ring and a remote branch office connected through ATM.
The branch office contains Nokia Platform B, which routes traffic between a local gigabit Ethernet network and ATM. It provides access to the main office and the Internet. This example configures the gigabit Ethernet interface on Nokia Platform B.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click eth-s2p1 in the Physical column of the table.
4. Click on or off in the Flow Control field of the Physical configuration table.
5. Click Apply.
6. Click eth-s2p1c0 in the Logical interfaces table to go to the Interface page.
7. Enter 192.168.4.1 in the New IP address text box.
8. Enter 24 in the New mask length text box.
9. Click Apply.
10. Click Up to go the Interface Configuration page.
11. Click On for eth-s5p1c0.
12. Click Apply.
13. Click Save.

Point-to-Point Over Ethernet

Introduction to Point-to-Point Over Ethernet

Point-to-Point Over Ethernet (PPPoE) for IPSO provides you with the ability to create multiple point-to-point connections from your Ethernet network to your ISP. Configuration is simple and your network can be connected over a bridging device such as a DSL modem.

Configuring PPPoE

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the pppoe0 link.

This takes you to the PPPoE physical interface page.

Note
The PPPoE physical interface and the associated link trap is on by default. If you wish to change either setting, click the appropriate setting next to the feature you wish to enable or disable and click Apply.
4. Click PPPOE Profile link.  
    This takes you to the PPPOE Profile Configuration page. Here you can create PPPoE profiles, change profiles, and view existing profiles on your system.

5. In the Profile Name text box, enter a name for the profile.

6. (Optional) In the Description text box, enter a description.

7. In the Ethernet Interface drop-down box, select the Ethernet interface you wish to associate with the PPPoE logical interface in the.

8. In the Mode drop-down box, select a connection mode.

9. In the Timeout text-box, enter a time in seconds.

10. (Optional) In the Peername text-box, enter the name of the PPPoE server.

    **Note**  
    If you use the Peername field, only the PPPoE server named in the field will be allowed to connect to the system.

11. In the MTU text-box, enter the maximum byte size to be transmitted. The default is 1492 bytes.

12. Enter a value in the MSS Clamping text box if end devices connected to this interface are experiencing connectivity problems with specific destinations. See “Configuring MSS Clamping” for more information.

13. In the Authentication Type drop-down box, select an authentication type. If you selected PAP or CHAP, you must enter a user name in the Username text box and a password in the Password text box.

14. Click Apply

15. Click Save to make your changes permanent.

To create more configuration profiles, repeat steps 4 through 14.

16. Click UP.
    This takes you back to the physical interface page.

17. Chose a configuration profile you created in the preceding steps from the Create a new interface with PPPoE profile drop-down box.

18. Click Apply.

19. Click the logical interface link you wish to configure in the Logical Interface box.
    This takes you to the Logical interface page.

20. In the Interface type drop-down box, select an interface type. If you select Static Interface, you must provide the IP address of the logical interface in the Local Address text box and the IP address of remote point-to-point interface in the Remote Address text box.
Note
The PPPoE logical interface is on by default and the associated link trap is disabled by default. If you wish to change either setting, click the appropriate setting next to the feature you wish to enable or disable and click Apply.

21. Click Apply.
22. Click Save to make your changes permanent.

Configuring MSS Clamping
When end devices use path MTU discovery, it can cause connectivity problems when their connections pass through PPPoE interfaces. Use the MSS Clamping field to prevent these problems by reducing the maximum segment size (MSS) that is advertised across the outgoing link.

IPSO advertises the value in this field as the MSS for packets that transit this interface. If a connected device (such as a host system) advertises a greater MSS, IPSO advertises the value in this field instead of the value advertised by the device. There is no default value for the MSS Clamping field. If you do not enter a value, the MSS advertised by end devices is always advertised across the link.

If hosts connected to this interface experience connectivity problems with some destinations, use this field to restrict the MSS that they can advertise. Entering a value of 1452 will probably solve any such problems.

See RFC 2923 for more information about how path MTU discovery that can cause connectivity problems.

Creating PPPoE Logical Interfaces

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the pppoe0 link.
4. In the Create a new interface with PPPoE profile, select a profile name.
5. Click Apply.
6. Click Save to make your changes permanent.

Deleting PPPoE Logical Interfaces

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the pppoe0 link.
4. Click Delete in the Logical interfaces box associated with the PPPoE profile to delete.
5. Click Apply.
6. Click Save to make your changes permanent.

**Changing Configuration Profiles**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the pppoe0 link.
4. Click the name of the PPPoE profile in the PPPoE Profile field.
5. Make changes to the profile as needed. See (link to Configuring PPPoE steps 8 through 15.)
6. Click Apply.
7. Click Save to make your changes permanent.

**Deleting Configuration Profiles**

**Note**
You must first delete the configuration profile interface before you can delete a configuration profile. For more information, see “Deleting PPPoE Logical Interfaces.”

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the pppoe0 link.
4. Click the PPPoE Profile link
5. Click Delete.
6. Click Apply.

**Virtual LAN Interfaces**

**Virtual LAN Description**

Nokia supports virtual LAN (VLAN) interfaces on all supported ethernet interfaces. VLAN interfaces lets you configure subnets with a secure private link to Check Point FW-1/VPN-1 with the existing topology. VLAN enables the multiplexing of ethernet traffic into channels on a single cable.

The Nokia implementation of VLAN supports adding a logical interface with a VLAN ID to a physical interface. In a VLAN packet, the OSI layer-two header, or MAC header, contains four more bytes than the typical Ethernet header for a total of 18 bytes. When traffic arrives at the
physical interface, the system examines it for the VLAN layer-two header and accepts and forwards the traffic if a VLAN logical interface is configured. If the traffic that arrives at the physical interface does not have a VLAN header, it is directed to the channel 0, or untagged, interface. In the Nokia implementation, the untagged channel-0 interface drops VLAN packets that are sent to the subnets on that interface.

Outgoing traffic from a VLAN interface is tagged with the VLAN header. The Nokia appliance can receive and generate fully conformant IEEE 802.1Q tags. The IEEE802.1Q standard defines the technology for virtual bridged networks. The Nokia implementation is completely interoperable as a router, not as a switch.

**Configuring a VLAN Interface**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the link to the physical ethernet interface for which to enable a VLAN interface in the Physical field.
   This action takes you to the physical interface page for that interface.
4. Enter a value to identify the VLAN interface in the Create a new VLAN Id text box. The range is 2 to 4094. The values 0 and 4095 are reserved by the IEEE standard. VLAN ID 1 is reserved by convention. There is no default. Click Apply.
   The new logical interface for the VLAN appears in the Logical Interfaces field with the name `eth-sXpYcZ`, where `X` is the slot number, `Y` is the physical port number and `Z` is the channel number. The channel numbers increment starting with 1 with each VLAN ID that you create.
5. Click Save to make your changes permanent.
   Repeat steps 4 through 6 for each VLAN interface to create.
6. To assign an IP address to the new logical VLAN interface, click the link for the logical interface in the Interface field of the Logical Interfaces table. Enter the IP address in the New IP address text box. Enter the mask length in the New mask length text box. Click Apply.
7. Click Save to make your changes permanent.
   The new logical interface appears as active on the interface configuration page. Click Up to view that page.
   (Optional) To disable the interface, click off in the Active field in the row for the logical interface. Click Apply.
   Click Save to make your change permanent.
Note
You can assign multiple IP addresses to each logical VLAN interface. Repeat steps 6 and 7 for each IP address to assign to the same VLAN logical interface.

Deleting a VLAN Interface
1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the link for the physical interface for which to delete a VLAN interface in the Physical field.
   This action takes you to the physical interface page for the interface.
4. In the Logical Interface table, click Delete in the row for the logical VLAN interface to delete.
5. Click Apply.
6. Click Save to make your change permanent.
   The entry for the logical VLAN interface disappears from the Logical Interfaces table.

Defining the Maximum number of VLANs
1. Click Config on the home page.
2. Click the Interfaces link.
3. Enter a number in the Maximum number of vlans allowed text box.
   The maximum value is 1015.
4. Click Apply.
5. Click Save to make your change permanent.

VLAN Example Topology
The following topology represents a fully redundant firewall with load sharing and VLAN. Each Nokia appliance running Check Point FW-1 is configured with the Virtual Router Redundancy Protocol (VRRP). This protocol provides dynamic failover of IP addresses from one router to another in the event of failure. For more information see VRRP Description. Each appliance is configured with Gigabit Ethernet and supports multiple VLANs on a single cable. The appliances receive and forward VLAN-tagged traffic to subnets configured for VLAN, creating
a secure private network. In addition, the appliances are configured to create VLAN-tagged messages for output.

FDDI Interfaces

Configuring an FDDI Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: `fddi-s2p1`
4. Click Full or Half in the Physical Configuration table Duplex field.
5. Click Apply.

Note
Set device attached to a ring topology to half duplex. If the device is running in point-to-point mode, set the duplex setting to full. This setting must be the same for all hosts on the network to which the device connects.

6. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.
7. Enter the IP address for the device in the New IP address text box.

8. Enter the subnet mask length in the New mask length text box.
   
   Click Apply.
   
   Each time you click Apply, the configured IP address and mask length are added to the table. The entry fields remain blank to allow you to add more IP addresses.
   
   To enter another IP address and IP subnet mask length, repeat steps 6 through 7.

9. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.

10. Click Apply.

11. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   
   Click Apply.

12. Click Up to go the Interface Configuration page.

13. Click On button that corresponds to the logical interface you configured.
   
   Click Apply.
   
   The FDDI interface is now available for IP traffic and routing.

14. To make your changes permanent, click Save.

**Changing the Duplex Setting of an FDDI Interface**

**Note**

If the duplex setting of an FDDI interface is incorrect, it might not receive data, or it might receive duplicates of the data it sends.

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the physical interface link to change in the Physical column.
   
   Example:
   
   fddi-s2p1

4. Click Full or Half in the Physical Configuration table Duplex field.
   
   Click Apply.

**Note**

Set device attached to a ring topology to half duplex. If the device is running in point-to-point mode, set the duplex setting to full. This setting must be the same for all hosts on the network to which the device connects.
5. To make your changes permanent, click Save.

Changing the IP Address of an FDDI Interface

Note
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security appliance device with your browser.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical interface link for which to change the IP address in the Logical column.
   Example: fddi-s2p1c0
4. To remove the old IP address, click the delete check box that corresponds to the address to delete. Click Apply.
5. To add the new IP address, enter the IP address for the device in the New IP address text box.
6. Enter the subnet mask length in the New mask length text box. Click Apply.
   Each time you click Apply, the new IP address and mask length are added to the table. The entry fields remain blank to allow you to add more IP addresses.
7. To make your changes permanent, click Save.

FDDI Example

This section describes how you might configure the interfaces of your IP security appliance device in an example network, by using Network Voyager.

Before you can configure the device using Network Voyager, you must configure an IP address on one of the interfaces. You can do this through the console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the device through that interface. You can use any graphical web browser to configure the other interfaces on the device by entering the IP address of the device in the location field of the browser.
The following figure below shows the network configuration for this example.

In a company's main office, Nokia platform A terminates a serial line to an Internet service provider, running PPP with a keepalive value of 10.

Nokia platform A also provides internet access for an FDDI ring and a remote branch office connected through ATM PVC 93.

The branch office contains Nokia platform B, which routes traffic between a local Fast Ethernet network and ATM PVC 52. The branch office provides access to the main office and the Internet. This example configures the FDDI interface on Nokia platform A.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click fddi-s3p1 in the Physical column of the table.
4. Click Half to select the duplex setting.
5. Click Apply.
6. Click fddi-s3p1c0 in the logical interfaces table to go to the Interface page.
7. Enter 192.168.1.1 in the New IP address text box.
8. Enter 24 in the New mask length text box.
9. Click Apply.
10. Click Up to go to the Interfaces page.
11. Click On for fddi-s3p1c0.

12. Click Apply.

13. Click Save.

ISDN Interfaces

Integrated Services Digital Network (ISDN) is a system of digital phone connections that allows voice, digital network services, and video data to be transmitted simultaneously using end-to-end digital connectivity.

The Nokia IP Security Appliance offers support for an ISDN Basic Rate Interface (BRI) physical interface. The ISDN BRI comprises one 16 Kbps D-channel for signalling and control, and two 64 Kbps B-channels for information transfer. Nokia’s physical interface is certified to conform to the European Telecommunications Standards Institute (ETSI) ISDN standard.

The physical interface is the manageable representation of the physical connection to ISDN. One physical interface is visible in Network Voyager for every ISDN BRI card in the Nokia platform chassis. The physical interface enables management of the parameters specific to each ISDN connection. The physical interface permits enabling or disabling of the ISDN connection and is the entity under which logical interfaces are created.

The logical interface is the logical communication end point. It contains all information used to set up and maintain the ISDN call. The logical interface includes:

- Data link encapsulation and addressing
- Call connection information such as call direction, data rate, and the number to call
- Authentication information such as names, passwords, and authentication method
- Bandwidth allocation for Multilink PPP

After configuring the physical interface, then creating and configuring the logical interfaces, the Nokia platform is ready to make and accept ISDN calls. Detailed information on how to create and configure ISDN interfaces begins in “Configuring a Physical Interface.”

Features

The features that the ISDN interface supports are summarized below:

- **Port**—ISDN Basic Rate S/T interface with RJ45 connector
- **ISDN signaling**—ETSI EURO-ISDN (ETS 300 102)
- **B-channel protocols**—IETF PPP (RFC 1661 and 1662); IETF Multilink PPP (RFC 1990)
- **Security**—PAP (RFC 1334), CHAP (RFC 1994), and ISDN Caller ID
- **Dial-on-demand routing**—You can configure the ISDN interface so that only certain types of traffic establish and maintain an ISDN connection. Circuits are automatically removed if they are not required.
- **Dynamic bandwidth allocation**—You can configure the ISDN interface to add or remove additional bandwidth as the traffic requires it.
- **Multiple destination support**—You can configure the ISDN interface to connect to two different destinations simultaneously.
- **Dial-in support**—You can configure the ISDN interface to accept incoming calls from remote sites.

### Configuring a Physical Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column. Example:
   
isdn-s2p1
4. In the Switch Type pull-down menu, in the Physical Configuration table, select the service provider-switch type that corresponds to the interface network connection.
5. In the Line Topology field in the Physical Configuration table, click Point-to-Point or MultiPoint to describe the connection type of the interface.
6. Click Automatic or Manual in the TEI Option (terminal-endpoint identifier) field in the Physical Configuration table.
   
   Generally, automatic TEIs are used with multipoint connections, while fixed TEIs are used in point-to-point configurations.
7. Click Apply.
8. (Optional) If you selected Manual as the TEI option, enter the TEI assigned to the ISDN interface in the TEI field.
9. In the Physical Configuration table, click First-Call or PowerUp in the TEI Assign field to specify when the ISDN Layer 2 (TEI) negotiation to occur.
   
   - **First-Call**—ISDN TEI negotiation should occur when the first ISDN call is placed or received.
     
     The first-call option is mainly used in European ISDN switch types (for example, ETSI).
   - **PowerUp**—ISDN TEI negotiation should occur when the router is powered on.
10. Click Apply.
11. To make your changes permanent, click Save.

### Creating a Logical Interface

#### To Configure an ISDN Logical Interface to Place Calls

1. Click **CONFIG** on the home page.
2. Click the **Interfaces** link.
3. In the **PHYSICAL** column, click on the ISDN physical-name interface link to configure.
   Example: `isdn-s2p1`

4. In using the Encapsulation text box in the Create new Logical Interface table, select whether to run PPP or multilink PPP on the interface.
   Click Apply.
   A newly created logical interface appears in the Interface column of the Logical Interfaces table.

5. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

6. If the interface should be unnumbered, perform steps a and b. If the interface should be numbered, skip to step 7.
   In unnumbered mode the interface does not have its own unique IP address—the address of another interface is used.
   a. Click Yes next to Unnumbered interface.
   Click Apply.
   b. Use the Proxy interface pull-down menu to select the logical interface from which the address for this interface is taken.

7. Enter the IP address for the local end of the connection in the Local address text box in the Interface Information table.
   You must enter a valid IP address. IPSO does not support dynamically assigned IP addresses for ISDN interfaces. Do not enter 0.0.0.0.

8. Enter the IP address of the remote end of the connection in the Remote address text box in the Interface Information table.

9. (Optional) Enter a string comment in the Description text box in the Connection Information table to describe the purpose of the logical interface, for example, *Connection to Sales Office*.

10. Click Outgoing in the Connection Information table.

11. (Optional) Enter the value for the idle timeout in the Idle Time text box in the Connection Information table.
   This time entry defines the time in seconds that an active B-channel can be idle before it is disconnected. A value of zero indicates that the active B-channel will never disconnect. The range is 0 to 99999. The default value is 120.

12. (Optional) Enter the value for the minimum call time in the Minimum Call Time text box in the Connection Information table.
   This entry defines 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 the call can be disconnected immediately upon expiration of the idle timer. If the service provider has a minimum charge for each call, Nokia recommends the minimum call time be set to this value. The range is 0 to 99999. The default value is 120.
13. Click the 64 Kbps or 56 Kbps radio button in the Rate field in the Connection Information table to set the data rate for outgoing calls.

14. Enter values for a remote number and subaddress in the Remote Number and (optional) Remote Sub Number text boxes in the Connection Information table.

15. (Optional) Enter values for a calling number and subaddress in the Calling Number and Calling Sub Number text boxes in the Connection Information table.

   The calling number and subaddress are inserted in a SETUP message when an outgoing call is made.

**Note**

The Authentication table entries, which follow, allow the user to manage the parameters used to authenticate both ends of the communication link.

16. In the To Remote Host section of the Authentication table, in the Name text box, enter the name that needs to be returned to a remote host when it attempts to authenticate this host.

17. In the To Remote Host section of the Authentication table, in the Password text box, enter the password to be returned to the remote host for PAP authentication, or the secret used to generate the challenge response for CHAP authentication.

**Note**

The To Remote Host information must be the same as the From Remote Host information (or its equivalent) at the remote end of the link.

18. In the From Remote Host section of the Authentication table select the authentication method used to authenticate the remote host.

19. In the From Remote Host section of the Authentication table, in the Name text box, enter the name that will be returned from the remote host when this host attempts to authenticate the remote host.

20. In the From Remote Host section of the Authentication table, in the Password text box, enter a password to be returned by the remote host for PAP authentication, or the secret used to validate the challenge response for CHAP authentication.

**Note**

The From Remote Host information must be the same as the To Remote Host information (or its equivalent) at the remote end of the link.

**Note**

The Bandwidth Allocation table entries that follow allow the network administrator to manage the parameters that are used to determine when to add or remove an additional B-channel only when using Multilink PPP.
21. In the Bandwidth Allocation table, in the Utilization Level text box, enter a percentage bandwidth use level at which the additional B-channel is added or removed.
   
   When the measured use of an outgoing B-channel exceeds the utilization level threshold for a period greater than the use period, the second B-channel is brought into operation. When the outgoing B-channel use falls below the use level for a period greater than the value of the use period, the second B-channel is removed from operation.
   
   A use level of zero means that the second B-channel is never brought into operation. To bring the second B-channel into operation quickly, set the use level to a low number, such as one.

22. In the Bandwidth Allocation table, in the Utilization Period text box, enter the use period.
   
   This value specifies the number of seconds the outgoing B-channel use must remain above the use level before a second channel is brought into operation. When a second B-channel has been added, this value specifies the number of seconds that the use of the outgoing B-channel must be below the use level before the second B-channel is removed from operation.
   
   A use period set to zero will cause the second B-channel to be brought into operation immediately; the utilization level has been exceeded. It will also cause the second B-channel to be removed from operation; immediately the measured utilization drops below the use level.

23. Click Apply.

24. To make your changes permanent, click Save.

For troubleshooting information, see “ISDN Troubleshooting.”

To Configure an Interface to Receive Calls

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the physical interface to configure in the PHYSICAL column.
   
   Example: isdn-s2p1

4. Select whether to run PPP or multilink PPP on the interface from the Encapsulation text box in the Create New Logical Interface table; then click Apply.
   
   A new logical interface appears in the Interface column of the Logical Interfaces table.

5. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

6. Enter the IP address for the local end of the connection in the Local address text box in the Interface Information table.

7. Enter the IP address of the remote end of the connection in the Remote address text box in the Interface Information table.

8. Click Incoming in the Connection Information table.

9. Click Apply.
10. To configure the list of incoming numbers with permission to call into this interface, click the Incoming Numbers link.

**Note**
If no incoming call numbers are configured, all incoming calls will be accepted.

11. In the To Remote Host section of the Authentication table, in the Name text box, enter the name to be returned to a remote host when it attempts to authenticate this host.

12. In the To Remote Host section of the Authentication table, in the Password text box, enter the password to be returned to the remote host for PAP authentication, or the secret used to generate the challenge response for CHAP authentication.

**Note**
The To Remote Host information must be the same as the From Remote Host information (or its equivalent) at the remote end of the link.

13. In the From Remote Host section of the Authentication table select the authentication method used to authenticate the remote host.

14. In the From Remote Host section of the Authentication table, in the Name text box, enter the name that is returned from the remote host when this host attempts to authenticate the remote host.

15. In the From Remote Host section of the Authentication table, in the Password text box, enter a password to be returned by the remote host for PAP authentication, or the secret used to validate the challenge response for CHAP authentication.

**Note**
The From Remote Host information must be the same as the To Remote Host information (or its equivalent) at the remote end of the link.

16. To make your changes permanent, click Save.

For troubleshooting information, see “ISDN Troubleshooting.”

**To configure Calling Line-Identification Screening**

You can filter incoming calls to the Nokia platform by using the calling number in the received SETUP message. The network must support Calling Line Identification (CLID) to filter calls by using the calling number.

When an incoming call is received, the calling number in the received SETUP message is checked against the incoming numbers configured on each logical interface. The calling number is compared with each incoming call using the right-most-digits algorithm. A number matches if the shortest string between the received calling number and the incoming number is the same.
For example, if the calling number received was 345 and the logical interface has an incoming number of 12345, then this is deemed a match.

The call is answered on the interface that is configured with the incoming number with the highest number of matching digits. If no matching incoming number is found, the call is rejected.

If no incoming numbers are configured on an interface, any incoming call is deemed a match. Detailed information on how to add and delete incoming numbers to the logical interface follows.

**To Add an Incoming Number**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link in the Physical column.
   
   Example: isdn-s2p1
4. Click the logical interface link in the Logical Interfaces table.
5. Click the Incoming Numbers link.
6. In the Number text box, enter the telephone number on which to accept incoming calls; Click Apply.
   
   An x is used to represent a wild-card character.
7. Click Yes in the Callback field for the incoming call to be disconnected, and an outgoing call attempted; otherwise, click No to have the incoming call answered.
   
   If Callback is set to Yes, the Nokia platform uses the number in the Remote Number field on the logical interface to make the outgoing call.
8. If Callback is set to Yes, enter the value for the timeout in the timeout field.
   
   This is the amount of time (in seconds) that the Nokia platform waits before placing a call back to the remote system. The range is 0 to 999. The default is 15.
9. Click Apply.
10. To record your changes, click Save.

For troubleshooting information, see “ISDN Troubleshooting.”

**To Remove an Incoming Number**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link in the Physical column.
   
   Example:
   
   isdn-s2p1
4. Click the logical interface link in the Logical Interfaces table.
5. Click the Incoming Numbers link.
6. Find the incoming number to remove in the Numbers table, click its corresponding Delete button, and then click Apply.
7. To record your changes, click Save.

**To Configure an Interface to Place and Receive Calls**
1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   
   *Example:* isdn-s2p1
4. Select whether to run PPP or multilink PPP on the interface from the Encapsulation text box in the Create New Logical Interface section.
   
   Click Apply.
   
   A new logical interface appears in the Interface column.
5. Click the logical interface name in the Interface column of the Logical interfaces table to go to the *Interface* page.
6. Enter the IP address for the local end of the connection in the Local address text box.
7. Enter the IP address of the remote end of the connection in the Remote address text box.
8. Click Both Direction.
9. Click Apply.

---

**Note**
Follow steps 8 through 21 in “To Configure an ISDN Logical Interface to Place Calls” to set the information for outgoing calls.
For more information about how to set up incoming numbers see “To Add an Incoming Number”.

---

10. To make your changes permanent, click Save.
For troubleshooting information, see “ISDN Troubleshooting.”

**To Delete a Logical Interface**
1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link in the Physical column.
   
   *Example:* isdn-s2p1
4. Find the logical interface to remove in the Logical Interfaces table and click the corresponding Delete button. Click Apply.

5. To make your changes permanent, click Save.

**Dial-on-Demand Routing Lists**

As ISDN connections attract charges to establish and maintain connections, it is useful to have only certain types of packets cause the connection to be set up. It is also useful to have timers determine how long the connection should be maintained in the absence of these packets.

A Dial-on-Demand Routing (DDR) list is used to determine the packets that should bring up and maintain an ISDN connection. This section explains how to configure DDR lists for ISDN interfaces. To aid in the discussion of DDR lists, packets that establish and maintain a connection are called “interesting.”

A DDR list is composed of one or more rules that are used to determine if a packet is interesting. Each rule has a set of values used to match a packet and an action to take when a match occurs. The following are the possible actions:

- **Accept**—this is an interesting packet.
- **Ignore**—this is not an interesting packet.
- **Skip**—this rule is ignored.

When a packet matches a rule in the DDR list with an accept action, that packet is regarded as interesting. An interesting packet causes the ISDN interface to set up a call by using the is passed over the interface. The traffic passed could include traffic, which configured in the DDR list, with an “ignore” action. If no packets that match an accept rule in the DDR list are transmitted in the configured idle time, the connection is automatically disconnected. A DDR list is created with a default rule that matches all packets. The associated action is accept. This action can be set to skip so that all unmatched packets are deemed uninteresting.

**Note**

Setting a rule to skip effectively turns the rule off.

It is important to understand the difference between Access lists and DDR lists and how the two interoperate. When a packet is sent over an interface, any Access list applied to that interface is checked first. If the packet matches any rule in the Access list, the associated action is taken. Therefore, if the packet matched a rule in the Access list that had an associated action of drop, the packet is never sent over the ISDN interface. After the packet is checked against the Access list, the DDR list applied to the interface (if any) is then checked.
Creating a DDR List
1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Enter a name for the DDR list in the Create New DDR List text box.
   Click Apply.
   The DDR list name, Delete check box, and Add Interfaces drop-down window will appear.
   Only the default rule will display in the DDR list until you create your own rule.
4. To make your changes permanent, click Save.

Deleting a DDR List
1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Click the Delete check box next to the DDR list name to delete; then click Apply.
   The DDR list name disappears from the DDR List Configuration page.
4. To make your changes permanent, click SAVE.

Adding a New Rule to a DDR List
1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Locate the DDR list to which to add the new rule.
4. Click the Add New Rule Before check box.
   Click Apply.
   The new rule appears above the default rule.
Note
When you create more rules, you can add rules before other rules. For example, if you have four rules—rules 1, 2, 3, and 4—you can place a new rule between rules 2 and 3 by checking the Add Rule Before check box on rule 3.

5. To make your changes permanent, click SAVE.

Modifying a Rule

1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Locate the DDR list that contains the rule to modify.
   You can modify the following items:
   - Action
   - Source IP address
   - Source mask length
   - Destination IP address
   - Destination mask length
   - Source port range
     You can specify the source port range only if the selected protocol is either “any,” “6,” “TCP,” “17,” or “UDP.”
   - Destination port range
     You can specify the destination port range only if the selected protocol is either “any,” “6,” “TCP,” “17,” or “UDP.”
   - Protocol
4. Modify the values in one or more of the text boxes or drop-down window or deselect a button.
   Click Apply.
5. To make your changes permanent, click Save.

Deleting a Rule

1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Locate the DDR list that contains the rule to delete.
4. Click the Delete check box next to the rule to delete.
   Click Apply.
5. To make your changes permanent, click Save.
Applying a DDR List to an Interface
1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Locate the appropriate DDR list.
4. Select the appropriate interface from the Add Interfaces drop-down window.
   Click Apply.
   The new interface appears in the Selected Interfaces section.
5. To make your changes permanent, click Save.

Removing a DDR List from an Interface
1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Locate the appropriate DDR list.
4. Click the Delete check box next to the interface under the Selected Interfaces section to remove.
   Click Apply.
   The interface disappears from the Selected Interfaces section.
5. To make your changes permanent, click Save.

Example DDR List
The following example illustrates how to configure a DDR list so that RIP packets do not cause an ISDN connection to be established nor keep an active connection running. RIP packets can, however, be exchanged over an established ISDN connection.

The DDR list is added to the isdn-s2p2c1 ISDN interface.
1. Click Config on the home page.
2. Click the Dial on Demand Routing Configuration link under the Traffic Management section.
3. Enter NotRIP in the Create New DDR List text box.
   Click Apply.
4. Under the Existing rules for NotRIP table, click the Add New Rule Before check box.
   Click Apply.
5. Enter 520 in the Dest Port Range text box in the Existing rules for NotRIP table.
7. Select isdn-s2p1c1 from the Add Interfaces drop-down window.
ISDN Network Configuration Example

The following figure shows the network configuration for the example explained below.

A Nokia Security Platform IP330 at a remote branch office connects to a Nokia Security Platform IP650 in a company’s main office through ISDN by using PPP.

Considering the nature of the traffic being transmitted and the charging rates on an ISDN network, the ISDN interface on the Nokia IP330 in this example has its minimum-call timer set to four minutes and its idle timer set to one minute. The Nokia IP330 is configured to send a username and password to the main office.

The Nokia IP650 is configured so that only incoming calls that originate from the Nokia IP330 is answered. The PPP connection is in this example, the default values for the ISDN interface are acceptable. Therefore, no configuration of the physical interface is required.

Configuring the IP330 to Place an Outgoing Call

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click isdn-s2p1 in the Physical column of the table.
4. Select PPP from the Encapsulation text box in the Create New Logical Interface table. Click Apply.
A new logical interface appears in the Interface column of the Logical Interfaces table.

5. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

6. Enter 206.226.15.2 in the Local Address text box in the Interface Information table.

7. Enter 206.226.15.1 in the Remote Address text box in the Interface Information table.

8. In the Connection Information table, enter Main Office in the Description text box so that the connection is easily identified.

9. Check Outgoing.

10. Enter 60 in the Idle Time text box in the Connection Information table.

11. Enter 240 in the Minimum Call Time text box in the Connection Information table.

12. Enter the number 384020 in the Remote Number text box in the Connection Information table.

13. Enter User in the Name text box under the To Remote Host heading in the Authentication table.

14. Enter Password in the Password text box under the To Remote Host heading in the Authentication table.

15. Click Apply.

16. Click Save.

Configuring the IP650 to Handle an Incoming Call

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click isdn-s4p1 in the Physical column of the table.

4. Select PPP from the Encapsulation text box in the Create New Logical INTERFACE table.
   Click Apply.
   A new logical interface appears in the Interface column of the Logical Interfaces table.

5. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

6. Enter 206.226.15.1 in the Local Address text box in the Interface Information table.

7. Enter 206.226.15.2 in the Remote Address text box in the Interface Information table.

8. In the Connection Interface table, enter Remote Office in the Description text box so that the connection is easily identified.

9. Click Incoming.

10. Select CHAP as the authentication method in the Authentication table.

11. Enter User in the Name text box under the From Remote Host section in the Authentication table.
12. Enter Password in the Password text box under the From Remote Host section in the Authentication table.

13. Click Apply.

14. Click the Incoming Numbers link.

15. Enter 384000 in the Number text box under the Add Incoming Call Information section.

16. Click Apply.

17. Click Save.

Sample Call Traces

Sample traces for call setup between the Nokia IP Security platform follow. The traces were produced by issuing the following command on each device: "tcpdump -i <interface>.” Traffic was generated by doing a “ping 206.226.15.1” on the Nokia IP330.

Note

To display the negotiated PPP values, run the tcpdump command with the -v switch.

The trace for connecting a call from the Nokia IP330 is:

```
06:23:45.186511 O > PD=8 CR=23(Orig) SETUP:Bc:88 90.
CalledNb:80 33 38 34 30 32 30.SendComp:
06:23:45.255708 I < PD=8 CR=23(Dest) CALL-PROC:ChanId:89.
06:23:45.796351 I < PD=8 CR=23(Dest) ALERT:
06:23:45.832848 I < PD=8 CR=23(Dest) CONN:DateTime:60 06 05 05 2d.
06:23:45.833274 O B1: ppp-lcp: conf_req(mru, magicnum)
06:23:45.971476 I B1: ppp-lcp: conf_req(mru, authtype, magicnum)
06:23:45.971525 O B1: ppp-lcp: conf_ack(mru, authtype, magicnum)
06:23:49.070050 O B1: ppp-lcp: conf_req(mru, magicnum)
06:23:49.078165 I B1: ppp-lcp: conf_ack(mru, magicnum)
06:23:49.085662 I B1: challenge, value=0311bb3b42dec57d1108c728e575 ecc22ddf0a06b3d0b1fe46687c970bb91fa4688d417bf72a0bca572c7e4e16, name=
06:23:49.085729 O B1: response,
value=dd379d2b5e692b6afe2bee361e32bca, name=User
06:23:49.094922 I B1: success
06:23:49.094969 O B1: ppp-ipcp: conf_req (addr)
06:23:49.097161 I B1: ppp-ipcp: conf_req (addr)
06:23:49.097194 O B1: ppp-ipcp: conf_ack (addr)
```
06:23:49.102200 O B1: 206.226.15.2 > 206.226.15.1: icmp: echo request
06:23:49.102224 O B1: 206.226.15.2 > 206.226.15.1: icmp: echo request
06:23:49.102241 O B1: 206.226.15.2 > 206.226.15.1: icmp: echo request
06:23:49.102257 O B1: 206.226.15.2 > 206.226.15.1: icmp: echo request
06:23:49.128295 I B1: 206.226.15.1 > 206.226.15.2: icmp: echo reply
06:23:49.139918 I B1: 206.226.15.1 > 206.226.15.2: icmp: echo reply
06:23:49.151558 I B1: 206.226.15.1 > 206.226.15.2: icmp: echo reply
06:23:49.163297 I B1: 206.226.15.1 > 206.226.15.2: icmp: echo reply
06:23:49.220161 O B1: 206.226.15.2 > 206.226.15.1: icmp: echo request
06:23:49.246309 I B1: 206.226.15.1 > 206.226.15.2: icmp: echo reply

The trace for receiving an incoming on IP650 follows:

15:10:09.141877 I < PD=8 CR=36(Orig) SETUP:SendComp:Bc:88
90.ChanId:89.CallingNb:00 83 33 38 34 30 30.CalledNb:80 33 38 34 30 32 30.
15:10:09.186313 O > PD=8 CR=36(Dest) CONN:
15:10:09.250372 I < PD=8 CR=36(Orig) CONN ACK:
15:10:09.425571 O B1: ppp-lcp: conf_req(mru, authtype, magicnum)
15:10:09.434996 I B1: ppp-lcp: conf_ack(mru, authtype, magicnum)
15:10:12.420103 O B1: ppp-lcp: conf_req(mru, authtype, magicnum)
15:10:12.532897 I B1: ppp-lcp: conf_req(mru, magicnum)
15:10:12.533133 O B1: challenge,value=0311bb3b42dec57d1108c728e575ecc22ddf0a06b30b1fe46687c970bb
91fa4688d417bf72a0bca572c7e4e16, name=15:10:12.549898 I
B1:response,value=dd379d2b5e692b6afef2bee361e32bca, name=User
15:10:12.549968 O B1: success
15:10:12.573896 I B1: 206.226.15.2 > 206.226.15.1: icmp: echo request
ISDN Troubleshooting

Logging

ISDN sends messages to the system message log. Whether a message is sent to the log or not depends on the logging setting of the ISDN interface. A log message can be generated in the following ways:

- **Error**—an error condition occurred
- **Warning**—a warning condition
- **Informational**—a normal event of note

Setting a logging to a particular level means all messages of this severity and higher are sent to the message log. For example, if you set logging to Error, all error messages are sent to the message log.

ISDN logs messages for the following informational events:

- ISDN layer 1 protocol activated or deactivated
- Expiration of layer 1, layer 2, and layer 3 timers
- An attempted outgoing call
- An incoming call being received
- A call being connected
- A call being disconnected

Setting Level of Messages to be Logged

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column. *Example:* isdn-s2p1
4. From the pull-down menu in the **LOGGING** field, select the level of messages for ISDN to log.
   
   All messages of this level and below are sent to the message log.

Viewing the Message Log

1. Click Monitor on the home page.
2. Click the View Message Log link under the System logs heading.
   
   The most recent system log messages appear.

Tracing

You can use the tcpdump utility to trace ISDN D-channel traffic (Q.921 and Q.931 protocols) and B-channel traffic (PPP/multilink PPP and TCP/IP protocols).
When running tcpdump on an ISDN interface, if no options are given on the command line, the following messages are decoded and displayed:

- Q.931 messages
- PPP messages and the fields inside them
- Any IP traffic on the B-channels

If the -e option is specified on the command line, in addition to the preceding messages, all Q.921 messages are also decoded and displayed.

If the -v option is used, Q.931 messages are displayed. Also the fields in all PPP messages and their values are displayed in an extended format.

**Tracing ISDN Traffic Using tcpdump**

1. Create a telnet session and log in to the firewall.
2. Enter `tcpdump -i <isdn-interface>`

**Troubleshooting Cause Codes**

Use the following debug commands to display the ISDN cause code fields in the following table:

```
i=0xy1y2z1z2a1a2
```

**ISDN Cause Code Fields**

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>y1</td>
<td>8 - ITU-T standard coding</td>
</tr>
<tr>
<td>y2</td>
<td>0 - User</td>
</tr>
<tr>
<td></td>
<td>1 - Private network serving local user</td>
</tr>
<tr>
<td></td>
<td>2 - Public network serving local user</td>
</tr>
<tr>
<td></td>
<td>3 - Transit network</td>
</tr>
<tr>
<td></td>
<td>4 - Public network serving remote user</td>
</tr>
<tr>
<td></td>
<td>5 - Private network serving remote user</td>
</tr>
<tr>
<td></td>
<td>7 - International network</td>
</tr>
<tr>
<td>z1</td>
<td>A - Network beyond internetworking point</td>
</tr>
<tr>
<td>z2</td>
<td>Class of cause value</td>
</tr>
<tr>
<td>a1</td>
<td>Value of cause value</td>
</tr>
<tr>
<td></td>
<td>(Optional) Diagnostic field that is always 8</td>
</tr>
</tbody>
</table>
ISDN Cause Values

Descriptions of the cause-value field of the cause-information element are shown in the following ISDN cause value table. Cause-value numbers are not consecutive.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Cause Description</th>
<th>Diagnostics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unallocated (unassigned) number</td>
<td>Note 12</td>
</tr>
<tr>
<td>2</td>
<td>No route to specified transit network</td>
<td>Transit-network identity (Note 11)</td>
</tr>
<tr>
<td>3</td>
<td>No route to destination</td>
<td>Note 12</td>
</tr>
<tr>
<td>6</td>
<td>Channel unacceptable</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Call awarded and being delivered in an established channel</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Normal call clearing Note 12</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>User busy</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>No user responding</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>No answer from user (user alerted)</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Call rejected</td>
<td>User-supplied diagnostic (Notes 4 &amp; 12)</td>
</tr>
<tr>
<td>22</td>
<td>Number changed</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Non-selected user clearing</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Designation out of order</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Invalid number format</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Facility rejected</td>
<td>Facility identification (Note 1)</td>
</tr>
<tr>
<td>30</td>
<td>Response to STATUS ENQUIRY</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Normal, unspecified</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>No circuit or channel available</td>
<td>Note 10</td>
</tr>
<tr>
<td>38</td>
<td>Network out of order</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Temporary failure</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Switching-equipment congestion</td>
<td></td>
</tr>
</tbody>
</table>

a2  (Optional) Diagnostic field that is one of the following values: 0 is Unknown, 1 is Permanent, and 2 is Transient
<table>
<thead>
<tr>
<th>Cause</th>
<th>Cause Description</th>
<th>Diagnostics</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>Access information discarded</td>
<td>Discarded information-element identifier(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Note 6)</td>
</tr>
<tr>
<td>44</td>
<td>Requested circuit / channel not available</td>
<td>Note 10</td>
</tr>
<tr>
<td>47</td>
<td>Resources unavailable or unspecified</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Quality of service unavailable.</td>
<td>See ISDN Cause Values table.</td>
</tr>
<tr>
<td>50</td>
<td>Requested facility not subscribed</td>
<td>Facility identification (Note 1)</td>
</tr>
<tr>
<td>57</td>
<td>Bearer capability not authorized</td>
<td>Note 3</td>
</tr>
<tr>
<td>58</td>
<td>Bearer capability not presently available</td>
<td>Note 3</td>
</tr>
<tr>
<td>63</td>
<td>Service or option not available or specified</td>
<td>Note 3</td>
</tr>
<tr>
<td>65</td>
<td>Bearer capability not implemented</td>
<td>Note 3</td>
</tr>
<tr>
<td>66</td>
<td>Channel type not implemented</td>
<td>Channel Type (Note 7)</td>
</tr>
<tr>
<td>69</td>
<td>Requested facility not implemented</td>
<td>Facility Identification (Note 1)</td>
</tr>
<tr>
<td>70</td>
<td>Only restricted digital-information bearer is available</td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>Service or option not available or specified</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>Invalid call-reference value</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>Identified channel does not exist</td>
<td>Channel identity</td>
</tr>
<tr>
<td>83</td>
<td>A suspended call exists, but call identity does not exist</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>Call identity in use</td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>No call suspended</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Call having the requested-call identity has been cleared</td>
<td>Clearing cause</td>
</tr>
<tr>
<td>88</td>
<td>Incompatible destination</td>
<td>Incompatible parameter (Note 2)</td>
</tr>
<tr>
<td>91</td>
<td>Invalid transit-network selection</td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>Invalid message, unspecified</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>Mandatory information element is missing</td>
<td>Information-element identifiers is missing</td>
</tr>
<tr>
<td></td>
<td>Information element identifiers</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>Message type non-existent or not implemented</td>
<td>Message type</td>
</tr>
</tbody>
</table>
1. The coding of facility identification is network dependent.

2. Incompatible parameter is composed of incompatible information element identifier.

3. The format of the diagnostic field for cause 57, 58, and 65 is shown in the ITU-T Q.931 specification.

4. User-supplied diagnostic field is encoded according to the user specification, subject to the maximum length of the cause-information element. The coding of user-supplied diagnostics should be made in such a way that it does not conflict with the coding described in Table B-2.

5. New destination is formatted as the called-party number information element, including information element identifier. Transit network selection might also be included.

6. Locking and non-locking shift procedures described in the ITU-T Q.931 specification apply. In principle, information element identifiers are in the same order as the information elements in the received message.

7. The following coding applies:
   - Bit 8, extension bit
   - Bits 7 through 5, spare
   - Bits 4 through 1, according to Table 4-15/Q.931 octet 3.2, channel type in ITU-T Q.931 specification.

8. When only the locking shift-information element is included and no variable length information-element identifier follows, it means that the codeset in the locking shift itself is not implemented.

9. The timer number is coded in IA5 characters.
   The following coding is used in each octet:

<table>
<thead>
<tr>
<th>Cause</th>
<th>Cause Description</th>
<th>Diagnostics</th>
</tr>
</thead>
<tbody>
<tr>
<td>98</td>
<td>Message not compatible with call state or message type or not implemented</td>
<td>Message type non-existent</td>
</tr>
<tr>
<td>99</td>
<td>Information-element non-existent or not implemented</td>
<td>Information-element identifiers not implemented (Notes 6 &amp; 8)</td>
</tr>
<tr>
<td>100</td>
<td>Invalid-information element</td>
<td>Information-element identifiers contents (Note 6)</td>
</tr>
<tr>
<td>101</td>
<td>Message not compatible with call</td>
<td>Message type state</td>
</tr>
<tr>
<td>102</td>
<td>Recovery on timer expires</td>
<td>Timer number (Note 9)</td>
</tr>
<tr>
<td>111</td>
<td>Protocol error, unspecified</td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>Internetworking, unspecified</td>
<td></td>
</tr>
</tbody>
</table>
- Bit 8, Spare “0”
- Bits 7 through 1, IA5 character

10. Examples of the cause values to be used for various busy or congested conditions appear in Annex J of the ITU-T Q.931 specification.

11. The diagnostic field contains the entire transit network selection or network-specific facilities information element, as applicable.

12. For the coding that is used, see ISDN Cause Codes table.

**ISDN Bearer-Capable Values**

The ISDN bearer-capability values that display in the SETUP packet using the tracing tcpdump command follows:

- 0x8890 for 64 Kbps
- 0x218F for 56 Kbps

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>ITU-T coding standard; unrestricted digital information</td>
</tr>
<tr>
<td>90</td>
<td>Circuit mode, 64 Kbps</td>
</tr>
<tr>
<td>21</td>
<td>Layer 1, V.110 / X.30</td>
</tr>
<tr>
<td>8F</td>
<td>Synchronous, no in-band negotiation, 56 Kpbs</td>
</tr>
</tbody>
</table>

**Token Ring Interfaces**

**Configuring a Token Ring Interface**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   - Example: tok-s3p1
   - The physical interface setup page appears.
4. In the Ring Speed column of the Physical configuration table, select the desired value: 16 Mbit/sec or 4 Mbit/sec.
   - There is no default value.
5. In the MTU field, enter the desired value.
   - The minimum for both ring speeds is 560. The maximum MTU for 4 Mbs is 4442, and the maximum MTU for 16 Mbs is 17792.
6. In the Allow Source routes (Multi-Ring) field, select On or Off. 
   Default is On. This feature specifies whether or not to support source routes.

7. In the Select Use Broadcast instead of Multicast field, select On or Off. 
   Default is Off. This option specifies the mapping of an IP multicast address. When the option is on, it maps a multicast address to an all-ring broadcast address: [ff:ff:ff:ff:ff:ff]. When the option is off, it maps a multicast IP address to an IEEE-assigned IP multicast group address: [noncanonical form: c0:00:00:04:00:00].

8. Click the logical interface name in the Interface column of the Logical interfaces table to go to the Interface page.

9. In the Active column of the Logical interfaces table, select On or Off.
   Default is On. This setting enables or disables the logical interface. Use this switch to control access to the network or virtual circuit that corresponds to the logical interface.

10. Click Apply.
   Click Up to return to the interface configuration page.

11. Click the logical interface link to configure in the Logical column.

   Example: tok-s3p1c0

   The logical interface setup page appears.

12. Enter the IP address for the device in the New IP address text box.

13. Enter the IP subnet mask length in the New mask length text box.

   Click Apply.

   Each time you click Apply, the configured IP address and mask length are added to the table. The entry fields remain blank to allow you to add more IP addresses.

   To enter another IP address and IP subnet mask length, repeat steps 12 through 13.

14. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.

   Click Apply.

15. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.

   Click Apply.

16. To make your changes permanent, click Save.

**Deactivating a Token Ring Interface**

1. Click Config on the home page.

2. Click the Interfaces link.

3. In the Active column of the interface to deactivate, click off.

4. Click Apply.
5. Click Save.

**Changing a Token Ring Interface**

1. Click Config on the home page.
2. Click the Interfaces link.
3. In the Physical column, click the physical interface link to change.
   To change only the properties of a logical interface, proceed to Step 6.
   
   **Example:** tok-s3p1
   
   The physical interface setup page appears.
4. Perform the following procedures to make the desired changes.
   If no change is desired, skip the step.
   
   **a.** In the Ring Speed column of the Physical configuration table, select the desired value: 16 Mbit/sec or 4 Mbit/sec. There is no default value.
   
   **b.** In the MTU field, enter the desired value. The minimum for both ring speeds is 560. The maximum MTU for 4 Mbs is 4442, and the maximum MTU for 16 Mbs is 17792.
   
   **c.** In the Allow Source routes (Multi-Ring) field, select On or Off. Default is On.
   
   **d.** In the Select Use Broadcast instead of Multicast, select On or Off. Default is Off.
   
   **e.** In the Active column of the Logical interfaces table, select On or Off. Default is On.
5. Click Apply.
   Click Up to return to the interface configuration page.
6. **(Optional)** To change a logical interface link, click the logical interface link to change in the Logical column.
   **Example:** tok-s3p1c0
   
   The logical interface setup page appears.
7. Perform the following procedures to make the desired changes.
   If no change is desired, skip the step.
   
   **a.** To change the IP address, enter the appropriate IP address in the New IP address field.
   There is no default.
   
   **b.** In the New mask length field, enter the appropriate value. The range is 8 to 30, and there is no default.
   
   **c.** To delete an IP address, click the Delete box.

**Note**

Changing an IP address and deleting an IP address at the same time prevents multiple addresses from being assigned to a single interface.
8. Click Apply.
9. Click Save.

**Token Ring Example**

This section describes how you might use Network Voyager to configure the interfaces of your IP security platform (unit) in an example network.

Before you can configure interfaces by using Network Voyager, you must first configure an IP address on one of the interfaces. You can do this through the unit console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the device through that interface. You can use any graphical web browser to configure the other interfaces on the device by entering the IP address of the device in the location field of the browser.

In a company’s main office, IP650 A terminates a serial line to an Internet service provider, running PPP with a keepalive value of 10.

IP650 A also provides internet access for an FDDI ring and a remote branch office connected with token ring.

The branch office contains IP650 B, which routes traffic between a local fast Ethernet network and a token ring. IP650 B provides access to the main office and the Internet. This example configures the token ring interface on IP650 A.
The following figure shows the network configuration for this example.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Select tok-s2p1 in the Physical column of the table.
4. Set the desired value in the Ring Speed column of the Physical configuration table.

**Note**
This setting must be the same for all hosts on the network to which the device connects.

5. Enter the desired MTU value.
6. In the Allow Source routes (Multi-Ring) field, select On or Off.
7. In the Select Use Broadcast instead of Multicast, select On or Off.
8. Under the Active column of the Logical interfaces table, select On or Off.
9. Click Apply.
   Click Up to return to the interface configuration page.
10. Click the logical interface link to configure in the Logical column.
11. In the New IP address field, enter the appropriate IP address.
12. In the New mask length field, enter the appropriate value.
13. Click Apply.
14. Click Save.

**Point-to-Point Link over ATM**

**Configuring an ATM Interface**

**Note**

An ATM interface cannot be configured with an IP address until at least one logical interface is created for the interface.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column on the *Interface Configuration* page.

   **Example:** atm-s2p1

   The *Physical Interface* page is displayed.

4. Select SONET or SDH as the framing format in the Physical Configuration table.

   **Note**

   SONET and SDH settings are available only if the ATM interface card supports them.

   The setting should match the type of transmission network to which the interface is connected.

5. Select Freerun or Loop Timing as the transmit clock choice in the Physical Configuration table.

   **Note**

   The Transmit Clock settings are available only if the ATM interface card supports them.

   Freerun uses the internal clock. If two ATM interfaces are directly connected, at least one of them must use the internal clock.

   Loop timing derives the transmit clock from the recovered receive clock.

6. Select the VPI/VCI range in the VPI/VCI Range Configuration list box.
7. Select point-to-point in the Type list box in the Create a new LLC/SNokia Platform RFC1483 interface section.
   Enter the VPI/VCI number in the VPI/VCI text box.
   Click Apply.
   A new logical interface appears in the Interface column. The new interface is on by default.
   You can add more ATM logical interfaces by repeating this step.
8. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Logical Interface page.
9. Enter the IP address for the local end of the PVC in the Local Address text box.
10. Enter the IP address of the remote end of the PVC in the Remote Address text box.
    Click Apply.
11. Enter a number in the IP MTU text box to configure the device’s maximum length (in bytes) of IP packets transmitted in this interface. Click Apply.
    The default value is 1500.

   **Note**
   The maximum packet size must match the MTU of the link partner.

12. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical Name text box.
    Click Apply.
13. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
    Click Apply.
14. To make your changes permanent, click Save.

### Changing the VPI/VCI of an ATM Interface

**Note**
To move an IP address from one PVC to another, you must first delete the logical interface for the old PVC, then create a new logical interface for the new PVC.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: atm-s2p1
4. Find the ATM logical interface you wish to remove in the Logical Interfaces table and click the corresponding Delete button.
   Click Apply.
   The logical interface disappears from the list. Any IP addresses configured on this interface are also removed.

5. Select the VPI/VCI range in the VPI/VCI Range Configuration selection box.

6. Select point-to-point in the Type selection box in the Create a new LLC/SNokia Platform RFC1483 interface section. Enter the VPI/VCI number in the VPI/VCI text box.
   Click Apply.
   A new logical interface appears in the Interface column. The new interface is turned on by default.

7. Click the logical interface name in the Interface column of the Logical Interfaces table to go the Interface page.

8. Enter the IP address for the local end of the PVC in the Local Address text box.

9. Enter the IP address of the remote end of the PVC in the Remote Address text box.
   Click Apply.

10. (Optional) Enter the desired value in the IP MTU text box.
    Click Apply.

11. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical Name text box.
    Click Apply.

12. To make your changes permanent, click Save.

**Changing the IP Address of an ATM Interface**

**Note**
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security platform (unit) with your browser.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical interface link for which to change the IP address in the Logical column.
   *Example:* atm-a2p1c8
4. Delete the current addresses from the Local Address and Remote Address text boxes, and replace with new address entries.
   Click Apply. The original MTU value is retained.
5. To make your changes permanent, click Save.
Changing the IP MTU of an ATM Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. In the Logical column, click the Logical interfaces link for the item on which to change the IP address.
   Example: atm-s2p1
4. Enter a number in the IP MTU text box to configure the device’s maximum length (in bytes) of IP packets transmitted on this interface.
   Click Apply.

Note
The maximum packet size must match the MTU of the link partner. Packets longer than the length you specify are fragmented before transmission.

5. To make your changes permanent, click Save.

Removing an ATM Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link in the Physical column on the Interface Configuration page.
   Example: atm-s2p1
4. Find the ATM logical interface to remove in the Logical Interfaces table and click the corresponding Delete button.
   Click Apply.
   The ATM logical interface disappears from the list.
5. To make your changes permanent, click Save.

ATM Example

This section describes how you might configure the interfaces of your IP security platform in an example network, using Nokia Network Voyager.

Before you can configure interfaces by using Network Voyager, you must first configure an IP address on one of the interfaces. You can do this through the console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the device through that interface. You can use any graphical web browser to configure the other interfaces on the device by entering the IP address of the device in the location field of the browser.
The following figure shows the network configuration for this example.

![Network Configuration Diagram]

In a company’s main office, Nokia Platform A terminates a serial line to an Internet service provider, running PPP with a keepalive value of 10.

Nokia Platform A also provides internet access for an FDDI ring and a remote branch office connected through ATM PVC 93.

The branch office contains Nokia Platform B, which routes traffic between a local fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. This example configures the ATM interface on Nokia Platform A.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Select atm-s2p1 in the Physical column of the table.
4. Enter 93 in the VCI text box in the Create a new LLC/SNokia Platform RFC1483 interface section.
   
   The channel number of the interface is no longer the VCI number but an automatically allocated number. Therefore, the logical name of the interface in step 6 is something that depends on what other logical ATM interfaces there are. Find the newly created interface from the table before you continue.

   Click Apply.

5. Click atm-s2p1c93 in the Logical Interfaces table to go to the Interface page.
6. Enter 192.168.3.2 in the Local Address text box.
7. Enter 192.168.3.1 in the Remote Address text box.
8. Click Apply.
9. Enter 9180 in the IP MTU text box.
10. Click Apply.
11. Click Save.

**Note**
The steps for configuring the ATM interface on Nokia Platform B are the same except that you should set the VPI to 52 when you create the logical interface and reverse the IP addresses should be reversed.

---

**IP over ATM (IPoA)**

**Configuring an ATM Logical IP Subnet (LIS) Interface**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   
   Example: atm-s2p1
   
   You are taken to the Physical Interface page.
4. Select SONET or SDH as the framing format in the Physical Configuration table.
   The setting should match the type of transmission network to which the interface is connected.
5. Select Freerun or Loop Timing as the transmit clock choice in the Physical Configuration table.
   Freerun uses the internal clock. If two ATM interfaces are directly connected, at least one of them must use the internal clock.
   Loop timing derives the transmit clock from the recovered receive clock.
6. Select the VPI/VCI range in the VPI/VCI Range Configuration list box.
7. Create a logical interface with the Create a new LLC/SNokia Platform RFC1483 interface section by selecting LIS in the Type list box and entering the set of VPI/VCI numbers that the interface in the VPI/VCI text box will use.
   The set of VPI/VCIs can be given as a comma-separated list of VPI/VCIs or VPI/VCI ranges such as 1/42, 1/48, 1/50 to 60.
8. Click Apply.
A new logical interface appears in the Interface column. The new interface is on by default. You can create multiple logical interfaces by repeating steps 6 through 7.

9. Click the logical interface name in the Interface column of the Logical Interfaces table to reach the Logical Interface page.

10. Enter the IP address of the interface in the IP Address text box.

11. Enter the IP subnet mask length in the Mask Length text box.

12. Enter a number in the IP MTU text box to configure the device’s maximum length (in bytes) of IP packets transmitted in this interface.
   The default value and range depend on the hardware configuration. The standard value is 9180.
   Click Apply.

**Note**
All hosts in the same LIS must use the same IP MTU in their interface to the LIS.

13. (Optional) Change the interfaces logical name to a more meaningful one by typing the preferred name in the Logical name text box.
   Click Apply.

14. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   Click Apply.

15. To make your changes permanent, click Save.

### Changing the VPI/VCIs of an ATM LIS Interface

**Note**
Do not change the VCI address of the connection you are using. If you do, you can no longer access the IP security platform with your browser.

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the physical interface link to configure in the Physical column.
   Example: atm-a2p1
   You are taken to the Physical Interface page.

4. Select the VPI/VCI range in the VPI/VCI Range Configuration list box.

5. Find the ATM logical interface to reconfigure in the Logical Interfaces table and enter a new set of VPI/VCIs in the VPI/VCI field.
Changing the IP Address of an ATM LIS Interface

**Note**
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security platform with your browser.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical interface link for which to change the IP address in the Logical column.
   
   Example: atm-s2p1c8
   
   You are taken to the Logical Interface page.
4. Enter the IP address for the interface in the IP Address text box.
5. Enter the IP subnet mask length in the Mask Length text box.
6. Click Apply.
7. To make your changes permanent, click Save.

Changing the IP MTU of an ATM Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. In the Logical column, click the Logical interface link for the item on which to change the IP MTU.
   
   Example: atm-s2p1c8
4. Enter a number in the IP MTU text box to configure the devices maximum length (in bytes) of IP packets transmitted on this interface.
   
   Click Apply.

**Note**
All hosts in the same LIS must use the same IP MTU in their interface to the LIS.

**Note**
Packets longer than the length you specify are fragmented before transmission.

5. To make your changes permanent, click Save.
Removing an ATM Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link in the Physical column on the Interface Configuration page.
   Example: atm-s2p1
4. Find the ATM logical interface to remove in the Logical Interfaces table and click the corresponding Delete button.
   Click Apply.
   The ATM logical interface disappears from the list.
5. To make your changes permanent, click Save.

IPoA Example

This section describes how you might configure the interfaces of your IP security platform (Nokia platform) in an example network, using Network Voyager.

Before you can configure interfaces by using Network Voyager, you must first configure an IP address on one of the interfaces. You can do this through the Nokia platform console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the Nokia Platform through that interface. You can use any graphical Web browser to configure the other interfaces on the device by entering the IP address of the device in the location field of the browser.

The following figure shows the network configuration for this example.
A company has five ethernet networks in three separate locations. The networks are connected to each other with three routers that belong to the same logical IP subnet over ATM. This example configures the ATM interface on Nokia Platform A. The interface is connected to Nokia Platform B through ATM PVC 42 and to Nokia Platform C through ATM PNC 53. Nokia Platform B and Nokia Platform C are connected to each other through an ATM PVC; their ATM interfaces have already configured.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   
   Example: atm-s2p1

   You are taken to the Physical Interface page.

4. Create a logical interface in the Create a new LLC/SNokia Platform RFC1483 interface section by selecting LIS in the Type list box.
5. Enter 42, 53 in the VCI(s) text box.
6. Click Apply.
7. Click the newly created interface (atm-s2p1c0) in the Logical Interfaces table to reach the Logical Interface page.
8. Enter 10.0.0.1 in the IP Address text box.
9. Enter 24 in the Mask Length text box.
10. Click Apply.
11. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.
   
   Click Apply.
12. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   
   Click Apply.
13. Click Save.

**Serial (V.35 and X.21) Interfaces**

**Configuring a Serial Interface for Cisco HDLC**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   
   Example: ser-s2p1
4. (Optional) Click On or Off in the Physical configuration table Internal Clock field to set the internal clock on the serial device.
   Click Apply.
   Set the internal clock to On when you are connecting to a device or system that does not provide a clock source. Otherwise, set the internal clock to Off.

5. If you turned the internal clock on, enter a value in the Internal clock speed text box.
   If the device can generate only certain line rates, and the configured line rate is not one of these values, the device selects the next highest available line rate.

6. Click Full Duplex or Loopback in the Channel Mode field.
   Full duplex is the normal mode of operation.

7. Click Cisco HDLC in the Encapsulation field.
   Click Apply.
   A logical interface appears in the Logical Interfaces table.

8. Enter a number in the Keepalive text box to configure the Cisco HDLC keepalive interval.
   Click Apply.
   This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

   **Note**
   This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

9. Click the logical interface name in the Interface column of the Logical interfaces table to go to the Interface page.

10. Enter the IP address for the local end of the link in the Local address text box.

11. Enter the IP address of the remote end of the link in the Remote address text box.
    Click Apply.

12. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.
    Click Apply.

13. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
    Click Apply.

14. To make your changes permanent, click Save.
Configuring a Serial Interface for PPP

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: `ser-s2p1`
4. (Optional) Click On or Off in the Physical configuration table Internal Clock field to set the internal clock on the serial device.
   Click Apply.
   Set the internal clock to On when you are connecting to a device or system that does not provide a clock source. Otherwise, set the internal clock to Off.
5. If you turned the internal clock on, enter a value in the Internal clock speed text box.
   If the device can generate only certain line rates, and the configured line rate is not one of these values, the device selects the next highest available line rate.
6. Click Full Duplex or Loopback in the Channel Mode field.
   Full duplex is the normal mode of operation.
7. Click the PPP radio button in the Encapsulation field. Click Apply.
   A logical interface appears in the Logical Interfaces table.
8. Enter a number in the Keepalive text box to configure the PPP keepalive interval.
   Click Apply.
   This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.
   
   **Note**
   This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

9. Enter a number in the Keepalive maximum failures text box.
   This value sets the number of times a remote system can fail to send a keepalive protocol message within a keepalive interval before the system considers the link down.
10. Click Apply.
11. Click the Advanced PPP Options link.
    The `PPP Advanced Options` page appears.
12. Click Yes or No in the Negotiate Magic Number field.
    Clicking Yes enables the interface to send a request to negotiate a magic number with a peer.
13. Click Yes or No in the Negotiate Maximum Receive Unit field.
    Clicking Yes enables the interface to send a request to negotiate an MRU with a peer.
14. Click Apply.
15. Click Up to return to the Physical Interface page.
16. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.
17. Enter the IP address for the local end of the link in the Local address text box.
18. Enter the IP address of the remote end of the link in the Remote address text box. Click Apply.
19. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box. Click Apply.
20. (Optional) Add a comment to further define the logical interfaces function in the Comments text box. Click Apply.
21. To make your changes permanent, click Save.

**Configuring a Serial Interface for Frame Relay**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   
   Example: ser-s2p1
4. (Optional) Click On or Off in the Physical configuration table Internal Clock field to set the internal clock on the serial device.
   
   Click Apply.

   Set the internal clock to On when you are connecting to a device or system that does not provide a clock source. Otherwise, set the internal clock to Off.
5. If you turned the internal clock on, enter a value in the Internal clock speed text box.

   If the device can generate only certain line rates, and the configured line rate is not one of these values, the device selects the next highest available line rate.
6. Click Full Duplex or Loopback radio in the Channel Mode field.

   Full duplex is the normal mode of operation.
7. Click the Frame relay radio button in the Encapsulation field.

   Click Apply.
8. Enter a number in the Keepalive text box to configure the frame relay keepalive interval.

   Click Apply.

   This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.
9. Click DTE or DCE in the Interface Type field.
DTE is the usual operating mode when the device is connected to a Frame Relay switch.

10. Click On or Off in the Active Status Monitor field.
This action sets the monitoring of the connection-active status in the LMI status message.

11. (Optional) Click the Advanced Frame Relay Options link to go to the Frame Relay Advanced Options page.
The Frame Relay Advanced Options page allows you to configure frame relay protocol and LMI parameters for this device.

Note
The values you enter depend on the settings of the frame relay switch to which you are connected or to the subscription provided by your service provider.

12. From the Frame Relay Advanced Options page, click Up to return to the Physical Interface page.

13. Enter the DLCI number in the Create a new interface DLCI text box.
Click Apply.
A new logical interface appears in the Interface column. The DLCI number appears as the channel number in the logical interface name. The new interface is on by default.

14. (Optional) Enter another DLCI number in the DLCI text box to configure another frame relay PVC.
Click Apply.
Each time you click Apply after you enter a DLCI, a new logical interface appears in the Interface column. The DLCI entry field remains blank to allow you to add more frame relay logical interfaces.

15. Click the logical interface name in the Interface column of the Logical interfaces table to go to the Interface page.

16. Enter the IP address for the local end of the PVC in the Local address text box.

17. Enter the IP address of the remote end of the PVC in the Remote address text box.
Click Apply.

18. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.
Click Apply.
To make your changes permanent, click Save.
Serial Interface Example

This section describes how you might configure the interfaces of your IP security platform in an example network, using Network Voyager.

Before you can configure the unit by using Network Voyager, you must first configure an IP address on one of the interfaces. You can do this through the console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the device through that interface. You can use any graphical Web browser to configure the other interfaces on the device by entering the IP address of the device in the location field of the browser.

The following figure shows the network configuration for this example.

In a company’s main office, Nokia Platform A terminates a serial line to an Internet service provider, running PPP with a keepalive value of 10.

Nokia Platform A also provides internet access for a FDDI ring and a remote branch office connected through ATM PVC 93.

The branch office contains Nokia Platform B, which routes traffic between a local Fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. This example configures the serial interface on Nokia Platform A.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Select ser-s1p1 in the Physical column of the table.
4. Click PPP in the Encapsulation field.
5. Click Apply.
6. Enter 10 in the Keepalive text box.
7. Click Apply.
8. Click ser-s1p1c0 in the logical interfaces table to go to the Interface page.
9. Enter 192.168.2.1 in the Local address text box.
10. Enter 192.168.2.93 in the Remote address text box.
11. Click Apply.
12. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.
   Click Apply.
13. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   Click Apply.
14. Click the Up button to go to the Interfaces page.
15. Click the On radio button for ser-s1p1c0.
16. Click Apply.
17. Click Save.

T1(with Built-In CSU/DSU) Interfaces

Configuring a T1 Interface for Cisco HDLC

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the interface link to configure in the Physical column.
   Example: ser-s2p1
4. (Optional) Click On or Off in the Internal Clock field to set the internal clock on the T1 device.
   Click Apply.
   If you are connecting to a device or system that does not provide a clock source, set Internal Clock to On; otherwise, set it to Off. Internal clocking for T1 is fixed at 1.544 Mbps. To configure slower speeds, you must configure fractional T1 on the Advanced T1 CSU/DSU Options page.
5. Click the Full Duplex or Loopback radio button in the Channel Mode field.
Full duplex is the normal mode of operation.

6. Click AMI or B8ZS in the T1 Encoding field to select the T1 encoding.
   Click Apply.
   This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

7. Click Superframe (D4) or Extended SF in the T1 Framing field to select the T1 Framing format.
   Click Apply.
   Use T1 framing to divide the data stream into 64 Kbps channels and to synchronize with the remote CSU/DSU. This setting must match the frame format that the CSU/DSU uses at the other end of the point-to-point link.

8. Click 64bps or 56bps in the T1 Channel Speed field to select the DS0 channel speed for the T1 line.
   Some older trunk lines use the least-significant bit of each DS0 channel in a T1 frame for switching-equipment signaling. T1 frames designed for data transfer can be set to **not** use the least-significant bit of each DS0 channel. This setting allows data to be sent over these trunk lines without corruption but at a reduced throughput. This mode is called the **56 Kbps mode** because each DS0 channel now has an effective throughput of 56 Kbps instead of 64 Kbps. All T1 functions still work in the 56 Kbps mode, including all framing modes and fractional T1 configurations.

9. If you selected Extended SF as the T1 Framing format, click ANSI or None in the FDL Type field to select the FDL type.

10. Click Cisco HDLC in the Encapsulation field.
    Click Apply.
    A logical interface appears in the Logical interfaces table.

11. Enter a number in the Keepalive text box to configure the Cisco HDLC keepalive interval.
    Click Apply.
    This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

    **Note**
    This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

12. (Optional) Click the Advanced T1 CSU/DSU Options link to select advanced T1 options.
    The **T1 CSU/DSU Advanced Options** page allows you to configure fractional T1 channels, line build-out values and other advanced settings for the T1 device. The values you enter on this page are dependent on the subscription provided by your service provider.

13. From the **Advanced T1 CSU/DSU Options** page, click Up to return to the physical interface page.
14. Click the logical interface name in the Interface column of the Logical interfaces table to go to the Interface page.

15. Enter the IP address for the local end of the link in the Local address text box.

16. Enter the IP address of the remote end of the link in the Remote address text box.

   Click Apply.

17. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.

   Click Apply.

18. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.

   Click Apply.

19. To make your changes permanent, click Save.

**Configuring a T1 Interface for PPP**

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the interface link to configure in the Physical column.

   Example: ser-s2p1

4. (Optional) Click On or Off in the Internal Clock field to set the internal clock on the T1 device.

   Click Apply.

   When you connect to a device or system that does not provide a clock source, set Internal Clock to On; otherwise, set it to Off. Internal clocking for T1 is fixed at 1.544 Mbps. To configure slower speeds, you must configure fractional T1 on the Advanced T1 CSU/DSU Options page.

5. Click Full Duplex or Loopback in the Channel Mode field.

   Full duplex is the normal mode of operation.

6. Click AMI or B8ZS in the T1 Encoding field to select the T1 encoding.

   Click Apply.

   This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

7. Click Superframe (D4) or Extended SF in the T1 Framing field to select the T1 Framing format.

   Click Apply.

   Use T1 framing to divide the data stream into 64 Kbps channels and to synchronize with the remote CSU/DSU. This setting must match the frame format used by the CSU/DSU at the other end of the point-to-point link.
8. Click 64bps or 56bps in the T1 Channel Speed field to select the DS0 channel speed for the T1 line.

Some older trunk lines use the least-significant bit of each DS0 channel in a T1 frame for switching-equipment signaling. T1 frames designed for data transfer can be set to not use the least-significant bit of each DS0 channel. This setting allows data to be sent over these trunk lines without corruption but at a reduced throughput. This mode is called the 56 Kbps mode because each DS0 channel now has an effective throughput of 56 Kbps instead of 64 Kbps. All T1 functions still work in the 56 Kbps mode, including all framing modes and fractional T1 configurations.

9. If you selected Extended SF as the T1 Framing format, click ANSI or None in the FDL Type field to select the FDL type.

10. Click the PPP in the Encapsulation field.

Click Apply.

A logical interface appears in the Logical Interfaces table.

11. Enter a number in the Keepalive text box to configure the PPP keepalive interval.

Click Apply.

This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

**Note**

This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

12. Enter a number in the Keepalive maximum failures text box.

This value sets the number of times a remote system may fail to send a keepalive protocol message within a keepalive interval before the systems considers the link down.

13. Click Apply.

14. (Optional) Click the Advanced T1 CSU/DSU Options link to select advanced T1 options.

The T1 CSU/DSU Advanced Options page allows you to configure fractional T1 channels, line build-out values, and other advanced settings for a T1 device. The values you enter on this page depend on the subscription provided by your service provider.

15. From the Advanced T1 CSU/DSU Options page, click Up to return to the physical interface page.

16. Click the Advanced PPP Options link.

The PPP Advanced Options page appears.

17. Clicking Yes or No in the Negotiate Magic Number field.

Clicking Yes enables the interface to send a request to negotiate a magic number with a peer.

18. Click Yes or No in the Negotiate Maximum Receive Unit field.

Clicking Yes enables the interface to send a request to negotiate an MRU with a peer.
19. Click Apply.

20. Click Up to return to the Physical Interface page.

21. Click the logical interface name in the INTERFACE column of the LOGICAL INTERFACES table to go to the Interface page.

22. Enter the IP address for the local end of the link in the Local address text box.

23. Enter the IP address of the remote end of the link in the Remote address box.

24. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.

25. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.

26. To make your changes permanent, click Save.

Configuring a T1 Interface for Frame Relay

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the physical interface link to configure in the Physical column.

   Example: ser-s2p1

4. (Optional) Click On or Off in the Internal Clock field to set the internal clock on the T1 device.

   Click Apply.

   If you're connecting to a device or system that does not provide a clock source, set Internal Clock to On; otherwise, set it to Off. Internal clocking for T1 is fixed at 1.544 Mbps. To configure slower speeds, you must configure fractional T1 on the Advanced T1 CSU/DSU Options page.

5. Click Full Duplex or Loopback in the Channel Mode field.

   Full duplex is the normal mode of operation.

   Click the AMI or B8ZS radio button in the T1 Encoding field to select the T1 encoding.

   Click Apply.

   This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

6. Click Superframe (D4) or Extended SF radio button in the T1 Framing field to select the T1 Framing format.

   Click Apply.
Use T1 framing to divide the data stream into 64Kbps channels and to synchronize with the remote CSU/DSU. This setting must match the frame format used by the CSU/DSU at the other end of the point-to-point link.

7. Click 64bps or 56bps in the T1 Channel Speed field to select the DS0 channel speed for the T1 line.

Some older trunk lines use the least-significant bit of each DS0 channel in a T1 frame for switching-equipment signaling. T1 frames designed for data transfer can be set to not use the least-significant bit of each DS0 channel. This setting allows data to be sent over these trunk lines without corruption but at a reduced throughput. This mode is called the 56 Kbps mode because each DS0 channel now has an effective throughput of 56 Kbps instead of 64 Kbps. All T1 functions still work in the 56 Kbps mode, including all framing modes and fractional T1 configurations.

8. If you selected Extended SF as the T1 Framing format, click ANSI or None in the FDL Type field to select the FDL type.

9. Click Frame relay in the Encapsulation field.

Click Apply.

10. Enter a number in the Keepalive text box to configure the frame relay keepalive interval. Click Apply.

This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

**Note**

This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

11. Click DTE or DCE in the Interface Type field.

DTE is the usual operating mode when the device is connected to a Frame Relay switch.

12. Click On or Off in the Active Status Monitor field.

Click Apply.

Sets the monitoring of the connection-active status in the LMI status message.

13. (Optional) Click Advanced T1 CSU/DSU Options link to select advanced T1 options.

The T1 CSU/DSU Advanced Options page allows you to configure fractional T1 channels, line build-out values and other advanced settings for the T1 device. The values you enter on this page depend the subscription provided by your service provider.

14. From the Advanced T1 CSU/DSU Options page, click Up to return to the physical interface page.

15. (Optional) Click the Advanced Frame Relay Options link to go to the Frame Relay Advanced Options page.

The Frame Relay Advanced Options page allows you to configure frame relay protocol and LMI parameters for this device.
Note
The values you enter depend on the settings of the frame relay switch to which you are connected or to the subscription provided by your service provider.

16. From the Frame Relay Advanced Options page, click Up to return to the Physical Interface page.

17. Enter the DLCI number in the Create a new interface DLCI text box.
   Click Apply.
   A new logical interface appears in the Interface column. The DLCI number appears as the channel number in the logical interface name. The new interface is on by default.

18. (Optional) Enter another DLCI number in the DLCI text box to configure another frame relay PVC.
   Click Apply.
   Each time you click Apply after entering a DLCI, a new logical interface appears in the Interface column. The DLCI entry field remains blank to allow you to add more frame relay logical interfaces.

19. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

20. Enter the IP address for the local end of the PVC in the Local address text box.

21. Enter the IP address of the remote end of the PVC in the Remote address text box.
   Click Apply.

22. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.
   Click Apply.

23. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   Click Apply.

24. To make your changes permanent, click Save.

T1 Interface Example

This section describes how you might use Voyager to configure the interfaces of your IP security platform in an example network.

Before you can configure the device by using Network Voyager, you must first configure an IP address on one of the interfaces. You can do this through the console port during installation or by using the Lynx browser. This procedure allows a graphical browser such as Internet Explorer or Netscape Navigator to access the device through that interface. You can use any graphical web browser to configure the other interfaces on the device by entering the IP address of the device in the location field of the browser.
The following figure shows the network configuration for this example.

![Network Configuration Diagram]

In a company’s main office, Nokia Platform A terminates a T1 line to an Internet service provider, running PPP with a keepalive value of 10. The T1 line uses B8ZS line encoding, Extended Super Frame, T1 framing, and 64 Kbps channels.

Nokia Platform A also provides internet access for an FDDI ring and a remote branch office connected through ATM PVC 93.

The branch office contains Nokia Platform B, which routes traffic between a local fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. This example configures the serial interface on Nokia Platform A.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Select ser-s1p1 in the Physical column of the table.
4. Click B8ZS in the T1 Encoding field.
5. Click Extended SF in the T1 Framing field.
6. Click 64 Kbps in the T1 Channel Speed field.
7. Click PPP in the Encapsulation field.
8. Click Apply.
9. Enter 10 in the Keepalive text box.
10. Click Apply.

11. Click ser-s1p1c0 in the logical interfaces table to go to the Interface page.

12. Enter **192.168.2.1** in the Local address text box.

13. Enter **192.168.2.93** in the Remote address text box.

14. Click Apply.

15. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.

   Click Apply.

16. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.

   Click Apply.

17. Click Up to go to the Interfaces page.

18. Click On for ser-s1p1c0.

19. Click Apply.

20. Click Save.

---

**E1 (with Built-In CSU/DSU) Interfaces**

**Configuring an E1 Interface for Cisco HDLC**

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the physical interface link to configure in the Physical column.

   Example: **ser-s2p1**

4. (Optional) Click On or Off in the Internal Clock field to set the internal clock on the E1 device.

   Click Apply.

   If you are connecting to a device or system that does not provide a clock source, set Internal Clock to On; otherwise, set it to Off. Internal clocking for E1 is fixed at 2.048 Mbps/sec. To configure slower speeds, you must configure fractional E1 on the *Advanced E1 CSU/DSU Options* page.

5. Click Full Duplex or Loopback in the Channel Mode field.

   Full duplex is the normal mode of operation.

6. Click AMI or HDB3 in the E1 Encoding field to select the E1 encoding.

   Click Apply.
This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

7. Click E1 (channel 0 framing) or No Framing in the E1 Framing field to select the E1 framing format.
   Use E1 framing to select whether timeslot-0 is used for exchanging signaling data.

8. Click On or Off for the E1 CRC-4 Framing field.

   **Note**
   This option appears only if you set the E1 Framing field to E1 (channel 0 framing).

   This option chooses the framing format for timeslot-0. On means that CRC-multiframe format is used; the information is protected by CRC-4. Off means that double-frame format is used. This setting must match the setting of the CSU/DSU at the other end of the link.

9. Click On or Off for the E1 Timeslot-16 Framing.
   Click Apply.

   **Note**
   This option appears only if you set the E1 Framing field to E1 (channel 0 framing).

   This option controls whether timeslot-16 is used in channel associated signaling (CAS). Setting this value to On means that timeslot-16 cannot be used as a data channel. See fractional settings on the Advanced E1 CSU/DSU Options page.

10. Click Cisco HDLC in the Encapsulation field.
    Click Apply.
    A logical interface appears in the Logical Interfaces table.

11. Enter a number in the Keepalive text box to configure the Cisco HDLC keepalive interval.
    Click Apply.
    This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system. The range is 0-255. The default is 10.

    **Note**
    This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

12. (Optional) Click the Advanced E1 CSU/DSU Options link to select advanced E1 options.
    The *E1 CSU/DSU Advanced Options* page allows you to configure fractional E1 channels and other advanced settings for the E1 device. The values you enter on this page depend on the subscription provided by your service provider.
13. From the Advanced E1 CSU/DSU Options page, click Up to return to the physical interface page.

14. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

15. Enter the IP address for the local end of the link in the Local Address text box.

16. Enter the IP address of the remote end of the link in the Remote Address text box.

   Click Apply.

17. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.

   Click Apply.

18. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.

   Click Apply.

19. To make your changes permanent, click Save.

   

**Note**

Try to ping the remote system from the command prompt. If the remote system does not work, contact your service provider to confirm the configuration.

---

**Configuring an E1 Interface for PPP**

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the physical interface link to configure in the Physical column.

   Example: `ser-s2p1`

4. (Optional) Click On or Off in the Internal Clock field to set the internal clock on the E1 device.

   Click Apply.

   If you’re connecting to a device or system that does not provide a clock source, set Internal Clock to On; otherwise, set it to Off. Internal clocking for E1 is fixed at 2.048 Mbits/sec. To configure slower speeds, you must configure fractional E1 on the Advanced E1 CSU/DSU Options page.

5. Click Full Duplex or Loopback in the Channel Mode field.

   Full duplex is the normal mode of operation.

6. Click AMI or HDB3 in the E1 Encoding field to select the E1 encoding.

   Click Apply.
This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

7. Click E1 (channel 0 framing) or No Framing in the E1 Framing field to select the E1 Framing format.

Use E1 framing to select whether timeslot-0 is used for exchanging signaling data.

8. Click On or Off for the E1 CRC-4 Framing field.

**Note**
This option appears only if you have set the E1 Framing field to E1 (channel 0 framing).

This button chooses the framing format for timeslot-0. On means that CRC-multiframe format is used; the information is protected by CRC-4. Off means that double-frame format is used. This setting must match the setting of the CSU/DSU at the other end of the link.

9. Click On or Off for the E1 Timeslot-16 Framing.

Click Apply.

**Note**
This option appears only if you set the E1 Framing field to E1 (channel 0 framing).

This value controls whether timeslot-16 is used in channel associated signaling (CAS). Setting this value to On means that timeslot-16 cannot be used as a data channel. See fractional settings on the *Advanced E1 CSU/DSU Options* page.

10. Click PPP in the Encapsulation field.

Click Apply.

A logical interface appears in the Logical Interfaces table.

11. Enter a number in the Keepalive text box to configure the PPP keepalive interval.

Click Apply.

This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system. The range is 0-255. The default is 5.

**Note**
This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

12. Enter a number in the Keepalive Maximum Failures text box.

This value sets the number of times a remote system may fail to send a keepalive protocol message within a keepalive interval before the systems consider the link down. The range is a positive integer. The default is 30.
13. Click Apply.

14. (Optional) Click the Advanced E1 CSU/DSU Options link to select advanced E1 options.

The E1 CSU/DSU Advanced Options page allows you to configure fractional E1 channels and other advanced settings for an E1 device. The values you enter on this page depend on the subscription provided by your service provider.

15. From the Advanced E1 CSU/DSU Options page, click Up to return to the physical interface page.

16. Click the Advanced PPP Options link.

The PPP Advanced Options page appears.

17. Click Yes or No in the Negotiate Magic Number field.

Clicking Yes enables the interface to send a request to negotiate a magic number with a peer.

18. Click Yes or No in the Negotiate Maximum Receive Unit field.

Clicking Yes enables the interface to send a request to negotiate an MRU with a peer.

19. Click Apply.

20. Click Up to return to the Physical Interface page.

21. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

22. Enter the IP address for the local end of the link in the Local Address text box.

23. Enter the IP address of the remote end of the link in the Remote Address text box.

Click Apply.

24. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.

Click Apply.

25. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.

Click Apply.

26. To make your changes permanent, click Save.

---

**Note**

Try to ping the remote system from the command prompt. If the remote system does not work, contact your service provider to confirm the configuration.

---

**Configuring an E1 Interface for Frame Relay**

1. Click Config on the home page.

2. Click the Interfaces link.
3. Click the interface link to configure in the Physical column.
   Example: **ser-s2p1**

4. (Optional) Click On or Off in the Internal Clock field to set the internal clock on the E1 device.
   Click Apply.
   If you’re connecting to a device or system that does not provide a clock source, set Internal Clock to On; otherwise, set it to Off. Internal clocking for E1 is fixed at 2.048 Mbits/sec. To configure slower speeds, you must configure fractional E1 on the *Advanced E1 CSU/DSU Options* page.

5. Click Full Duplex or Loopback in the Channel Mode field.
   Full duplex is the normal mode of operation.

6. Click AMI or HDB3 in the E1 Encoding field to select the E1 encoding.
   Click Apply.
   This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

7. Click E1 (channel 0 framing) or No Framing in the E1 Framing field to select the E1 Framing format.
   Use E1 framing to select whether timeslot-0 is used for exchanging signaling data.

8. Click On or Off for the E1 CRC-4 Framing field.

   **Note**
   This option appears only if you have set the E1 Framing field to E1 (channel 0 framing).
   This button chooses the framing format for timeslot-0. On means that CRC-multiframe format is used; the information is protected by CRC-4. Off means that doubleframe format is used. This setting must match the setting of the CSU/DSU at the other end of the link.

9. Click On or Off for the E1 timeslot-16 Framing.
   Click Apply.

   **Note**
   This option appears only if you set the E1 Framing field to E1 (channel 0 framing).
   This value controls whether timeslot-16 is used in channel associated signaling (CAS). Setting this value to On means that timeslot-16 cannot be used as a data channel. See fractional settings on the *Advanced E1 CSU/DSU Options* page.

10. Click Frame Relay in the Encapsulation field.
    Click Apply.
11. Enter a number in the Keepalive text box to configure the frame relay keepalive interval. Click Apply.

This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system. The range is 0 to 255. The default is 10.

**Note**
This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

12. Click DTE or DCE in the Interface Type field.

DTE is the usual operating mode when the device is connected to a frame relay switch.

13. Click On or Off in the Active Status Monitor field.

Click Apply.

This value sets the monitoring of the connection-active status in the LMI status message.

14. (Optional) Click the Advanced E1 CSU/DSU Options link to select advanced E1 options.

The *E1 CSU/DSU Advanced Options* page allows you to configure fractional E1 channels and other advanced settings for the E1 device. The values you enter on this page depend on the subscription provided by your service provider.

15. From the *Advanced E1 CSU/DSU Options* page, click Up to return to the physical interface page.

16. (Optional) Click the Advanced Frame Relay Options link to go to the *Frame Relay Advanced Options* page.

The *Frame Relay Advanced Options* page allows you to configure frame relay protocol and LMI parameters for this device.

**Note**
The values you enter depend on the settings of the frame relay switch to which you are connected or to the subscription that your service provider provides.

17. From the *Frame Relay Advanced Options* page, click Up to return to the *Physical Interface* page.

18. Enter the DLCI number in the Create a New Interface DLCI text box.

Click Apply.

A new logical interface appears in the Interface column. The DLCI number appears as the channel number in the logical interface name. The new interface is turned on by default.

19. (Optional) Enter another DLCI number in the DLCI text box to configure another frame relay PVC.

Click Apply.
Each time you click Apply after you enter a DLCI, a new logical interface appears in the Interface column. The DLCI entry field remains blank to allow you to add more frame relay logical interfaces.

20. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the Interface page.

21. Enter the IP address for the local end of the PVC in the Local Address text box.

22. Enter the IP address of the remote end of the PVC in the Remote Address text box.
   Click Apply.

23. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.
   Click Apply.

24. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   Click Apply.

25. To make your changes permanent, click Save.

---

**Note**
Try to ping the remote system from the command prompt. If the remote system does not work, contact your service provider to confirm the configuration.

---

**HSSI Interfaces**

**Configuring an HSSI Interface for Cisco HDLC**

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the interface link to configure in the Physical column.
   
   **Example:** ser-s2p1

4. (Optional) Click On or Off in the Physical configuration table Internal Clock field to set the internal clock on the serial device.
   Click Apply.
   
   Set the internal clock to On when you are connecting to a device or system that does not provide a clock source. Otherwise, set the internal clock to Off.

5. If you turned the internal clock on, enter a value in the Internal clock speed text box.
   
   If the device can generate only certain line rates, and the configured line rate is not one of these values, the device selects the next highest available line rate.
6. Click Full Duplex or Loopback in the Channel Mode field.
   Full duplex is the normal mode of operation.

7. Click Cisco HDLC in the Encapsulation field.
   Click Apply.
   A logical interface appears in the Logical Interfaces table.

8. Enter a number in the Keepalive text box to configure the Cisco HDLC keepalive interval.
   Click Apply.
   This value sets the interval, in seconds, between keepalive protocol message transmissions.
   These messages are used periodically to test for an active remote system.

   **Note**
   This value must be identical to the keepalive value configured on the system at the other
   end of a point-to-point link, or the link state fluctuates.

9. Click the logical interface name in the Interface column of the Logical interfaces table to go
to the Interface page.

10. Enter the IP address for the local end of the link in the Local address text box.

11. Enter the IP address of the remote end of the link in the Remote address text box.
   Click Apply.

12. (Optional) Change the interface’s logical name to a more meaningful one by typing the
    preferred name in the Logical name text box.
    Click Apply.

13. (Optional) Add a comment to further define the logical interfaces function in the Comments
    text box.
    Click Apply.

14. To make your changes permanent, click Save.

**Configuring an HSSI Interface for PPP**

1. Click Config on the home page.

2. Click the Interfaces link.

3. Click the physical interface link to configure in the Physical column.
   **Example:** ser-s2p1

4. (Optional) Click On or Off in the Physical configuration table Internal Clock field to set the
   internal clock on the HSSI device.
   Click Apply.
   Set the internal clock to On when you are connecting to a device or system that does not
   provide a clock source. Otherwise, set the internal clock to Off.
5. If you turned the internal clock on, enter a value in the Internal clock speed text box. If the device can generate only certain line rates, and the configured line rate is not one of these values, the device selects the next highest available line rate.

6. Click Full Duplex or Loopback in the Channel Mode field. Full duplex is the normal mode of operation.

7. Click the PPP in the Encapsulation field. Click Apply. A logical interface appears in the Logical interfaces table.

8. Enter a number in the Keepalive text box to configure the PPP keepalive interval. Click Apply. This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

**Note**
This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

9. Enter a number in the Keepalive maximum failures text box to configure the PPP keepalive maximum failures. This value sets the number of times a remote system may fail to send a keepalive protocol message within a keepalive interval before the systems considers the link down. Click Apply.

10. Click the Advanced PPP Options link. The **PPP Advanced Options** page appears.

11. Click Yes or No in the Negotiate Magic Number field. Clicking Yes enables the interface to send a request to negotiate a magic number with a peer.

12. Click Yes or No in the Negotiate Maximum Receive Unit field. Clicking Yes enables the interface to send a request to negotiate an MRU with a peer.

13. Click Up to return to the **Physical Interface** page.

14. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the **Interface** page.

15. Enter the IP address for the local end of the link in the Local address text box.

16. Enter the IP address of the remote end of the link in the Remote address text box. Click Apply.

17. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.
Click Apply.

18. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
Click Apply.

19. To make your changes permanent, click Save.

**Configuring an HSSI Interface for Frame Relay**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: `ser-s2p1`
4. (Optional) Click On or Off in the Physical configuration table Internal Clock field to set the internal clock on the HSSI device.
   Click Apply.
   Set the internal clock to On when you are connecting to a device or system that does not provide a clock source. Otherwise, set the internal clock to Off.
5. If you turned the internal clock on, enter a value in the Internal clock speed text box.
   If the device can generate only certain line rates, and the configured line rate is not one of these values, the device selects the next highest available line rate.
6. Click Full Duplex or Loopback in the Channel Mode field.
   Full duplex is the normal mode of operation.
7. Click Frame relay in the Encapsulation field.
   Click Apply.
8. Enter a number in the Keepalive text box to configure the frame relay keepalive interval.
   Click Apply.
   This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

   **Note**
   This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

9. Click DTE or DCE in the Interface Type field.
   DTE is the usual operating mode when the device is connected to a Frame Relay switch.
10. Click On or Off in the Active Status Monitor field.
    Sets the monitoring of the connection-active status in the LMI status message.
11. (Optional) Click the Advanced Frame Relay Options link to go to the *Frame Relay Advanced Options* page.

The *Frame Relay Advanced Options* page allows you to configure frame relay protocol and LMI parameters for this device.

**Note**
The values you enter depend on the settings of the frame relay switch to which you are connected or to the subscription that your service provider provides.

12. From the *Frame Relay Advanced Options* page, click Up to return to the *Physical Interface* page.

13. Enter the DLCI number in the Create a new interface DLCI text box.

   Click Apply.

   A new logical interface appears in the Interface column. The DLCI number appears as the channel number in the logical interface name. The new interface is on by default.

14. (Optional) Enter another DLCI number in the DLCI text box to configure another frame relay PVC.

   Click Apply.

   Each time you click Apply after entering a DLCI, a new logical interface appears in the Interface column. The DLCI entry field remains blank to allow you to add more frame relay logical interfaces.

15. Click the logical interface name in the Interface column of the Logical Interfaces table to go to the *Interface* page.

16. Enter the IP address for the local end of the PVC in the Local address text box.

17. Enter the IP address of the remote end of the PVC in the Remote address text box.

   Click Apply.

18. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.

   Click Apply.

19. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.

   Click Apply.

20. To make your changes permanent, click Save.
Unnumbered Interfaces

Unnumbered Interfaces Description

Traditionally, each network interface on an IP host or router has its own IP address. This situation can cause inefficient use of the scarce IP address space because every point-to-point link must be allocated an IP network prefix. To solve this problem, a number of people have proposed and implemented the concept of unnumbered point-to-point lines. An unnumbered point-to-point line does not have any network prefix associated with it. As a consequence, the network interfaces connected to an unnumbered point-to-point line do not have IP addresses. Whenever the unnumbered interface generates a packet, it uses the address of the interface that the user has specified as the source address of the IP packet. Thus, for a router to have an unnumbered interface, it must have at least one IP address assigned to it.

The Nokia implementation of Unnumbered Interfaces supports OSPF (Open Shortest Path First) and Static Routes only. Virtual links are not supported.

Configuring an Unnumbered Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical interface link to configure in the Logical column.
   Example: atm s3p1c1

   **Note**
   Only point-to-point interfaces can be configured as unnumbered interfaces. Tunnels cannot be configured as unnumbered interfaces.

4. Click Yes in the Unnumbered Interface field.
5. Click Apply.

   **Note**
   If that interface was associated with either a local or remote address or both, they are automatically deleted.

   **Note**
   You do not see local and remote address configuration fields for unnumbered interfaces. The proxy interface field replaces those fields.
Note
The interface must not be used by a tunnel, and OSPF is the only protocol that the interface can be running.

6. Select an interface from the Proxy Interface drop-down window.
   The Proxy Interface drop-down window shows only those interfaces that have been assigned addresses.
7. Click Apply.

Note
You must choose a proxy interface for the unnumbered interface to function.

Note
You cannot delete the only IP address of the proxy interface. First, select another proxy interface and then delete the IP address of the original proxy interface. If the proxy interface has multiple IP addresses associated with it, you can delete or add addresses. A proxy interface must have at least one IP address associated with it.

8. To make your changes permanent, click Save.

Changing an Unnumbered Interface to a Numbered Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical interface link to configure in the Logical column.
   Example: atm s3p1c1

Note
Only point-to-point interfaces can be configured as unnumbered interfaces. Tunnels cannot be configured as unnumbered interfaces.

Note
This interface must not be the next hop of a static route.

4. Click No in the Unnumbered Interface field.
   Click Apply.
5. To make your change permanent, click Save.
Configuring a Static Route over an Unnumbered Interface

1. Complete “Configuring an Unnumbered Interface” for the interface.
2. Click Config on the home page.
3. Click the Static Routes link in the Routing Configuration section.
4. Enter the IP address of the destination network in the New Static Route text box.
5. Enter the mask length (in bits) in the Mask Length text box.
6. Select the type of next hop the static route will take from the Next Hop Type drop-down window. Your options are Normal, Reject, and Black Hole. The default is Normal.
7. Select Gateway Logical to specify the next-hop gateway type from the Gateway Type drop-down window.

Note
You select an unnumbered logical interface as the next-hop gateway when you do not know the IP address of the next-hop gateway.

Click Apply.
8. Click on the Gateway Logical drop-down window to view the list of unnumbered interfaces that are configured. Select the unnumbered logical interface to use as a next-hop gateway to the destination network.
9. Click Apply, and then click Save to make your change permanent.
Configuring OSPF over an Unnumbered Interface

The following graphic represents an example configuration for running OSPF over an unnumbered interface.

1. Configure the interfaces on Nokia Platform A and Nokia Platform B as in "Configuring an Unnumbered Interface."
2. For each Nokia Platform, configure an OSPF area as in "Configuring OSPF."
3. In the Interfaces section, click on the Area drop-down window next to the configured unnumbered interface and select Backbone.
4. Click Apply.
5. Click Save to make your change permanent.

---

**Note**
Because the unnumbered interface uses the IP address of the selected proxy interfaces whenever you change this proxy interface, OSPF adjacencies are re-established.

**Note**
Whenever you change the underlying encapsulation of the unnumbered serial interfaces, for example from Cisco HDLC to PPP or from PPP to Frame Relay, OSPF adjacencies are re-established.

---

Configuring OSPF over an Unnumbered Interface Using Virtual Links

The following graphic below shows a network configuration that uses both virtual links and an unnumbered serial link. Nokia Platform A has two OSPF areas configured (Area 1 and Area 3), but it is not physically connected to the Backbone area. Thus, a virtual link is configured between Nokia Platform A and Nokia Platform C. A virtual link is also configured between Nokia Platform B and Nokia Platform C because Nokia Platform B also is not physically...
connected to the backbone area. Both Nokia Platform B and Nokia Platform C are configured with IP addresses (10.10.10.2 and 101.10.10.1 respectively).

The interfaces that comprise the virtual link between Nokia Platform A and Nokia Platform C are both configured as unnumbered. This link will fail because OSPF does not support a virtual link that uses an unnumbered interface on either end of the link. Underlying encapsulation. For more information see RFC 2328. Any virtual link that uses OSPF must have an IP address configured on both ends. The virtual link between Nokia Platform B and Nokia Platform C functions because each Nokia Platform is configured with an IP address.

**Cisco HDLC Protocol**

**Changing the Keepalive Interval for Cisco HDLC**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: `ser-s2p1`

4. Enter a number in the Keepalive text box of the Physical Configuration table to configure the Cisco HDLC keepalive interval.
   Click Apply.
   This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

   **Note**
   This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

5. To make your changes permanent, click Save.

## Changing the IP Address in Cisco HDLC

**Note**
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security platform with your browser.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical interface link for which to change the IP address in the Logical column.
   Example: `ser-s2p1c0`
4. Delete the address from the Local address text box and from the Remote address text box.
   Click Apply.
   This removes the old IP address pair.
5. Enter the IP address of the local end of the connection in the Local address text box and the IP address of the remote end of the connection in the Remote address text box.
   Click Apply.
   This adds the new IP address pair.
6. To make your changes permanent, click Save.
Point-to-Point Protocol

Changing the Keepalive Interval in PPP

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: ser-s2p1
4. Enter a number in the Keepalive text box to configure the PPP keepalive interval.
   Click Apply.
   This value sets the interval, in seconds, between keepalive protocol message transmissions.
   These messages are used periodically to test for an active remote system.

   **Note**
   This value must be identical to the keepalive value configured on the system at the other
   end of a point-to-point link, or the link state fluctuates.

5. To make your changes permanent, click Save.

Changing the Keepalive Maximum Failures in PPP

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: ser-s2p1
4. Enter a number in the Keepalive maximum failures text box of the Physical Configuration
   table to configure the PPP keepalive maximum failures.
   Click Apply.
   This value sets the number of times the remote system may fail to send a keepalive protocol
   message within the keepalive interval before this IP security platform considers the link
down.
5. To make your changes permanent, click Save.
Changing the IP Address in PPP

Note
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security platform with your browser.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical interface link for which to change the IP address in the Logical column.
   Example: ser-s2p1c0
4. Delete the address from the Local address text box and from the Remote address text box.
   Click Apply.
   This deletes the old IP address pair.
5. Enter the IP address of the local end of the connection in the Local address text box and the IP address of the remote end of the connection in the Remote address text box.
   Click Apply.
   This adds the new IP address pair.
6. To make your changes permanent, click Save.

Frame Relay Protocol

Changing the Keepalive Interval in Frame Relay

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   Example: ser-s2p1
4. Enter a number in the Keepalive text box to configure the Frame Relay keepalive interval.
   Click Apply.
   This value sets the interval, in seconds, between keepalive protocol message transmissions.
   These messages are used periodically to test for an active remote system.

Note
This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

5. To make your changes permanent, click Save.
Changing the DLCI in Frame Relay

To move an IP address from one PVC to another, you must first delete the logical interface for the old PVC, then create a new logical interface for the new PVC.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   
   Example: ser-s2p1

4. Locate the logical interface to delete in the Logical interfaces table for this device.
5. Click the corresponding Delete button.
   
   Click Apply.
   
   The logical interface disappears from the list. Any IP addresses configured on this interface are also removed.

6. Enter the DLCI number in the Create a new interface DLCI text box.
   
   Click Apply.
   
   A new logical interface appears in the Interface column. The DLCI number appears as the channel number in the logical interface name. The new interface is on as default.

7. Click the logical interface name to go the Interface page.

8. Enter the IP address for the local end of the PVC in the Local address text box.

9. Enter the IP address of the remote end of the PVC in the Remote address text box.
   
   Click Apply.

10. (Optional) Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.
    
    Click Apply.

11. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
    
    Click Apply.

12. To make your changes permanent, click Save.

Changing the LMI Parameters in Frame Relay

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to configure in the Physical column.
   
   Example: ser-s2p1

4. Click the Advanced Frame Relay Options link to go the Frame Relay Advanced Options page.
The Frame Relay Advanced Options page allows you to configure frame relay protocol and LMI parameters for this device.

**Note**
The values you enter are dependent on the settings of the frame relay switch to which you are connected or to the subscription provided by your service provider.

5. From the Frame Relay Advanced Options page, click Up to return to the Physical Interface page.
6. To make your changes permanent, click Save.

### Changing the Interface Type in Frame Relay

When connected to a Frame Relay switch or network, the interface type is usually set to DTE. You may need to change the interface type to DCE if it is connected point-to-point with another router.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to change in the Physical column.
   
   Example: *ser-s2p2*

4. Change DTE or DCE in the Interface type field.
   
   Click Apply.
5. To make your changes permanent, click Save.

### Changing the Active Status Monitor Setting in Frame Relay

When connected to a Frame Relay switch or network, the interface type is usually set to DTE. You may need to change the interface type to DCE if it is connected point-to-point with another router.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link to change in the Physical column.
   
   Example: *ser-s2p2*

4. Click on or off in the Active Status Monitor field.
   
   Click Apply.
5. To make your changes permanent, click Save.
Changing the IP Address in Frame Relay

**Note**
Do not change the IP address you use in your browser to access Network Voyager. If you do, you can no longer access the IP security platform with your browser.

1. Click Config on the home page.
2. Click the Interfaces link.
   Click the logical interface link for which to change the IP address in the Logical column.
   Example: `ser-s2p1c17`
3. Delete the address from the Local address text box and from the Remote address text box.
   Click Apply.
   This deletes the old IP address pair.
4. Enter the IP address of the local end of the connection in the Local address text box and the IP address of the remote end of the connection in the Remote address text box.
   Click Apply.
   This adds the new IP address pair.
5. To make your changes permanent, click Save.

Removing a Frame Relay Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the physical interface link in the Physical column on the Interface Configuration page.
   Example: `ser-s2p1`
4. Find the logical interface you wish to remove and click the corresponding Delete button in the Logical Interfaces table.
   Click Apply.
   This removes the logical interface from the list.
5. To make your changes permanent, click Save.
Loopback Interfaces

Adding an IP Address to a Loopback Interface

You might want to assign an address to the loopback interface that is the same as the OSPF router ID, or is the termination point of a BGP session. This allows firewall adjacencies to stay up even if the outbound interface is down.

Note
The loopback interface always has a logical interface created and enabled.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the loopback logical interface link in the Logical column (loop0c0).
4. To add an IP address, enter the IP address for the device in the New IP address text box. Click Apply.
   Each time you click Apply, the configured IP address appears in the table. The entry fields remain blank to allow you to add more IP addresses.
5. To make your changes permanent, click Save.

Changing the IP Address of a Loopback Interface

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the loopback logical interface link in the Logical column (loop0c0).
4. To remove the old IP address, click the Delete check box that corresponds to the address to delete.
   Click Apply.
5. To add the new IP address, enter the IP address for the device in the New IP address text box.
   Click Apply.
   Each time you click Apply, the configured IP address appears in the table. The entry fields remain blank to allow you to add more IP addresses.
6. To make your changes permanent, click Save.
GRE Tunnels

Creating a GRE Tunnel

GRE tunnels encapsulate IP packets by using Generic Routing Encapsulation (GRE) with no options. The encapsulated packets appear as unicast IP packets. GRE tunnels provide redundant configuration between two sites for high availability.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click Tunnels in the Physical column.
4. Click the drop-down window in the Create a new tunnel interface with encapsulation field and select GRE.
5. Click Apply.
   Each time you select a tunnel encapsulation and click Apply, the new tunnel appears in the logical interfaces table.
6. Click the logical interface name in the Interface column of the Logical interfaces table to go to the Interface page for the specified tunnel.
   Example: tun0c1
7. Enter the IP address of the local end of the GRE tunnel in the Local address text box.
   The local address cannot be one of the system’s interface addresses and must be the remote address configured for the GRE tunnel at the remote router.
8. Enter the IP address of the remote end of the GRE tunnel in the Remote address text box.
   The remote address cannot be one of the systems interface addresses and must be the local address configured for the GRE tunnel at the remote router.
9. Enter the IP address of the local interface the GRE tunnel is bound to in the Local endpoint text box.
   The local endpoint must be one of the systems interface addresses and must be the remote endpoint configured for the GRE tunnel at the remote router.
10. Enter the IP address of the remote interface the GRE tunnel is bound to in the Remote endpoint text box.
    The remote endpoint must not be one of the systems interface addresses and must be the local endpoint configured for the GRE tunnel at the remote router.
11. Bind the tunnel to the outgoing interface:
    - On means that all packets that egress through the tunnel will exit through the outgoing interface (local endpoint). If the local endpoint link fails, traffic does not egress through the tunnel. You might use this setting to prevent possible routing loops.
- Off means that packets that egress through the tunnel can be routed through any interface. Use this setting to allow the system to use a different interface in case the local endpoint link fails.

**Note**
If the local endpoint is a loopback address, you must set this option to Off to allow traffic to egress through the tunnel.

12. **(Optional)** Select a value from the TOS value drop-down window.
   Click Apply.
   On GRE tunnels, it is desirable to copy or specify the TOS bits when the router encapsulates the packet. After you select the TOS feature, intermediate routers between the tunnel endpoints may take advantage of the QoS features and possibly improve the routing of important packets. By default, the TOS bits are copied from the inner IP header to the encapsulating IP header.
   If the desired TOS value is not displayed in the drop-down window, select Custom Value from the menu.
   Click Apply. An entry field appears.

13. **(Optional)** If you selected a custom value from the TOS value drop-down window, enter a value in the range of 0-255.
    Click Apply.

14. **(Optional)** Change the interface’s logical name to a more meaningful one by typing the preferred name in the Logical name text box.
    Click Apply.

15. **(Optional)** Add a comment to further define the logical interfaces function in the Comments text box.
    Click Apply.

16. To make your changes permanent, click Save.

### Changing the Local and/or Remote Address or Local/Remote Endpoint of a GRE Tunnel

1. Click Config on the home page.
2. Click the Interfaces link.
3. In the Logical column, click the Logical Interface link for which to change the IP address.
   Example: tun0c1
4. **(Optional)** Enter the IP address of the local end of the GRE tunnel in the Local address text box.
The local address cannot be one of the systems interface addresses and must be the remote address configured for the GRE tunnel at the remote router.

5. (Optional) Enter the IP address of the remote end of the GRE tunnel in the Remote address text box.
   The remote address cannot be one of the systems interface addresses and must be the local address configured for the GRE tunnel at the remote router.

6. (Optional) Enter the IP address of the local interface the GRE tunnel is bound to in the Local endpoint text box.
   The local endpoint must be one of the systems interface addresses and must be the remote endpoint configured for the GRE tunnel at the remote router.

7. (Optional) Enter the IP address of the local interface the GRE tunnel is bound to in the Remote endpoint text box.
   The remote endpoint must not be one of the systems interface addresses and must be the local endpoint configured for the GRE tunnel at the remote router.
   Click Apply.

8. To make your changes permanent, click Save.

Changing IP TOS Value of a GRE Tunnel

1. Click Config on the home page.
2. Click the Interfaces link.
3. In the Logical column, click the Logical Interface link of the item for which to change the TOS.
   Example: tun0c1
4. Select a value from the TOS value drop-down window.
   Click Apply.
   On GRE tunnels, it is desirable to copy or specify the TOS bits when the router encapsulates the packet. After you select the TOS value, intermediate routers between the tunnel endpoints may take advantage of the QoS features and possibly improve the routing of important packets. By default, the TOS bits are copied from the inner IP header to the encapsulating IP header.
   If the desired TOS value is not displayed in the drop-down window, select CUSTOM VALUE from the menu.
   Click Apply. An entry field appears.
5. (Optional) If you selected custom value from the TOS value drop-down window, enter a value in the range of 0-255.
   Click Apply.
6. To make your changes permanent, click Save.
**Removing a GRE Tunnel**

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click Tunnels in the Physical column.
4. Locate the tunnel logical interface to delete in the Logical Interfaces table and click the corresponding Delete checkbox.
   - Click Apply.
   - The tunnel logical interface disappears from the list.
5. To make your changes permanent, click Save.

**GRE Tunnel Example**

The following steps provide directions on how to configure a sample GRE tunnel. The following figure below shows the network configuration for this example.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click Tunnels in the Physical column.
4. Click the drop-down window in the Create a new tunnel interface with encapsulation field and select GRE.
5. Click Apply.
6. From the Interface column on the Logical interfaces table, select tun01.
7. Enter 10.0.0.1 in the Local address text box.
8. Enter 10.0.0.2 in the Remote address text box.
9. Enter 192.68.26.65 in the Local endpoint text box.
10. Enter 192.68.26.74 in the Remote endpoint text box.
11. (Optional) Select a value from the TOS value drop-down window.
    Click Apply.

On GRE tunnels, it is desirable to copy or specify the TOS bits when the router encapsulates
the packet. After you select the TOS feature, intermediate routers between the tunnel
endpoints may take advantage of the QoS features and possibly improve the routing of
important packets. By default, the TOS bits are copied from the inner IP header to the
encapsulating IP header.

If the desired TOS value is not displayed in the drop-down window, select Custom Value
from the menu.

Click Apply. An entry field appears.
12. (Optional) If you selected custom value from the TOS value drop-down window, enter a
    value in the range of 0-255.
13. Click Apply.
14. (Optional) Change the interface’s logical name to a more meaningful one by typing the
    preferred name in the Logical name text box.
    Click Apply.
15. (Optional) Add a comment to further define the logical interfaces function in the Comments
    text box.
    Click Apply.
16. To make changes permanent, click Save.

HA GRE Tunnels Description

High Availability GRE Tunnels provide redundant encrypted communication among multiple
hosts. They are created by performing the procedures associated with the configuration of GRE
tunnels, OSPF, VRRP, and Check Point firewall.

HA GRE Tunnel Example

In our example, we configure two-way tunnels between IP Units 1 and 2, and IP Units 3 and 4.
Since the steps required to configure a HA GRe tunnel are addressed in the appropriate sections
of this reference guide, they are not individually repeated here. The following figure shows the network configuration for this example.

![Network Configuration Diagram]

**Note**
You must complete step 1 in the following procedure before you continue to other steps. You can complete steps 2 through 4 in any order.

1. Perform the steps as presented in the *Creating a GRE Tunnel* and *GRE Tunnel Example* sections. Since this example shows you how to create an HA GRE tunnel, we need to create multiple tunnels and in two directions. This example requires repeating steps 7 through 10 of the GRE Tunnel example four times as follows:

   a. Configuring from IP Unit 1 to IP Unit 2:
      Enter 10.0.0.1 in the Local address text box.
      Enter 10.0.0.2 in the Remote address text box.
Enter 170.0.0.1 in the Local endpoint text box. Enter 171.0.0.1 in the Remote endpoint text box.

b. Configuring from IP Unit 2 to IP Unit 1:
Enter 10.0.0.2 in the Local address text box. Enter 10.0.0.1 in the Remote address text box. Enter 171.0.0.1 in the Local endpoint text box. Enter 170.0.0.1 in the Remote endpoint text box.

c. Configuring from IP Unit 3 to IP Unit 4:
Enter 11.0.0.1 in the Local address text box. Enter 11.0.0.2 in the Remote address text box. Enter 170.0.1.1 in the Local endpoint text box. Enter 171.0.1.1 in the Remote endpoint text box.

d. Configuring from IP Unit 4 to IP Unit 3:
Enter 11.0.0.2 in the Local address text box. Enter 11.0.0.1 in the Remote address text box. Enter 171.0.1.1 in the Local endpoint text box. Enter 170.0.1.1 in the Remote endpoint text box.

2. OSPF provides redundancy in case a tunnel becomes available. OSPF detects when the firewall at the other end of an HA GRE tunnel is no longer reachable and then obtains a new route by using the backup HA GRE tunnel and forwards the packets to the backup firewall. Perform the steps as presented in the “Configuring OSPF” and “Configuring OSPF Example” sections. For this example, enable OSPF by using the following interface values:
   IP Unit 1: 10.0.0.1 and 192.168.0.1
   IP Unit 2: 10.0.0.2 and 192.168.1.1
   IP Unit 3: 11.0.0.1 and 192.168.0.2
   IP Unit 4: 11.0.0.2 and 192.168.1.2

   Use iclid to show all OSPF neighbors. Each firewall should show two neighbors and also show that the best route to the destination network is through the corresponding HA GRE tunnel.

3. VRRP provides redundancy in case one of the firewalls is lost. Perform the steps as presented in “Configuring VRRP.” Use the following values to configure VRRP:
   IP Unit 1: Enable VRRP on 192.168.0.1 with 192.168.0.2 as a backup
   IP Unit 2: Enable VRRP on 192.168.1.1 with 192.168.1.2 as a backup
   IP Unit 3: Enable VRRP on 192.168.0.2 with 192.168.0.1 as a backup
   IP Unit 4: Enable VRRP on 192.168.1.2 with 192.168.1.1 as a backup

4. HA GRE tunnels work by encapsulating the original packet and resending the packet through the firewall. The first time the firewall sees the packet, it has the original IP header; the second time, the packet has the end points of the tunnels as the src and dst IP addresses.

   The firewall needs to be configured to accept all packets with the original IP header so the encapsulation can take place. An encryption rule is then defined to encrypt those packets that match the tunnel endpoints.
DVMRP Tunnels

Creating a DVMRP Tunnel

DVMRP tunnels encapsulate multicast packets as IP unicast packets. This feature allows two multicast routers to exchange multicast packets even when they are separated by routers that cannot forward multicast packets.

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click Tunnels in the Physical column.
4. From the pulldown menu in the Create a new tunnel interface with encapsulation, select DVMRP.
5. Click Apply.
   Each time you select a tunnel encapsulation and click Apply, a new tunnel appears in the table.
6. Click the logical interface name in the Interface column of the Logical interfaces table; this takes you to the interface page for the specified tunnel.
   Example: tun0c1
7. Enter the IP address of the local end of the DVMRP tunnel in the Local address text box.
   The local address must be one of the systems interface IP addresses and must also be the remote address configured on the DVMRP tunnel on the remote router.
8. Enter the IP address of the remote end of the DVMRP tunnel in the Remote Address text box.
   The remote address must be the IP address of the multicast router at the remote end of the DVMRP tunnel. It cannot be one of the system’s interface addresses.
9. (Optional) Change the interface’s logical name to a more meaningful name by typing the preferred name in the Logical name text box.
   Click Apply.
10. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
    Click Apply.
11. To make your changes permanent, click Save.

Note
When the DVMRP tunnel interface is created, set all other DVMRP configuration parameters from the DVMRP page.
Changing the Local or Remote Addresses of a DVMRP Tunnel

1. Click Config on the home page.
2. Click the Interfaces link.
3. In the Logical column, click the Logical Interface link on the tunnel that is to have the IP address changed.
   
   Example: tun0c1
4. (Optional) Enter the IP address of the local end of the DVMRP tunnel in the Local Address text box.
   The local address must be one of the systems interface IP addresses and must also be the remote address configured on the DVMRP tunnel on the remote router.
5. (Optional) Enter the IP address of the remote end of the DVMRP tunnel in the Remote Address text box.
   The remote address must be the IP address of the multicast router at the remote end of the DVMRP tunnel. It cannot be one of the systems interface addresses.
6. Click Apply.
7. To make your changes permanent, click Save.

Note
When the tunnel interface has been created, set all other DVMRP configuration parameters from the DVMRP page.

Removing a DVMRP Tunnel

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click Tunnels in the Physical column.
4. Locate the tunnel logical interface to delete in the Logical Interfaces table and click corresponding Delete.
5. Click Apply.
   The tunnel logical interface disappears from the list.
6. To make your changes permanent, click Save.

DVMRP Tunnel Example

The following example contains one connection to the Internet through an Internet Service Provider (ISP). This ISP provides a multicast traffic tunnel. Multicast traffic uses the address
space above 224.0.0.0 and below 238.0.0.0. Multicast traffic is different from unicast (point-to-point) traffic in that is in one-to-many traffic forwarded by routers.

A router forwards Multicast traffic to an adjacent router only if that router has a client that accepts multicast traffic. Nokia IP security platforms require Distance Vector Multicast Routing Protocol (DVMRP) to be enabled on the interfaces to which you forward multicast traffic.

In the preceding example, a DVMRP tunnel originates from the ISP at 22.254/24. This tunnel has a present endpoint of 22.1/24. A DVMRP tunnel set up on Nokia Platform A points to 22.254/24.

1. Initiate a Network Voyager session to Nokia Platform A. In this example, we use Nokia Platform A as the starting point.
2. Click Config on the home page.
3. Click the Interfaces link.
4. Click Tunnels in the Physical column.
5. From the pulldown menu in the Create a new tunnel interface with encapsulation, select DVMRP.
6. Click Apply.
   Each time you select a tunnel encapsulation and click Apply, a new tunnel appears in the table.
7. Click the logical interface name in the Interface column of the Logical interfaces table; this takes you to the interface page for the specified tunnel.
   Example: tun0c1
8. Enter the following in the Local IP Address text box:
   192.168.22.1
9. Enter 192.168.22.254 in the Remote IP Address text box
10. (Optional) Change the interfaces logical name to a more meaningful name by typing the preferred name in the Logical name text box.
11. Click Apply.
12. To make your changes permanent, click Save to make changes permanent.

Note
Steps 17 through 21 require that you use the Routing Configuration page by first completing steps 13 through 16.

13. Click Config on the home page.
14. Click the DVMRP link in the Routing configuration section.
15. For each interface to configure for DVMRP, click On for the interface.
16. Click Apply.
17. (Optional) Define the time-to-live (TTL) threshold for the multicast datagram. Enter it as follows in the Threshold text box: 128
   This example 128 is for the purpose of broadcasting. A 128 TTL is defined as internet broadcast.
18. (Optional) Define the cost of the tunnel. Enter this cost in the Metric text box. This shows the route preference. Leave this as the default unless there are many other multicast tunnels present in your network.
19. Click Apply.
20. Perform steps 1 through 13 with addresses reversed on the exit point for the multicast tunnel. In this example, the ISP has already done this for us.
21. Ensure that DVMRP is running on all interfaces (Ethernet, ATM, FDDI) on which the multicast is to be received (See “Configuring DVMRP”).

ARP Table Entries

Changing ARP Global Parameters
1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Enter the keep time (in seconds) in the Keep Time field in the Global ARP Settings section. Keep time specifies the time, in seconds, to keep resolved dynamic ARP entries. If the entry is not referenced and not used by traffic after the given time elapses, the entry is removed.
The range of the Keep Time value is 60 to 86400 seconds with a default of 14400 seconds (4 hours).

4. Enter the retry limit in the Retry Limit field in the Global ARP Settings section.
   The Retry Limit specifies the number of times to retry ARP requests until holding off requests for 20 seconds. Retry requests occur at a rate of up to once per second. The range of retry limit is 1 to 100 and the default value is 3.

5. If your network configuration requires it, click the button to enable the appliance to accept multicast ARP replies.
   Enable this feature if this system is connected to an IPSO cluster. Because all the nodes of an IPSO cluster share a single multicast MAC address, routers that connect to a cluster (either directly or through a switch or hub) must be able to accept ARP replies that contain a multicast MAC address.

6. Click Apply.
7. To make your changes permanent, click Save.

Adding a Static ARP Entry

1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Enter the new IP address in the IP Address field in the Add a New Static ARP Entry section.
4. In the same table, enter the MAC address corresponding to the IP address in the MAC Address text box
5. Click Apply.
6. To make your changes permanent, click Save.

Adding a Proxy ARP Entry

A proxy ARP entry makes this system respond to ARP requests for a given IP address received through any interface. This system does not use proxy ARP entries when it forwards packets.

1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Enter the new IP address in the IP Address field in the Add a New Proxy ARP Entry section.
4. In the Interface field of the Add a new Proxy ARP Entry section, select the interface whose MAC address is returned in ARP replies.
   Selecting User-defined MAC Address allows you to specify an arbitrary MAC address for the entry.
   Click Apply.
5. (Optional) If User-Defined MAC Address was selected, enter the MAC address corresponding to the IP address in the MAC Address text box in the Proxy ARP Entries table.
   
   Click Apply.

6. To make your changes permanent, click Save.

Deleting a Static ARP Entry

1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Click the checkbox in the Delete column next to the table entry to delete.
   
   Click Apply.
4. To make your changes permanent, click Save.

Viewing Dynamic ARP Entries

1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Click the Display or Remove Dynamic ARP Entries link.

Deleting Dynamic ARP Entries

1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Click the Display or Remove Dynamic ARP Entries link.
4. Click the check box in the Delete column next to the ARP entry to delete.
   
   Click Apply.

Flushing All Dynamic ARP Entries

1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Click Flush.
Configuring ARP for the ATM Interface

Changing Global Parameters

The InATMARP protocol is used for finding a mapping from IP addresses to ATM PVCs in a logical IP subnet (LIS) on top of an ATM network.

1. Click Config on the home page.
2. Click the ARP link under the Interfaces section.
3. Enter a value for one or more of the Keep Time, Timeout, Retry Limit and Holdoff Time parameters in the corresponding fields in the Global InATMARP Settings table.
   - Keep Time specifies time, in seconds, to keep resolved dynamic ATM ARP entries. The range of Keep Time value is 1 to 900 seconds (15 minutes).
   - Timeout specifies an InATMARP request retransmission interval in seconds. Network Voyager enforces that the timeout must be less than a third of Keep Time. The Range of Timeout value is 1 to 300 with a default value of five seconds.
   - Retry Limit specifies the number of times to retry InATMARP requests after which the Holdoff Timer is started. The range of Retry Limit value is 1 to 100 with a default value of 5.
   - Holdoff Time specifies time, in seconds, to hold off InATMARP requests after the maximum number of retries. The range of Holdoff Time value is 1 to 900 seconds (15 minutes), with a default value of 60 seconds (one minute).
4. Click Apply.
5. To make your changes permanent, click Save.

Adding a Static ATM ARP Entry

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical ATM interface to configure in the Logical column.
4. Click the ATM ARP Entries link.
5. Enter the IP address of the new static ATM ARP entry in the IP Address field in the Create a new static ATM ARP entry section and enter the VPI/VCI number of the corresponding PVC in the VPI/VCI field.

   The IP address must belong to the subnet of the logical ATM interface and the VCI must be one of those configured for the interface.

   **Note**
   Whenever static ATM ARP entries are applied, dynamic entries are no longer updated; therefore, new neighbors cannot be seen through a dynamic InATMARP mechanism.
6. Click Apply.
   The newly created static ATM ARP entry appears in the Static ATM ARP Entries table. The
   IP datagrams destined to the IP address of the entry are sent to the PVC specified in the
   entry.
7. To make your changes permanent, click Save.

Deleting a Static ATM ARP Entry

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical ATM interface to change in the Logical column.
4. Click the ATM ARP Entries link.
5. Click the Delete checkbox of the ATM ARP entry to delete.
   Click Apply.
6. To make your changes permanent, click Save.

Viewing and Deleting Dynamic ATM ARP Entries

1. Click Config on the home page.
2. Click the Interfaces link.
3. Click the logical ATM interface to configure in the Logical column.
4. Click the ATM ARP Entries link.
   Dynamic ATM ARP entries appear in a table at the bottom of the page.
5. Click the Delete check box next to the dynamic ATM ARP entry to delete.
   Click Apply.

Note
Deleting a dynamic entry triggers a transmission of an InATMARP request on the PVC. If the
remote end responds and its IP address is not changed, a new dynamic ATM ARP entry
identical to the deleted one appears in the table immediately.
Configuring Transparent Mode

Transparent Mode Description

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

Note
Transparent mode interoperates with Check Point FireWall-1. There is no special code or software required for the bridging functionality to be supported in FireWall-1.

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

Transparent mode has the following limitations.

- Transparent mode supports only Ethernet interfaces (10/100/1000 Mbps).
- Transparent mode does not provide full-fledged bridging functionality such as loop detection or spanning tree.
- The IP2250 appliance does not support transparent mode.
- Transparent mode is not supported in a cluster environment. Transparent mode is supported with VRRP.
- You cannot use transparent mode on interfaces that participate in an IPSO cluster.
- Interfaces configured for transparent mode do not pass non-IP traffic. In fact, all non-IP traffic is simply dropped at the ethernet input layer before it reaches the transparent mode layer which only registers to receive IP traffic.

You configure transparent mode by first creating a transparent mode group and then adding interfaces to the group. When interfaces are in the same transparent mode group, then they are logically in the same subnet. A transparent mode group is disabled until you enable it.

Note
In the disabled mode, the transparent mode group drops all packets received on or destined to the interfaces in that group. Because transparent mode groups are disabled by default, do not associate interfaces to a transparent mode group that is in use or you will lose connectivity to those interfaces.

If you have more than one transparent mode group on the same platform, the groups must be visible to each other on the routing layer (Layer 3). If you need routing, then at least one interface in each group should have an IP address.
**Processing**

When you configure transparent mode, it is added to the IPSO kernel as a module situated between the layer 2 and the upper protocol layers. When a logical interface is configured for the transparent mode, transparent mode Address Resolution Protocols (ARP) and IP receive handlers replace the common ARP and IP receive handlers. This enables the transparent mode operation to essentially intercept all packets between the link layer (layer 2) and IPv4 and IPv6 network layer (layer 3).

Besides transmitting packets that are bridged from one interface to another based on MAC addresses, the transparent mode module also transmits packets that originate locally or are forwarded based on routing. Locally originated ARP packets are broadcast on all interfaces of the transparent mode group. Locally originated IP packets are also broadcast on all interfaces of the transparent mode group if the egress interface is not found in the forwarding table.

If there are any VLAN interfaces among the interfaces in the transparent mode group, the link header of a bridged packet is modified to have the proper format for the egress interface.

Neighbor learning is the process of associating a MAC address with an interface whenever a packet is received with an unknown source MAC address. This association is called a neighbor control block. The neighbor control block is deleted from the address table after a period of inactivity (age time out). The age timeout is reset to this initial value for the neighbor control block on receiving any packet from that neighbor.

Packet processing for a firewall consists of ingress and egress processing. This applies only to IP packets; ARP packets are never delivered to the firewall. Egress processing occurs when a packet returns from the firewall’s ingress filtering, the packet is delivered to the firewall again for egress filtering. The packet is delivered with the interface index of the egress interface. If it is a link multicast packet, a copy of the packet is made for each interface of the transparent mode group, except the received interface. It is then delivered to the firewall with the associated interface index.

---

**Note**

Network Address Translation (NAT) is not supported in transparent mode. Transparent mode does support implicit “NATing” of the packet’s destination IP address to a local IP address to deliver packets to the security server on the local protocol stack. It does this by performing a route lookup for the packet’s destination IP address to determine whether the packet destination is local after the packet returns from the firewall’s ingress filtering. If the packets destination is local, the packet is delivered to the IP layer for local processing.
VPN Support

To configure transparent mode in a virtual private network environment, you must create a range or group of addresses that will be protected behind the IP address on the bridge. This must be done because addresses cannot be learned dynamically behind a firewall.

In this example, the network administrator of Network A wants to provide Network B with access to certain addresses behind the Nokia Platform with Firewall, which is in transparent mode. To do this, the network administrator would do the following in the firewall software.

1. Create a group of addresses on Firewall A.
   
   In this case, the network administrator groups together addresses x, y, and z into group M.

2. Create an object for the remote Firewall B.

3. Create a rule, for example, Group M; Network B; Encrypt.

The network administrator on Network B also creates a rule for encrypted traffic through Firewall B.
Note
For information on how to create groups, objects, and rules on the firewall, see your Check Point documentation that was included with your Nokia IPSO software package.

Example of Transparent Mode

The following illustration shows a network connected to an internet service provider (ISP) through a switch. In this configuration, all addressing to the local area network (LAN) is done at Layer 2.

Below, the network administrator wants to protect the LAN with a firewall. Installing a conventional firewall requires the network administrator to obtain another IP address from the ISP, IP 1.5.4.0/24.

Nokia’s transparent mode solution provides firewall protection for the LAN without having to obtain new IP addresses or reconfigure addresses on the LAN. Packet traffic continues to run at Layer 2, rather than at Layer 3 with a conventional firewall solution.

To configure transparent mode in the preceding network configuration, do the following in Network Voyager.

1. Click Config on the home page.
2. Click Transparent Mode in the Interface section
3. Enter any positive integer (an integer greater than 0) in the edit box, for example 100 and click Apply.

4. Click the link of the transparent mode group you created. It will appear as XMG with the number you entered in step 3, for example XMG 100.

5. In the Add Interface drop-down box, select an interface to associate with the transparent mode group. In this case, select the logical interfaces associated with IP address 1.5.3.3/24 and click Apply.

**Note**
Because transparent mode groups are disabled by default, do not associate interfaces to a transparent mode group that is in use. If you do, you will lose connectivity to those interfaces.

**Note**
An interface can be in at most one group. Once you have associated an interface to a group, you will not have the option to associate it with another group.

6. In the Add Interface drop-down box, select the logical interfaces associated with IP address 1.5.3.4/24 and click Apply.

7. Click Up.

8. Select Yes in the Enable column associated with XMG 100 and click Apply.

9. Click Save to make your changes permanent

**Note**
When you make changes to a transparent mode group, you must stop and restart the firewall.

Once you have enabled transparent mode and restarted your firewall, packets destined for your LAN are sent at Layer 2. Packets destined for an IP address are sent at Layer 3.

**Creating a Transparent Mode Group**

You create a transparent mode group by first creating the group then adding the interfaces to the group. (See “Adding or Removing Interfaces to/from Transparent Mode Groups.”) By default, a transparent mode group stays disabled unless explicitly enabled. In the disabled mode, the transparent mode group drops all packets received on or destined to the interfaces in that group. (See “Enabling or Disabling a Transparent Mode Group.”)

**To create a transparent mode group**

1. Click Config on the home page.

2. Click Transparent Mode in the Interface section
3. Enter any positive integer (an integer greater than 0) in the edit box.
4. Click Apply.

Deleting a Transparent Mode Group

If you make delete a transport mode group or add or remove interfaces, the firewall sometimes does not learn of the changes when you get the topology. If you get the topology and your changes to interfaces are not shown, stop and restart the firewall.

To delete a transparent mode group
1. Click Config on the home page.
2. Click Transparent Mode in the Interface section
3. Click the Delete radio button associated with the group you would like to delete and click Apply.
4. Click Save to make your changes permanent.

Adding or Removing Interfaces to/from Transparent Mode Groups

If you delete a transport mode group or add or remove interfaces, the firewall sometimes does not learn of the changes when you get the topology. If you get the topology and your changes to interfaces are not shown, you can stop and restart the firewall to view your changes.

To add or remove an interface to/from a transparent mode group
1. Click Config on the home page.
2. Click Transparent Mode in the Interface section
3. Click the link of the appropriate transparent mode group.
4. To add an interface to the transparent mode group, select it from the Add Interface drop-down box.

---

**Note**
Because transparent mode groups are disabled by default, do not associate interfaces to a transparent mode group that is in use. If you do, you will lose connectivity to those interfaces.

---

**Note**
An interface can be in at most one group. Once you have associated an interface to a group, you will not have the option to associate it with another group.
5. To delete an interface from the transparent mode group, select the Remove radio button associated with the interface you want to delete and click Apply.

6. (Optional) Repeat to add or remove other interfaces to or from the transparent mode group.

7. Click Save to make your changes permanent.

Enabling or Disabling a Transparent Mode Group

By default, a transparent mode group is disabled unless explicitly enabled. In the disabled mode, the transparent mode group drops all packets received on or destined to the interfaces in that group. You must enable the transparent mode group to start the operation of the group.

Note
A transparent mode group must have at least one interface associated with it before you can enable the group.

To enable or disable a transparent mode group
1. Click Config on the home page.
2. Click Transparent Mode in the Interface section
3. Select Yes or No in the Enable column associated with the transparent mode group you want to enable or disable.
4. Click Apply.
5. Click Save to make your changes permanent

Enabling or Disabling VRRP for a Transparent Mode Group

If you are enabling VRRP on a VRRP master, the node will perform transparent mode operations as described in the section, “Transparent Mode Description.” As a VRRP standby, it will drop all packets except those with local destinations.

For more information on configuring VRRP, see “Configuring VRRP.”

To enable or disable VRRP for a transparent mode group
1. Click Config on the home page.
2. Click Transparent Mode in the Interface section
3. Click the link of the transparent mode group to which you would like to enable VRRP.
4. Select the Yes or No radio button in the VRRP Enabled table.
5. Click Apply.
6. Click Save to make your changes permanent.
Transparent Mode and Check Point NGX SmartDashboard

When you use the Check Point NGX SmartDashboard to configure the Gateway Cluster properties of a VRRP pair that uses IPSO transparent mode, you must follow this procedure.

To add nodes configured for transparent mode to a cluster using SmartDashboard

1. Create a gateway object for each of the VRRP nodes.
2. Define the topology for each gateway object. Make sure that transparent mode is properly configured with the address ranges to the external and internal networks correctly defined.
3. Create the cluster object.
4. Add each gateway to the cluster object using the Add Gateway to Cluster button.

If you use the New Cluster Member button to add a VRRP member that uses transparent mode to a cluster, you cannot correctly configure the Topology.

Monitoring Transparent Mode Groups

To monitor transparent mode groups

1. Click Monitor on the home page.
2. Click Transparent Mode Monitor.
3. Click a transparent mode group under XMODE Group Id.
Chapter Contents

- Routing Overview
- OSPF
  - OSPF Description
  - Configuring OSPF
  - Configuring OSPF Example
- RIP
  - RIP Description
  - Configuring RIP
  - Configuring RIP Timers
  - Configuring Auto-Summarization
  - RIP Example
- PIM
  - PIM Description
  - Configuring Dense-Mode PIM
  - Disabling PIM
  - Setting Advanced Options for Dense-Mode PIM (Optional)
  - Configuring Sparse-Mode PIM
  - Configuring High-Availability Mode
  - Configuring this Router as a Candidate Bootstrap and Candidate Rendezvous Point
  - Configuring a PIM-SM Static Rendezvous Point
  - Setting Advanced Options for Sparse-Mode PIM (Optional)
  - Debugging PIM
- IGRP
  - IGRP Description
  - Configuring IGRP
  - IGRP Example
- DVMRP
  - DVMRP Description
- Configuring DVMRP
- Configuring DVMRP Timers
- IGMP
  - IGMP Description
  - Configuring IGMP
- Static Routes
  - Static Routes Description
  - Configuring a Default Route
  - Creating a Static Route
  - Setting the Rank for Static Routes
  - Configuring Multiple Static Routes
  - Adding and Managing Static Routes Example
- Backup Static Routes
  - Backup Static Routes Description
  - Creating a Backup Static Route
  - Deleting a Backup Static Route
- Route Aggregation
  - Route Aggregation Description
  - Creating Aggregate Routes
  - Removing Aggregate Routes
  - Route Aggregation Example
- Route Rank
  - Route Rank Description
  - Setting Route Rank
  - Routing Protocol Rank Example
  - Setting Rank for Static Routes
- BGP
  - BGP Description
  - BGP Memory Requirements
  - BGP Neighbors Example
  - Path Filtering Based on Communities Example
  - BGP Multi Exit Discriminator Example
  - Changing the Local Preference Value Example
  - BGP Confederation Example
  - Route Reflector Example
  - BGP Community Example
  - EBGP Load Balancing Example: Scenario #1
  - EBGP Load Balancing Example: Scenario #2
Routing Overview

Nokia Routing Subsystem

The Nokia routing subsystem, Ipsilon Routing Daemon (IPSRD), is an essential part of your firewall. IPSRD’s role is to dynamically compute paths or routes to remote networks. Routes are calculated by a routing protocol. Besides providing routing protocols, IPSRD also allows routes to be converted or redistributed between routing protocols. Finally, when there are multiple protocols with a route to a given destination, IPSRD allows you to specify a ranking of protocols. Based on this ranking, a single route is installed in the forwarding table for each destination.

You can configure each of the supported routing protocols, route redistribution, and other routing options via the Configuring Routing section in Network Voyager.

Routing monitoring is available by following links from the individual protocol pages or by clicking on the Monitor button in Network Voyager. Another monitoring tool is ICLID. This tool provides interactive, text-based monitoring of the routing subsystem.

Routing Protocols

Routing protocols compute the best route to each destination. Routing protocols also exchange information with adjacent firewalls. The best route is determined by the cost or metric values.

Routing protocols can be broken up into two major categories: exterior gateway protocols (EGPs) and interior gateway protocols (IGPs). Interior gateway protocols exchange routing information inside an autonomous system (AS). An AS is a routing domain, such as inside an
organization, that contacts its own routing. An EGP exchanges routing information between ASes and provides for specialized policy-bound filtering and configuration.

IPSRD supports three interior gateway protocols: RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), and OSPF (Open Shortest Path First).

Static routes and aggregate routes are also supported. For more information on static routes, see “Static Routes Description” on page 210. For more information on aggregate routes, see “Route Aggregation Description” on page 215.

**RIP**

RIP is a commonly used IGP. There are two versions of RIP, RIP version 1 and RIP version 2. IPSRD supports both versions. RIP uses a simple distance vector algorithm called Bellman Ford to calculate routes. In RIP, each destination has a cost or metric value, which is based solely on the number of hops between the calculating firewall and the given destination.

The maximum metric value is 15 hops, which means that RIP is not suited to networks within a diameter greater than 15 firewalls. The advantage of RIP version 2 over RIP version 1 is that it supports non-classful routes. Classful routes are old-style class A, B, C routes. You should use RIP version 2 instead of RIP version 1 whenever possible.

Nokia also supports RIPng, the version of RIP that supports IPv6 interfaces.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Described in RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP version 1</td>
<td>RFC1058</td>
</tr>
<tr>
<td>RIP version 2</td>
<td>RFC1723</td>
</tr>
<tr>
<td>RIPng</td>
<td></td>
</tr>
</tbody>
</table>

**IGRP**

IGRP (Interior Gateway Routing Protocol) is a distance vector protocol. IGRP has a number of metrics for each destination. These metrics include link delay, bandwidth, reliability, load, MTU, and hop count. A single composite metric is formed by combining metrics with a particular weight.

Like RIP version 1, IGRP does not fully support non-classful routing.

**OSPF**

OSPF (Open Shortest Path First) is a modern link-state routing protocol. It fully supports non-classful networks. OSPF has a single, 24-bit metric for each destination. You can configure this metric to any desired value.

OSPF allows the AS to be broken up into areas. Areas allow you to increase overall network stability and scalability. At area boundaries, routes can be aggregated to reduce the number of routes each firewall in the AS must know about. If there are multiple paths to a single destination with the same computed metric, OSPF can install them into the forwarding table.
DVMRP

DVMRP (Distance Vector Multicast Routing Protocol) is a multicast routing protocol (RIP, OSPF, and IGRP are unicast routing protocols). Multicasting is typically used for real-time audio and video when there is a single source of data and multiple receivers. DVMRP uses a hop-based metric and, like RIP, a distance-vector route calculation.

BGP

BGP (Border Gateway Protocol) is an exterior gateway protocol that is used to exchange network reachability information between BGP-speaking systems running in each AS. BGP is unlike interior gateway protocols (IGRP or OSPF), which periodically flood an intra-domain network with all the known routing table entries and build their own reliability on top of a datagram service. Instead, BGP uses TCP as its underlying transport mechanism.

BGP is also a path-vector routing protocol, which limits the distribution of a firewall’s reachability information to its peer or neighbor firewalls. BGP uses path attributes to provide more information about each route. BGP maintains an AS path, which includes the number of each AS that the route has transited. Path attributes may also be used to distinguish between groups of routes to determine administrative preferences. This allows greater flexibility in determining route preference and achieves a variety of administrative ends.

BGP supports two basic types of sessions between neighbors: internal (IBGP) and external (EBGP). Internal sessions run between firewalls in the same autonomous systems, while external sessions run between firewalls in different autonomous systems.

Redistributing Routes Overview

*Route redistribution* controls which routes are advertised by IPSRD to other systems, as well as which routes are redistributed between the protocols run on the firewall.

A *metric* is set for any redistributed route. This metric is sent to the peer by certain protocols and may be used by the peer to choose a better route to a given destination. Some routing protocols can associate a metric with a route when announcing the route.

A *route filter* can be used to explicitly list all the redistributed routes.

Redistributing Routes with BGP

Redistributing to BGP is controlled by an AS. The same policy is applied to all firewalls in the AS. BGP metrics are 16-bit, unsigned quantities; that is, they range from 0 to 65535 inclusive, with zero being the most attractive. While BGP version 4 supports 32-bit unsigned quantities, IPSRD does not.
Note
If you do not specify a redistribution policy, only routes to attached interfaces are redistributed. If you specify any policy, the defaults are overridden. You must explicitly specify everything that should be redistributed.

Redistributing Routes with RIP and IGRP

Redistributing to RIP and IGRP is controlled by any one of three parameters:

- Protocol
- Interface
- Gateway

If more than one parameter is specified, they are processed from most general (protocol) to most specific (gateway).

It is not possible to set metrics for redistributing RIP routes into RIP or for redistributing IGRP routes into IGRP. Attempts to do this are silently ignored. It is also not possible to set the metrics for redistributing routes into IGRP.

Note
If no redistribution policy is specified, RIP and interface routes are redistributed into RIP and IGRP, and interface routes are redistributed into IGRP. If any policy is specified, the defaults are overridden. You must explicitly specify everything that should be redistributed.

RIP version 1 assumes that all subnets of the shared network have the same subnet mask, so they are able to propagate only subnets of that network. RIP version 2 removes that restriction and is capable of propagating all routes when not sending version 1-compatible updates.

Redistributing Routes with OSPF

It is not possible to create OSPF intra-area or inter-area routes by redistributing routes from the IPSRD routing table into OSPF. It is possible to redistribute from the IPSRD routing table only into OSPF ASE routes. In addition, it is not possible to control the propagation of OSPF routes within the OSPF protocol.

There are two types of OSPF ASE routes:

- Type 1
- Type 2

See the OSPF protocol configuration for a detailed explanation of the two types.
Route Redistribution Between Protocols

The *redistribute_list* specifies the source of a set of routes based on parameters like the protocol from which the source has been learned. The *redistribute_list* indirectly controls the redistribution of routes between protocols.

The syntax varies slightly per source protocol. BGP routes may be specified by source AS. RIP and IGRP routes may be redistributed by protocol, source interface, and/or source gateway. Both OSPF and OSPF ASE routes may be redistributed into other protocols. All routes may be redistributed by AS path.

When BGP is configured, all routes are assigned an AS path when they are added to the routing table. For all interior routes, this AS path specifies IGP as the origin and no ASes in the AS path. The current AS is added when the route is redistributed. For BGP routes, the AS path is stored as learned from BGP.

OSPF

OSPF Description

*Open Shortest Path First* (OSPF) is an interior gateway protocol (IGP) used to exchange routing information between routers within a single autonomous system (AS). OSPF calculates the best path based on true costs using a metric assigned by a network administrator. RIP, the oldest IGP protocol chooses the least-cost path based on hop count. OSPF is more efficient than RIP, has a quicker convergence, and provides equal-cost multipath routing where packets to a single destination can be sent using more than one interface. OSPF is suitable for complex networks with a large number of routers. It can coexist with RIP on a network.

IPSO supports OSPFv2, which supports IPv4 addressing, and OSPFv3, which supports IPv6 addressing.

Link State Advertisements

Routers using OSPF send packets called Link State Advertisements (LSA) to all routers in an area. *Areas* are smaller groups within the AS that you can design to limit the flooding of an LSA to all routers. LSAs do not leave the area from which they originated, thus increasing efficiency and saving network bandwidth. You must specify at least one area in your OSPF network—the *backbone area*, which has the responsibility to propagate information between areas. The backbone area has the identifier 0.0.0.0. You can designate other areas depending on your network design. It is generally recommended that you limit OSPF areas to about 50 routers based on the limitations of OSPF (traffic overhead, table size, convergence, and so on).

All OSPF areas must be connected to the backbone area. If you have an area that is not connected to the backbone area, you can connect it by configuring a *virtual link*, enabling the backbone area to appear contiguous despite the physical reality.
Note
If you need to connect two networks that both already have backbone areas and you do not want to reconfigure one to something other than 0.0.0.0, you can connect the two backbone areas using a virtual link.

Each router records information about its interfaces when it initializes and builds an LSA packet. The LSA contains a list of all recently seen routers and their costs. The LSA is forwarded only within the area it originated in and is flooded to all other routers in the area. The information is stored in the link-state database, which is identical on all routers in the AS.

Area Border Routers

Routers called Area Border Routers (ABR) have interfaces to multiple areas. ABRs compact the topological information for an area and transmit it to the backbone area. Nokia supports the implementation of ABR behavior as outlined in the internet draft of the Internet Engineering Task Force (IETF). The definition of an ABR in the OSPF specification as outlined in RFC 2026 does not require a router with multiple attached areas to have a backbone connection. However, under this definition, any traffic destined for areas that are not connected to an ABR or that are outside the OSPF domain is dropped. According to the Internet draft, a router is considered to be an ABR if it has more than one area actively attached and one of them is the backbone area. An area is considered actively attached if the router has at least one interface in that area that is not down.

Rather than redefine an ABR, the Nokia implementation includes in its routing calculation summary LSAs from all actively attached areas if the ABR does not have an active backbone connection, which means that the backbone is actively attached and includes at least one fully adjacent neighbor. You do not need to configure this feature; it functions automatically under certain topographies.

OSPF uses the following types of routes:

- **Intra-area** Have destinations within the same area.
- **Interarea** Have destinations in other OSPF areas.
- **Autonomous system external (ASE)** Have destinations external to the autonomous system (AS).

All routers on a link must agree on the configuration parameters of the link. All routers in an area must agree on the configuration parameters of the area. A separate copy of the SPF algorithm is run for each area. Misconfigurations prevent adjacencies from forming between neighbors, and routing black holes or loops can form.
High Availability

- VRRP

IPSO supports the advertising of the virtual IP address of the VRRP virtual router. You can configure OSPF to advertise the virtual IP address rather than the actual IP address of the interface.

You must use monitored-circuit VRRP, not VRRP v2, when configuring virtual IP support for OSPF or any other dynamic routing protocol. If you enable this option, OSPF runs only on the master of the virtual router; on a failover, OSPF stops running on the old master and then starts running on the new master. A traffic break might occur during the time it takes both the VRRP and OSPF protocols to learn the routes again. The larger the network, the more time it takes OSPF to synchronize its database and install routes again. For more information on enabling the advertising of a virtual IP address when running OSPF, see “Configuring OSPF,” step 14f.

IPSO also supports OSPF over VPN tunnels that terminates at a VRRP group. Only active-passive VRRP configurations are supported, active-active configurations are not.

- IP Clustering

IPSO supports OSPF in a cluster. Each member of a cluster runs OSPF tasks, but only the master changes the state and sends OSPF messages to the external routers. For more information on IP Clustering, see “IP Clustering Description.”

Note
IPSO does not support OSPF v3 in an IP cluster.

Nokia strongly recommends that you not configure OSPF or any other routing protocol on the primary or secondary cluster protocol interfaces of an IP cluster.

Interoperability with Cisco Routers Running OSPF

Builds of IPSO 3.8 prior to Build 039 do not support interoperability with Cisco routers that implement link-local signaling (LLS) when running OSPF. 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.

Configuring OSPF

When you configure OSPF on your system, you must define the OSPF areas and global settings on each platform, as described in “Configuring OSPF Areas and Global Settings.” You must also configure each interface that participates in OSPF as described in “Configuring OSPF Interfaces.”
**Note**

OSPFv3, which supports IPv6, has essentially the same configuration parameters as OSPFv2, except that you enter them from the Network Voyager page accessed by clicking Config > IPv6 Configuration > OSPFv3.

---

**Configuring OSPF Areas and Global Settings**

Table 3 lists the parameters for areas and global settings that you use when configuring OSPF on your system. As you add areas, each is displayed with its own configuration parameters under the Areas section.

**Table 3 OSPF Configuration Parameters for Areas and Global Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>Uniquely identifies the router in the autonomous system. By default, the system selects a non-loopback address assigned to the loopback interface, if one is available, or an address from the list of active addresses. Nokia recommends that you configure the router ID rather than accepting the system default value. This prevents the router ID from changing if the interface used for the router ID goes down. In a cluster environment, you must select a router ID because there is no default value. Although you do not need to use an IP address as the router ID, you must enter a dotted quad value ([0-255].[0-255].[0-255].[0-255]. Do not use 0.0.0.0 as a router ID.</td>
</tr>
<tr>
<td>Virtual links</td>
<td>For any area that does not connect directly to the backbone area, you must configure a virtual link. You configure the virtual link on both the ABR for the discontiguous area and another ABR that does connect to the backbone. The virtual link acts like a point-to-point link. The routing protocol traffic that flows along the virtual link uses intra-area routing only. In the Add a New Virtual Link text field, enter the router ID of the remote endpoint of the virtual link. You must also select the transit area from the drop-down box. This is the area that connects both to the backbone and to the discontiguous area.</td>
</tr>
<tr>
<td>Stub area</td>
<td>If an area has only one entry and exit point for external traffic, you can configure it as a stub area and thus reduce the number of entries in its routing table. A stub area blocks the import of the external (ASE) link advertisements and, as a result, does not add routes external to the OSPF domain to the stub area's database.</td>
</tr>
<tr>
<td>Cost for default stub area router</td>
<td>This field appears only if you define the area as a stub area. Enter a cost for the default route to the stub area. Range: 1-16777215. There is no default.</td>
</tr>
<tr>
<td>Totally stubby area</td>
<td>You can further restrict the LSAs by specifying the area as a totally stubby area. In addition to blocking external (ASE) link advertisements, a totally stubby area also blocks summary link advertisements. Summary link advertisements are originated by ABRs and flooded throughout the advertisement's associated area. Each summary link advertisement describes a route to a destination outside the area, yet still inside the AS (i.e. an inter-area route). These include routes to networks and routes to AS boundary routers.</td>
</tr>
</tbody>
</table>
To configure OSPF

1. Complete “Configuring Ethernet Interfaces” for the interface and assign an IP address to the interface.
2. Click Config on the home page.
3. Click the OSPF link in the Routing Configuration section.
4. Enter the router ID in the Router ID text box.
5. If you want to define additional OSPF areas besides the backbone area:
   a. Enter each name in the Add New OSPF Area text field and click Apply.
   b. If a newly defined areas is a stub area, click yes for the Stub Area, then click Apply and enter the cost for the default route to originate into the stub area in the Cost for Default Stub Area Route text field. Click Apply again.
   c. If a newly defined stub area is a totally stubby area, click yes in the Totally Stubby Area field. Click Apply.
6. (Optional) For each area, you can add one or more address ranges if you want to reduce the number of routing entries that the area advertises into the backbone.
7. (Optional) For each summary you do not want to define, click OFF in the Restrict section where the network prefix summary is defined.

---

### Table 3  OSPF Configuration Parameters for Areas and Global Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC1583 Compatibility</td>
<td>This implementation of OSPF is based on RFC2178, which fixed some looping problems in an earlier specification of OSPF. If your implementation is running in an environment with OSPF implementations based on RFC1583 or earlier, enable RFC 1583 compatibility to ensure backwards compatibility.</td>
</tr>
<tr>
<td>SPF delay</td>
<td>Specifies the time in seconds the system will wait to recalculate the OSPF routing table after a change in topology. Default is 2. Range is 1-60.</td>
</tr>
<tr>
<td>SPF hold</td>
<td>Specifies the minimum time in seconds between recalculations of the OSPF routing table. Default is 5. Range is 1-60.</td>
</tr>
<tr>
<td>Default ASE route cost</td>
<td>Specifies a cost for routes redistributed into OSPF as ASEs. Any cost previously assigned to a redistributed routed overrides this value.</td>
</tr>
</tbody>
</table>
| Default ASE route type | Specifies a route type for routes redistributed into OSPF as ASEs, unless these routes already have a type assigned. There are two types:  
- Type 1 external: Used for routes imported into OSPF which are from IGPs whose metrics are directly comparable to OSPF metrics. When a routing decision is being made, OSPF adds the internal cost to the AS border router to the external metric.  
- Type 2 external: Used for routes whose metrics are not comparable to OSPF internal metrics. In this case, only the external OSPF cost is used. In the event of ties, the least cost to an AS border router is used. |

---

RFC1583 Compatibility

This implementation of OSPF is based on RFC2178, which fixed some looping problems in an earlier specification of OSPF. If your implementation is running in an environment with OSPF implementations based on RFC1583 or earlier, enable RFC 1583 compatibility to ensure backwards compatibility.

SPF delay

Specifies the time in seconds the system will wait to recalculate the OSPF routing table after a change in topology. Default is 2. Range is 1-60.

SPF hold

Specifies the minimum time in seconds between recalculations of the OSPF routing table. Default is 5. Range is 1-60.

Default ASE route cost

Specifies a cost for routes redistributed into OSPF as ASEs. Any cost previously assigned to a redistributed routed overrides this value.

Default ASE route type

Specifies a route type for routes redistributed into OSPF as ASEs, unless these routes already have a type assigned. There are two types:

- Type 1 external: Used for routes imported into OSPF which are from IGPs whose metrics are directly comparable to OSPF metrics. When a routing decision is being made, OSPF adds the internal cost to the AS border router to the external metric.
- Type 2 external: Used for routes whose metrics are not comparable to OSPF internal metrics. In this case, only the external OSPF cost is used. In the event of ties, the least cost to an AS border router is used.
8. Configure the OSPF interfaces, as described in “To configure an OSPF interface” on page 177.

Configuring OSPF Interfaces

Table 4 lists the parameters for interfaces that you use when configuring OSPF on your platform.

Table 4 Configuration Parameters for OSPF Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>The drop-down list displays all of the areas configured and enabled on your platform. An entry for the backbone area is displayed even if it is disabled. An OSPF area defines a group of routers running OSPF that have the complete topology information of the given area. OSPF areas use an area border router (ABR) to exchange information about routes. Routes for a given area are summarized into the backbone area for distribution into other non-backbone areas. An ABR must have at least two interfaces in at least two different areas. For information on adding an area “Configuring OSPF Areas and Global Settings” on page 174.</td>
</tr>
</tbody>
</table>
| Hello interval | Specifies the length of time in seconds between hello packets that the router sends on this interface. For a given link, this value must be the same on all routers, or adjacencies do not form.  
Range: 1-65535 in seconds  
Default: For broadcast interfaces, the default hello interval is 10 seconds. For point-to-point interfaces, the default hello interval is 30 seconds. |
| Dead interval | Specifies the number of seconds after the router stops receiving hello packets that it declares the neighbor is down. Typically, this value should be four times the hello interval. For a given link, this value must be the same on all routers, or adjacencies do not form. The value must not be 0.  
Range: 1-4294967295 in seconds.  
Default: For broadcast interfaces, the default dead interval is 40 seconds. For point-to-point interfaces, the default dead interval is 120 seconds. |
| Retransmit interval | Specifies the number of seconds between LSA retransmissions for this interface. This value is also used when retransmitting database description and link state request packets. Set this value well above the expected round-trip delay between any two routers on the attached network. Be conservative when setting this value to prevent necessary retransmissions.  
Range is 1-4294967295 in seconds. Default is 5. |
| OSPF cost | Specifies the weight of a given path in a route. The higher the cost you configure, the less preferred the link as an OSPF route. For example, you can assign different relative costs to two interfaces to make one more preferred as a routing path. You can explicitly override this value in route redistribution.  
Range is 1-65535. Default is 1. |
To configure an OSPF interface

1. Assign the appropriate area to each interface by selecting the OSPF area that this interface participates in from the Area drop-down list for the interface, then click Apply.

   The OSPF interface configuration parameters are displayed showing the default settings. If you want to accept the default settings for the interface, no further action is necessary.

### Table 4 Configuration Parameters for OSPF Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Election priority</td>
<td>Specifies the priority for becoming the designated router (DR) on this link. When two routers attached to a network both attempt to become a designated router, the one with the highest priority wins. If there is a current DR on the link, it remains the DR regardless of the configured priority. This feature prevents the DR from changing too often and applies only to a shared-media interface, such as ethernet or FDDI. A DR is not elected on point-to-point type interfaces. A router with priority 0 is not eligible to become the DR. Range is 0-255. Default is 1.</td>
</tr>
<tr>
<td>Passive mode</td>
<td>Specifies that the interface does not send hello packets, which means that the link does not form any adjacencies. This mode enables the network associated with the interface to be included in the intra-area route calculation rather than redistributing the network into OSPF and having it as an ASE. In passive mode, all interface configuration information, with the exception of the associated area and the cost, is ignored. Options are On or Off. Default is Off.</td>
</tr>
<tr>
<td>Virtual address</td>
<td>Makes OSPF run only on the VRRP Virtual IP address associated with this interface. If this router is not a VRRP master, then OSPF will not run if this option is On. It will only run on the VRRP master. You must also configure VRRP to accept connections to VRRP IPs. For more information, see “Configuring Monitored-Circuit VRRP” on page 280. Options are On or Off. Default is Off.</td>
</tr>
</tbody>
</table>
| Authorization type | Specifies which type of authentication scheme to use for a given link. In general, routers on a given link must agree on the authentication configuration to form neighbor adjacencies. This feature guarantees that routing information is accepted only from trusted routers. Options for authentication are:  
  • Null: Does not authenticate packets. This is the default option.  
  • Simple: Uses a key of up to eight characters. Provides little protection because the key is sent in the clear, and it is possible to capture packets from the network and learn the authentication key.  
  • MD5: Uses a key of up to 16 characters. Provides much stronger protection, as it does not include the authentication key in the packet. Instead, it provides a cryptographic hash based on the configured key. The MD5 algorithm creates a crypto checksum of an OSPF packet and an authentication key of up to 16 characters. The receiving router performs a calculation using the correct authentication key and discards the packet if the key does not match. In addition, a sequence number is maintained to prevent the replay of older packets. |
2. (Optional) Change any configuration parameters for the interface, then click Apply.

**Note**
The hello interval, dead interval, and authentication method must be the same for all routers on the link.

3. To make your changes permanent, click Save.

### Configuring OSPF Example

This example consists of the following:
- Enabling OSPF with backbone area (Area 0) on one interface
- Enabling OSPF on Area 1 on another interface
- Summarizing and aggregating the 192.168.24.0/24 network from Area 0 to Area 1

In the following diagram:
- Nokia Platform A and Nokia Platform D are gateways.
- Nokia Platform C is an area border router with Interface `e1` on the backbone area (Area 0), and Interface `e2` on Area 1.
- Nokia Platform A and Nokia Platform B are on the backbone area.
- Nokia Platform D is on Area 1.

The routes in Area 0 are learned by Nokia Platform D when the ABR (Nokia Platform C) injects summary link state advertisements (LSAs) into Area 1.

1. Configure the interfaces as in "Configuring Ethernet Interfaces."
2. Initiate a Network Voyager session to Nokia Platform C.
3. Click Config on the home page.
4. Click the OSPF link in the Routing Configuration section.
5. Click the backbone area in the drop-down list for e1; then click Apply.
6. In the Add New OSPF Area text box, enter 1; then click Apply.
7. In the Add new address range: prefix text box for the backbone area, enter 192.168.24.0.
8. In the Mask Length text box, enter 24; then click Apply.
9. Click 1 area in the drop-down list for e2; then click Apply.
10. Click Save.
11. Initiate a Network Voyager session to Nokia Platform D.
12. Click Config on the home page.
13. Click the OSPF link in the Routing Configuration section.
14. In the Add New OSPF Area text box, enter 1; then click Apply.
15. Click 1 area in the drop-down list for e3, then click Apply.
16. Click Save.

RIP

RIP Description

The Routing Information Protocol (RIP) is one of the oldest, and still widely used, interior gateway protocols (IGP). RIP uses only the number of hops between nodes to determine the cost of a route to a destination network and does not consider network congestion or link speed. Other shortcomings of RIP are that it can create excessive network traffic if there are a large number of routes and that it has a slow convergence time and is less secure than other IGPs, such as OSPF.

Routers using RIP broadcast their routing tables on a periodic basis to other routers, whether or not the tables have changed. Each update contains paired values consisting of an IP network address and a distance to that network. The distance is expressed as an integer, the hop count metric. Directly connected networks have a metric of 1. Networks reachable through one other router are two hops, and so on. The maximum number of hops in a RIP network is 15 and the protocol treats anything equal to or greater than 16 as unreachable.

RIP 2

The RIP version 2 protocol adds capabilities to RIP. Some of the most notable RIP 2 enhancements follow.
Network Mask

The RIP 1 protocol assumes that all subnetworks of a given network have the same network mask. It uses this assumption to calculate the network masks for all routes received. This assumption prevents subnets with different network masks from being included in RIP packets. RIP 2 adds the ability to explicitly specify the network mask for each network in a packet.

Authentication

RIP 2 packets also can contain one of two types of authentication methods that can be used to verify the validity of the supplied routing data.

The first method is a simple password in which an authentication key of up to 16 characters is included in the packet. If this password does not match what is expected, the packet is discarded. This method provides very little security, as it is possible to learn the authentication key by watching RIP packets.

The second method uses the MD5 algorithm to create a crypto checksum of a RIP packet and an authentication key of up to 16 characters. The transmitted packet does not contain the authentication key itself; instead, it contains a crypto-checksum called the digest. The receiving router performs a calculation using the correct authentication key and discards the packet if the digest does not match. In addition, a sequence number is maintained to prevent the replay of older packets. This method provides stronger assurance that routing data originated from a router with a valid authentication key.

RIP 1

Network Mask

RIP 1 derives the network mask of received networks and hosts from the network mask of the interface from which the packet was received. If a received network or host is on the same natural network as the interface over which it was received, and that network is subnetted (the specified mask is more specific than the natural network mask), then the subnet mask is applied to the destination. If bits outside the mask are set, it is assumed to be a host; otherwise, it is assumed to be a subnet.

Auto Summarization

The Nokia implementation of RIP 1 supports auto summarization; this allows the router to aggregate and redistribute nonclassful routes in RIP 1.

Virtual IP Address Support for VRRP

Beginning with IPSO 3.8.1, Nokia supports the advertising of the virtual IP address of the VRRP virtual router. You can configure RIP to advertise the virtual IP address rather than the actual IP address of the interface. If you enable this option, RIP runs only on the master of the virtual router; on a failover, RIP stops running on the old master and then starts running on the new
master. A traffic break might occur during the time it takes both the VRRP and RIP protocols to
learn the routes again. The larger the network, the more time it would take RIP to synchronize its
database and install routes again. For more information on enabling the advertising of a virtual
IP address when running RIP, see “Configuring RIP,” step 12.

**Note**
Nokia also provides support for BGP, OSPF, and PIM, both Sparse-Mode and Dense-Mode,
to advertise the virtual IP address of the VRRP virtual router, beginning with IPSO 3.8.

**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
any dynamic routing protocol.

## Configuring RIP

Using Network Voyager, you can configure the following options:

### Table 5 RIP 1 Configuration Options Available from Network Voyager

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>You can use either RIP 1 or RIP 2.</td>
</tr>
<tr>
<td>RIP interfaces</td>
<td>You can specify the interfaces on which to run RIP.</td>
</tr>
<tr>
<td>Metric</td>
<td>You can adjust the metric to a given interface to something other than the number of hops. You can use this adjustment to trick the router into taking a better path, for example one that has a faster link speed even though it may have more hops.</td>
</tr>
<tr>
<td>Accept updates</td>
<td>You can configure whether or not to accept updates from other routers speaking RIP. Accepting updates specifies whether RIP packets received from a specified interface is accepted or ignored. Ignoring an update can result in suboptimal routing. Therefore, Nokia recommends that you retain the default setting for accepting updates.</td>
</tr>
<tr>
<td>Transport</td>
<td>You can set this option only for RIP 2. You can set either broadcast or multicast. The RIP 2 option should always be set to multicast unless RIP 1 neighbors exist on the same link and it is desired that they hear the routing updates.</td>
</tr>
<tr>
<td>Auto summarization</td>
<td>You should set auto summarization to aggregate and redistribute nonclassful routes in RIP 1.</td>
</tr>
</tbody>
</table>
To configure RIP

1. Complete “Configuring Ethernet Interfaces” for the interface.

2. Click Config on the home page.

3. Click the RIP link in the Routing Configuration section.

4. Click on for each interface to configure; then click Apply.

5. Click either 1 or 2 in the Version field to select RIP 1 or RIP 2, respectively, for each interface; then click Apply.

6. (Optional) Enter a new cost in the Metric text box for each interface; then click Apply.

7. (Optional) To configure the interface to not accept updates, click on the on radio button in the Accept updates field; then click Apply.

8. (Optional) If you want to configure the interface to not send updates, click on in the Send updates field; then click Apply.

9. (Optional) If you selected RIP 2 for an interface, make sure that Multicast is turned on for that interface; then click Apply.

**Note**
When you use RIP 2, always select the multicast option. Nokia recommends that you not operate RIP 1 and RIP 2 together.

10. (Optional) If you selected RIP 2 for an interface, select the type of authentication scheme to use from the AuthType drop-down list; then click Apply.

    For simple authentication, select Simple from the AuthType drop-down window. Enter the password in the Password edit box; then click Apply.
    The password must be from 1 to 16 characters long.

    For MD5 authentication, select MD5 from the AuthType drop-down list. Enter the password in the MD5 key text box; then click Apply.

11. (Optional) If you selected MD5 as your authentication type and want to ensure interoperability with Cisco routers running RIP MD5 authentication, click **YES** in the Cisco Interoperability field. The default is no, which means that RIP MD5 is set to conform to Nokia platforms. Click Apply.

12. To enable RIP on the virtual IP address associated with this interface, click On; then click Apply.

    This option functions only if this router is a VRRP master. You must also configure VRRP to accept connections to VRRP IPs.

    **Note**
    You must use Monitored Circuit mode when configuring virtual IP support. Do not use VRRPv2 when configuring virtual IP support.

13. To make your changes permanent, click Save.
Configuring RIP Timers

Configuring RIP timers allows you to vary the frequency with which updates are sent as well as when routes are expired. Use care when you set these parameters, as RIP has no protocol mechanism to detect misconfiguration.

**Note**
By default, the update interval is set to 30 seconds and the expire interval is set to 180 seconds.

1. Click Config on the home page.
2. Click the RIP link in the Routing Configuration section.
3. To modify the update interval, enter the new update interval in the Update Interval text box; then click Apply.
4. To modify the expire interval enter the new expire interval in the Expire Interval text box; then click Apply.
5. To make your changes permanent, click Save.

Configuring Auto-Summarization

Auto-summarization allows you to aggregate and redistribute non-classful routes in RIP 1.

**Note**
Auto-summarization applies only to RIP 1.

1. Click Config on the home page.
2. Click the RIP link in the Routing Configuration section.
3. To enable auto-summarization, click on in the Auto-Summarization field; then click Apply.
4. To disable auto-summarization click off in the Auto-Summarization field; then click Apply.
5. To make your changes permanent, click Save.

**Note**
By default, auto-summarization is enabled.
RIP Example

Enabling RIP 1 on an Interface

RIP 1 is an interior gateway protocol that is most commonly used in small, homogeneous networks.

1. First configure the interface as in “Configuring Ethernet Interfaces.”
2. Click Config on the home page.
3. Click the RIP link in the Routing Configuration section.
4. Click on for the eth-s2p1c0 interface; then click Apply.
5. (Optional) Enter a new cost in the Metric edit box for the eth-s2p1c0 interface; then click Apply.

Enabling RIP 2 on an Interface

RIP 2 implements new capabilities to RIP 1: authentication—simple and MD5—and the ability to explicitly specify the network mask for each network in a packet. Because of these new capabilities, Nokia recommends RIP 2 over RIP 1.

1. First configure the interface as in “Configuring Ethernet Interfaces.”
2. Click Config on the home page.
3. Click the RIP link in the Routing Configuration section.
4. Click on for the eth-s2p1c0 interface; then click Apply.
5. Click on in the Version 2 field for the eth-s2p1c0 interface; then click Apply.
6. (Optional) Enter a new cost in the Metric text box for the eth-s2p1c0 interface; then click Apply.
7. (Optional) Select MD5 in the Auth Type drop-down list; then click Apply. Enter a key in the MD5 key text box; then click Apply.

Protocol-Independent Multicast

PIM Description

Protocol-Independent Multicast (PIM) gets its name from the fact that it can work with any existing unicast protocol to perform multicast forwarding. It supports two types of multipoint traffic distribution patterns: dense and sparse.

Dense mode is most useful when:

- Senders and receivers are in close proximity.
- There are few senders and many receivers.
The volume of multicast traffic is high.
The stream of multicast traffic is constant.
Dense-mode PIM resembles Distance Vector Multicast Routing Protocol (DVMRP). Like DVMRP, dense-mode PIM uses Reverse Path Forwarding and the flood-and-prune model.
Sparse mode is most useful when:
- A group has few receivers.
- Senders and receivers are separated by WAN links.
- The type of traffic is intermittent.
Sparse-mode PIM is based on the explicit join model; the protocol sets up the forwarding state for traffic by sending join messages. This model represents a substantial departure from flood-and-prune protocols, such as dense-mode PIM, which set up the forwarding state through the arrival of multicast data.
The implementation does not support enabling both dense mode and sparse mode or either mode of PIM and DVMRP on the same appliance. For more information about PIM, read the following Internet Engineering Task Force (IETF) drafts.

Configuring Virtual IP Support for VRRP
The virtual IP option lets you configure either a PIM sparse-mode or PIM dense-mode interface to advertise the VRRP virtual IP address if the router transitions to become VRRP master after a failover. When you enable virtual IP support for VRRP on a PIM interface, it establishes the neighbor relationship by using the virtual IP if the router is a VRRP master. The master in the VRRP pair sends hello messages that include the virtual IP as the source address and processes PIM control messages from routers that neighbor the VRRP pair. For more information on how to configure this option through Network Voyager, see either “Configuring Dense-Mode PIM” or “Configuring Sparse-Mode PIM.”

Note
You must use monitored-circuit VRRP when configuring virtual IP support for any dynamic routing protocol, including PIM. Do not use VRRPv2 when configuring virtual IP support for any dynamic routing protocol.

PIM Support for IP Clustering
Beginning with IPSO 3.8.1, Nokia supports PIM, both Dense-Mode and Sparse-Mode, in a cluster. Nokia also supports IGMP in a cluster beginning with IPSO 3.8.1.
IPSO clusters have three modes of operation. To use PIM, either Dense-Mode or Sparse-Mode, in an IP cluster, you must use either multicast mode or multicast mode with IGMP as the cluster
mode. Do not use forwarding mode. For more information about IP clustering, see “IP Clustering Description.”

**Note**
Nokia strongly recommends that you not configure PIM or any other routing protocol on the primary or secondary cluster protocol interfaces of an IP cluster.

---

**PIM Dense-Mode**

In the Nokia implementation of PIM Dense-Mode (PIM-DM), all the nodes process PIM control traffic received by the cluster, and only the master processes most of the control traffic sent from the cluster. However, hello messages, for example, are sent by all nodes. Some multicast switches do not forward multicast traffic to interfaces from which they have not received any multicast traffic. To avoid having a multicast switch fail to forward multicast traffic, all cluster nodes send periodic PIM hello messages. All messages from each cluster member have the same source IP address, generation ID, holdtime and designated router priority. Therefore, all neighboring routers view the cluster as a single neighbor even though they receive hello messages from all members of the cluster.

**Note**
The generation ID included in all PIM hello messages does not change when IP clustering is used, regardless of whether and how many times PIM is re-enabled. When IP clustering is implemented, the generation ID is based on the cluster IP address so that all members advertise the same address. The generation ID included in PIM hello messages of all cluster nodes does not change unless the cluster IP address is changed.

The multicast data traffic is load-balanced and can be processed by any of the cluster members. All cluster members sync the dense-mode forwarding state with each other member; therefore, if any cluster member fails, the new member responsible for the corresponding data traffic has the same state as the member that failed.

**PIM Sparse-Mode**

In the Nokia implementation of PIM Sparse-Mode (PIM-SM), depending on its location, the cluster can function as the designated router, the bootstrap router, the rendezvous point or any location in the source or shortest-path tree (SPT). All the nodes process PIM control traffic received by the cluster, and only the master processes most of the control traffic sent from the cluster. However, hello messages, for example, are sent by all nodes. Some multicast switches do not forward multicast traffic to interfaces from which they have not received any multicast traffic. To avoid having a multicast switch fail to forward multicast traffic, all cluster nodes send periodic PIM hello messages. All messages from each cluster member have the same source IP address, generation ID, holdtime and designated router priority. Therefore, all neighboring routers view the cluster as a single neighbor even though they receive hello messages from all members of the cluster.
The generation ID included in all PIM hello messages does not change when IP clustering is used, regardless of whether and how many times PIM is re-enabled. When IP clustering is implemented, the generation ID is based on the cluster IP address so that all members advertise the same address. The generation ID included in PIM hello messages of all cluster nodes does not change unless the cluster IP address is changed.

The multicast data traffic is load-balanced and can be processed by any member of the cluster. However, the cluster is the elected rendezvous point, only the master processes the encapsulated register messages until the SPT is created.

For both PIM-SM and PIM-DM, the Nokia implementation of IP clustering does not forward traffic addressed to 244.0.1.144. IP clustering uses multicast to communicate synchronization messages and has reserved multicast group address 244.0.1.144 for this purpose. When IP clustering is enabled, IGMP membership messages for this group are sent on all interfaces that are part of the cluster. Moreover, since this multicast group is not a link-local group, the designated router on the LAN sends PIM (*, g) PIM messages for this group to the rendezvous point when PIM-SM is implemented. If the Nokia appliance is the designated router, it does not generated such a join message, but it propagates these join messages when sent by another router.

To configure Check Point VPN-1 Pro/Express with IP clustering and either PIM-SM or PIM-DM, make sure you:

1. Use Check Point SmartDashboard to create and configure the cluster gateway object. For more information on how to configure the cluster gateway object, see “Configuring VPN-1 NG for Clustering.”

2. Click the 3rd Party Configuration tab and configure as follows only when PIM-SM or PIM-DM is enabled with IP Clustering:
   a. For the availability mode of the gateway cluster object, select load sharing.
   b. In the third-party drop-down list, select Nokia IP clustering.
   c. Make sure that the check box next to Forward Cluster Members’ IP addresses is not checked. If it is checked, click on the check box to remove the check.
      Make sure that all the other available check boxes are checked.

   All available check boxes should be checked if you are not enabling PIM-SM or PIM-DM in an IP cluster.

   d. Click Ok to save your changes.
PIM and Check Point SecureXL

To make sure that your PIM connections stay accelerated if you have enabled SecureXL, you need to increase the Check Point firewall stateful inspection timeout. To do so:

1. In Check Point SmartDashboard, select Policy > Global Properties > Stateful Inspection.
2. Increase the Other IP protocols virtual session timeout field to 120 seconds.

Configuring Dense-Mode PIM

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the Interfaces section, click On for each interface on which to run PIM.

**Note**
The number of interfaces on which you can run PIM is unlimited.

4. Click Apply, and then click Save to make your changes permanent.
5. (Optional) To configure this interface to use the VRRP virtual IP address, in the Virtual address field, click On.

**Note**
You must use Monitored Circuit mode when configuring virtual IP support for dense-mode PIM. Do not use VRRPv2 when configuring virtual IP support for dense-mode PIM.

6. Click Apply.
7. (Optional) For each interface that is running PIM, enter the specified local address in the Local Address text box. PIM uses this address to send advertisements on the interface.

**Note**
You cannot configure a local address or a virtual address when IP clustering is enabled.

**Note**
If neighboring routers choose advertisement addresses that do not appear to be on a shared subnet, all messages from the neighbor are rejected. A PIM router on a shared LAN must have at least one interface address with a subnet prefix that all neighboring PIM routers share.

8. (Optional) For each interface that is running PIM, enter a new designated router priority in the DR Election Priority text box. The router with the highest priority and the highest IP
The designated router address is elected as the designated router. The default is 1, and the range is 0 to 4294967295 ($2^{32} - 1$).

**Note**
Although you can configure this option, PIM-DM does not use DR Election Priority. On a LAN with more than one router, data forwarding is implemented on the basis of PIM Assert messages. The router with the lowest cost (based on unicast routing) to reach the source of data traffic is elected as the router that forwards traffic. In the case of a tie, the router with the highest IP address is elected to forward traffic.

9. Click Apply, and then click Save to make your change permanent.

**Disabling PIM**

You can disable PIM on one or more interfaces you configured on each Nokia platform.

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the Interfaces section, click Off for each interface on which to disable PIM. To disable PIM entirely, click Off next to each interface that is currently running PIM.
4. Click Apply; then click Save to make your change permanent.

**Setting Advanced Options for Dense-Mode PIM (Optional)**

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the Interfaces section, click On for each interface on which to run PIM.

**Note**
The number of interfaces on which you can run PIM is unlimited.

4. Click Apply, and then click Save to make your changes permanent.
5. (Optional) For each interface that is running PIM, enter the specified local address in the Local Address text box. PIM uses this address to send advertisements on the interface.

**Note**
You cannot configure a local address or a virtual address when IP clustering is enabled.

**Note**
If neighboring routers choose advertisement addresses that do not appear to be on a shared subnet, all messages from the neighbor are rejected. A PIM router on a shared LAN must
have at least one interface address with a subnet prefix that all neighboring PIM routers share.

6. (Optional) For each interface that is running PIM, enter a new designated router priority in the DR Election Priority text box. The router with the highest priority and the highest IP address is elected as the designated router. The default is 1, and the range is 0 to 4294967295 ($2^{32} - 1$).

7. Click Apply, and then click Save to make your changes permanent.

8. Click the Advanced PIM Options link. In the General Timers section, enter a value for the hello interval (in seconds) in the Hello Interval text box. The router uses this interval to send periodic Hello messages on the LAN.

9. In the General Timers section, enter a value for the data interval (in seconds) in the Data Interval text box. This value represents the interval after which the multicast (S, G) state for a silent source is deleted.

10. In the General Timers section, enter a value for the assert interval (in seconds) in the Assert Interval text box. This value represents the interval between the last time an assert is received and when the assert is timed out.

11. In the General Timers section, enter a value for the assert rate limit in the Assert Rate Limit text box. The value represents the number of times per second at which the designated router sends assert messages. The upper limit is 10,000 assert messages per second.

12. In the General Timers section, enter a value (in seconds) for the interval between sending join or prune messages in the Join/Prune Interval text box.

13. In the General Timers section, enter a value for the random delay join or prune interval (in seconds) in the Random Delay Join/Prune Interval text box. This value represents the maximum interval between the time when the Reverse Path Forwarding neighbor changes and when a join/prune message is sent.

14. In the General Timers section, enter a value for the join/prune suppression interval (in seconds) in the Join/Prune Suppression Interval text box. This value represents the mean interval between receiving a join/prune message with a higher hold time and allowing duplicate join/prune messages to be sent again.

**Note**
The join/prune suppression interval should be set at 1.25 times the join/prune interval.

15. In the Assert Ranks section, in the appropriate text box, enter a value for the routing protocol(s) you are using. Assert Rank values are used to compare protocols and determine which router forwards multicast packets on a multiaccess LAN. Assert messages include these values when more than one router can forwarding the multicast packets.
Note
Assert rank values must be the same for all routers on a multiaccess LAN that are running the same protocol.

16. Click Apply.
17. To make your changes permanent, click Save.

Configuring Sparse-Mode PIM

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the PIM Instance Mode field, click On for sparse.
4. Click Apply.
5. In the Interfaces section, click On for each interface on which to run PIM.

Note
The number of interfaces on which you can run PIM is unlimited.

6. Click Apply.
7. (Optional) To configure this interface to use the VRRP virtual IP address, in the Virtual address field, click On.

Note
You must use Monitored Circuit mode when configuring virtual IP support for sparse-mode PIM. Do not use VRRPv2 when configuring virtual IP support for sparse-mode PIM.

8. Click Apply.
9. (Optional) For each interface that is running PIM, enter the specified local address in the Local Address text box. PIM uses this address to send advertisements on the interface. This option is useful only when multiple addresses are configured on the interface.

Note
If neighboring routers choose advertisement addresses that do not appear to be on a shared subnet, then all messages from the neighbor are rejected. A PIM router on a shared LAN must have at least one interface address with a subnet prefix that all neighboring PIM routers share.

10. (Optional) For each interface that is running PIM, enter a new designated router priority in the DR Election Priority text box. The router with the highest priority and the highest IP
The designated router with the highest IP address is chosen. If even one router does not advertise a DR election priority value in its hello messages, DR election is based on the IP addresses. The default is 1, and the range is 0 to 4294967295 (2^32 - 1).

**Note**
To verify whether a PIM neighbor supports DR Election Priority, use the following command, which you can execute from iclid and CLI:

```
show pim neighbor <ip_address>
```
For neighbors that advertise a DR election priority value, the following message appears in the summary:

```
DRPriorityCapable Yes.
```

11. Click Apply.
12. To make your changes permanent, click Save.

### Configuring High-Availability 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 if all of its valid addresses are deleted, then all PIM-enabled interfaces become unavailable and remain in that state until all interfaces are back up.

Beginning with IPSO 3.8, you can configure either a PIM-SM or a PIM-DM interface to advertise the VRRP virtual IP address if the router transitions to become VRRP master after a failover. If you enable this option, you do not need to enable HA mode. For more information about the VRRP virtual IP address option, see “VRRP.”

**Note**
The HA mode applies only to sparse-mode PIM. The HA mode feature does not affect the functioning of dense-mode PIM. You cannot enable HA mode if you enable IP clustering.

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the PIM Instance Mode field, click On for sparse.
4. Click Apply.
5. In the HA Mode field, click On to enable the high-availability mode.
6. Click Apply.
7. In the Interfaces section, click On for each interface to run PIM.
8. Click Apply.
9. (Optional) For each interface that is running PIM, enter the specified local address in the Local Address edit box. PIM uses this address to send advertisements on the interface. This option is useful only when multiple addresses are configured on the interface.

**Note**
If neighboring routers choose advertisement addresses that do not appear to be on a shared subnet, then all messages from the neighbor are rejected. A PIM router on a shared LAN must have at least one interface address with a subnet prefix that all neighboring PIM routers share.

10. (Optional) For each interface that is running PIM, enter a new designated router priority in the DR Election Priority text box. The router with the highest priority and the highest IP address is elected as the designated router. To break a tie, the designated router with the highest IP address is chosen. If even one router does not advertise a DR election priority value in its hello messages, DR election is based on the IP addresses. The default is 1, and the range is 0 to 4294967295 ($2^{32} - 1$).

**Note**
To verify whether a PIM neighbor supports DR Election Priority, use the following command, which you can executed from iclid and CLI:
```
show pim neighbor <ip_address>
```
For neighbors that advertise a DR election priority value, the following message appears in the summary:
```
DRPriorityCapable Yes.
```

11. Click Apply.
12. To make your changes permanent, click Save.

**Configuring this Router as a Candidate Bootstrap and Candidate Rendezvous Point**

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the PIM Instance Mode field, click On button for sparse.
4. Click Apply.
5. In the Interfaces section, click On for each interface on which to run PIM.
**Note**  
The number of interfaces on which you can run PIM is unlimited.

6. Click Apply.

7. In the Sparse Mode Rendezvous Point (RP) Configuration section, to enable this router as a candidate bootstrap router:
   a. Click On in the Bootstrap Router field.
   b. (Optional) Enter the address of the bootstrap router in the Local Address text box. Configure an address for the candidate bootstrap router to help specify the local address used as the identifier in the bootstrap messages. By default, the router chooses an address from one of the interfaces on which PIM is enabled.
   c. (Optional) Enter the bootstrap router priority (0 to 255) in the Priority text box. Use the priority option to help specify the priority to advertise in bootstrap messages. The default priority value is 0.

**Note**  
The domain automatically elects a bootstrap router, based on the assert rank preference values configured. The candidate bootstrap router with the highest preference value is elected the bootstrap router. To break a tie, the bootstrap candidate router with the highest IP address is elected the bootstrap router.

8. In the Sparse Mode Rendezvous Point (RP) Configuration section, to enable this router as a Candidate Rendezvous Point:
   a. Click On in the Candidate RP Router field.
   b. (Optional) Enter the local address of the Candidate Rendezvous Point router in the Local Address field. This router sends Candidate Rendezvous Point messages. Configure an address for the Candidate Rendezvous Point to select the local address used in candidate-RP-advertisements sent to the elected bootstrap router. By default, the router chooses an address from one of the interfaces on which PIM is enabled.
   c. (Optional) Enter the Candidate Rendezvous Point priority (0 to 255) in the Priority text box. Use the priority option to set the priority for this rendezvous point. The lower this value, the higher the priority. The default priority value is 0.

9. (Optional) To configure a multicast address for which this router is designated as the rendezvous point, in the Local RPSET field, enter an IP address in the Multicast address group text box and the address mask length in the Mask length text box.

**Note**  
If you do not configure a multicast address for the router, it advertises as able to function as the rendezvous point for all multicast groups (224/4)
10. Click Apply.
11. To make your changes permanent, click Save.

### Configuring a PIM-SM Static Rendezvous Point

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the PIM Instance Mode field, click On for sparse.
4. Click Apply.
5. In the Interfaces section, click On for each interface on which to run PIM.

**Note**
The number of interfaces on which you can run PIM is unlimited.

6. Click Apply.
7. In the Sparse Mode Rendezvous Point (RP) Configuration section, to enable a Static Rendezvous Point router, click On in the Static RP Router field.

**Note**
Static Rendezvous Point configuration overrides rendezvous point (RP) information received from other RP-dissemination mechanisms, such as bootstrap routers.

8. Enter the IP address of the router to configure as the static rendezvous point in the RP Address text box. Click Apply.
9. (Optional) Enter the multicast group address and prefix length in the Multicast group address and Mask length text boxes. Click Apply.

**Note**
If you do not configure a multicast group address and prefix length for this Static Rendezvous Point, it functions by default as the rendezvous point for all multicast groups (224.0.0.0/4).

10. Click Save to make your changes permanent.

### Setting Advanced Options for Sparse-Mode PIM (Optional)

1. Click Config on the home page.
2. Click the PIM link in the Routing Configuration section.
3. In the PIM Instance Mode field, click On for sparse.
4. Click Apply.

5. In the Interfaces section, click On each interface on which to run PIM.

**Note**
The number of interfaces on which you can run PIM is unlimited.

6. Click Apply.

7. Click the Advanced PIM Options link.
   In the Sparse Mode Timers section, enter a value for the register suppression interval (in seconds) in the Register-Suppression Interval text box.
   This value represents the mean interval between receiving a Register-Stop message and allowing Register messages to be sent again.

8. In the Sparse Mode Timers section, enter a value for the bootstrap interval for candidate bootstrap routers (in seconds) in the Bootstrap Interval text box.
   This value represents the interval between which bootstrap advertisement messages are sent.

9. In the Sparse Mode Timers section, enter a value for the candidate rendezvous point advertisement interval (in seconds) in the Candidate RP-Advertisement Interval text box.
   This value represents the interval between which Candidate Rendezvous Point routers send Candidate-RP-Advertisement messages.

10. In the Sparse Mode Timers section, enter a value for the shortest path tree threshold (in kilobits per second) in the Threshold (kpbs) text box.
    Enter an IP address for the multicast group to which the SPT threshold applies in the Multicast Group ID text box. Enter the mask length for the group multicast address in the Mask Length edit box. When the data rate for a sparse-mode group exceeds the shortest-path-tree threshold at the last-hop router, an (S,G) entry is created and a join/prune message is sent toward the source. Setting this option builds a shortest-path tree from the source S to the last-hop router.

11. Click Apply, and then click Save to make your changes permanent.

12. (Optional) In the General Timers section, enter a value for the hello interval (in seconds) in the Hello Interval edit box.
    The router uses this interval to send periodic Hello messages on the LAN.

13. (Optional) In the General Timers section, enter a value for the data interval (in seconds) in the Data Interval text box.
    This value represents the interval after which the multicast (S, G) state for a silent source is deleted.

14. (Optional) In the General Timers section, enter a value for the assert interval (in seconds) in the Assert Interval text box.
    This value represents the interval between the last time an assert is received and when the assert is timed out.

15. (Optional) In the General Timers section, enter a value for the assert rate limit in the Assert Rate Limit text box.
The value represents the number of times per second at which the designated router sends assert messages. The upper limit is 10,000 assert messages per second.

16. (Optional) In the General Timers section, enter a value (in seconds) for the interval between sending join/prune messages in the Join/Prune Interval text box.

17. (Optional) In the General Timers section, enter a value for the random delay join/prune interval (in seconds) in the Random Delay Join/Prune Interval text box. This value represents the maximum interval between the time when the reverse path forwarding neighbor changes and when a join/prune message is sent.

18. (Optional) In the General Timers section, enter a value for the join/prune suppression interval (in seconds) in the Join/Prune Suppression Interval text box. This value represents the mean interval between receiving a join/prune message with a higher Holdtime and allowing duplicate join/prune messages to be sent again.

**Note**
The join/prune suppression interval should be set at 1.25 times the join/prune interval.

19. (Optional) In the Assert Ranks section, enter a value for the routing protocol(s) you are using in the appropriate text box. Assert Rank values are used to compare protocols and determine which router forwards multicast packets on a multiaccess LAN. Assert messages include these values when more than one router can forwarding the multicast packets.

**Note**
Assert rank values must be the same for all routers on a multiaccess LAN that are running the same protocol.

20. Click Apply.

21. (Optional) The checksum of the PIM register messages is calculated without including the multicast payload. Earlier releases of the Cisco IOS calculate the checksum by including the multicast payload. If you experience difficulties having PIM register messages sent by the 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.

   a. To enable Cisco compatibility for register checksums, click On in the Cisco Compatibility Register Checksums field.

   b. Click Apply, and then click Save to make your change permanent.

22. To make your changes permanent, click Save.
Debugging PIM

The following iclid commands can assist you in debugging PIM:

<table>
<thead>
<tr>
<th>Command</th>
<th>Shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim interface</td>
<td>which interfaces are running PIM, their status, and the mode they are running. This command also displays the interface and its DR priority and the number of PIM neighbors on the interface.</td>
</tr>
<tr>
<td>show pim neighbors</td>
<td>the IP address of each PIM neighbor and the interface on which the neighbor is present. This command also displays the neighbor’s DR priority, generation ID, holdtime and the time the neighbor is set to expire based on the holdtime received in the most recent hello message.</td>
</tr>
<tr>
<td>show pim statistics</td>
<td>the number of different types of PIM packets received and transmitted and any associated errors.</td>
</tr>
<tr>
<td>show mfc cache</td>
<td>multicast source and group forwarding state by prefix.</td>
</tr>
<tr>
<td>show mfc interfaces</td>
<td>shows multicast source and group forwarding state by interface.</td>
</tr>
</tbody>
</table>

The following iclid commands can assist you in debugging sparse-mode PIM (PIM-SM):

<table>
<thead>
<tr>
<th>Command</th>
<th>Shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim bootstrap</td>
<td>the IP address and state of the Bootstrap router.</td>
</tr>
<tr>
<td>show pim candidate-rp</td>
<td>the state of the Candidate Rendezvous Point state machine.</td>
</tr>
<tr>
<td>show pim joins</td>
<td>PIM’s view of the join-prune (*, G and S, G) state, including RP for the group, incoming, and outgoing interface(s), interaction with the multicast forwarding cache and the presence of local members. To view the equivalent information for dense-mode PIM, use the show mfc cache command.</td>
</tr>
<tr>
<td>show pim rps</td>
<td>the active RP-set, including the RP addresses, their type (or source of information about them) and the groups for which they are configured to act as RP.</td>
</tr>
<tr>
<td>show pim group-rp-mapping &lt;group-address&gt;</td>
<td>the RP selected for a particular group based on information from the active RP-set.</td>
</tr>
<tr>
<td>show pim sparse-mode statistics</td>
<td>error statistics for multicast forwarding cache (MFC); Bootstrap Router (BSR) messages; Candidate Rendezvous Point (CRP) advertisements; and the Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>

Use the Trace Options feature to log information about errors and events.

1. Click Config on the home page.
2. Click the Routing Options link in the Routing Configuration section.
3. In the Trace Options section, click on the Add Option drop-down window in the PIM field. Select each option for which you want to log information. You must select each option one at a time and click Apply after you select each option. For each option you select, its name and on and off radio buttons appear just above the drop-down window. To disable any of the options you have selected, click the off radio button, and then click Apply.

4. Click Save to make your changes permanent.

The following trace options apply both to dense-mode and sparse-mode implementations:
- **Assert**: traces PIM assert messages.
- **Hello**: traces PIM router hello messages.
- **Join**: traces PIM join/prune messages
- **MFC**: traces calls to or from the multicast forwarding cache
- **MRT**: traces PIM multicast routing table events.
- **Packets**: traces all PIM packets.
- **Trap**: Trace PIM trap messages.
- **All**: traces all PIM events and packets.

The following trace options apply to sparse-mode implementations only:
- **Bootstrap**: traces bootstrap messages.
- **CRP**: traces candidate-RP-advertisements.
- **RP**: traces RP-specific events, including both RP set-specific and bootstrap-specific events.
- **Register**: traces register and register-stop packets.

The following trace option applies to dense-mode implementations only:
- **Graft**: traces graft and graft acknowledgment packets

**IGRP**

**IGRP Description**

The *Inter-Gateway Routing Protocol (IGRP)* is a widely used interior gateway protocol (IGP). Like RIP, IGRP is an implementation of a distance-vector, or Bellman-Ford, routing protocol for local networks. As specified, IGRP modifies the basic Bellman-Ford algorithm in three ways:
- Uses a vector of metrics.
- Allows for multiple paths to a single destination, thus allowing for load sharing.
- Provides stability during topology changes because new features.

This document provides background information and cites differences with other IGRP implementations.

A router running IGRP broadcasts routing updates at periodic intervals, in addition to updates that are sent immediately in response to some type of topology change. An update message includes the following information:
An IGRP update packet contains three types of routine entries.

- Interior
- System
- Exterior

Each entry includes three bytes of an IP address. The fourth byte is determined by the type of the route entry. Interior routes are passed between links that are subnetted from the same class IP address. System routes are classful IP routes exchanged within an autonomous system. Exterior routes are like system routes, but also are used for installing a default route. In addition, the following metrics are included for each entry:

- Delay
- Bandwidth
- Math MTU
- Reliability
- Load
- Hop count

IGRP calculates a single composite metric from this vector to compare routes. Since the metrics attempt to physically characterize the path to a destination, IGRP attempts to provide optimal routing.

IGRP has two packet types.

- Request packet
- Update packet

IGRP dynamically builds its routing table from information received in IGRP update messages. On startup, IGRP issues a request on all IGRP-enabled interfaces. If a system is configured to supply IGRP, it hears the request and responds with an update message based on the current routing database.

IGRP processes update messages differently depending on whether or not holddowns are enabled.

If all the following conditions are true, the route is deleted and put into a holddown:

- Holddowns are enabled.
- Route entry comes from the originator of the route.
- Calculated composite metric is worse than composite metric of the existing route by more than 10 percent.

During this holddown period, no other updates for that route are accepted from any source.

If all the following are true, the route is deleted (note that it does not enter a holddown period):
- Holddowns are disabled.
- Route entry comes from the originator of the route.
- Hop count has increased.
- Calculated composite metric is greater than the composite metric of the existing route.

In both cases, if a route is not in holddown and a route entry in an update message indicates it has a better metric, the new route is adopted. In general, routing updates are issued every 90 seconds. If a router is not heard from for 270 seconds, all routes from that router are deleted from the routing database. If holddowns are enabled and a route is deleted, the route remains in the holddown for 280 seconds. If a router is not heard from for 630 seconds, all routes from that router are no longer announced (that is, after the initial 270 seconds, such routes are advertised as unreachable).

This implementation of IGRP does not support all of the features listed in the specification. The following is a list of non-supported features:
- Multiple type of service (TOS) routing
- Variance factor set only to a value of one
- Equal or roughly equal cost path splitting

This implementation has interoperated with other vendor’s implementations of IGRP, namely Cisco IOS version 10.3(6) and 11.0(7). Listed here for completeness are a few minor observable differences between the Nokia and the Cisco implementations (no interoperability problems have occurred to date because to these differences):
- **Validity Checks**—packets that are malformed (that is, those that have trailing data on a request packet, have nonzero data in a field that must be zero, or have route counts in an update packet that do not agree with the actual packet size) are rejected. Other implementations allow such packets. You can disable some of these checks for request packets, but not for the update packets.
- **Valid Neighbors**— packets that have a source address from a non-local network are ignored. You cannot disable this behavior.
- **Duplicate Entries in an Update**—if an update message contains duplicate new paths, holddowns are enabled, and if each of the duplicate composite metrics differ by more than 10 percent, the route is not put in holddown. The path with the best metric is installed. Other implementations treat each duplicate path as if it arrived in separate update messages. In this case, place the route into holddown.
- **Triggered Update on Route Expiration**—when a route expires, a triggered update message is generated at the moment of expiration, marking the route as unreachable. Other implementations wait until the next scheduled update message to mark the route as unreachable. In this latter case, the route is actually not marked as unreachable until the next scheduled update cycle (although this seems somewhat contradictory).
- **Specific Split Horizon**—does not implement specific split horizon. Split horizon processing means that routes learned from an interface are not advertised back out that same interface. Specific split horizon occurs when a request is made. In this case, only routes that use the requestor as the next hop are omitted from the response.
■ **Poison Reverse**—uses simple split horizon; that is, poison reverse is not performed. Other implementations use a form of poison reverse in which at least a single update advertises an expired route as being unreachable on the interface from which the route was learned.

■ **Forwarding to Unreachable Routes**—when a route expires or is marked as unreachable from the originator, the route is removed from the forwarding table. In the absence of a default or more general route, packets destined for this address are dropped. Other implementations continue to forward packets to routes marked as unreachable until a route is flushed from the table.

### Generation of Exterior Routes

IGRP has three defined types of routes that an update packet can carry:

- Interior
- System
- Exterior

**Note**

For a detailed explanation of the different route types, see the IGRP specification

An exterior route is conceptually the same as a system route, with the added feature that an exterior route can be used as a default route. Exterior routes are always propagated as exterior. When it is necessary to locally generate an exterior default route, redistribute the default route into IGRP. The next-hop network of the default route, determined from the next-hop interface, is advertised in the appropriate IGRP update messages as exterior. A direct interface route is advertised only once. Therefore, a direct interface route that is marked exterior is not also advertised as interior or as system.

### Aliased Interfaces

When an interface has multiple addresses configured, each address is treated as a distinct interface since it represents a logical subnet. Such a configuration implies that an update is sent for each IGRP-configured address. In the configuration syntax, you can specify a particular address of an interface on which to run IGRP as opposed to the complete interface (all addresses of the interface).

### IGRP Aggregation

Most routing aggregation occurs only if explicitly configured; therefore, it is worth noting some of the implicit aggregation that occurs in IGRP. By definition, no mask information is included in the IGRP route entry. System and exterior routes have an implied mask of the natural classful mask. Interior routes are propagated from one interface to another only if the two interfaces are subnetted from the same IP class address and have the same subnet mask. Otherwise, an interior route is converted (an aggregation occurs) to a system route. Any supernetted routes
redistributed into IGRP are ignored. In sum, any route redistributed into IGRP that is marked as a system or exterior route has the natural class mask applied to the route to determine what route should be advertised in an update.

## Configuring IGRP

**Note**
IGRP configuration of an interface is available only if you are licensed for IGRP on your IP router. (See the *Licenses* link on the Configuration page.)

1. Complete “Configuring Ethernet Interfaces” for the interface.
2. Click Config on the home page.
3. Click the IGRP link in the Routing Configuration section.
4. Enter the AS number in the Autonomous System Number text box.
5. Click on for each interface to configure; then click Apply.
6. (Optional) Enter a new delay metric in the Delay text box for each interface (for example, 100 for 10 Mbps Ethernet); then click Apply.
   
   The delay is measured in units of 10 microseconds.
7. (Optional) Enter a new bandwidth metric in the Bandwidth text box for each interface (for example, 1000 for 10Mbps Ethernet); then click Apply.
   
   The bandwidth is entered in bits per second scaled by a factor of 10,000,000 (10,000,000/x Kbps), where x is the actual bandwidth of the interface.
8. (Optional) In the Protocol section, enter a new bandwidth multiplier in the K1 (bandwidth multiplier) text box; then click Apply.
   
   K1 is used to globally influence bandwidth over delay.
9. (Optional) In the Protocol section, enter a new delay multiplier in the K2 (delay multiplier) text box; then click Apply.
   
   K2 is used to globally influence delay over bandwidth.
10. (Optional) In the Protocol section, click No in the Holddown field; then click Apply.
    
    This action disables the global route holddown parameter.
11. (Optional) In the Protocol section, enter the new maximum hop count metric in the Maximum hop count text box; then click Apply.
    
    This option is used to prevent infinite looping.
12. (Optional) In the Protocol section, enter the new update interval metric in the Update interval text box; then click Apply.
    
    This number determines how often route updates are sent out on all of the interfaces.
13. (Optional) In the Protocol section, enter the new invalid interval metric in the Invalid interval text box; then click Apply.

14. (Optional) In the Protocol section, enter the new hold interval metric in the Hold interval text box; then click Apply.

15. (Optional) In the Protocol section, enter the new flush interval metric in the Flush interval text box; then click Apply.

16. (Optional) In the Protocol section, click Yes in the No Check Zero field; then click Apply.
   Leave this field set to No to interoperate with Cisco equipment.

17. To make your changes permanent, click Save.

IGRP Example

**Note**
You must have an IGRP license and the option selected on the Licenses page to use this feature.

**Enabling IGRP on an interface:**

1. Configure the interfaces as in “Configuring Ethernet Interfaces.”
2. Click Config on the home page.
3. Click the IGRP link in the Routing Configuration section.
4. Enter the AS number in the Autonomous System Number text box.
5. (Required) Enter a delay metric in the Delay text box for each interface; then click Apply.
6. (Required) Enter a bandwidth metric in the Bandwidth text box for each interface; then click Apply.
7. (Required) Enter a reliability metric in the Reliability text box for each interface; then click Apply.
8. (Required) Enter the load metric in the load text box for each interface; then click Apply.
   The load metric is a fraction of 255.
9. (Required) Enter the MTU metric in the metric text box for each interface; then click Apply.
   A larger MTU reduces the IGRP cost.
10. Click on for eth-s1p1c0; then click Apply.
DVMRP

DVMRP Description

The Distance Vector Multicast Routing Protocol (DVMRP) is a distance vector protocol that calculates a source-rooted multicast distribution tree and provides routing of IP multicast datagrams over an IP internetwork. DVMRP uses the Bellman-Ford routing protocol to maintain topological knowledge. DVMRP uses this information to implement Reverse Path Forwarding (RPF) a multicast forwarding algorithm.

RPF forwards a multicast datagram to members of the destination group along a shortest (reverse) path tree that is rooted at the subnet on which the datagram originates. Truncated Reverse Path Broadcasting (TRPB) uses the IGMP-collected group membership state to avoid forwarding on leaf networks that do not contain group members.

TRPB calculates a distribution tree across all multicast routers and only saves packet transmissions on the leaf networks that do not contain group members. Reverse Path Multicast (RPM) allows the leaf routers to prune the distribution tree to the minimum multicast distribution tree. RPM minimizes packet transmissions by not forwarding datagrams along branches that do not lead to any group members.

Multicast capabilities are not always present in current Internet-based networks. Multicast packets must sometimes pass through a router that does not support IP multicasting to reach their destination. This behavior is allowed because DVMRP defines a virtual tunnel interface between two multicast-capable routers that might be connected by multiple non-multicast capable IP hops.

DVMRP encapsulates IP multicast packets for transmission through tunnels so that they look like normal unicast datagrams to intervening routers and subnets. DVMRP adds the encapsulation when a packet enters a tunnel and removes it when the packet exits from a tunnel. The packets are encapsulated with the IP-in-IP protocol (IP protocol number 4). This tunneling mechanism allows you to establish a virtual internet that is independent from the physical internet.

Features

- Supports DVMRP v.3
- Prune and graft messages
- Generation ID
- Capability flags
- Supports interface metric and threshold configuration.
- Supports interface administrative scoping on the 239.X.X.X addresses.
- Supports interfaces with secondary addresses.
- Supports iclid wizards.
- Supports the Monitoring template.
- Correctly tracks the number of subordinate routers per route.

**Network Voyager Interface**

Using Network Voyager, you can configure the following options:

- DVMRP interfaces
- New minimum time to live (TTL) threshold for each interface
- New cost metric for sending multicast packets for each interface

**Configuring DVMRP**

1. Complete “Configuring Ethernet Interfaces” for the interface.
2. Click Config on the home page.
3. Click the DVMRP link in the Routing Configuration section.
4. For each interface you want to configure for DVMRP, Click on for the interface; then click Apply.
5. (Optional) Enter a new minimum IP time to live (TTL) threshold in the Threshold text box for each interface; then click Apply.
6. (Optional) Enter a new cost metric for sending multicast packets in the Metric text box for each interface; then click Apply.
7. To make your changes permanent, click Save.

**Configuring DVMRP Timers**

You can configure values for DVMRP timers. Nokia recommends that if you have a core multicast network, you configure the timer values so that they are uniform throughout a network. Otherwise, you can rely on the default timer values. You can configure two neighbor-specific timers, three routing specific-timers and a cache-specific timer.

1. Click Config on the home page.
2. Click the DVMRP link in the Routing Configuration section.
3. Click the Advanced DVMRP options link.
   This action takes you to Advanced Options for DVMRP page.
4. (Optional) Enter a value between 5 and 30 in the Neighbor probe interval text box to set the interval, in seconds, at which DVMRP neighbor probe messages are sent from each interface.
   The default is 10 seconds
5. (Optional) Enter a value between 35 and 8000 in the Neighbor time-out interval text box to set the interval, in seconds, after which a silent neighbor is timed out.
The default for DVMRPv3 neighbors is 35, and for non-DVMRPv3 neighbors the default is 140.

6. (Optional) Enter a value between 10 and 2000 in the Route report interval text box to set the interval, in seconds, at which routing updates are sent on each DVMRP interface. The default is 60 seconds.

7. (Optional) Enter a value between 20 and 4000 in the Route expiration time text box to set the interval, in seconds, after which a route that has not been refreshed is placed in the route hold-down queue. The default is 140 seconds.

8. (Optional) Enter a value between 0 and 8000 in the Route hold-down period text box to set the interval, in seconds, for which an expired route is kept in the hold-down queue before it is deleted from the route database. Set this interval to twice the value of the route report interval. The default is 120 seconds.

9. (Optional) Enter a value between 60 and 86400 in the Cache lifetime text box to set the interval, in seconds, that a cached multicast forwarding entry is maintained in the kernel forwarding table before it is timed out because of inactivity. The default is 300 seconds.

10. Click Apply, and then click Save to make your changes permanent.

**IGMP**

**IGMP Description**

Internet Group Management Protocol (IGMP) allows hosts on multiaccess networks to inform locally attached routers of their group membership information. Hosts share their group membership information by multicasting IGMP host membership reports. Multicast routers listen for these host membership reports, and then exchange this information with other multicast routers.

The group membership reporting protocol includes two types of messages: host membership query and host membership report. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2. Protocol operation requires that a designated querier router be elected on each subnet and that it periodically multicast a host membership query to the all-hosts group.

Hosts respond to a query by generating host membership reports for each multicast group to which they belong. These reports are sent to the group being reported, which allows other active members on the subnet to cancel their reports. This behavior limits the number of reports generated to one for each active group on the subnet. This exchange allows the multicast routers to maintain a database of all active host groups on each of their attached subnets. A group is declared inactive (expired) when no report is received for several query intervals.

The IGMPv2 protocol adds a leave group message and uses an unused field in the IGMPv1 host membership query message to specify a maximum response time. The leave group message allows a host to report when its membership in a multicast group terminates. Then, the IGMP
querier router can send a group-directed query with a very small maximum response time to probe for any remaining active group members. This accelerated leave extension can reduce the time required to expire a group and prune the multicast distribution tree from minutes, down to several seconds.

The unicast traceroute program allows the tracing of a path from one device to another, using mechanisms that already exist in IP. Unfortunately, you cannot apply such mechanisms to IP multicast packets. The key mechanism for unicast traceroute is the ICMP TTL exceeded message that is specifically precluded as a response to multicast packets. The traceroute facility implemented within IPSRD conforms to the traceroute facility for IP multicast draft specification.

Features

- Complete IGMPv.2 functionality
- Multicast traceroute
- Complete configurability of protocol timers
- Administratively-blocked groups
- Support for interfaces with secondary addresses
- iclid wizards
- Monitoring template

Network Voyager Interface

Using Network Voyager, you can configure the following options:

- Version number
- Loss robustness
- Query interval
- Query response interval
- Last-member query interval

Additionally, you can enable and disable router alert.

IGMP Support for IP Clustering

Beginning with IPSO 3.8.1, Nokia supports IGMP in an IP cluster as part of the new support for PIM, both dense-mode and sparse-mode, in an IP cluster. The support for IGMP in an IP cluster ensures synchronization of IGMP state from master to members when a new node running PIM joins the cluster. For more information about PIM and IP Clustering, see “PIM Description,” and “IP Clustering Description.”
Configuring IGMP

1. Complete “Configuring Ethernet Interfaces” for the interface.

2. Configure a multicast routing protocol, such as PIM or DVMRP. The IGMP feature supports IP multicast groups on a network and functions only in conjunction with a multicast routing protocol to calculate a multicast distribution tree. For more information on multicast routing protocols supported by IPSO, see “PIM Description” or “DVMRP Description.”

3. Click Config on the home page.

4. Click the IGMP link in the Routing Configuration section.

5. Complete the following steps for each interface on which you enabled a multicast routing protocol.

6. Click the appropriate Version button to enable either version 1 or 2; then click Apply. The default is version 2

Note
A router configured for IGMP version 2 can interoperate with hosts running either IGMP version 1 or version 2. Nokia recommends that you use version 1 only on networks that include multicast routers that are not upgraded to IGMP version 2.

7. (Optional) Enter the loss robustness value in the Loss robustness text box; then click Apply. The range is 1 to 255, and the default is 2.

8. (Optional) Enter the query interval in the Query interval text box; then click Apply. This value specifies the interval, in seconds, that the querier router sends IGMP general queries. The default is 125, and the range is 1 to 3600.

9. (Optional) Enter the query response interval in the Query response interval text box; then click Apply. This value specifies the maximum response time, in seconds, inserted into the periodic IGMP general queries. The higher the value the longer the interval between host IGMP reports, which reduces burstiness. This value must be lower than that of the query interval. The default is 10, and the range is 1 to 25.

10. (Optional) Enter the last member query interval in the Last member query interval text box; then click Apply. This value specifies the maximum response time, in seconds, inserted into IGMP group-specific queries. A lower value results in less time to detect the loss of the last member of a multicast group. This value must be lower than that of the query interval. The default is 1, and the range is 1 to 25.

11. (Optional) Click On in the Disable router alert field to actively disable the insertion of the IP router alert typically included in IGMP messages. Disabling this option is useful when interoperating with broken IP implementations that might otherwise discard packets from the specified interface. The default is Off, meaning that the IGMP messages include the IP router alert. Click Apply.
12. To make your changes permanent, click Save.

Static Routes

Static Routes Description

Static routes are routes that you manually configure in the routing table. Static routes do not change and are not dynamic (hence the name). Static routes cause packets addresses to the destination to take a specified next hop. Static routes allow you to add routes to destinations that are not known by dynamic routing protocols. Statics can also be used in providing a default route.

Static routes consist of the following:

- Destination
- Type
- Next-hop gateway

Static routes can be one of the following types:

- Normal
  A normal static route is one used to forward packets for a given destination in the direction indicated by the configured router.

- Black hole
  A black hole static route is a route that uses the loopback address as the next hop. This route discards packets that match the route for a given destination.

- Reject
  A reject static route is a route that uses the loopback address as the next hop. This route discards packets that match the route for a given destination and sends an ICMP unreachable message back to the sender of the packet.

Configuring a Default Route

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
3. To enable a default route, click on in the Default field; then click Apply.
4. Select the type of next hop the static route will take from the Next Hop Type drop-down list.
5. Select the gateway type of the next hop router from the Gateway Type drop-down list.
Note
Gateway Address specifies the IP address of the gateway to which forwarding packets for each static route are sent. This must be the address of a router that is directly connected to the system you are configuring.

Note
Gateway Logical Name is valid only if the next-hop gateway is an unnumbered interface and you do not know the IP address of the gateway.

6. Click Apply.
7. Enter the IP address of the default router in the Gateway text box; then click Apply.
8. To disable a default route, click off in the Default field; then click Apply.
9. To make your changes permanent, click Save.

Creating a Static Route

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
3. Enter the network prefix in the New Static Route text box.
4. Enter the mask length (number of bits) in the Mask Length text box.
5. Select the type of next hop the static route will take from the Next Hop Type drop-down list.
6. Select the gateway type of the next hop router from the Gateway Type drop-down list.

Note
Gateway Address specifies the IP address of the gateway to which forwarding packets for each static route are sent. This must be the address of a router that is directly connected to the system you are configuring.

Note
Gateway Logical Name is valid only if the next-hop gateway is an unnumbered interface and you do not know the IP address of the gateway.

7. Click Apply.
8. Enter the IP address of the next hop router in the Gateway edit box; then click Apply.
9. To make your changes permanent, click Save.
Setting the Rank for Static Routes

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
   You are now in the Static Routes page. Click the Advanced Options link.
3. To set the rank for each static route you have configured, enter a value in the Rank text box.
   The system uses the rank value to determine which route to use when routes are present from different protocols to the same destination. For each route, the system uses the route from the protocol with the lowest rank number.
   The default for static routes is 60. The range you can enter is 0 to 255.
4. Click Apply, and then click Save to make your changes permanent.

Configuring Multiple Static Routes

The implementation allows you to add and configure many static routes at the same time.

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
3. In the Quick-add static routes field, click the Quick-add next hop type drop-down list, and select Normal, Reject, or Black hole.
   The default is Normal. For more information on static route types, see “Static Routes Description.”
4. In the Quick-add static routes edit box, enter an IP address, its mask length, and add one or more next-hop IP addresses for each static route you want to add. Use the following format:
   IP address/mask length next hop IP address
   The IP addresses must be specified in a dotted-quad format ([0 to 255],[0 to 255],[0 to 255],[0 to 255])
   The range for the mask length is 1 to 32.
   For example, to add a static route to 205.226. 10.0 with a mask length of 24 and next hops of 10.1.1.1 and 10.1.1.2, enter:
   205.226.10.0/24 10.1.1.1 10.1.1.2
5. Press Enter after each entry you make for a static route.

Note
You cannot configure a logical interface through the quick-add static routes option.

6. Click Apply.
   The newly configured additional static routes appear in the Static Route field at the top of the Static Routes page.
7. Click Save to make your changes permanent.

Adding and Managing Static Routes Example

The figure below shows the network configuration for the example.

In this example, Nokia Platform A is connected to the Internet, with no routing occurring on the interface connected to the Internet (no OSPF or BGP). A corporate WAN is between Nokia platform B and Nokia platform C, and no routing occurs on this link. Use static routes so that the remote PC LAN can have Internet access.

Static routes apply in many areas, such as connections to the Internet, across corporate WANs, and creating routing boundaries between two routing domains.

Creating/Removing Static Routes

For the preceding example, one static default route to the Internet is created through 192.168.22.1/22, and a static route is created across the corporate WAN to the remote PC LAN across 192.168.26.68/30.

Creating a static default route

1. Use Network Voyager to connect to Nokia Platform A.
2. Click Config on the home page.
3. Click the Static Routes link in the Routing Configuration section.
4. Click on in the Default field; then click Apply.
5. In the gateway text box enter: 192.168.22.1; then click Apply.
You should now have one static default route in your routing tables on Nokia Platform A. For the rest of the network to know about this route, you must redistribute the static route to OSPF. After you complete this task, any gateway connected to Nokia Platform B has the default route with 192.168.22.1 as the next hop in the routing tables. Any packet not destined for the 192.168.22.0/22 net is directed towards 192.168.22.1.

**Creating a static route (non-default)**

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
3. In the New Static Route text box enter: 192.168.24.0.
4. In the Mask Length text box enter: 24.
5. In the Gateway text box enter: 192.168.26.70; then click Apply.

If you have configured OSPF or RIP on your remote office network, you now have connectivity to the Internet.

**Disabling a static route**

1. Click Config on the Home page.
2. Click the Static Routes link in the Routing Configuration section.
3. Click off for the route you want to disable; then click Apply.

### Backup Static Routes

**Backup Static Routes Description**

Static routes can become unavailable if the interface related to the currently configured gateway is down. In this scenario, you can use a backup static route instead.

To implement backup static routes, you need to prioritize them. The priority values range from 1 to 8, with 1 having the highest priority. If more than one gateway belongs to the same priority, a multipath static route is installed. If a directly attached interface is down, all the gateways that belong to the interface are deleted from the list of next-hop selections.

Backup static routes are useful for default routes, but you can't use them for any static route.

**Creating a Backup Static Route**

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
Note
This example assumes that a static route has already been configured and the task is to add backup gateways.

3. Enter the IP address of the gateway in the Additional gateway text box.
4. Enter the priority value in the Priority text box; then click Apply.

   The IP address of the additional gateway that you entered appears in the Gateway column, and new Additional gateway and Priority edit boxes are displayed.

   To add more backup static routes, repeat steps 3 and 4.
5. To make your changes permanent, click Save.

Deleting a Backup Static Route

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
3. Click off for the backup static route to delete; then click Apply.
4. To make your changes permanent, click Save.

Route Aggregation

Route Aggregation Description

Route aggregation allows you to take numerous specific routes and aggregate them into one encompassing route. Route aggregation can reduce the number of routes that a given protocol advertises. The aggregates are activated by contributing routes. For example, if a router has many interface routes subnetted from a class C and is running RIP 2 on another interface, the interface routes can be used to create an aggregate route (of the class C) that can then be redistributed into RIP. Creating an aggregate route reduces the number of routes advertised using RIP. You must take care must be taken when aggregating if the route that is aggregated contains holes.

An aggregate route is created by first specifying the network address and mask length. Second, a set of contributing routes must be provided. A contributing route is defined when a source (for example, a routing protocol, a static route, an interface route) and a route filter (a prefix) are specified. An aggregate route can have many contributing routes, but at least one of the routes must be present to generate an aggregate.

Aggregate routes are not used for packet forwarding by the originator of the aggregate route, only by the receiver. A router receiving a packet that does not match one of the component routes that led to the generation of an aggregate route responds with an ICMP network unreachable message. This message prevents packets for unknown component routes from
following a default route into another network where they would be continually forwarded back
to the border router until their TTL expires.

Creating Aggregate Routes

1. Click Config on the home page.
2. Click the Route Aggregation link in the Routing Configuration section.
3. Enter the prefix for the new contributing route in the Prefix for new aggregate text box.
4. Enter the mask length (number of bits) in the Mask Length field; then click Apply.
   The mask length is the prefix length that matches the IP address to form an aggregate to a
   single routing table entry.
5. Scroll through the New Contributing Protocol list and click the protocol to use for the new
   aggregate route; then click Apply.
6. Click on in the Contribute All Routes from <protocol> field.
7. (Optional) If you want to specify a prefix, fill in the address and mask in the New
   Contributing Route from <protocol> field; then click Apply.
8. To make your changes permanent, click Save.

Removing Aggregate Routes

1. Click Config on the home page.
2. Click the Aggregation link in the Routing Configuration section.
3. Click off for the aggregate route disable; then click Apply.
4. To make your changes permanent, click Save.
Route Aggregation Example

The figure below shows the network configuration for the example.

In the preceding figure Nokia Platform B, Nokia Platform C, and Nokia Platform D are running OSPF with the backbone area. Nokia Platform A is running OSPF on one interface and RIP 1 on the backbone side interface.

Assume that all the interfaces are configured with the addresses and the routing protocol as shown in the figure. Configure route aggregation of 192.168.24.0/24 from the OSPF side to the RIP side.

1. Initiate a Network Voyager session to Nokia Platform A.
2. Click Config on the home page.
3. Click the Route Aggregation link in the Routing Configuration section.
4. Enter 192.168.24.0 in the Prefix for new aggregate text box.
5. Enter 24 in the Mask Length edit box; then click Apply.
6. Click OSPF2 in the New Contributing Protocol drop-down list; then click Apply.
7. Click on in the Contribute all matching routes from OSPF2 field; then click Apply.
8. Click direct in the New Contributing Protocol drop-down list; then click Apply.
9. Click on in the Contribute All Matching Routes from direct field; then click Apply.
10. Click Top.
11. Click the Route Redistribution link in the Routing Configuration section.
12. Click the Aggregates Routes link in the Redistribute to RIP section.
13. Click on radio button in the Export all aggregates into RIP field; then click Apply.
Note
If the backbone is running OSPF as well, you can enable aggregation only by configuring the 192.168.24.0 network in a different OSPF Area.

Route Rank

Route Rank Description

The route rank is the value that the routing subsystem uses to order routes from different protocols to the same destination.

You cannot use rank to control the selection of routes within a dynamic interior gateway protocol (IGP); this is accomplished automatically by the protocol and is based on the protocol metric. You can use rank to select routes from the same external gateway protocol (EGP) learned from different peers or autonomous systems.

The rank value is an arbitrarily assigned value used to determine the order of routes to the same destination in a single routing database. Each route has only one rank associated with it, even though rank can be set at many places in the configuration. The route derives its rank from the most specific route match among all configurations.

The active route is the route installed into the kernel forwarding table by the routing subsystem. In the case where the same route is contributed by more than one protocol, the one with the lowest rank becomes the active route.

Some protocols—BGP and aggregates—allow for routes with the same rank. To choose the active route in these cases, a separate tie breaker is used. This tie breaker is called LocalPref for BGP and weight for aggregates.

Rank Assignments

A default rank is assigned to each protocol. Rank values range from 0 to 255, with the lowest number indicating the most preferred route.

The table below summarizes the default rank values.

<table>
<thead>
<tr>
<th>Preference of</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface routes</td>
<td>0</td>
</tr>
<tr>
<td>OSPF routes</td>
<td>10</td>
</tr>
<tr>
<td>Static routes</td>
<td>60</td>
</tr>
<tr>
<td>IGRP routes</td>
<td>80</td>
</tr>
</tbody>
</table>
Setting Route Rank

1. Click Config on the home page.
2. Click the Route Options link in the Routing Configuration section.
3. Enter the route rank for each protocol; then click Apply.

   These numbers do not generally need to be changed from their defaults. Be careful when you modify these numbers; strange routing behavior might occur as a result of arbitrary changes to these numbers.

4. To make your changes permanent, click Save.

Routing Protocol Rank Example

When a destination network is learned from two different routing protocols, (for example, RIP and OSPF) a router must choose one protocol over another.

The figure below shows the network configuration for the example:

In the preceding figure, the top part of the network is running OSPF and the bottom part of the network is running RIP. Nokia Platform D learns network 192.168.22.0 from two routing
protocols: RIP from the bottom of the network, and OSPF from the top of the network. When other hosts want to go to 192.168.22.0 through Nokia Platform D, Nokia Platform D can select one protocol route, such as an OSPF route first, to reach the destination. If that route is broken, then Nokia Platform D uses another available route to reach the destination.

To configure the routing preferences

1. Click Config on the home page.
2. Click the Routing Options link in the Routing Configuration section.
3. Enter 10 in the OSPF edit box.
4. Enter 40 in the RIP edit box; then click Apply.

This configuration makes the OSPF route the preferred route. To make the RIP route be the preferred route, enter 40 for OSPF and 10 for RIP.

Setting Rank for Static Routes

1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
3. Click the Advanced Options link.
4. Select the route for which to set the rank.
5. Set the rank to the value that you want; then click Apply.
6. To make your changes permanent, click Save.

BGP

BGP Description

Border Gateway Protocol (BGP) is an inter-AS protocol, meaning that it can be deployed within and between autonomous systems (ASes). An autonomous system is a set of routers under a single technical administration. An AS uses an interior gateway protocol and common metrics to route packets within an AS; it uses an exterior routing protocol to route packets to other ASes.

Note
This implementation supports only BGP version 4.

BGP sends update messages that consist of network number-AS path pairs. The AS path contains the string of ASes through which the specified network can be reached. An AS path has some structure in order to represent the results of aggregating dissimilar routes. These update messages are sent over TCP transport mechanism to ensure reliable delivery. BGP contrasts with IGPs, which build their own reliability on top of a datagram service.
As a path-vector routing protocol, BGP limits the distribution of router reachability information to its peer or neighbor routers.

**BGP Sessions (Internal and External)**

BGP supports two basic types of sessions between neighbors: internal (sometimes referred to as IBGP) and external (EBGP). Internal sessions run between routers in the *same* autonomous systems, while external sessions run between routers in *different* autonomous systems. When sending routes to an external peer, the local AS number is prepended to the AS path. Routes received from an internal neighbor have, in general, the same AS path that the route had when the originating internal neighbor received the route from an external peer.

BGP sessions might include a single metric (Multi-Exit Discriminator or MED) in the path attributes. Smaller values of the metric are preferred. These values are used to break ties between routes with equal preference from the same neighbor AS.

Internal BGP sessions carry at least one metric in the path attributes that BGP calls the local preference. The size of the metric is identical to the MED. Use of these metrics is dependent on the type of internal protocol processing.

BGP implementations expect external peers to be directly attached to a shared subnet and expect those peers to advertise next hops that are host addresses on that subnet. This constraint is relaxed when the multihop option is enabled in the BGP peer template during configuration.

Type internal groups determine the immediate next hops for routes by using the next hop received with a route from a peer as a forwarding address and uses this to look up an immediate next hop in IGP routes. Such groups support distant peers, but they need to be informed of the IGP whose routes they are using to determine immediate next hops.

Where possible, for internal BGP group types, a single outgoing message is built for all group peers based on the common policy. A copy of the message is sent to every peer in the group, with appropriate adjustments to the next hop field to each peer. This minimizes the computational load of running large numbers of peers in these types of groups.

**BGP Path Attributes**

A path attribute is a list of AS numbers that a route has traversed to reach a destination. BGP uses path attributes to provide more information about each route and to help prevent routing loops in an arbitrary topology. You can also use path attributes to determine administrative preferences.

BGP collapses routes with similar path attributes into a single update for advertisement. Routes that are received in a single update are readvertised in a single update. The churn caused by the loss of a neighbor is minimized, and the initial advertisement sent during peer establishment is maximally compressed.

BGP does not read information that the kernel forms message by message. Instead, it fills the input buffer. BGP processes all complete messages in the buffer before reading again. BGP also performs multiple reads to clear all incoming data queued on the socket.
Note
This feature might cause a busy peer connection to block other protocols for prolonged intervals.

The following table displays the path attributes and their definitions:

<table>
<thead>
<tr>
<th>Path Attribute</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS_PATH</td>
<td>Identifies the autonomous systems through which routing information carried in an UPDATE message passed. Components of this list can be AS_SETs or AS_SEQUENCES.</td>
</tr>
<tr>
<td>NEXT_HOP</td>
<td>Defines the IP address of the border router that should be used as the next hop to the destinations listed in the UPDATE message.</td>
</tr>
<tr>
<td>MULTI_EXIT_DISC</td>
<td>Discriminates among multiple exit or entry points to the same neighboring autonomous system. Used only on external links.</td>
</tr>
<tr>
<td>LOCAL_PREF</td>
<td>Determines which external route should be taken and is included in all IBGP UPDATE messages. The assigned BGP speaker sends this message to BGP speakers within its own autonomous system but not to neighboring autonomous systems. Higher values of a LOCAL_PREF are preferred.</td>
</tr>
<tr>
<td>ATOMIC_AGGREGATE</td>
<td>Specifies to a BGP speaker that a less specific route was chosen over a more specific route. The BGP speaker attaches the ATOMIC_AGGREGATE attribute to the route when it reproduces it to other BGP speakers. The BGP speaker that receives this route cannot remove the ATOMIC_AGGREGATE attribute or make any Network Layer Reachability Information (NLRI) of the route more specific. This attribute is used only for debugging purposes.</td>
</tr>
</tbody>
</table>

All unreachable messages are collected into a single message and are sent before reachable routes during a flash update. For these unreachable announcements, the next hop is set to the local address on the connection, no metric is sent, and the path origin is set to incomplete. On external connections, the AS path in unreachable announcements is set to the local AS. On internal connections, the AS path length is set to zero.

Routing information shared between peers in BGP has two formats: announcements and withdrawals. A route announcement indicates that a router either learned of a new network attachment or made a policy decision to prefer another route to a network destination. Route withdrawals are sent when a router makes a new local decision that a network is no longer reachable.

**BGP Multi-Exit Discriminator**

Multi-exit Discriminator (MED) values are used to help external neighbors decide which of the available entry points into an AS are preferred. A lower MED value is preferred over a higher MED value and breaks the tie between two or more preferred paths.
A BGP session does not accept MEDs from an external peer unless the Accept MED field is set for an external peer.

BGP Interactions with IGPs

All transit ASes must be able to carry traffic that originates from locations outside of that AS, is destined to locations outside of that AS, or both. This requires a certain degree of interaction and coordination between BGP and the Interior Gateway Protocol (IGP) that the particular AS uses. In general, traffic that originates outside of a given AS passes through both interior gateways (gateways that support the IGP only) and border gateways (gateways that support both the IGP and BGP). All interior gateways receive information about external routes from one or more of the border gateways of the AS that uses the IGP.

Depending on the mechanism used to propagate BGP information within a given AS, take special care to ensure consistency between BGP and the IGP, since changes in state are likely to propagate at different rates across the AS. A time window might occur between the moment when some border gateway (A) receives new BGP routing information (which was originated from another border gateway (B) within the same AS) and the moment the IGP within this AS can route transit traffic to the border gateway (B). During that time window, either incorrect routing or black holes can occur.

To minimize such routing problems, border gateway (A) should not advertise to any of its external peers a route to some set of exterior destinations associated with a given address prefix using border gateway (B) until all the interior gateways within the AS are ready to route traffic destined to these destinations by using the correct exit border gateway (B). Interior routing should converge on the proper exit gateway before advertising routes that use the exit gateway to external peers.

If all routers in an AS are BGP speakers, no interaction is necessary between BGP and an IGP. In such cases, all routers in the AS already have full knowledge of all BGP routes. The IGP is then only used for routing within the AS, and no BGP routes are imported into the IGP. The user can perform a recursive lookup in the routing table. The first lookup uses a BGP route to establish the exit router, while the second lookup determines the IGP path to the exit router.

Inbound BGP Route Filters

BGP routes can be filtered, or redistributed by AS number or AS path regular expression, or both.

BGP stores rejected routes in the routing table with a negative preference. A negative preference prevents a route from becoming active and prevents it from being installed in the forwarding table or being redistributed to other protocols. This behavior eliminates the need to break and re-establish a session upon reconfiguration if importation policy is changed.

The only attribute that can add or modify when you import from BGP is the local preference. The local preference parameter assigns a BGP local preference to the imported route. The local
preference is a 32-bit unsigned value, with larger values preferred. This is the preferred way to bias a routing subsystem preference for BGP routes.

BGP Redistribution

When redistributing routes to BGP, you can modify the community, local preference, and MED attributes. Redistribution to BGP is controlled on an AS or AS path basis.

BGP 4 metrics (MED) are 32-bit unsigned quantities; they range from 0 to 4294967295 inclusive, with 0 being the most desirable. If the metric is specified as IGP, any existing metric on the route is sent as the MED. For example, this allows OSPF costs to be redistributed as BGP MEDs. If this capability is used, any change in the metric causes the route to be redistributed with the new MED, or to flap, so use it with care.

The BGP local preference is significant only when used with internal BGP. It is a 32-bit unsigned quantity and larger values are preferred. The local preference should normally be specified within the redistribution list unless no BGP sources are present in the redistribution list.

Note
If BGP routes are being redistributed into IBGP, the local preference cannot be overridden, and this parameter is ignored for IBGP sources. The same is true for confederation peers (CBGP).

Communities

BGP communities allow you to group a set of IP addresses and apply routing decisions based on the identity of the group or community.

To implement this feature, map a set of communities to certain BGP local preference values. Then you can apply a uniform BGP configuration to the community as a whole as opposed to each router within the community. The routers in the community can capture routes that match their community values.

Use community attributes to can configure your BGP speaker to set, append, or modify the community of a route that controls which routing information is accepted, preferred, or distributed to other neighbors. The following table displays some special community attributes that a BGP speaker can apply.

<table>
<thead>
<tr>
<th>Community attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO_EXPORT (0xFFFFFFFF01)</td>
<td>Not advertised outside a BGP confederation boundary. A stand-alone autonomous system that is not part of a confederation should be considered a confederation itself.</td>
</tr>
<tr>
<td>NO_ADVERTISE (0xFFFFFFFF02)</td>
<td>Not advertised to other BGP peers.</td>
</tr>
</tbody>
</table>
Route Reflection

Generally, all border routers in a single AS need to be internal peers of each other; all nonborder routers frequently need to be internal peers of all border routers. While this configuration is usually acceptable in small networks, it can lead to unacceptably large internal peer groups in large networks. To help address this problem, BGP supports route reflection for internal and routing peer groups (BGP version 4).

When using route reflection, the rule that specifies that a router can not readvertise routes from internal peers to other internal peers is relaxed for some routers called route reflectors. A typical use of route reflection might involve a core backbone of fully meshed routers. This means that all the routers in the fully meshed group peer directly with all other routers in the group. Some of these routers act as route reflectors for routers that are not part of the core group.

Two types of route reflection are supported. By default, all routes received by the route reflector that originate from a client are sent to all internal peers (including the client group but not the client). If the no-client reflect option is enabled, routes received from a route reflection client are sent only to internal peers that are not members of the client group. In this case, the client group must be fully meshed. In either case, all routes received from a non-client internal peer are sent to all route reflection clients.

Typically, a single router acts as the reflector for a set, or cluster, of clients; for redundancy, two or more routers can also be configured to be reflectors for the same cluster. In this case, a cluster ID should be selected to identify all reflectors serving the cluster, using the cluster ID keyword.

**Note**
Nokia recommends that you not use multiple redundant reflectors unnecessarily as it increases the memory required to store routes on the peers of redundant reflectors.

No special configuration is required on the route reflection clients. From a client perspective, a route reflector is a normal IBGP peer. Any BGP version 4 speaker should be able to be a reflector client.
for further details, refer to the route reflection specification document (RFC 2796 as of this writing).

AS1 has five BGP-speaking routers. With Router B working as a route reflector, there is no need to have all the routers connected in a full mesh.

Confederations

An alternative to route reflection is BGP confederations. As with route reflectors, you can partition BGP speakers into clusters where each cluster is typically a topologically close set of routers. With confederations, this is accomplished by subdividing the autonomous system into multiple, smaller ASes that communicate among themselves. The internal topology is hidden from the outside world, which perceives the confederation to be one large AS.

Each distinct sub-AS within a confederation is referred to as a routing domain (RD). Routing domains are identified by using a routing domain identifier (RDI). The RDI has the same syntax as an AS number, but as it is not visible outside of the confederation, it does not need to be globally unique, although it does need to be unique within the confederation. Many confederations find it convenient to select their RDIs from the reserved AS space (ASes 64512 through 65535 (see RFC 1930)). RDIs are used as the ASes in BGP sessions between peers within the confederation.

The confederation as a whole, is referred to by a confederation identifier. This identifier is used as the AS in external BGP sessions. As far as the outside world is concerned, the confederation ID is the AS number of the single, large AS. For this reason, the confederation ID must be a globally unique, normally assigned AS number.

Note
Do not nest confederations.
For further details, refer to the confederations specification document (RFC 1965 as of this writing).

AS1 has seven BGP-speaking routers grouped under different routing domains: RDI A, RDI B, and RDI C. Instead of having a full-mesh connection among all seven routers, you can have a full-meshed connection within just one routing domain.

**EBGP Multihop Support**

Connections between BGP speakers of different ASes are referred to as EBGP connections. BGP enforces the rule that peer routers for EBGP connections need to be on a directly attached network. If the peer routers are multiple hops away from each other or if multiple links are between them, you can override this restriction by enabling the EBGP multihop feature. TCP connections between EBGP peers are tied to the addresses of the outgoing interfaces. Therefore, a single interface failure severs the session even if a viable path exists between the peers.

EBGP multihop support can provide redundancy so that an EBGP peer session persists even in the event of an interface failure. Using an address assigned to the loopback interface for the EBGP peering session ensures that the TCP connection stays up even if one of the links between them is down, provided the peer loopback address is reachable. In addition, you can use EBGP multihop support to balance the traffic among all links.
**Caution**

Enabling multihop BGP connections is dangerous because BGP speakers might establish a BGP connection through a third-party AS. This can violate policy considerations and introduce forwarding loops.

Router A and Router B are connected by two parallel serial links. To provide fault tolerance and enable load-balance, enable EBGP multihop and using addresses on the loopback interface for the EBGP peering sessions.

**Route Dampening**

Route dampening lessens the propagation of flapping routes. A flapping route is a route that repeatedly becomes available then unavailable. Without route dampening, autonomous systems continually send advertisement and withdrawal messages each time the flapping route becomes available or unavailable. As the Internet has grown, the number of announcements per second has grown as well and caused performance problems within the routers.

Route dampening enables routers to keep a history of the routes that are flapping and prevent them from consuming significant network bandwidth. This is achieved by measuring how often a given route becomes available and then unavailable. When a set threshold is reached, that route is no longer considered valid, and is no longer propagated for a given period of time, usually about 30 minutes. If a route continues to flap even after the threshold is reached, the time out period for that route grows in proportion to each additional flap. Once the threshold is reached, the route is dampened or suppressed. Suppressed routes are added back into the routing table once the penalty value is decreased and falls below the reuse threshold.

Route dampening can cause connectivity to appear to be lost to the outside world but maintained on your own network because route dampening is only applied to BGP routes. Because of increasing load on the backbone network routers, most NSPs (MCI, Sprint, UUNet etc.) have set up route suppression.

**TCP MD5 Authentication**

The Internet is vulnerable to attack through its routing protocols and BGP is no exception. External sources can disrupt communications between BGP peers by breaking their TCP connection with spoofed RST packets. Internal sources, such as BGP speakers, can inject bogus routing information from any other legitimate BGP speaker. Bogus information from either external or internal sources can affect routing behavior over a wide area in the Internet.
The TCP MD5 option allows BGP to protect itself against the introduction of spoofed TCP segments into the connection stream. To spoof a connection using MD5 signed sessions, the attacker not only has to guess TCP sequence numbers, but also the password included in the MD5 digest.

**BGP Support for Virtual IP for VRRP**

Beginning with IPSO 3.8, the Nokia BGP implementation supports advertising the virtual IP address of the VRRP virtual router. You can force a route to use the virtual IP address as the local endpoint for TCP connections for a specified internal or external peer autonomous system. You must also configure a local address for that autonomous system for the VRRP virtual IP option to function. Only the VRRP master establishes BGP sessions. For more information on VRRP, see “Understanding VRRP.”

**Note**
You must use monitored-circuit VRRP when configuring virtual IP support for BGP or any other dynamic routing protocol. Do not use VRRPv2 when configuring virtual IP support for BGP.

Perform the following procedure to configure an a peer autonomous system, corresponding local address, and to enable support for virtual IP for VRRP.

1. Click Config on the home page of Network Voyager.
2. Click the BGP link in the Routing Configuration section.
3. Enter a value between 1 and 65535 in the Peer autonomous system number edit box.
4. Click the Select the peer group type drop-down list and click either Internal or External.
   - If the peer autonomous system number is different from the local autonomous system of this router, click External.
   - If the peer autonomous system number is the same as that of the local autonomous system of this router, click Internal. You must also select Internal if the local autonomous system is part of a confederation. For more information on confederations, see “Confederations.”
5. Click Apply.
6. Click the Advanced BGP Options link on the BGP page.
7. For the specific external or routing group, enter an IP address in the Local address text box.

**Note**
You must configure a local IP address for the specific external or routing group for virtual IP for VRRP support to function.

8. Click on in the Virtual Address field to enable virtual IP for VRRP support.
9. Click Apply, and then click Save to make your changes permanent.
BGP Support for IP Clustering

Beginning with IPSO 3.8, Nokia supports BGP in IP clusters. With previous versions of IPSO, clusters did not support dynamic routing. On a failover, BGP stops running on the previous master and establishes its peering relationship on a new master. You must configure a cluster IP address as a local address when you run BGP in clustered mode. For more information on IP Clustering, see “IP Clustering Description.”

**Note**
Nokia recommends that you configure BGP in an IP cluster so that peer traffic does not run on the primary and secondary cluster protocol interfaces.

BGP Memory Requirements

**Tables**

BGP stores its routing information in routing information bases (RIBs).

<table>
<thead>
<tr>
<th>RIB Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjacency RIB In</td>
<td>Stores routes received from each peer.</td>
</tr>
<tr>
<td>Local RIB</td>
<td>Forms the core routing table of the router.</td>
</tr>
<tr>
<td>Adjacency RIB Out</td>
<td>Stores routes advertised to each peer.</td>
</tr>
</tbody>
</table>

**Memory Size**

- Base IPSRD is approximately 2 MB
- Route entry in the local route table is 76 bytes
- Inbound route entry in the BGP table is 20 bytes
- Outbound route entry in the BGP table is 24 bytes

To calculate the amount of memory overhead on the routing daemon because of BGP peers, calculate the memory required for all of the RIBs according to the following procedures. Add the result to the base IPSRD size.

Inbound RIB: Multiply the number of peers by the number of routes accepted. Multiply the result by the size of each inbound route entry.

Local RIB: Multiply the number of routes accepted by a local policy by the size of each local route entry.

Outbound RIB: Multiply the number of peers by the number of routes advertised. Multiply the result by the size of each BGP outbound route entry.
Example

Assume that a customer is peering with two ISPs that are dual homed and is accepting full routing tables from these two ISPs. Each routing table contains 50,000 routes. The customer is only advertising its local routes (2,000) to each ISP. With these figures, you can compute the total memory requirements:

The base IPSRD memory is 2 MB. Add this value to the following values to calculate the total memory requirements.

1. To calculate the **inbound memory requirements**, multiply the number of peers (two ISPs) by the number of routes accepted (50,000).
   Multiply the resulting value by the size of each inbound route entry in the BGP table (20 bytes).
   The answer is 2,000,000 or 2 MB.

2. To calculate the **local memory requirements**, multiply the number of routes accepted (50,000) by the size of each route entry in the local route table (76 bytes).
   The answer is 4,000,000 or 4MB.

3. To calculate the outbound memory requirements, multiply the number of peers (only one customer) by the number routes advertised (2,000).
   Multiply the result by the size of each outbound route entry in the BGP table (24 bytes).
   The answer is 48,000 or 50 K.

4. Add all of the results together (2MB + 2MB + 4MB + 50K).
   The answer is 8.05MB, which means that IPSRD requires 8.05MB of memory for this example.

**Note**

Make sure that IPSRD is not swapping memory. Look at the memory sizes occupied by user-level daemons like Check Point, ifm, xpand, etc.

To find out how much memory IPSRD occupies, run the following command:

```
ps -auxww | grep ipsrd
```

The fourth column labeled, %MEM, displays the percentage of memory that IPSRD occupies.

BGP Neighbors Example

BGP has two types: internal and external. Routers in the same autonomous system that exchange BGP updates run internal BGP; routers in different autonomous systems that exchange BGP updates run external BGP.
In the diagram below, AS100 is running IBGP, and AS200 and AS300 are running external BGP.

**Configuring IBGP on Nokia Platform A**

1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Configure an internal routing protocol such as OSPF or configure a static route to connect the platforms within AS100 to each other. For more information see “Configuring OSPF” or “Creating a Static Route.”
3. Click **CONFIG** on the home page.
4. Click the BGP link in the Routing Configuration section.
5. Enter a router ID in the Router ID text box. The default router ID is the address of the first interface. An address on a loopback interface that is not the loopback address (127.0.0.1) is preferred.
6. Enter 100 in the AS number text box.
7. Enter 100 in the Peer autonomous system number text box.
8. Click Internal in the Peer group type drop-down list; then click Apply.
9. Enter 10.50.10.2 in the Add remote peer IP address edit box; then click Apply.
10. Configure an inbound route filter for AS 100 according to “BGP Route Inbound Policy Example.”

**Configuring IBGP on Nokia Platform B**

1. Configure the interface as in “Configuring an Ethernet Interface”.
2. Configure an internal routing protocol such as OSPF or configure a static route to connect the platforms in AS100 to each other. For more information see “Configuring OSPF” or “Creating a Static Route.”
3. Click **Config** on the home page.
4. Click the BGP link in the Routing Configuration section.
5. Enter a router ID in the ROUTER ID text box. The default router ID is the address of the first interface. An address on a loopback interface that is not the loopback address (127.0.0.1) is preferred.

6. Enter 100 in the AS number edit box.

7. Enter 100 in the Peer autonomous system number text box.

8. Enter 10.50.10.1 in the Add remote peer IP address text box; then click Apply.

9. Enter 170.20.1.1 in the Add remote peer IP address text box; then click Apply.

10. Configure an inbound route filter for AS100 according to “BGP Route Inbound Policy Example.”

**Configuring IBGP on Nokia Platform C**

1. Configure the interface as in “Configuring an Ethernet Interface”.

2. Configure an internal routing protocol such as OSPF or configure a static route to connect the platforms in AS100 to each other. For more information, see “Configuring OSPF”or “Creating a Static Route.”

3. Click Config on the home page.

4. Click the BGP link in the Routing Configuration section.

5. Enter a router ID in the ROUTER ID edit box. The default router ID is the address of the first interface. An address on a loopback interface that is not the loopback address (127.0.0.1) is preferred.

6. Enter 100 in the AS number text box.

7. Enter 100 in the Peer autonomous system number text box.

8. Click Internal in the Peer group type drop-down list; then click Apply.

9. Enter 170.20.1.2 in the Add remote peer IP address text box; then click Apply.

10. Configure an inbound route policy for AS100 according in “BGP Route Inbound Policy Example.”

**Configuring Nokia Platform C as an IBGP Peer to Nokia Platform A**

1. Click Config on the home page.

2. Click the BGP link in the Routing Configuration section.

3. Enter 10.50.10.1 in the Add remote peer IP address text box; then click Apply.

**Configuring Nokia Platform A as an IBGP Peer to Nokia Platform C**

1. Click Config on the home page.

2. Click the BGP link in the Routing Configuration section.
3. Enter 170.20.1.1 in the Add remote peer IP address text box; then click Apply.

**Configuring EBGP on Nokia Platform A**

1. Configure the interface on Nokia Platform A as in “Configuring Ethernet Interfaces.”
2. Click Config on the home page.
3. Click the BGP link in the Routing Configuration section.
4. Enter 200 in the Peer autonomous system number text box.
5. Click External in the Peer group type drop-down list; then click Apply.
6. Enter 129.10.21.2 in the Add Remote Peer IP Address text box; then click Apply.
7. Configure route redistribution policy according to “BGP Route Redistribution Example.”
8. Configure an inbound route filter according to “BGP Route Inbound Policy Example.”

**Configuring EBGP on Nokia Platform C**

1. Click Config on the home page of Platform C.
2. Click the BGP link in the Routing Configuration section.
3. Enter 300 in the AS number text box.
4. Click External in the Peer group type drop-down list; then click Apply.
5. Enter 172.17.10.2 in the Add remote peer IP address text box; then click Apply.
6. Configure route redistribution policy according to “BGP Route Redistribution Example.”
7. Configure an inbound route filter according to “BGP Route Inbound Policy Example” to allow Nokia Platform C to accept routes from its EBGP peer.

**Configuring EBGP on Nokia Platform D**

1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click Config on the home page.
3. Click the BGP link in the Routing Configuration section.
4. Enter a router ID in the Router ID text box.
   The default router ID is the address of the first interface. An address on a loopback interface that is not the loopback address (127.0.0.1) is preferred.
5. Enter 200 in the AS Number text box.
6. Enter 100 in the Peer Autonomous System Number text box
7. Click External in the Peer group type drop-down window; then click Apply.
8. Enter 129.10.21.1 in the Add remote peer IP address text box; then click Apply.
9. Configure route inbound policy according to “BGP Route Inbound Policy Example.”
10. Configure route redistribution policy according to “BGP Route Redistribution Example.”
11. Configure an inbound route filter according to “BGP Route Inbound Policy Example.”

**Configuring EBGP on Nokia Platform E**

1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click Config on the home page.
3. Click the BGP link in the Routing Configuration section.
4. Enter 300 in the AS number edit box.
5. Enter 100 in the Peer autonomous system number text box.
6. Click External in the Peer group type drop-down list; then click Apply.
7. Enter 172.17.10.1 in the Add remote peer IP address edit box; then click Apply.
8. Configure route inbound policy according to “BGP Route Inbound Policy Example.”
9. Configure route redistribution policy according to “BGP Route Redistribution Example.”
10. Configure an inbound route filter according to “BGP Route Inbound Policy Example.”

**Verification**

To verify that you configured BGP neighbors correctly, run the following command in iclid:
```
show bgp neighbor
```
For more information about this command, see to “Displaying Routing Protocol Information.”

**Path Filtering Based on Communities Example**

**Note**
To filter BGP updates based on peer AS numbers, see “Configuring Route Inbound Policy on Nokia Platform D Based on an Autonomous System Number.”

To filter BGP updates based on community ID or special community, specify an AS number along with the community ID or the name of one of the following possible special community attributes: no export, no advertise, no subconfed, or none.

1. Click the Advanced BGP options link.
2. Click on in the Enable Communities field; then click Apply.
3. Follow the steps described in the “Configuring Route Inbound Policy on Nokia Platform D Based on an Autonomous System Number” example.
4. Enter the community ID or the name of one of the special attributes in the Community ID/ Special community text box; then click Apply.
5. Click on button in the Redistribute All Routes field or enter specific IP prefixes to redistribute as described in the “Configuring Route Inbound Policy on Nokia Platform D Based on an Autonomous System Number” example, then click Apply.
BGP Multi Exit Discriminator Example

Multi Exit Discriminator (MED) values are used to help external neighbors decide which of the available entry points into an AS is preferred. A lower MED value is preferred over a higher MED value.

In the above diagram, MED values are being propagated with BGP updates. This diagram shows four different configurations.

- Configuring Default MED for Nokia Platform D
- Configuring MED Values for all Peers of AS200
- Configuring MED Values for each External BGP Peer for Nokia Platform D
- Configuring MED Values and a Route Redistribution Policy on Nokia Platform D

Configuring Default MED for Nokia Platform D

1. Click Config on the home page.
2. Click the BGP link in the Routing Configuration section.
3. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”
4. Click the Advanced BGP Options link on the main BGP page. This action takes you to the Advanced Options for BGP page.
5. In the Miscellaneous settings field, enter a MED value in the Default MED edit box; then click Apply.
6. Click Save to make your changes permanent.

This MED value is propagated with all of the BGP updates that are propagated by Nokia Platform D to all of its EBGP peers in AS100 and AS200.

Configuring MED Values for all Peers of AS200

1. Click Config on the home page.
2. Click the BGP link in the Routing Configuration section.
3. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”
4. Click Advanced BGP Options link on the main BGP page. 
   This action takes you to the Advanced Options for BGP page.

5. Go to the configuration section for the AS4 routing group. Enter 100 in the MED text box 
   for the AS4 routing group.

   Setting a MED value here propagates updates from all peers of AS4 with this MED value.

**Note**
Setting an MED value for all peers under the local AS overwrites the default MED setting of 
the respective internal peers.

### Configuring MED Values for each External BGP Peer for Nokia 
Platform D

1. Click Config on the home page.
2. Click the BGP link in the Routing Configuration section.
3. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”
4. Click the link for the peer IP address for Nokia Platform A under AS100.
5. Enter 100 in the MED sent out text box.
6. Click on in the Accept MED from external peer field; then click Apply.
7. Click the link for the peer IP address for Nokia Platform B under AS100.
8. Enter 200 in the MED sent out text box.
9. Click on in the Accept MED from external peer field; then click Apply.
10. Click the link for the peer IP address for Nokia Platform C under AS200.
11. Enter 50 in the MED sent out text box.
12. Click on in the Accept MED from external peer field; then click Apply.
13. Click Save to make your changes permanent.

   This configuration allows Nokia Platform D to prefer Nokia Platform A (with the lower 
   MED value of 100) over Nokia Platform B (with the higher MED value of 200) as the entry 
   point to AS100 while it propagates routes to AS100. Similarly, this configuration propagates 
   routes with an MED value of 50 to AS200, although no multiple entry points exist to AS200.

### Configuring MED Values and a Route Redistribution Policy on 
Nokia Platform D

1. Click Config on the home page.
2. Click the BGP link in the Routing Configuration section.
3. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”
4. Click the Route Redistribution link the Routing Configuration section.
5. Click the BGP link in the Redistribute to BGP section.
6. Enter 100 in MED edit box next to the Enable redistribute bgp routes to AS100 field.
7. Enter necessary information for route redistribution according to the “BGP Multi Exit Discriminator Example”; then click Apply.
8. Click Save to make your changes permanent.

Setting an MED value along with route redistribution policy allows Nokia Platform D to redistribute all routes to AS100 with an MED value set to 100.

---

**Note**

Setting an MED value along with route redistribution overwrites the MED value for the external BGP peer for Nokia Platform D.

---

**Verification**

To verify that you configured BGP MED values correctly, run the following commands in iclid.

- `show route`
- `show bgp neighbor <peerid> advertised`
- `show route bgp metrics`

For more information on these commands, see “Displaying Routing Protocol Information.”

---

**Changing the Local Preference Value Example**

This example shows how to set up two IBGP peers, and how to configure routes learned using Nokia Platform A to have a higher local preference value over Nokia Platform B (which has a default local preference value of 100).

1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the BGP link in the Routing Configuration section.
3. Enter 100 in the AS number text box; then click Apply.
The following steps describe how to configure an IBGP peer for Nokia Platform B.

1. Enter 100 in the Peer Autonomous System Number text box.
2. Click Internal in the Peer Group type drop-down list; then click Apply.
3. Enter 20.10.10.2 in the Add Remote Peer IP Address text box; then click Apply.

**Setting the Local Preference Value for an IBGP Peer**

1. Click Up to take you back to the main Config page for Network Voyager.
   Click the Inbound Route Filters link in the Routing Configuration section.
2. Click the Based on Autonomous System Number link.
3. Enter 512 (or any unique number in the range of 512 to 1024) in the Import ID text box.
4. Enter 100 in the AS text box.
5. Enter 200 in the LocalPref text box.
6. Click Apply.
7. Click Accept in the All Routes from BGP AS 100 field; then click Apply.

**Configuring the Static Routes Required for an IBGP Session**

1. Click Top at the top of the configuration page.
2. Click the Static Routes link in the Routing Configuration section.
3. Enter 10.10.10.0 in the New static route text box.
4. Enter 24 in the Mask length text box.
5. Enter 20.10.10.2 in the Gateway text box; then click Apply.

**Configuring the Static Routes Required for Nokia Platform B**

1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the BGP link in the Routing Configuration section.
3. Enter 20.10.10.2 in the Router ID text box.
4. Enter 100 in the AS number text box.
5. Enter 20.10.10.1 in the Add remote peer ip address text box, then click Apply.
6. Click Top button at the top of the configuration page.
7. Click the Static Routes link in the Routing Configuration section.
8. Enter 10.10.10.0 in the New Static Route text box.
9. Enter 24 in the Mask Length text box.
10. Enter 20.10.10.1 in the Gateway text box; then click Apply.
BGP Confederation Example

In the above diagram, all the routers belong to the same Confederation 65525. Nokia platform A and Nokia platform B belong to routing domain ID 65527, Nokia platform C and Nokia platform D belong to routing domain ID 65528, and Nokia platform E belongs to routing domain ID 65524. In this example, you configure Nokia platform B and Nokia platform C as members of Confederation 65525 and as members of separate routing domains within the confederation. You also configure each platform as confederation peers to Nokia platform E, which has a direct route to the external AS.

Configuring Nokia Platform C

1. Set up the confederation and the routing domain identifier.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 65525 in the Confederation text box.
   e. Enter 65528 in the Routing domain identifier text box; then click Apply.

2. Create confederation group 65524.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 65524 in the Peer Autonomous System Number text box.
e. Click Confederation in the Peer Group Type drop-down list; then click Apply.
Define properties for the above group.

f. Click On in the All field.

g. Click On in the All Interfaces field; then click Apply.

h. Enter 192.168.40.1 in the Add a new peer text box; then click Apply.

3. Create confederation group 65528.

   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Enter 65528 in the Peer Autonomous System Number text box.
   d. Click Confederation in the Peer Group Type drop-down list; then click Apply.
Define properties for the above group.
   e. Click on in the all field.
   f. Click on in the All Interface field; then click Apply.
   g. Enter 192.168.45.1 in the Add a new peer text box; then click Apply.

4. Define BGP route inbound policy by using regular expressions for any AS path and from any origin.

   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Based on ASPath Regular Expressions link.
   d. Enter 1 in the Import ID text box and enter .* in the ASPATH Regular Expression text box; then click Apply.
   e. Click On in the Import All Routes From AS Path field; then click Apply.

5. Define route redistribution.

   a. Click Config on the home page.
   b. Click the Route Redistribution link in the Routing Configuration section.
   c. Click the BGP link in the Redistribute to BGP section.
   d. Click 65528 in the Redistribute to Peer AS drop-down list.
   e. Click 65524 in the From AS drop-down list; then click Apply.
   f. Click On in the Enable Redistribution of Routes From AS 65524 into AS 65528 field; then click APPLY.
   g. Click On in the all BGP AS 65524 routes into AS 65528; then click Apply.
   h. Click Save.
Configuring Platform B

1. Set up the confederation and the routing domain identifier.
   a. Click Config on the Network Voyager home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 65525 in the Confederation text box.
   e. Enter 65527 in the Routing domain identifier text box; then click Apply.

2. Create confederation group 65524.
   a. Click Config on the Network Voyager home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 65524 in the Peer Autonomous System Number text box.
   e. Click Confederation in the Peer Group Type drop-down list; then click Apply.
   Define properties for the above group.
   f. Click On in the All field.
   g. Click On in the All Interfaces field; then click Apply.
   h. Enter 192.168.30.1 in the Add a new peer text box; then click Apply.

3. Create confederation group 65527.
   a. Click Config on the Network Voyager home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Enter 65528 in the Peer Autonomous System Number text box.
   d. Click Confederation in the Peer Group Type drop-down list; then click Apply.
   Define properties for the above group.
   e. Click On in the All field.
   f. Click On in the All Interface field; then click Apply.
   g. Enter 192.168.35.1 in the Add a new peer text box; then click Apply.

4. Define BGP route inbound policy by using regular expressions for any AS path and from any origin.
   a. Click Config on the Network Voyager home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Based on ASPath Regular Expressions link.
   d. Enter 1 in the Import ID text box and enter .* in the ASPATH Regular Expression text box; then click Apply.
   e. Click On in the Import All Routes from AS path field; then click Apply.
5. Define route redistribution.
   a. Click Config on the Network Voyager home page.
   b. Click the Route Redistribution link in the Routing Configuration section.
   c. Click the BGP link in the Redistribute to BGP section.
   d. Click 65528 in the Redistribute to Peer AS drop-down list.
   e. Click 65524 in the From AS drop-down list; then click Apply.
   f. Click On in the Enable Redistribution of Routes From AS 65524 Into AS 65527 field; then click Apply.
   g. Click On in the All BGP AS 65524 Routes Into AS 65528 field; then click Apply.
   h. Click Save to make your changes permanent.

Route Reflector Example

This example shows configuration for setting up route reflection for BGP. Route reflection is used with IBGP speaking routers that are not fully meshed.

![Diagram showing route reflector configuration]

In the above diagram, router Nokia platform A is on AS 65525, and routers Nokia platform B, Nokia platform C, and Nokia platform D are in AS 65526. This example shows how to configure Nokia platform B to act as a route reflector for clients Nokia platform C and Nokia platform D: You then configure platforms C and D and IBGP peers to platform D, as the example shows. You configure inbound route and redistribution policies for AS 65526.

Configuring Platform B as Route Reflector

1. Assign an AS number for this router.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Enter 65526 in the AS number text box; then click Apply.
2. Create an external peer group.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 65525 in the Peer Autonomous System Number text box.
   e. Click External in the Peer Group Type drop-down list; then click Apply.

3. Enter the peer information.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 192.168.10.2 in the Add Remote Peer IP Address text box under the AS65525 External Group; then click Apply.

4. Create an internal group.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 65526 in the Peer auto autonomous system number text box.
   e. Select Internal in the Peer group type drop-down list; then click Apply.

5. Configure parameters for the group.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Click On in the All field.
      This option covers all IGP and static routes.
   e. Click On in the All Interfaces field; then click Apply.

6. Enter the peer information.
   a. Click Config on the home page.
   b. Click the BGP link in the Routing Configuration section.
   c. Click the Advanced BGP Options link.
   d. Enter 192.168.20.2 in the Add remote peer ip address text box under the AS65526 routing group.
   e. Select Reflector Client from the Peer type drop-down list; then click Apply.
   f. Click Config on the home page.
   g. Click the BGP link in the Routing Configuration section.
h. Click the Advanced BGP Options link.

i. Enter \texttt{192.168.30.2} in the Add remote peer ip address text box under the AS65526 routing group.

j. Select Reflector Client from the Peer type drop-down list; then click Apply.

**Configuring Platform C as IBGP Peer of Platform B**

1. Click Config on the Network Voyager home page of Platform C.
2. Click the BGP link in the Routing Configuration section.
3. Enter a router ID in the Router ID text box.
   
   The default router ID is the address of the first interface. An address on a loopback interface that is not the loopback address (127.0.0.1) is preferred.
4. Enter \texttt{65526} in the AS Number text box.
5. Enter \texttt{65526} in the Peer Autonomous System Number text box.
6. Click Internal in the Peer group type drop-down list; then click Apply.
7. Enter \texttt{192.168.20.1} in the Add remote peer IP address text box; then click Apply.
8. Click Save to make your changes permanent.

**Configuring Platform D as IBGP Peer of Platform B**

1. Click Config on the Network Voyager home page of Platform C.
2. Click the BGP link in the Routing Configuration section.
3. Enter a router ID in the Router ID text box.
   
   The default router ID is the address of the first interface. An address on a loopback interface that is not the loopback address (127.0.0.1) is preferred.
4. Enter \texttt{65526} in the AS Number text box.
5. Enter \texttt{65526} in the Peer Autonomous System Number text box.
6. Click Internal in the Peer Group Type drop-down list; then click Apply.
7. Enter \texttt{192.168.30.1} in the Add remote peer IP address text box; then click Apply.
8. Click Save to make your changes permanent.

**Configuring BGP Route Inbound Policy on Platform B**

1. Click Config on the home page.
2. Click the Inbound Route Filters link in the Routing Configuration section.
3. Click the Based on Autonomous System Number link.
4. Enter \texttt{512} in the Import ID text box and enter \texttt{65526} in the AS edit box; then click Apply.
5. Click Accept in the All BGP Routes From AS 65526 field; then click Apply.
6. Enter \texttt{513} in the Import ID edit box and enter 65525 in the AS edit box; then click Apply.
7. Click Accept in the All BGP Routes From AS 65525 field; then click Apply.
8. Click Save to make your changes permanent.

**Configuring Redistribution of BGP Routes on Platform B**

Complete this procedure to redistribute BGP routes to BGP that section a different AS. This is equivalent to configuring an export policy. In this example, as the diagram shows, platform B, which is part of AS 65526, is an EBGP peer to platform A, which belongs to AS 65525.

1. Click Config on the home page.
2. Click the Route Redistribution link in the Routing Configuration section.
3. Click the BGP Routes Based on AS link in the Redistribute to BGP section.
4. Select 65526 in the Redistribute to Peer AS drop-down list and select 65525 in the From AS drop-down list.
5. Click On in the Enable Redistribute BGP Routes From AS 65525 Into AS 65526 field; then click Apply.
6. Click Accept in the All BGP ASPATH 65525 Routes Into AS 65526 field; then click Apply.
7. Select 65525 in the Redistribute to Peer AS drop-down list and select 65526 in the From AS drop-down list.
8. Click On in the Enable Redistribute BGP Routes From AS 65526 Into AS 65525 field; then click Apply.
9. Click Accept in the All BGP ASPATH 65526 Routes Into AS 65525 field; then click Apply.
10. Click Save to make your changes permanent.

**BGP Community Example**

A BGP community is a group of destinations that share the same property. However, a community is not restricted to one network or AS.

Communities are used to simplify the BGP inbound and route redistribution policies. Each community is identified by either an ID or one of the following special community names: no export, no advertise, no subconfed, or none.

**Note**
Specify the community ID and the AS number in order to generate a unique AS number-community ID combination.

To restrict incoming routes based on their community values, see “Path Filtering Based on Communities Example.”

To redistribute routes that match a specified community attribute, append a community attribute value to an existing community attribute value, or both.
Note
The examples that follows is valid only for redistributing routes from any of the specified routing protocols to BGP. For example, configuring community-based route redistribution policy from OSPF to BGP automatically enables the same community-based redistribution policies for all of the other configured policies. In such an example, if you configure a route redistribution policy for OSPF to BGP, these changes also propagate to the redistribution policy for the interface routes into BGP.

1. Follow the steps in the “Redistributing OSPF to BGP Example.”

2. Match the following ASes with the following community IDs—AS 4 with community ID 1 (4:1), AS 5 with community ID 2 (5:2), AS with no export—by entering the AS values in the AS text box and the community IDs in the Community ID/Special community text box; then click Apply.

Note
Matching an AS with the no export option only matches those routes that have all of the preceding AS number and community ID values.

3. To append an AS number and community ID combination to the matched routes, click on in the Community field; then click Apply.

4. Match AS 6 with community ID 23 (6:23) by entering 6 in the AS edit box and 23 in the Community ID/Special community text box; then click Apply.

5. Match AS with no advertise; then click Apply.

Note
Matching an AS with the no advertise option appends the community attribute with the values described in step 2. Thus, all of the routes with the community attributes set to 4:1, 5:2, and no export are redistributed with the appended community attributes 4:1, 5:2, no export, 6:23, and no advertise.

**EBGP Load Balancing Example: Scenario #1**

Loopback interfaces are used to configure load balancing for EBGP between two ASes over two parallel links.

This example consists of the following:

- Enabling BGP function
- Configuring loopback addresses
- Adding static routes
- Configuring peers
- Configuring inbound and route redistribution policies
In the following diagram:

- Nokia Platform A is in autonomous system AS100, and Nokia Platform B is in autonomous system AS200.
- Nokia Platform A has a loopback address of 1.2.3.4, and Nokia Platform B has a loopback address of 5.6.7.8.

### Configuring a Loopback Address on Platform A
1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the Interfaces link on the Configuration page.
3. Click the Logical Address Loopback link.
4. Enter 1.2.3.4 in the New IP Address text box; then click Apply.

### Configuring a Loopback Address on Platform B
1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the Interfaces link on the Configuration page.
3. Click the Logical Address Loopback link.
4. Enter the 5.6.7.8 in the New IP address text box; then click Apply.

### Configuring a Static Route on Platform A
1. Click the Static Routes link in the Routing Configuration section.
2. Enter 5.6.7.8 in the New static route text box to reach the loopback address of Platform B.
3. Enter 32 in the Mask length edit box; then click Apply.
4. Enter 129.10.2.2 in the Additional Gateway edit box; then click Apply.
5. Enter 129.10.1.2 in the Additional Gateway edit box; then click Apply.

### Configuring a Static Route on Platform B
1. Click Config on the home page.
2. Click the Static Routes link in the Routing Configuration section.
3. Enter 1.2.3.4 in the New static route text box to reach the loopback address of Platform A.
4. Enter 32 in the Mask length text box; then click Apply.
5. Enter 129.10.2.1 in the Additional Gateway edit box; then click Apply.
6. Enter 129.10.1.1 in the Additional Gateway text box; then click Apply.

Configuring an EBGP Peer on Platform A
1. Configure an EBGP peer on Platform A as in “Configuring Ethernet Interfaces.”
2. Enter 1.2.3.4 as the local address on the main BGP configuration page. Click Apply.
3. Configure the inbound and route redistribution policies.
4. Click the link for specific peer you configured in Step 1. This action takes you the page that lets you configure options for that peer.
5. In the Nexthop field, click on next to EBGP Multihop to enable the multihop option; then click Apply.
6. (Optional) Enter a value in the TTL text box to set the number of hops over which the EBGP multihop session is established. The default value is 64 and the range is 1 to 255. Click Apply.

Configuring an EBGP Peer on Platform B
1. Configure an EBGP peer on Platform B as in “Configuring Ethernet Interfaces.”
2. Enter 5.6.7.8 as the local address on the main BGP configuration page.
3. Configure the inbound and route redistribution policies.
4. Click the link for specific peer you configured in Step 1. This action takes you the page that lets you configure options for that peer.
5. In the Nexthop field, click on next to EBGP Multihop to enable the multihop option; then click Apply.
6. (Optional) Enter a value in the TTL text box to set the number of hops over which the EBGP multihop session is established. The default value is 64 and the range is 1 to 255. Click Apply.

EBGP Load Balancing Example: Scenario #2

Configuring a Loopback Address on Platform A
1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the Interfaces link on the Configuration page.
3. Click the Logical Address Loopback link.
4. Enter 1.2.3.4 in the New IP Address text box; then click Apply.
Configuring a Loopback Address on Platform B
1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the Interfaces link on the Configuration page.
3. Click the Logical Address Loopback link.
4. Enter the **5.6.7.8** in the New IP Address text box; then click Apply.

Configuring OSPF on Platform A
1. Click the OSPF link in the Routing Configuration section.
2. Select the backbone area in the drop-down list for the interface whose IP address is 129.10.1.1; then click Apply.
3. Select the backbone area in the drop-down list for the interface whose IP address is 129.10.2.1; then click Apply.
4. Enter **1.2.3.4** in the Add a new stub host column, then click Apply.

Configuring OSPF on Platform B
1. Click the OSPF link in the Routing Configuration section.
2. Select the backbone area in the drop-down list for the interface whose IP address is 129.10.1.2; then click Apply.
3. Select the backbone area in the drop-down list for the interface whose IP address is 129.10.2.2; then click Apply.
4. Enter **5.6.7.8** in the Add a New Stub Host column and then click Apply.

Configuring an EBGP Peer on Platform A
1. Configure an EBGP peer on Platform A as in “Configuring Ethernet Interfaces.”
2. Enter **1.2.3.4** as the local address on the main BGP configuration page.
3. Configure the inbound and route redistribution policies.
4. Click the link for specific peer you configured in Step 1. This action takes you the page that lets you configure options for that peer.
5. In the Nexthop field, click on next to EBGP Multihop to enable the multihop option; then click Apply.
6. (Optional) Enter a value in the TTL text box to set the number of hops over which the EBGP multihop session is established. The default value is 64 and the range is 1 to 255. Click Apply.

Configuring an EBGP Peer on Platform B
1. Configure an EBGP peer on Nokia Platform B as in “Configuring Ethernet Interfaces.”
2. Enter **5.6.7.8** as the local address on the main BGP configuration page.
3. Configure the inbound and route redistribution policies.

4. Click the link for specific peer you configured in Step 1. This action takes you the page that lets you configure options for that peer.

5. In the Nexthop field, click on next to EBGP Multihop to enable the multihop option, and then click Apply.

6. (Optional) Enter a value in the TTL text box to set the number of hops over which the EBGP multihop session is established.
   
   The default value is 64 and the range is 1 to 255.

7. Click Apply.

Verification

To verify that you have configured load balancing correctly, run the following commands in iclid:

```
show bgp neighbor
show route bgp
```

For more information on these commands, see “Displaying Routing Protocol Information.”.

Adjusting BGP Timers Example

1. Configure a BGP neighbor as in the “BGP Neighbors Example.”

2. Click the link for the peer IP address to configure peer-specific parameters.

3. Enter a value in seconds in the Holdtime text box.

   Holdtime indicates the maximum number of seconds that can elapse between the receipt of successive keepalive or update messages by the sender before the peer is declared dead. It must be either zero (0) or at least 3 seconds.

   The default value is 180 seconds.

4. Enter a value in seconds in the Keepalive text box; then click Apply.

   BGP does not use any transport-protocol-based keepalive mechanism to determine whether peers are reachable. Instead, keepalive messages are exchanged between peers to determine whether the peer is still reachable.

   The default value is 60 seconds.

5. To make your changes permanent, click Save.
TCP MD5 Authentication Example

Configuring TCP MD5 Authentication on Nokia Platform A
1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the BGP link in the Routing Configuration section.
   The following two steps enable BGP function on Nokia Platform A.
3. Enter 10.10.10.1 (default is the lowest IP address on the appliance) in the Router ID text box.
4. Enter 100 in the AS number text box, then click Apply.
   The following 2 steps configure the EBGP peer for Nokia Platform B.
5. Enter 200 in the Peer autonomous system number text box.
6. Select External in the Peer group type drop-down list; then click Apply.
   The following steps configure an EBGP peer with MD5 authentication
7. Enter 10.10.10.2 in the Add remote peer ip address text box; then click Apply.
8. Click the 10.10.10.2 link to access the BGP peer configuration page
9. Select MD5 as the authentication type from the AuthType drop-down list; then click Apply.
10. Enter the MD5 shared key (test123 for example) in the Key text box; then click Apply.

Configuring BGP Route Redistribution on Nokia Platform B
1. Configure the interface as in “Configuring Ethernet Interfaces.”
2. Click the BGP link in the Routing Configuration section.
   The following three steps enable BGP function on Nokia Platform B.
3. Enter 10.10.10.2 (default is the lowest IP address on the appliance) in the Router ID text box.
4. Enter 200 in the AS number edit box; then click Apply.
   The following 2 steps configure the EBGP peer for Nokia Platform B.
5. Enter 100 in the Peer autonomous system number text box.
6. Click External in the Peer group type drop-down list; then click Apply.
   The following steps configure an EBGP peer with MD5 authentication
7. Enter 10.10.10.1 in the Add remote peer ip address text box; then click Apply.
8. Click the 10.10.10.1 link to access the BGP peer configuration page.
9. Select MD5 as the authentication type from the AuthType drop-down list; then click Apply.
10. Enter the MD5 shared key (test123 for example) in the Key edit box; then click Apply.

BGP Route Dampening Example

BGP route dampening maintains a stable history of flapping routes and prevents advertising these routes. A stability matrix is used to measure the stability of flapping routes. The value of this matrix increases as routes become more unstable and decreases as they become more stable. Suppressed routes that are stable for long period of time are re-advertised again.

This example consists of the following:
- Enabling BGP function
- Enabling weighted route dampening

1. Click Config on the home page.
2. Click the BGP link in the Routing Configuration section.
3. Click the Advanced BGP Options link.
4. Enable weighted route dampening by clicking on in the Enable Weighted Route Dampening field; then click Apply.

The following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Default value</th>
<th>Units of measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppress above</td>
<td>3</td>
<td>Number of route flaps or approximate value of the instability metric</td>
</tr>
<tr>
<td>Reuse below</td>
<td>2</td>
<td>Same as above</td>
</tr>
<tr>
<td>Max flaps</td>
<td>16</td>
<td>Same as above</td>
</tr>
<tr>
<td>Reachable decay</td>
<td>300</td>
<td>Seconds</td>
</tr>
<tr>
<td>Unreachable decay</td>
<td>900</td>
<td>Seconds</td>
</tr>
<tr>
<td>Keep history</td>
<td>1800</td>
<td>Seconds</td>
</tr>
</tbody>
</table>

5. Enter any changes in the text boxes that correspond to the appropriate fields, then click Apply.

Verification

To verify that you have configured route dampening correctly, run the following command in iclid:

```
show route bgp suppressed
```

For more information on this command, see “Displaying Routing Protocol Information.”
**BGP Path Selection**

The following rules will help you understand how BGP selects paths:

- If the path specifies a next hop that is inaccessible, drop the update.
- Prefer the path with the lowest weight. A route whose weight value is not specified is always less preferred than the path with the highest set weight value. Normally, the route with the highest set weight value is the least preferred.

**Note**
The Nokia implementation of weight value differs from that of other vendors.

- If the weights are the same, prefer the path with the largest local preference.
- If the local preferences are the same, prefer the route that has the shortest AS_path.
- If all paths have the same AS_path length, prefer the path with the lowest origin type (Origin IGP < EGP < Incomplete).
- If the origin codes are the same, prefer the path with the lowest MED attribute (if MED is not ignored).
- If the paths have the same MED, prefer the external path over the internal path.
- If the paths are still the same, prefer the path through the closest IGP neighbor.
- Prefer the path with the lowest IP address, as specified by the BGP router ID.

**Route Redistribution**

**Description**

Route redistribution allows routes learned from one routing protocol to be propagated to another routing protocol. This is necessary when routes from one protocol such as RIP, IGRP, OSPF, or BGP need to be advertised into another protocol (when two or more routing protocols are configured on the same router). Route redistribution is also useful for advertising static routes (for example, the default route) or aggregates into a protocol.

**Note**
Route metrics are not translated between different routing protocols.

When you leak routes between protocols, specify routes that are to be injected and routes that are to be excluded. In the case where the prefix is redistributed, you can the metric to advertise.

For each prefix that is to be redistributed or excluded, the prefix is matched against a filter. The filter is composed of a single IP prefix and one of the following modifiers: normal, exact, refines, and range. The default modifier is normal.

- Normal matches any route that is equal to or more specific than the given prefix.
Exact matches a route only if it equals the IP address and mask length of the given prefix.
Refines matches a route only if it is more specific than the given prefix.
Range matches any route whose IP address equals the given prefix’s IP address and whose mask length falls within the specified mask length range.

A sample route redistribution examples follow.

**Note**
The Route Redistribution link contains over thirty possible route redistribution options.

---

**BGP Route Redistribution Example**

Route redistribution allows you to redistribute routes from one autonomous system into another autonomous system.

**Configuring BGP Route Redistribution on Nokia Platform D**

1. Click Config on the home page.
2. Click the BGP Routes based on AS link under the Redistribute to BGP section.
3. Select 100 from the Redistribute to Peer AS drop-down list.
4. Select 4 from the From AS drop-down list; then click Apply.

This procedure enables route redistribution from AS 4 to AS 100. By default, all routes that are excluded from being redistributed from AS 4 are redistributed to AS 100.
Redistributing a Single Route

1. To restrict route redistribution to route 100.2.1.0/24, enter 100.2.1.0 in the New IP prefix to redistribute text box.

2. Enter 24 in the Mask length text box; then click Apply.

3. Select Exact from the Match Type drop-down list; then click Apply.

   This procedure enables redistribution of route 100.2.1.0/24 from AS 4 to AS 100. No other routes are redistributed.

Redistributing All Routes

1. To allow all routes to redistributed, click Accept next to All BGP AS 4 routes into AS 100 field.

2. Click Apply.

Redistributing RIP to OSPF Example

In this example, Nokia Platform A is connected to a RIP network and is redistributing RIP routes to and from OSPF for the Nokia OSPF Backbone. Nokia Platform D is connected to a subnet of Unix workstations that is running routed.

Note

routed is a utility that runs by default on most Unix workstations. This utility listens to RIP network updates and chooses a default route based on what is advertised. This process eliminates the need for static routes and provides route redundancy. Because routed does not send route updates, it is called a passive RIP listener. This subnet (192.168.26.64/28) is
categorized as a stub network, meaning that a particular subnet does not send RIP routing updates.

Redistributing Routes from RIP to OSPF External

Routes are redistributed from the corporate RIP network to the Nokia OSPF network through Nokia Platform A.

Note
Make sure that the Corporate net RIP router is advertising RIP on the interface connected to the Nokia network. It must be receiving and transmitting RIP updates. Nokia does not currently support the notion of trusted hosts for authentication of RIP routes.

1. Connect to Nokia Platform A using Voyager.
2. Click Config on the home page.
3. Click the Route Redistribution link under the Routing Configuration section.
4. Click the RIP link under the Redistribute to OSPF External section.
5. To redistribute all routes, click Accept in the All RIP routes into OSPF External field.
   (Optional) To change the cost metric for RIP Routes into OSPF Externals, enter the new cost metric in the Metric text box, then click Apply.
6. To prevent 192.168.22.0/24 and other more specific routes from being redistributed into OSPF External, define a route filter to restrict only this route as follows:
   a. To configure this filter, enter **192.168.22.0** in the New IP prefix to redistribute text box, and **24** in Mask length text box. Click Apply.
   b. Select Normal in the Match Type drop-down list. This specifies to prefer routes that are equal to or more specific than 192.168.22.0/24.
   c. Click Apply.

The filter is fully configured.

Redistributing Routes from OSPF to RIP

Routes are redistributed from the Nokia OSPF network to the Corporate RIP Network.

1. Use the Network Voyager connection to Nokia Platform A you have from “Redistributing Routes from RIP to OSPF External.”
2. Click Config on the home page.
3. Click the Route Redistribution link under the Routing Configuration section.
4. Click the OSPF link in the Redistribute to RIP section.
5. To export all OSPF routes into RIP, click Accept in the All OSPF routes into RIP field; then click Apply.
   (Optional) To change the cost metric for RIP Routes into OSPF Externals, enter the new cost metric in the Metric text box; then click Apply.
6. If you do not want to export all OSPF routes into RIP, click Restrict and define a route filter to advertise only certain OSPF routes into RIP.
7. Assume that Nokia Platform B has another interface not shown in the diagram and that it has two additional OSPF routes: 10.0.0.0/8 and 10.1.0.0/16. To exclude all routes that are strictly more specific than 10.0.0.0/8; that is, you want to propagate 10.0.0.0/8 itself, but you do not want to propagate the more specific route.
   a. To configure this filter, enter **10.0.0.0** in New IP Prefix to Import text box, and **8** in Mask length text box; Click Apply.
   b. Select Refines in the Match Type drop-down list. This specifies that you want routes that are strictly more specific than **10.0.0.0/8**.
   c. Finally, click Restrict in the Action field. This specifies that we want to discard the routes that match this prefix.
   d. Click Apply.

The filter is fully configured.
Redistributing OSPF to BGP Example

Nokia Platform A is running OSPF and BGP and its local AS is 4.
Nokia Platform E of AS 100 and Nokia Platform A of AS 4 are participating in an EBGP session. Nokia Platform F of AS 200 and Nokia Platform D of AS 4 are also participating in an EBGP session.

**Nokia Platform A**

1. Click Config on the home page.
2. Click the Route Redistribution link in the Routing Configuration section.
3. Click the OSPF link in the Redistribute to BGP section.
4. To redistribute OSPF routes into peer AS 100, select 100 from the Redistribute to Peer AS drop-down list, then click Apply.
5. (Optional) Enter the MED in the MED text box; then click Apply.
6. (Optional) Enter the local preference in the LocalPref text box, then click Apply.
7. To redistribute OSPF routes, enter the IP prefix in the New IP Prefix to Redistribute text box and the mask length in Mask Length text box; then click Apply.

**Inbound Route Filters**

**Description**

Inbound route filters allow a network administrator to restrict or constrain the set of routes that a given routing protocol accepts. The filters let an operator to include or exclude ranges of
prefixes from the routes that are accepted into RIP, IGRP, OSPF and BGP. These filters are configured in the same way as the filters for route redistribution.

An administrator can specify two possible actions for each prefix. These actions are either to accept the address into the routing protocol (with a specified rank), or to exclude the prefix.

You can specify the type of prefix matching that should be done for filter entries in the following ways:

1. Routes that exactly match the given prefix; that is, have the same network portion and prefix length.
2. Routes that match more specific prefixes but do not include the given prefix. For example, if the filter is 10/8, then any network 10 route with a prefix length greater than 8 matches, but those with a prefix length of 8 do not match.
3. Routes that match more specific prefixes and include the given prefix. For example, if the filter is 10/8, then any network 10 route with a prefix length greater than or equal to 8 matches.
4. Routes that match a given prefix with a prefix length between a given range of prefix lengths. For example, the filter could specify that it match any route in network 10 with a prefix length between 8 and 16.

### Configuring IGP Inbound Filters

1. Click Config on the home page.
2. Click the Inbound Route Filters link in the Routing Configuration section.
3. Click the Filter Inbound RIP Routes link.

**Note**

All other IGPs are configured in exactly the same way.

4. In the All Routes Action field, click either Accept or Restrict.
   If you select accept, routes can be rejected individually by entering their IP address and mask length in the appropriate fields. Similarly, if you select **RESTRICT**, routes can be accepted individually by entering their IP address and mask length in the appropriate fields.
5. If you set All Routes to accept and click Apply, the Rank field is displayed.
   In the Rank field you can specify the rank to a value that all routes should have. The range of values is 1 to 255.
6. Enter the appropriate IP address and mask length in the New Route to Filter and Mask Length fields; then click Apply.
   A new set of fields is displayed adjacent to the newly entered IP address and mask length.
7. Click On or Off to enable or disable filtering of this route.
8. From the Match Type field drop-down list, select Normal, Exact, Refines, or Range.
9. In the Action field, click Accept or Restrict to determine what to do with the routes that match the given filter.

10. In the Rank field, enter the appropriate value, and then click Apply.

11. If this completes your actions for this route filtering option, click Save.

12. If this does not complete your actions for this route filtering option, begin again at step 6.

BGP Route Inbound Policy Example

You can selectively accept routes from different BGP peers based on a peer autonomous system or an AS path regular expression.

Configuring Route Inbound Policy on Nokia Platform D Based on an Autonomous System Number

1. Click Config on the home page.

2. Click the Inbound Route Filters link in the Routing Configuration section.

3. Click the Based on Autonomous System Number link.

4. Enter 512 in the Import ID edit box.

   Import ID specifies the order in which the import lists are applied to each route. The range for filters based on AS numbers is from 512 to 1024.

5. Enter 100 in the AS text box; then click Apply.

   This is the AS number from which routes are to be filtered.

6. (Optional) Enter more values in the Import ID and AS text boxes to configure more inbound policies based on autonomous system numbers; then click Apply.

Note
By default, all routes originating from the configures ASes are accepted.
You can accept or reject all routes from a particular AS by enabling the accept or restrict option next to the All BGP routes from AS field.

1. You also can accept or reject particular routes from AS 100 by specifying a route filter.
   Route filters are specified as shown in the Route Redistribution section. Assume that you want to filter all routes that are strictly more specific than 10.0.0.0/8. In other words, allow all routes whose prefix is not 10.0.0.0/8 except for 10.0.0.0/8 itself, but exclude all routes that are more specific, such as 10.0.0.0/9 and 10.128.0.0/9.

2. To configure this filter, enter 10.0.0.0 in New IP prefix to import text box, and 8 in Mask Length text box; click Apply.

3. Select Refines in the Match type drop-down list.
   This specifies routes that are strictly more specific than 10.0.0.0/8.

4. Finally, click Restrict in the Action field.
   This specifies discard the routes that match this prefix.

5. Click Apply.
   The filter is fully configured.

### Configuring Route Inbound Policy on Nokia Platform D Based on ASPATH Regular Expressions

1. Click Config on the home page.

2. Click the Inbound Route Filters link in the Routing Configuration section.

3. Click the Based on ASPATH Regular Expressions link.

4. Enter 500 in the Import ID edit box.
   The import ID specifies the order in which the import lists are applied to each route. For route filters based on AS path regular expressions, the range of values is from 1 to 511.

5. Enter a regular expression that identifies a set of ASes that should be matched with the SPATH sequence of the route:
   100|200
   This sequence accepts all routes whose ASPATH sequence contains 100 or 200 or both.

6. Select one of the origin options from the Origin drop-down list; then click Apply.
   These options detail the completeness of AS path information. An origin of IGP indicates that an interior routing protocol-learned route was learned from an interior routing protocol and is most likely complete. An origin of EGP indicates the route was learned from an exterior routing protocol that does not support AS paths, and the path is most likely incomplete. When the path information is incomplete, an origin of incomplete is used.

7. Enter a new route filter. In this example assume that you want to filter all routes that are strictly more specific than 10.0.0.0/8. In other words, allow all routes whose prefix is not 10.0.0.0/8 except for 10.0.0.0/8 itself, but exclude all routes that are more specific, such as 10.0.0.0/9 and 10.128.0.0/9.

8. To configure this filter, enter 10.0.0.0 in New IP prefix to import edit box, and 8 in Mask length edit box; then click Apply.
9. Select Refines in the Match type drop-down list.
   This specifies routes that are strictly more specific than 10.0.0.0/8.
10. Finally, click Restrict in the Action field.
    This specifies to discard the routes that match this prefix.
11. Click Apply.
    The filter is fully configured.

BGP AS Path Filtering Example

BGP updates restrict the routes a router learns or advertises. You can filter these updates based on AS PATH regular expressions, neighbors (AS numbers), or community IDs.

To filter BGP updates based on AS PATH regular expressions, see “Configuring Route Inbound Policy on Nokia Platform D Based on AS PATH Regular Expressions.” The following examples, however, give a more detailed description of how to create AS PATH regular expressions.

AS PATH Regular Expressions

1. To accept routes that transit through AS 3662, enter the following AS PATH regular expression in the AS PATH Regular Expression text box:
   
   \((.* \s+3662 \s+.*)\)

   Select Any from the Origin drop-down list; then click Apply.

2. To accept routes whose last autonomous system is 3662, enter this AS PATH regular expression in the AS PATH Regular Expression text box:
   
   \((.* \s+3662)\)

   Select Any from the Origin drop-down list; then click Apply.

3. To accept routes that originated from 2041 and whose last autonomous system is 701, enter the following AS PATH regular expression in the AS PATH Regular Expression text box:

   \(2041 \s+701\)

   Select Any from the Origin drop-down list; then click Apply.

4. To accept SPRINT (AS number 1239) routes that transit through AT&T (AS number 7018) or InternetMCI (AS number 3561), enter the following AS PATH regular expression in the AS PATH Regular Expression text box:

   \((1239 \s+.* \s+7018 \s+.*) \s| \s(1239 \s+.* \s+3561 \s+.*)\)

   Select Any from the Origin drop-down window; then click Apply.

5. Click Save to make your changes permanent.
6 Configuring Router Services

Chapter Contents

- Bootp Relay
  - Bootp Relay Description
  - Enabling Bootp Relay on an Interface
  - Disabling Bootp Relay on an Interface
- IP Broadcast Helper
  - IP Broadcast Helper Description
  - Configuring IP Helper Services
  - Enabling Forward Nonlocal
  - Disabling IP Helper Services
- Router Discovery
  - Router Discovery Overview
  - Enabling Router Discovery Services
  - Disabling Router Discovery Services
- VRRP
  - Understanding VRRP
  - How VRRP Works
  - Understanding Monitored-Circuit VRRP
  - Configuring VRRP
  - Configuring Check Point NGX with Application Intelligence for VRRP
  - Monitoring VRRP
  - Troubleshooting VRRP
- NTP
  - NTP Description
  - Configuring NTP
Bootp Relay

Bootp Relay Description

Bootp Relay extends Bootstrap Protocol (Bootp) and Dynamic Host Configuration Protocol (DHCP) operation across multiple hops in a routed network. In standard Bootp, all interfaces on a LAN are loaded from a single configuration server on the LAN. Bootp Relay allows configuration requests to be forwarded to and serviced from configuration servers located outside the single LAN. Bootp Relay has the following advantages over standard Bootp:

- It makes it possible to bootstrap load from redundant servers by allowing multiple servers to be configured for a single interface. If one of the redundant configuration servers is unable to perform its job, another takes its place.
- It provides load balancing by allowing different servers to be configured for different interfaces instead of requiring all interfaces to be loaded from a single configuration server.
- It allows more centralized management of the bootstrap loading of clients. This advantage becomes more important as the network becomes larger.

The IPSO implementation of Bootp Relay is compliant with RFC 951, RFC 1542, and RFC 2131. Bootp Relay supports Ethernet and IEEE 802 LANs by using canonical MAC byte ordering, that is, clients that specify Bootp htype=1: 802.3 and FDDI.

When an interface configured for Bootp Relay receives a boot request, it forwards the request to all the servers in its server list. It does this after waiting a specified length of time to see if a local server answers the boot request. If a primary IP is specified, it stamps the request with that address, otherwise it stamps the request with the lowest numeric IP address specified for the interface.

You can use Network Voyager to enable Bootp Relay on each interface. If the interface is enabled for relay, you can set up a number of servers to which to forward Bootp requests. Enter a new IP address in the New Server text box for each server. To delete a server, turn it off.

You can set the number of seconds to wait for a local configuration server to answer the boot request before it forward the request through the interface. Enter the number of seconds to wait in the Wait Time text box. Set the wait time to be of sufficient length to allow the local configuration server to respond before the request is forwarded. If is no local server is present, set the time to zero (0).

If you enter an IP address in the Primary IP text box, all Bootp requests received on the interface are stamped with this gateway address. This can be useful on interfaces with multiple IP addresses (aliases).

Enabling Bootp Relay on an Interface

1. Click Config on the home page.
2. Click the Bootp Relay link in the Router Services section.
3. Locate the interface on which you want to enable Bootp.
4. Click **ON** for that interface.
5. Click **APPLY** to enable the interface.
6. (Optional) Enter the minimum client-elapsed time (in seconds) before forwarding a Bootp request in the Wait Time text box.
7. (Optional) Enter the IP address to use as the Bootp router address in the Primary IP text box.
8. (Optional) Enter the IP address of the Bootp/DHCP configuration server to which to relay Bootp requests in the New Server text box.
9. Click Apply.
10. (Optional) Repeat steps 8 and 9 to relay Bootp requests to more than one server.
11. To make your changes permanent, click Save.

**Disabling Bootp Relay on an Interface**

---

**Note**
When you disable Bootp relay on an interface, the Wait Time, Primary IP, and New Server fields disappear, but the parameters are still stored in the system.

---

1. Click Config on the home page.
2. Click the Bootp Relay link in the Router Services section.
3. Locate the Bootp relay interface to be disabled.
4. Click off for the interface you want to disable.
5. Click Apply to disable the interface.
   - When you click off, then apply, the Bootp relay parameters no longer appear.
   - When you click on in the Bootp/DHCP relay interfaces field, then apply, the Bootp relay parameters appear again.
6. To make your changes permanent, click Save.

**IP Broadcast Helper**

**IP Broadcast Helper Description**

IP Broadcast Helper is a form of static addressing that uses directed broadcasts to forward local and all-nets broadcasts to desired destinations within the internetwork.

You cannot pass BOOTP UDP packets by using the IP Broadcast helper (UDP port 67). The BOOTP functionality on a router is different from generic UDP packet forwarding to a specified IP address.
While the IP Broadcast Helper forwards the UDP packet to the IP address without modification, the BOOTP implementation is more complex. The following is a brief explanation of BOOTP forwarding in a router:

Client> Sends broadcast bootp packet> [router]> Sends modified packet to server

The router modifies the packet by inserting its IP address in the giaddr field of the BOOTP packet (this is needed for the server to identify the network where the packet originated).

Note
For further information, see RFC1542 section 4.

Configuring IP Helper Services

1. Click Config on the home page.
2. Click the IP Broadcast Helper link in the Router Services section.
3. Click on for each interface to support IP Helper service. Click Apply.
4. (Optional) To add a new UDP Port to the helper services, enter the new UDP port number in the New UDP Port text box. Click Apply.
5. (Optional) If you want to add a new server to a UDP port, enter the new server IP address in the New Address for UDP Port x text box. Click Apply.
6. Verify that each interface, UDP port, or server is enabled (on checked) or disabled (off checked) for IP helper support according to your needs.
7. To make your changes permanent, click Save.

Enabling Forward Nonlocal

The Forward Nonlocal feature allows you to forward packets that are not originated by a source that is directly on the receiving interface. When you enable Forward Nonlocal, it applies to all interfaces that are running the IP Helper service.

1. Click Config on the home page.
2. Click the IP Broadcast Helper link in the Router Services section.
3. Click Enabled in the Forward Nonlocal field.
4. Click Apply, and then click Save to make your change permanent.

Note
The default is disabled, which requires that packets be generated by a source directly on the receiving interface to be eligible for relay.

5. To disable the Forward Nonlocal feature if you have enabled it, click Disabled in the Forward Nonlocal field.
6. Click **APPLY**, and then click **SAVE** to make your change permanent.

**Disabling IP Helper Services**

1. Click Config on the home page.
2. Click the IP Broadcast Helper link in the Router Services section.
3. Click off for each interface to disable for IP Helper service. Click Apply.
4. Click off for each UDP port to disable for IP Helper service. Click Apply.
5. Click off radio button for each server to disable for IP Helper service. Click Apply.
6. To make your changes permanent, click Save.

**Router Discovery**

**Router Discovery Overview**

The **ICMP Router Discovery Protocol** is an IETF standard protocol used to inform hosts of the existence of routers. It is intended to be used instead of having hosts *wiretap* routing protocols such as RIP. It is used in place of, or in addition to, statically configured default routes in hosts.

The ICMP Router Discovery Service provides a mechanism for hosts attached to a multicast or broadcast network to discover the IP addresses of their neighboring routers. This section describes how you can configure a router to advertise its addresses by using ICMP Router Discovery.

---

**Note**

*Only the server portion of the Router Discovery Protocol is supported.*

---

**Router Discovery Server**

The Router Discovery Server runs on routers and announces their existence to hosts. It does this by periodically multicasting or broadcasting a *router advertisement* to each interface on which it is enabled. These advertisements contain a list of all the router addresses on a given interface and their preference for use as a default router.

Initially, these router advertisements occur every few seconds, then fall back to every few minutes. In addition, a host can send a *router solicitation*, to which the router responds with a unicast router advertisement, unless a multicast or broadcast advertisement is due in a moment.

Each router advertisement contains an *advertisement lifetime* field indicating for how long the advertised addresses are valid. This lifetime is configured such that another router advertisement is sent before the lifetime expires. A lifetime of zero (0) indicates that one or more addresses are no longer valid.
On systems that support IP multicasting, the router advertisements are sent by default to the all-hosts multicast address 224.0.0.1. However, you can specify the use of broadcast. When router advertisements are being sent to the all-hosts multicast address, or an interface is configured for the limited-broadcast address 255.255.255.255, all IP addresses configured on the physical interface are included in the router advertisement. When the router advertisements are being sent to a net or subnet broadcast, only the address associated with that net or subnet is included.

**Enabling Router Discovery Services**

1. Click Config on the home page.
2. Click the Router Discovery link in the Router Services section.
3. Click on for each interface to support router discovery service. Click Apply.
4. (Optional) Enter the minimum advertisement interval for each enabled interface in the Minimum advertisement interval text box.
   - Range: Between 3 seconds and the value in the Maximum advertisement interval field.
   - Default: 0.75 times the value in the Maximum advertisement interval field.
5. (Optional) Enter the maximum advertisement interval for each enabled interface in the Maximum advertisement interval text box. Click Apply.
   - Range: 4-1800.
   - Default: 600.
6. (Optional) Enter the lifetime of advertisement packets for each enabled interface in the Advertisement lifetime text box. Click Apply.
   - Range: Between the value in the Maximum advertisement interval field and 9000 seconds
   - Default: 3 times the values in the Maximum advertisement interval field.
7. (Optional) You can specify whether or not an IP address should be advertised in the Router Advertisement packets.
   - The default is Yes. To disable this feature and specify not to advertise an IP address, click No in the Advertise address field. Click Apply.

**Note**

This option applies to each address on the interface and not to the interface itself.

8. (Optional) You can specify the preferability of an IP address as a default router address, relative to other addresses on the same subnet. You can also make an IP address ineligible as a default router address.
   - Click Ineligible to remove an IP address as a possible default router address.
   - The default is Eligible. Enter a value to indicate the level of preference for the IP address as a default router address in the text box below the Eligible button. The default is 0.
   - Click Apply.
Note
This option applies to each address on the interface and not to the interface itself.

9. To make your changes permanent, click Save.

Disabling Router Discovery Services

1. Click Config on the home page.
2. Click the Router Discovery link in the Router Services section.
3. Click off for each interface to disable support for router discovery service. Click Apply.
4. To make your changes permanent, click Save.

VRRP

Understanding VRRP

Virtual Router Redundancy Protocol (VRRP) provides dynamic failover of IP addresses from one router to another in the event of failure. VRRP is defined in RFC 3768. The Nokia implementation of VRRP includes all of the features described in RFC 3768, plus the additional feature of monitored circuit, described below.

Nokia supports VRRP for IPv6. For more information about the Nokia implementation and how to configure VRRP for IPv6 interfaces, see “Configuring VRRP for IPv6.”

VRRP allows you to provide alternate router paths for end hosts that are configured with static default routes. Using static default routes minimizes configuration and processing overhead on end hosts. When end hosts are configured with static routes, normally the failure of the master router results in a catastrophic event, isolating all hosts that are unable to detect available alternate paths to their gateway. You can implement VRRP to provide a higher availability default path to the gateway without needing to configure dynamic routing or router discovery protocols on every end host.

How VRRP Works

VRRP uses a virtual router to allow end hosts to use an IP address that is part of the virtual router as the default first-hop router. A virtual router is defined as a unique virtual router ID (VRID) and the router IP addresses of the default route on a LAN, and is comprised of a master router and at least one backup router. If the master platform fails, VRRP specifies an election protocol that dynamically assigns responsibility to a backup platform for forwarding IP traffic sent to the IP address of the virtual router.
A virtual router, or VRID, consists of a master platform and one or more backups. The master sends periodic VRRP advertisements (also known as hello messages). To minimize network traffic, backups do not send VRRP advertisements.

Nokia provides support for OSPF, BGP, RIP, and PIM (both sparse and dense mode) to advertise the virtual IP address of the VRRP virtual router. You must use monitored-circuit VRRP, not VRRPv2, to configure virtual IP support for a dynamic routing protocol. You must also enable the Accept Connections to VRRP IPs option.

**Note**

IPSO also supports OSPF over VPN tunnels that terminates at a VRRP group. Only active-passive VRRP configurations are supported, active-active configurations are not.

The master is defined as the router with the highest setting for the *priority* parameter. You define a priority for each platform when you establish the VRID or add a platform to it. If two platforms have equivalent priorities, the platform that comes online and starts broadcasting VRRP advertisements first becomes the master.

Figure 2 shows a simple VRRP configuration with a master (Platform A) and one backup (Platform B).

**Figure 1  Simple VRRP Configuration**

A VRRP router (a router that is running VRRP) might participate in more than one VRID. The VRID mappings and priorities are separate for each VRID. You can use this type of configuration to create two VRIDs on the master and backup platforms, using one VRID for connections with the external network and one for connection with the internal network, as shown in Figure 2.
Figure 2  VRRP Configuration with Internal and External VRIDs

In this example, Platform A acts as the master for both VRID 1 and VRID 2 while Platform B acts as the backup for both VRID 1 and VRID 2.

You can configure several platforms to be part of multiple VRIDs while they simultaneously back up each other, as shown in Figure 3. This is known as an active-active configuration.

Figure 3  VRRP Configuration with Simultaneous Backup

In this active-active configuration, two VRIDs are implemented on the internal network for the purpose of load sharing. Platform A is the master for VRID 5 and serves as the default gateway for Host H1 and Host H2, while Platform B is the master for VRID 7 and serves as the default gateway for Host H3 and Host H4. Simultaneously, both Platform A and B are configured to back up each other. If one platform fails, the other takes over its VRID and IP addresses and provides uninterrupted service to both default IP addresses. This configuration provides both load balancing and full redundancy.
Understanding Monitored-Circuit VRRP

The Nokia implementation of VRRP includes additional functionality called monitored circuit. Monitored-circuit VRRP eliminates the black holes caused by asymmetric routes that can be created if only one interface on the master fails (as opposed to the entire box failing). IPSO does this by releasing priority over all of the VRRP-configured interfaces to allow the backup to take over entirely.

Note
You can choose to implement the industry standard VRRPv2 on your Nokia appliance instead of monitored-circuit VRRP. For information on implementing VRRPv2, see “Configuring VRRPv2” on page 284.

To understand the advantage of monitored-circuit VRRP, consider the configuration pictured in Figure 2. In this example, if you are using standard VRRPv2 and the external interface fails or becomes unreachable, the external virtual router fails over to the backup while the internal virtual router stays on the master. This can result in reachability failures, as the platform might accept packets from an internal end host but be unable to forward them to destinations that are reached through the failed interface to the external network.

Monitored-circuit VRRP monitors all of the VRRP-configured interfaces on the platform. If an interface fails, the master releases its priority over all of the VRRP-configured interfaces. This allows the backup platform to take over all of the interfaces and become master for both the internal and external VRID.

To release the priority, IPSO subtracts the priority delta, a Nokia-specific parameter that you configure when you set up the VRID, from the priority to calculate an effective priority. If you configured your system correctly, the effective priority is lower than that of the backup routers and, therefore, the VRRP election protocol is triggered to select a new master.

Configuring VRRP

You can configure VRRP on your appliance using three methods:

- Monitored-Circuit VRRP simplified method
  
  For most purposes, you should use this method. This is a simplified version of the VRRP with monitored circuit full configuration method. You cannot use both full and simplified methods to configure monitored-circuit VRRP on the same appliance. For more information, see “Configuring Monitored-Circuit VRRP using the Simplified Method”.

- Monitored-Circuit VRRP full method
  
  Use this method if you are working with a system on which VRRP has already been configured using this method or if you need control over the configuration of each individual interface. For more information see “Configuring Monitored-Circuit VRRP using the Full Method”.

- VRRPv2
Use this method only if you do not have an extra IP address to use for monitored-circuit VRRP. For more information see “Configuring VRRPv2”.

Selecting Configuration Parameters
Before you begin, plan your implementation by deciding how you want to set the following configuration parameters.

- Priority
- Hello Interval
- Authentication
- Priority Delta
- Backup Address
- VMAC Mode

Priority
The priority value determines which router takes over in the event of a failure; the router with the higher priority becomes the new master. The range of values for priority is 1 to 254. The default setting is 100.

Note
In Nokia’s monitored-circuit VRRP, the master is defined as the router with the highest priority setting, although RFC 3768 specifies that the master must have a priority setting of 255.

If two platforms have equivalent priorities, the platform that comes online and starts broadcasting VRRP advertisements first becomes the master. If there is a tie, the platform with the higher IP address is selected.

To prevent the unlikely event that the tie-breaking algorithm selects one platform as the master for the external network and another as the master router for the internal network, you should make all interfaces on one platform numerically greater than the interfaces on the peer. For example, Platform A should be the .1 host and Platform B should be the .2 host on all connected interfaces.

You should set the priority to 254 for least the master platform in each VRID to provide a faster transition in the event of a failure. Using higher values can decrease the time it takes for a backup router to take over for a failed router by close to one second.

Note
Setting a higher priority shortens the transition time because the time interval for a backup to declare the master down is calculated as

\[
\text{Master\_Down\_Interval} = (3 \times \text{Hello\_interval}) + \text{Skew\_time};\text{ and the skew time (seconds by which to skew the Master\_Down\_Interval) is calculated as } \text{Skew\_time} = (\frac{256 - \text{Priority}}{256}).
\]
You can configure your VRID to specify one platform as the *established master* by assigning it a higher priority, or you can assign *equivalent priority* to all platforms. If you specify an established master by assigning it a higher priority, the original master recovers control after a failover event and it takes back control of the VRID. If you assigned the original master equivalent priority with the backup, it does not resume control of the VRID. You might choose to specify one platform as the established master if it has more capacity than the other; for example if the master is an IP530 and the backup is an IP330. If both security platforms have the same capacity, you might choose to use equivalent priority in order to have fewer VRRP transitions. You can also use the preempt mode to accomplish the same thing.

**Hello Interval**

The hello interval is the time interval in seconds at which the master sends VRRP advertisements. The default (and minimum) value is 1 second.

Set the hello interval to the same value for all nodes of a given VRID. If the hello interval is different, VRRP discards packets, which results in both platforms going to the master state.

The hello interval also determines the failover interval; that is, how long it takes a backup router to take over from a failed master. If the master misses three hello advertisements, it is considered to be down. Because the minimum hello interval is 1 second, therefore the minimum failover time is 3 seconds (3 * Hello_interval).

**Authentication**

You must select the same authentication method selected for all nodes in a VRID.

Choose None to require no authentication for VRRP advertisements; choose Simple to require a password before a VRRP advertisement is accepted by the interface, then enter the password in the Password text field.

- **None**—Select only in environments where there is minimal security risk and little chance for configuration errors (for example, only two VRRP routers on a LAN).
- **Simple**—VRRP protocol exchanges are authenticated by a simple clear-text password. You can use this authentication method to protect against a router inadvertently backing up another router in cases where you have more than one VRRP group in a network.

Simple authentication does not protect against hostile attacks where the password can be learned by a node snooping VRRP packets on the LAN. However, when combined with the TTL check used by VRRP (TTL is set to 255 and is checked on receipt), simple authentication make it unlikely that a VRRP packet from another LAN will disrupt VRRP operation.

**Priority Delta**

Choose a value for the priority delta that ensures that the priority delta subtracted from the priority results in an effective priority that is lower than that of the backup routers (in case an interface fails).

You might find it useful to use a standard priority delta throughout your VRRP configurations to keep your configurations simple and easy to understand.
This parameter applies only to monitored-circuit VRRP, not to VRRPv2.

**Backup Address**

Also called the virtual IP address, the backup address is the IP address your end hosts and neighbor routers use for routing. The backup address is the address that is failed over between the master and the backup platforms.

The backup address parameter is added to standard VRRP for use with Nokia’s monitored-circuit VRRP. It does not apply to VRRPv2.

The backup address must be in the same network as the interface you want to use for the VRID. When you enter a backup address, the system uses the interface that is in that subnet for the VRID; if there is no interface configured on that subnet, the system displays an error message. You must also select backup addresses that do not match the real IP address of any device on the interface network nor the IP address of any of the interfaces on either VRRP node.

Before you modify backup addresses or delete an IP address from an interface, consider the following points. (These points apply only to monitored-circuit VRRP configured using the simplified method.)

- You must manually modify the list of backup addresses on each node of a VRRP group whenever the IP addresses of the other routers change.
- You cannot change the backup address from one interface to another interface while a platform is in the master state. To modify a virtual IP address, first cause a failover to the backup (you can do this by disabling one of the VRRP-configured interfaces), then delete the VRID and re-create it using the new IP address, then configure it as it was configured before.
- Before you delete an IP address from a logical interface, you must delete the corresponding backup addresses configured for monitored-circuit VRRP. The configuration for the virtual router might become corrupted if you delete the IP address before you delete the backup addresses. This issue does not apply either to the full method configuration of monitored-circuit VRRP or to VRRPv2.

**VMAC Mode**

For each VRID, a virtual MAC (VMAC) address is assigned to the backup address. The VMAC address is included in all VRRP packet transmissions as the source MAC address; the physical MAC address is not used.

When you configure a VRID, you specify which mode IPSO uses to select the VMAC address. You can use any of the modes for Virtual LAN deployments, which forward traffic based on the VLAN address and destination MAC address.

- **VRRP**—The default mode. IPSO sets the VMAC to the format outlined in the VRRP protocol specification RFC 3768. It is automatically set to the same value on all nodes of a VRID.
- **Interface mode**—IPSO sets the VMAC to the MAC address of the local interface. If you select interface mode for both master and backup, the VMAC is different for each. The VRRP IP addresses are associated with different VMACs because they depend on the MAC address of the physical interfaces of the platform that is master at the time.
Note
If you configure different VMACs on the master and backup, you must take care to choose the correct proxy ARP setting for Network Address Translation.

Interface mode can be useful with certain switches that have problems with packets on multiple ports with the same MAC address. In these cases, you can use Interface mode to ensure that the VMAC from the master and backup are not the same.

- **Static mode**—Select this mode if you want to set the VMAC address manually, then enter the 48-bit VMAC address in the Static VMAC text field.

Note
If you configure different VMACs on the master and backup, you must take care to choose the correct Proxy ARP settings when configuring proxy ARP setting for Network Address Translation.

- **Extended mode**—Similar to VRRP mode, except the system dynamically calculates three additional bytes of the interface hardware MAC address to generate a more random address. If you select this mode, IPSO constructs the same MAC address for master and backup platforms within the VRID.

Note
If you set the VMAC mode to interface or static, syslog error messages are displayed when you reboot or at failover, indicating duplicate IP addresses for the master and backup. This is expected behavior since both the master and backup routers are temporarily using the same virtual IP address until they resolve into master and backup.

**Before you Begin**

Before you begin, consider your hardware and configuration. Are all backup routers able to handle the traffic they will receive if the master fails? Will you implement load-sharing?
Plan values for the configuration parameters of each node, as described in the following table:

**Table 6 VRRP Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID</td>
<td>Range is 1 to 255; there is no default. Choose a numbering scheme for your virtual routers that will make sense to other people. For example, you might choose VRIDs that are the last octet of the backup address, such as 5 if the backup address is 192.168.2.5.</td>
</tr>
<tr>
<td>Priority</td>
<td>Range is 1 to 254; default is 100. Set the priority to 254 for least one platform in each VRID and choose values on the higher end of the scale for the backups. This provides a faster transition in the event of a failure. Decide whether you want an established master or equivalent priority for all or several routers. For more information, see “Priority”.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Range is 1 to 255; default setting is 1 second. Set the same value for all nodes in the VRID. For more information, see “Hello Interval”</td>
</tr>
<tr>
<td>Authentication</td>
<td>Choose whether you want to implement no authentication or simple password. You must select the same authentication method for all nodes in the VRID. For more information, see “Authentication”.</td>
</tr>
<tr>
<td>Priority Delta</td>
<td>Choose a value that will ensure that when an interface fails, the priority delta subtracted from the priority results in an effective priority that is lower than that of all of the backup routers. Nokia recommends you use a standard priority delta, such as 10, to simplify your configuration. For more information, see “Priority Delta”.</td>
</tr>
<tr>
<td>Backup address</td>
<td>The backup address must be in the same network as the interface you want to use for the VRID. Select a backup addresses that does not match the real IP address of any host or router on the interface network nor the IP address of any of the interfaces on either node. For more information, see “Backup Address”</td>
</tr>
<tr>
<td>VMAC mode</td>
<td>Choose the method by which the VMAC address is set. For more information, see “VMAC Mode”.</td>
</tr>
</tbody>
</table>

**Note**

You set values for priority delta and backup address only when configuring monitored-circuit VRRP. These parameters are not applicable to VRRPv2.
Complete these additional steps before you configure VRRP.

- Synchronize all platforms that are part of the VRRP group to have the same system times.
  
  The simplest way to ensure that system times are coordinated is to enable NTP on all nodes of the VRRP group. You can also manually change the time and time zone on each node so that it matches the other nodes to within a few seconds.

- Add hostnames and IP address pairs to the host table of each node in your VRRP group. This is not required but will enable you to use hostnames instead of IP addresses or DNS servers.

### Configuring Monitored-Circuit VRRP

You can configure monitored-circuit VRRP using either of two methods. You cannot use both the simplified and full configuration methods on the same platform; in fact, after you have created a VRID using one method, the selections for the other method are no longer visible.

- Simplified method—Nokia recommends you use this method. The simplified method automatically includes all VRRP-configured interfaces on the platform in the VRRP configuration. You do not have to separately specify settings for each interface. For more information, see “Configuring Monitored-Circuit VRRP using the Simplified Method”.

- Full method—Use this method if you are working with a system on which VRRP has already been configured using this method, or if you want control over the configuration of each individual interface. If you use this method, you must specify settings for each VRRP-configured interface, including which other interfaces are monitored by this one. For more information, see “Configuring Monitored-Circuit VRRP using the Full Method”.

### Configuring Monitored-Circuit VRRP using the Simplified Method

To implement monitored-circuit VRRP using the simplified method, you must first create a virtual router by specifying a VRID (the master router IP addresses are added to the virtual router automatically), and then specify values for priority, hello interval, priority delta, and backup address. You do this for each appliance in each VRRP group in turn. For firewall and VPN applications, you generally want to back up at least two interfaces on the appliance—the external network and the internal network.

---

**Note**

Before you delete an IP address from a logical interface, you must delete the corresponding backup addresses configured in the monitored-circuit VRRP for the specified virtual router. The configuration for the virtual router might become corrupted if you delete the IP address before you delete the backup addresses. This issue does not apply either to the full method configuration of monitored-circuit VRRP or to VRRPv2.

---

**To add a virtual router**

1. Log on to the platform you will use as the master.

2. If you have not done so already, assign IP addresses to the interfaces you will use for the virtual router.
3. Click Config (on the Home page) > VRRP (under Router Services).

4. (Optional) If you want to allow the system to accept and respond to IP packets sent to an adopted VRRP IP address, select the Enabled radio button for Accept Connections to VRRP IPs.

   The VRRP protocol specifies *not* to accept or respond to such IP packets. Overriding this specification is recommended if you are deploying applications whose service is tied to a VRRP IP address. You can also use it to allow logins to the master by using an adopted VRRP IP address. You must also enable this option if you configure a virtual IP for VRRP to run on OSPF, PIM, or OSPF.

5. In the Create a New Monitored-Circuit Virtual Router text box, enter a value for the VRID.

6. Click Apply.

7. Additional fields are displayed showing the configuration parameters. Enter values into these fields. For more information see “Selecting Configuration Parameters”.

8. Click Apply.

9. Click Save to make your changes permanent.

10. Log on to each backup appliance in turn and repeat step 2 through step 5.

    Make sure you use the same values for VRID, hello interval, authentication method, and backup address for all nodes in the VRID.

11. If you are using Check Point NGX with Application Intelligence, completely configure VRRP on each platform and make sure the firewall has begun synchronization before you put the VRRP group in service. Following this process ensures that all connections are properly synchronized.

To delete a virtual router

1. Choose Config (on the Home page) > VRRP (under Router Services).

2. In the row for the appropriate VRID, select the Delete checkbox.

3. Click Apply.

4. Click Save to make your changes permanent.

To change the configuration of an existing virtual router

1. Choose Config (on the Home page) > VRRP (under Router Services).

2. In the appropriate text box, you can change the priority, hello interval, authentication method, password for simple authentication, priority delta, and backup address for an existing virtual router.

   For information on these parameters, see “Selecting Configuration Parameters”.

   **Note**

   If you change the hello interval, authentication method, password, or backup address, you must change it on all other platforms which participate in the VRID.
3. Click Apply.
4. Click Save to make your changes permanent.

**Configuring Monitored-Circuit VRRP using the Full Method**

If you use the full method to configure monitored-circuit VRRP, you must manually select the list of interfaces that each interface will monitor. You can configure monitored-circuit VRRP using only one of the methods (simplified or full) on a given platform.

If your platform has monitored-circuit VRRP configurations configured using the full method and you wish to use the simplified method, you must delete the VRIDs and re-create them using the simplified method.

In addition to the configuration parameters used with the simplified configuration method (see Table 6 on page 279), you can also set the following additional parameters by using the full configuration method:

**Table 7 Additional Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preempt mode</td>
<td>Preempt mode is enabled by default. Check disabled 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. For example, if you disable preempt mode on a backup and the master fails over to it, then when the master becomes active again, the virtual router will not fail back to it. Rather the new master will remain the master even though it has a lower priority. Monitored-circuit VRRP operates by triggering the failover of all mcVRRP interfaces on a platform when one interface goes down. It triggers failover by subtracting the priority delta from the priority for each mcVRRP interface, causing the interface to fail over to a node with a higher priority. If you disable preempt mode, interfaces will no longer failover in this way; they will only failover if their effective priority is 0. Therefore, if you disable preempt mode, you must also apply the following settings to each interface in the VRRP group. These conditions do not apply to VRRPv2. • Enable auto-deactivation. This allows the effective priority to be set to 0. If you do not enable auto-deactivation, the lowest effective priority allowed is 1 even if the priority minus the delta mathematically equals 0. • Set the priority delta to the same value as the priority for each interface on the virtual router. This means that the priority minus the priority delta equals 0.</td>
</tr>
<tr>
<td>Monitor interface</td>
<td>Select an interface that this interface will monitor and specify a priority delta. As you select each interface and click Apply, it appears in the list above the Monitor interface drop-down box.</td>
</tr>
<tr>
<td>Auto-deactivation</td>
<td>Enable auto-deactivation if you want to allow the minimum value for effective priority to be 0. A VRRP router with an effective priority of 0 will not become the master even if there are no other VRRP routers with higher priority for this virtual router. If auto-deactivation is disabled (the default), the lowest allowable value for effective priority is 1.</td>
</tr>
</tbody>
</table>
Note
You cannot change the backup address from one interface to another interface while a platform is in the master state. To modify a virtual IP address, first cause a failover to the backup by reducing the priority or by pulling an interface, then delete the VRID on the interface and re-create using the new IP address, then configure it as it was configured before.

To add a virtual router
1. Choose Config (on the Home page) > VRRP (under Router Services) > VRRP Legacy Configuration link.
2. In the row for the interface you want to configure, select the Monitored Circuit radio button.
3. Click Apply.
   The Create Virtual Router text box appears.
4. Enter the value you want to use to identify the virtual router and click Apply.
   Additional fields appear.
5. Enter values for the configuration parameters for the virtual router.
   Most of these parameters are the same as those used in the simplified configuration method described in Table 6. The additional parameters displayed on this page are specific to the full configuration method—Preempt mode, Monitor interface, and Auto-deactivation—and are described Table 7.
6. Click Apply.
7. Click Save to make your changes permanent.

Note
This procedure describes how to implement monitored-circuit VRRP using Network Voyager. You can also use the CLI commands set mcvr to accomplish the same tasks. For more information, see the CLI Reference Guide for the version of IPSO you are using.

To delete a virtual router
1. Choose Config (on the Home page) > VRRP (under Router Services) > VRRP Legacy Configuration link.
2. Under the section showing the interface for which the VRID is configured, select the Off radio button for the virtual Router.
   Alternatively, you can select the Off radio button in the Mode section for the interface.
3. Click Apply.
4. Click Save to make your changes permanent.
Configuring VRRPv2

Use VRRPv2 rather than Nokia’s monitored-circuit VRRP only if you do not have an extra IP address to use for monitored-circuit VRRP.

Note
You must use monitored-circuit VRRP when configuring virtual IP support for any dynamic routing protocol. Do not use VRRPv2 when configuring virtual IP support for any dynamic routing protocol.

To add or back up a virtual router using VRRPv2

1. Choose Config (on the Home page) > VRRP (under Router Services) > VRRP Legacy Configuration link.
2. In the row for the interface you want to configure, select the VRRP v2 radio button in the Mode column.
3. Click Submit.
   Text boxes for Own VRID and Backup Router with VRID appear.
4. Configure the router as a master or a backup by doing one of the following.
   - If you want to configure this router as the master for a VRRP group, enter the VRID for the virtual router in the Own VRID text box.
   - If you want to configure this router as a backup, enter the VRID you want the router to back up in the Backup Router with VRID text box.
5. Click Apply.
   Additional fields appear.
6. Do one of the following, depending on whether this platform serves as a master or a backup.
   - If this platform serves as the master router, enter values in the Own VRID section for hello interval and VMAC mode for the VRID for which this platform serves as the master router. (For VRRPv2, the priority for the master is automatically set to 255 and the backup address is the physical address of the interface.)
   - If this platform serves as a backup router, enter values in the Router with VRID section for each VRID you are using the interface to backup.
7. Click Apply.
8. Click Save to make your changes permanent.

Note
To disable a virtual router, first remove the VRRP configuration for that virtual router from all backup routers. If you delete the virtual router on the master first, it stops sending VRRP advertisements and the backup router assumes it has failed and adopts the address of the
master automatically. This results in two routers having the address of the default router configured.

Configuring Check Point NGX with Application Intelligence for VRRP

The guidelines in this section list some considerations for configuring Check Point NGX with Application Intelligence for VRRP. For additional details, refer to the Check Point documentation.

- Each VRRP node must run the same feature pack and hot fix.
- You must install the same Check Point packages on each node; each VRRP node must have exactly the same set of packages as all the other nodes.
- Create the complete VRRP configuration before you put any of the systems into service. That is, make sure each system is completely configured and the firewall has begun synchronization before putting the VRRP group in service. Following this process ensures that all connections are properly synchronized. <31674>

When you use the Check Point cpconfig program (at the command line or using Network Voyager), follow these guidelines:

- Install Check Point NGX as an enforcement module only on each node. Do not install Check Point NGX as a management server and enforcement module.
- After you choose to install Check Point NGX as an enforcement module, you are asked if you want to install a Check Point clustering product. The screen displays the following question: "Would you like to install a Check Point clustering product (CPHA, CPLS or State Synchronization)? (y/n) [n] ? The default is no; be sure to enter yes.
- If you plan to use SecureXL, enable it when you are prompted to do so.

You then create and configure a gateway cluster object with the external VRRP IP address.

- Use the Check Point SmartDashboard application to create a gateway cluster object.
- Set the gateway cluster object address to the external VRRP IP address, that is, the VRRP IP address of the interface that faces the external network.
- Add a gateway object for each Nokia appliance to the gateway cluster object.
- In the General Properties dialog box for the gateway cluster object, do not check ClusterXL.
- Configure interfaces for each member of the VRRP cluster. Click the Topology tab for each VRRP cluster member and click Get.
- Configure interfaces for the VRRP cluster. Click the Topology tab for the gateway cluster object, and click Get.
- Enable state synchronization and configure interfaces for it.

Note
The firewall synchronization network should have bandwidth of 100 mbps or greater.
The interfaces that you configure for state synchronization should not be part of VLAN or have more than one IP address assigned to them.

When you finish configuring the gateway cluster object, you must also specify settings under the 3rd party configuration tab as described in the following procedure.

Configure settings under the 3rd party configuration tab

1. In the Specify Clustering Mode field, check High Availability.
2. From the Third-Party Solution drop-down list, select Nokia VRRP.
3. Check all the available check boxes.
4. Click OK to save your configuration changes.

Note
If you use different encryption accelerator cards in two appliances that are part of a VRRP group or an IP cluster (such as the Nokia Encrypt Card in one appliance and the older Nokia Encryption Accelerator Card in another appliance), you should select encryption/authentication algorithms that are supported on both cards. If the encryption/authentication algorithm is supported in the master and not supported by the backup and you also use NAT, tunnels do not fail over correctly. If the encryption/authentication algorithm is supported in the master and not supported by the backup and you do not use NAT, tunnels fail over correctly, but they are not accelerated after failover.

If you use sequence validation in VPN-1 NGX, you should be aware that in the event of a failover, sequence validation is disabled for connections that are transferred to another node. Sequence validation is enabled for connections that are created after the failover.

You might want to enable sequence validation in the Check Point management application and IPSO, as described in the following procedure.

To enable sequence validation in the Check Point management application and IPSO

1. On the main Configuration page in Nokia Network Voyager, click Advanced System Tuning (in the System Configuration section).

Note
This option is available only when SecureXL is enabled.

2. On the Advanced System Tuning page, click the button to enable sequence validation.
3. Enable sequence validation in the Check Point management application.
4. Push the new policy to the IPSO appliance.
Configuring VRRP Rules for Check Point NGX

When you are using Check Point NGX FP1 and FP2 or later, you must define an explicit VRRP rule in the rulebase to allow VRRP Multicast packets to be accepted by the gateway. You can also block the VRRP traffic with an explicitly defined rule.

Caution
VRRP rule constructions used in Check Point FireWall-1 4.1 and earlier does not work with Check Point NGX. Using these constructions could result in VRRP packets being dropped by the cleanup rule.

For information about how to configure VRRP rules for Check Point FireWall-1 4.1, contact the Nokia Technical Assistance Center (TAC).

Configuration Rule for Check Point NGX FP1

Locate the following rule above the Stealth Rule:

Note
The object for VRRP is not the same as the gateway cluster object for HA. Accordingly, in the example below, the gateway cluster object is designated `fwcluster-object`.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cluster-all-ips</code></td>
<td><code>fwcluster-object</code></td>
<td>vrrp</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td><code>mcast-224.0.0.18</code></td>
<td>igmp</td>
<td></td>
</tr>
</tbody>
</table>

Where:
- `cluster-all-ips` is the Workstation object you created with all IPs.
- `fwcluster-object` is the Gateway Cluster object.
- `mcast-224.0.0.18` is a Workstation object with the IP address 224.0.0.18 and of the type host.

Configuration Rules for Check Point NGX FP2 and Later

Locate the following rule above the Stealth Rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Firewalls</code></td>
<td><code>mcast-224.0.0.18</code></td>
<td>vrrp</td>
<td>Accept</td>
</tr>
<tr>
<td><code>fwcluster-object</code></td>
<td></td>
<td>igmp</td>
<td></td>
</tr>
</tbody>
</table>

Where:
- `Firewalls` is a Simple Group object containing the firewall objects.
- `fwcluster-object` is the gateway cluster object.
mcast-224.0.0.18 is a Node Host object with the IP address 224.0.0.18.

Configuring Rules if You Are Using OSPF or DVMRP

All of the solutions in “Configuration Rule for Check Point NGX FP1” and “Configuration Rules for Check Point NGX FP2 and Later” are applicable for any multicast destination.

If your appliances are running routing protocols such as OSPF and DVMRP, create new rules for each multicast destination IP address.

Alternatively, you can create a Network object to represent all multicast network IP destinations by using the following values:

Name: MCAST.NET
IP: 224.0.0.0
Netmask: 240.0.0.0

You can use one rule for all multicast protocols you are willing to accept, as shown below:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-all-ips</td>
<td>fwcluster-object</td>
<td>vrrp</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td>MCAST.NET</td>
<td>igmp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ospf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dvmrp</td>
<td></td>
</tr>
</tbody>
</table>

Link Aggregation (IP2250 Systems Only)

IP2250 appliances allow you to aggregate the built-in 10/100 mbps Ethernet ports so that they function as one logical port with higher bandwidth. These appliances offer link aggregation to accommodate firewall synchronization traffic in VRRP configurations.

If you configure two IP2250 appliances in a VRRP pair and run VPN-1/FireWall-1 on them, Nokia recommends that you create a 200 mbps logical link between them and configure VPN-1 NGX to use this network for firewall synchronization traffic. If you use a single 100 mbps connection for synchronization, connection information might not be properly synchronized if the appliance is handling a large number of connections.

See “Link Aggregation” for detailed information about link aggregation.
Monitoring VRRP

You can use the following CLI commands to view and monitor VRRP information:

Table 8 CLI commands for VRRP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vrrp</td>
<td>Displays a summary of the VRRP state on the node.</td>
</tr>
<tr>
<td>show vrrp interfaces</td>
<td>Displays VRRP information about all interfaces. Use with the name of an interface, for example show vrrp interface &lt;name&gt;, it displays VRRP information for that interface only.</td>
</tr>
<tr>
<td>show vrrp stat</td>
<td>Displays statistics for all VRRP interfaces.</td>
</tr>
<tr>
<td>show mcvr</td>
<td>Displays information about all monitored-circuit VRRP interfaces.</td>
</tr>
</tbody>
</table>

To view VRRP information using Network Voyager, click Monitor (on the Home Page) > VRRP Service Statistics (under System Health). The VRRP service status table appears.

The VRRP service status table contains per-interface and per-virtual router VRRP send and receive packet statistics. It is updated every 20 seconds.

State

A virtual router can be in one of three states:

- Master Forwarding IP packets addressed to the virtual router.
- Backup Eligible to become master and monitoring the state of the current master.
- Initialize Inactive; waiting for startup event.

If a virtual router is in initialize state for longer than 20 seconds, this typically indicates that you have a configuration problem, such as a virtual IP address that is not valid. Check your VRRP configuration.

Location

The location section of the VRRP service status table displays the virtual router flags or the primary address of the current virtual router master. The location options are:

- Local The virtual router applies to addresses owned by the local router.
- IP address Primary address of the current virtual router master. Address 0.0.0.0 indicates unknown.
Stats
The stats section of the VRRP service status table displays VRRP send and receive packet statistics. The Stats options are:

- Advertisement Transmitted: Number of VRRP Advertisement packets sent.
- Advertisement Received: Number of VRRP Advertisement packets received.
- Bad Address List Received: Number of VRRP packets received and discarded due to misconfigured address list.
  \[\text{Note: if the advertisement is from the address owner (priority=255) that packet is accepted, even with the configuration mismatch.}\]
- Bad Advertise Interval Received: Number of VRRP packets received and discarded due to misconfigured advertisement interval.
- Authentication Mismatch: Number of VRRP packets received and discarded due to misconfigured authentication type.
- Authentication Failure: Number of VRRP packets received and discarded due to authentication failure.

Monitoring the Firewall State
By default, IPSO monitors the state of the firewall and responds 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.

To enable or disable Monitor Firewall state
1. Choose Config (on the home page) > VRRP (in the Router Services section).
2. Click Enabled in the Monitor Firewall State field.
   To disable this option, if you have enabled it, click Disabled. The default is Enabled.
3. Click Apply
4. Click Save to make your changes permanent.

Troubleshooting VRRP
This section lists common problems with VRRP configurations. Please consult this section before contacting Customer Support. For information about contacting Nokia Customer Support, go to https://support.nokia.com/

You can log information about errors and events to troubleshoot VRRP by enabling traces for VRRP.
To enable traces for VRRP
1. Click Config on the home page.
2. Click the Routing Options link in the Routing Configuration section.
3. Scroll down the Trace Options section to VRRP and choose an option from the Add Option drop-down list.
4. Click Reset Routing.

The system restarts the routing subsystem and signals it to reread its configuration. The option you selected, its name and On/Off radio buttons are displayed on the page.

General Configuration Considerations
If VRRP failover does not occur as expected, verify that the following items are correctly configured.

- All routers of a VRRP group must have the same system times. The simplest way to synchronize times is to enable NTP on all nodes of the VRRP group. You can also manually change the time and time zone on each node so that it matches the other nodes. It should match to within a few seconds.
- All routers of a VRRP group must have the same hello interval.
- If you are testing monitored-circuit VRRP by pulling an interface, and the other interfaces do not release their IP addresses, check that the priority delta is large enough that the effective priority is lower than the master router.
- If you use different encryption accelerator cards in two appliances that are part of a VRRP group or an IP cluster, such as the Nokia Encrypt Card in one appliance and the older Nokia Encryption Accelerator Card in another appliance, you must select encryption algorithms for each card that are supported on both cards. If you select different encryption algorithms on the backup appliance than on the master, failover might not occur correctly.
- VRIDs must be the same on all routers in a VRRP group. If you are using monitored-circuit VRRP, verify that all platforms in the group that back up a single virtual IP address use the same VRID. If you are using VRRP v2, verify that the VRID used on each backup router uses the same VRID and IP address as the primary router.
- If the VRRP monitor in Network Voyager shows one of the interfaces in initialize state, it might indicate that the IP address used as the backup address on that interface is invalid or reserved.
- SNMP Get on Interfaces might list the wrong IP addresses, resulting in incorrect Policy. An SNMP Get (for the Firewall object Interfaces in the GUI Security Policy editor) fetches the lowest IP address for each interface. If the interfaces are created when the node is the VRRP master, the wrong IP address might be included in the object. To solve this problem, edit the interfaces by hand if necessary. <CR 1521>

Firewall Policies
If your platforms are running firewall software, you must enable the firewall policies to accept VRRP packets. The multicast destination assigned by the IANA for VRRP is 224.0.0.18. If the
firewall policy does not explicitly accept packets to 224.0.0.18, each firewall platform in the VRRP group assumes the VRRP master state.

Access Control Lists

If your platforms use access control lists, you must, at minimum, include the following in the access list criteria:

- The source IP addresses of all participants in the VRRP group.
- The VRRP multicast destination IP address, which is 224.0.0.18.
- The VRRP IP protocol value, which is 112.

If these most restrictive conditions are in place, then each VRRP participant on each access control interface must have a separate rule. Alternatively, you can define a more open rule. For example, a single rule allowing all packets with DST IP 224.0.0.18 and IP protocol value 112 would work for all interfaces controlled by an access control list.<CR1521>

Switched Environments

Monitored-Circuit VRRP in Switched Environments

- When you use monitored-circuit VRRP, some Ethernet switches might not recognize the VRRP MAC address after a transition from the master to a backup. This is because many switches cache the MAC address associated with the Ethernet device attached to a port and when the transition occurs to a backup router, the MAC address for the virtual router appears to shift to another port. Switches that cache the MAC address may not change to the appropriate port during a VRRP transition.

To solve this problem, you can take either of the following actions:

- Replace the switch with a hub.
- Disable MAC address caching on the switch or on the switch ports that the security platforms are connected to.

  If it is not possible to disable the MAC address caching, you may be able to set the address aging value to a number low enough that the addresses age out every second or two. This causes additional overhead on the switch, so you should determine whether this is a viable option for the model of switch you are running.

- Another issue is sometimes seen with switches using the spanning tree protocol. This protocol was created to prevent Layer 2 loops across multiple bridges. If spanning-tree is enabled on the ports connected to both sides of a VRRP pair and it sees multicast hello packets coming for the same MAC address from two different ports, then, in most cases, this would indicate a loop and the switch blocks traffic from one port or the other. If either port is blocked then neither of the security platforms in the VRRP pair can receive the hello packets from the other half of the VRRP pair and both would assume the master router state.

  If possible, turn off spanning-tree on the switch to resolve this issue. However, this can have deleterious effects if the switch is involved in a bridging loop. If you cannot disable spanning-tree, enable PortFast on the ports connected to the VRRP pair. PortFast causes a port to enter the spanning-tree forwarding state immediately, bypassing the listening and
learning states. The command to enable PortFast is `set spantree portfast 3/1-2 enable`; where 3/1-2 refers to slot 3 ports 1 and 2.

**VRRPv2 in Switched Environments**

In the event that you have two interfaces on a switch that are on different VLANs and each has a VRID that is the same as the other, the system can fail. Duplicate VRIDs create duplicate MAC addresses, which will probably confuse the switch.

**NTP**

**NTP Description**

Network Time Protocol (NTP) is an Internet standard protocol used to synchronize the clocks of computers in a network to the millisecond. Synchronized clock times are critical for distributed applications that require time synchronization, such as Check Point FireWall-1 Sync, and for purposes such as analyzing event logs from different devices, ensuring cron jobs execute at the correct time, and ensuring that applications that use system time to validate certificates find the correct time.

NTP runs as a continuous background client program on a computer, sending periodic time requests to the servers that you configure, obtaining server time stamps and using them to adjust the client’s clock. You should configure several servers for redundancy.

When you configure devices as peers, they listen to each other and move toward a common time. Peers are considered equal with each other as opposed to servers, which are considered masters. It is important that you configure several peers so that they can decide on the right time.

If an NTP server or peer is not available, you can turn on the NTP reference clock to have your server configured as a source of time information. In this mode, Nokia recommends that you keep the stratum value at its default (1). The stratum value tells how far away the NTP reference clock is from a valid time source.

The time server begins to provide time information 5 minutes after it is configured.

**Note**

IPSO does not implement SNTP.

**Configuring NTP**

To set the time manually, see “*Setting the System Time.*”

**To configure NTP**

1. Click Config on the home page.
2. Click the NTP link in the Router Services section.
3. Click Yes in the Enable NTP field and click Apply. The NTP configuration page will display.

4. Enter the new server IP address in the Add New Server Address edit box and click Apply. The IP address for the new NTP server appears in the NTP Servers field. By default, this new server is enabled, v3 is selected, and Prefer Yes is selected. As you add other servers, you might prefer them over the initial server you configured.

**Note**
Nokia recommends that you use the default setting of v3.

5. To add another new server, repeat step 4 and click Apply.

6. (Optional) Enable the NTP reference clock by clicking Yes in the NTP Master field and click Apply.

The Stratum edit box and Clock source drop-down list appear. By default, the Stratum value is 1, and the Clock source is set to Local Clock. Nokia recommends that you keep these defaults.

7. To configure a new peer, enter the new peer IP address in the Add New Peer: Address: edit box.

Click Apply.

The new peer IP address appears in the NTP Peers field. By default, this new peer is enabled, v3 is selected, and Prefer Yes is selected. As you add other peers, you might prefer them over the initial peer you configured.

**Note**
Nokia recommends that you use the default setting of v3.

8. To add another new peer, repeat step 8 and click Apply.

The new peer IP address appears in the NTP Peers field. By default, this new peer is enabled, v3 is selected, and Prefer No is selected. To prefer this peer over other peers, click Prefer Yes.

9. (Optional) Enable the NTP reference clock by clicking Yes in the NTP Master field.

Click Apply.

**Note**
Only enable the NTP reference clock if you cannot reach an NTP server.

The Stratum edit box and Clock source drop-down list appear. By default, the Stratum value is 1, and the Clock source is set to Local Clock. Nokia recommends that you keep these defaults.
10. Click Save to make your changes permanent.
7 Configuring Security and Access

Chapter Contents

- Password Procedures
  - Changing Passwords
  - Adding Users
  - Removing a User
  - Configuring S/Key
  - Using S/Key
  - Disabling S/Key
  - Changing the S/Key Password
- Group Procedures
  - Managing Groups
- Network Access Procedures
  - Network Voyager Web Access
  - FTP Access
  - Telnet Access
  - CLI Over HTTP
  - CLI Over HTTPs
  - Admin Network Login
  - COM2 Login
  - COM3 Login
  - Configuring a Modem on COM2
  - Configuring a Modem on COM3
  - Configuring a Modem on COM4 (PCMCIA)
- Services
  - Echo Service
  - Discard Service
  - Chargen Service
  - Daytime Service
  - Time Service
- Secure Shell (SSH)
  - Secure Shell Description
  - Configuring SSH
  - Configuring Advanced Secure Shell Server Options
  - Configuring Secure Shell Authorized Keys
  - Changing Secure Shell Key Pairs
  - Managing User RSA and DSA Identities
  - Tunneling HTTP Over SSH
- Secure Socket Layer (SSL)
  - SSL Description
  - Enabling SSL Network Voyager Web Access
  - Generating a Certificate and Private Key
  - Installing a Certificate and Private Key
  - Troubleshooting SSL Configuration
- Authentication, Authorization, and Accounting (AAA)
  - Creating an AAA Configuration
  - Configuring RADIUS
  - Configuring TACACS+
  - Deleting an AAA Authentication Server Configuration
  - Changing an AAA Configuration
  - Deleting an AAA Configuration
- Cryptographic Acceleration
  - Encryption Acceleration Description
  - Enabling Encryption Accelerator Cards
  - Monitoring Cryptographic Acceleration
- IPSec Tunnels
  - Introduction
  - Using PKI
  - IPSec Implementation in IPSO
  - IPSec Parameters
  - Creating an IPSec Policy
  - Creating an IPSec Tunnel Rule
  - Transport Rule
  - IPSec Tunnel Rule Example
  - IPSec Transport Rule Example
  - Changing the Local/Remote Address or Local/Remote Endpoint of an IPSec Tunnel
  - Removing an IPSec Tunnel
- Miscellaneous Security Settings
Password Procedures

Changing Passwords

To change passwords

1. Click Config on the home page.
2. Click the Users link in the Security and Access Configuration section.
3. Enter the current user password in the Old password text box.
4. Enter a new user password in the New password text box.
5. Enter the new user password again in the New password (verify) text box.
6. Click Apply.

To make your changes permanent, click Save.

Adding Users

To add users

1. Click Config on the home page.
2. Click the Users link in the Security and Access Configuration section.
3. In the Add new user: Username: text box, enter the name (eight or fewer characters) of the new user.
4. In the Add new user: Uid text box, enter the numeric user ID.
An admin account allows read/write access privileges. To create a new user with admin account privileges, enter 0 for the Uid. The monitor account allows read-only access. To create a new user with monitor account privileges, enter 10 for the Uid.

5. In the Add new user: Home directory: text box, enter the full UNIX path name of a directory where the user will log in. For example, if the name of the new user is tester, you could enter the path to /var/tester for the home directory.

6. Click Apply.
   The new user information appears on the page.

7. Enter a password in the New password text box. Leave the Old password text box empty.

8. Enter the same new password in the New password (verify) text box.

9. Click Apply.

10. You can modify Gid and Shell.

11. To make your changes permanent, click Save.

Removing a User

To remove a user

1. Click Config on the home page.

2. Click the Users link in the Security and Access Configuration section.

3. In the Add new user field, click Off next to the user name to remove.

4. Click Apply.

Note
When you remove, that user can no longer log in even though the user’s home directory remains on the system. To remove the user’s directory, you must use the command line.

5. To make your changes permanent, click Save.

Configuring S/Key

The following procedure describes how to enable S/Key-based authentication for admin and monitor accounts. S/Key is a one-time password (OTP) system that you can enable to protect the password of admin or monitor accounts when users connect through Telnet or FTP.

1. Click Config on the home page.

2. Click the Users link in the Security and Access Configuration section.

3. To enable the Admin S/Key, click either Allowed or Required in the S/Key Password field.

4. Click Apply.

5. Enter the current standard password in the Current Standard password text box.

6. Pick a secret password for S/Key that is between four and eight alphanumeric characters long, and enter it in the S/Key Secret Password text box.

7. Enter the S/Key secret password again in the S/Key Secret Password (verify) text box; then click Apply.

   The sequence number and the seed appear. The sequence number begins at 99 and goes backward after every subsequent S/Key password is generated. The seed is associated with the S/Key secret password.

8. Click Save to make your changes permanent.

Using S/Key

**Note**
You need an S/Key calculator on your platform to generate the S/Key one-time password (OTP). Many UNIX-derived and UNIX-like systems include the S/Key calculator command key. Many GUI calculators include support for MD4 (S/Key) algorithms and MD5 (OPIE) algorithms. Be sure to configure such calculators to use MD4 algorithms.

1. Log in to the firewall with a Telnet or FTP client.
2. At the prompt, enter either admin or monitor as a user name.
3. The server returns an S/Key challenge, which is comprised of the S/key sequence number and seed, for example, 95 ma74213.

   The server also returns a prompt for a password.

4. Copy the S/Key sequence number and seed into the S/Key calculator on your platform.
5. Copy the S/Key challenge into the S/Key calculator on your local platform.
6. Enter the S/Key Secret Password.

   The calculator returns the OTP for this session.

**Note**
For more help on how to enter S/Key information, see your S/Key calculator documentation.

7. Copy the OTP into the Telnet or FTP session.
Note
The OTP is typically a string, or strings, that contain a series of words, for example, NASH TINE LISA HEY WORE DISC. You must enter all the words in the valid string at the password prompt.

Disabling S/Key

1. To disable S/Key, click Disabled in the S/Key Password field.
2. Click Apply.
   The sequence number and seed disappear.
3. Click Save to make your changes permanent.

Changing the S/Key Password

1. Enter the current standard password in the Current Standard Password text box.
2. Enter a different S/Key secret password in the S/Key Secret Password text box.
3. Enter the same password you entered in step 2 in the S/Key Secret Password (verify) text box.
4. Click Apply.
5. To enable the Monitor S/Key, click either Allowed or Required in the S/Key Password field.
6. Click Apply.
7. Click Save to make your changes permanent.

Group Procedures

Managing Groups

To managing a group:
1. Click Config on the home page.
2. Click the Groups link in the Security and Access Configuration section.
3. In the Add new group: Group name text box, enter the name (eight or fewer characters) of the new group.
4. In the Gid field, enter a numeric ID.
Note
The number must be unique. Suggested values are between 100 and 65000.

5. Click Apply.
   The new group information appears on the page.
6. To add a new member to a group, enter the user name in the Add new member text box.
7. Click Apply.
8. To delete a member from the group, select the user name from the Delete member text box.
9. Click Apply.
10. Click Save to make your changes permanent.

Network Access Procedures

Network Voyager Web Access

To enable Web access by using Voyager
1. Click Config on the home page.
2. Click the Voyager Web Access link in the Security and Access Configuration section.
   yes in the Allow voyager web access field is the default.

Note
If you click No, you have to use the Network Voyager command line to access your IP security platform (Nokia Platform).

3. Enter the number of the port to activate in the Voyager port number text box.
4. Click Apply.
5. Click Save to make your changes permanent.

FTP Access

To enable FTP access
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Allow FTP Access field.
4. Click Apply.
5. Enter the number of the port where you want to receive FTP requests in the FTP port number text box (defaults to port 21).
6. Click Save to make your changes permanent.

**Telnet Access**

**To enable Telnet access**

1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Allow telnet access field.
4. Click Apply.
5. Click Save to make your changes permanent.

**CLI Over HTTP**

**To enable access to the command-line interface over HTTP**

1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Allow CLI over HTTP field.
4. Click Apply.
5. Click Save to make your changes permanent.

**CLI Over HTTPs**

To enable access to the command-line interface over HTTPs:

1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Allow CLI over HTTPs field.
4. Click Apply.
5. Click Save to make your changes permanent.
Admin Network Login

To enable network login access using the admin account
1. Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click Yes in the Allow admin network login field.
4. Click Apply.
5. Click Save to make your changes permanent.

COM2 Login

To login from the COM2 port
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Allow com2 login field.
4. Click Apply.
5. Click Save to make your changes permanent.

COM3 Login

To login from the COM3 port:
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Allow com3 login field.
4. Click Apply.
5. Click Save to make your changes permanent.

Configuring a Modem on COM2

To configure a modem on COM2
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Allow com2 login field; then click Apply.
4. Click the Modem Configuration link next to yes in the Allow com2 login field.
   This action takes you to the Modem Configuration page.
5. Click ON in the Modem on COM2 field to turn on the modem.
   The modem is configured to answer any incoming calls.
6. Enter a value, in minutes, in the Inactivity Timeout field.
   This value is the length of time, in minutes, that a connected call on the modem can remain
   inactive (that is, no traffic is sent or received) before the call is disconnected. Setting the
   value to 0 disables the timer (that is, the call will never be disconnected due to inactivity).
7. Enter a value, in minutes, in the Status Poll Interval field to configure the Modem Status
   monitor.
   This value is the length of time, in minutes, between modem-line status tests. Once every
   interval, the system tests that the modem is present and online. If the modem is not detected
   or is offline, a message is logged using syslog. Setting the value to 0 disables the Modem
   Status monitor.
8. Click yes in the Enable Dialback login field to enable modem dialback.
   When set to Yes, an incoming call on the modem is dropped after you log in, and the modem
   automatically calls the Dialback Number and connects a login process to the line.
9. If you enabled modem dialback, enter a value in the Dialback Number field.
   The dialback feature uses this number to back an authenticated user (for example, 408 555
   0093). If dialback is disabled, ignore this value.
10. Click Apply.
11. Click Save to make your changes permanent.

**Configuring a Modem on COM3**

To configure a modem on COM3

1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration
   section.
3. Click yes in the Allow com3 login field; then click Apply.
4. Click the Modem Configuration link next to yes in the Allow com3 login field.
   This action takes you to the Modem Configuration page.
5. Click ON in the Modem on COM3 field to turn on the modem.
   The modem is configured to answer any incoming calls.
6. Enter a value, in minutes, in the Inactivity Timeout field.
This value is the length of time, in minutes, that a connected call on the modem can remain inactive (that is, no traffic is sent or received) before the call is disconnected. Setting the value to 0 disables the timer (that is, the call will never be disconnected due to inactivity).

7. Enter a value, in minutes, in the Status Poll Interval field to configure the Modem Status monitor.

This value is the length of time, in minutes, between modem line status tests. Once every interval, the system tests that the modem is present and online. If the modem is not detected or is offline, a message is logged using syslog. Setting the value to 0 disables the Modem Status monitor.

8. Click yes in the Enable Dialback login field to enable modem dialback.

When set to Yes, an incoming call on the modem is dropped after you log in, and the modem automatically calls the Dialback Number and connects a login process to the line.

9. If you enabled modem dialback, enter a value in the Dialback Number field.

The dialback feature uses this number to call back an authenticated user (for example, 408 555 2186). If dialback is disabled, ignore this value.

10. Click Apply.

11. Click Save to make your changes permanent.

### Configuring a Modem on COM4 (PCMCIA)

**Note**
When you dial into a Nokia appliance that has an Ositech Five of Clubs III modem installed, be sure to set the connection rate to 9600 BPS. If you do not, the text you receive from the appliance will be unreadable.

**To configure a modem on COM4**

1. Click Config on the home page.

2. Click the Network Access and Services link in the Security and Access Configuration section.

3. To enable the PCMCIA modem card, click Yes next to the Allow com4 (PCMCIA) login field.

4. Click Apply.

5. Click the Modem Configuration link for the modem card.

The modem status field should read Modem Detected.

6. In the Inactiveness Timeout text box, enter the value, in minutes, that a connected call on the modem can remain inactive.

The default is 0, which disables the timer and means that the call will never be disconnected due to inactivity.
7. (Optional) To enable the Dialback feature, click Yes in the Enable Dialback field. When you enable this feature, an incoming call to the modem is dropped after the user logs in, and the modem automatically calls the dialback number and connects a login process to the line.

8. (Optional) In the Dialback Number text box, enter the dialback number that the Dialback feature uses when calling back an authenticated user.

9. In the Status Poll Interval text box, enter the time, in minutes, between the modem line status tests.

   If the modem is not detected or is offline, a message appears in syslog. The default is 0, which disables the modem line status test.

10. Enter the correct number in Country Code text box to select your country. To determine the correct number, see the two tables below. The first table refers to the Ositech Five of Clubs PCMCIA modem card, and the second table refers to the Ositech Five of Clubs II and III PCMCIA modem cards.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22 USA</td>
<td>17 Greece</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 Canada</td>
<td>99 Iceland</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Australia</td>
<td>7 Ireland</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Belgium</td>
<td>8 Italy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Denmark</td>
<td>9 Luxembourg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Finland</td>
<td>10 The Netherlands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 France</td>
<td>11 Norway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Germany</td>
<td>12 Portugal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Spain</td>
<td>14 Sweden</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25 Switzerland</td>
<td>16 United Kingdom</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B5 USA</td>
<td>59 Italy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 Canada</td>
<td>69 Luxembourg</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11. Click Apply
12. Click Save to make your changes permanent.

Services

Echo Service

Echo service sends any data it receives back to the originating source.

To enable echo service
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Enable ‘Echo’ service field.
4. Click Apply.
5. Click Save to make your changes permanent.

Discard Service

Discard service discards any data it receives.
To enable discard service
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Enable ‘discard’ service field.
4. Click Apply.
5. Click Save to make your changes permanent.

Chargen Service
Chargen service sends data without regard to input. The data sent is a repeating sequence of printable characters.

To enable chargen service
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Enable ‘chargen’ service field.
4. Click Apply.
5. Click Save to make your changes permanent.

Daytime Service
Daytime service sends the current date and time as a character string without regard to the input.

To enable daytime service
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Enable ‘daytime’ service field.
4. Click Apply.
5. Click Save to make your changes permanent.

Time Service
The time service sends back to the originating source a 32-bit number, which is the time in seconds since midnight on January 1, 1900.
To enable time service
1. Click Config on the home page.
2. Click the Network Access and Services link in the Security and Access Configuration section.
3. Click yes in the Enable ‘time’ service field.
4. Click Apply.
5. Click Save to make your changes permanent.

Secure Shell (SSH)

Secure Shell Description

Secure Shell (SSH) is a protocol that allows you to securely log in to another computer over a network, execute commands on a remote platform, and move files from one platform to another platform. You can use SSH instead of utilities such as Telnet or rlogin to securely manage your platform. You can also tunnel HTTP over SSH to use Network Voyager to securely manage your platform.

The Nokia SSH implementation supports both SSHv1 and SSHv2. Some of the differences between SSHv1 and SSHv2 include what part of the packet the protocol encrypts and how each protocol authenticates: SSHv1 authenticates with server and host keys, while SSHv2 authenticates by using only host keys. Even though SSHv1 uses server and host-key authentication, SSHv2 is a more secure, faster, and more portable protocol. In some cases, SSHv1 might be more suitable because of your client software or your need to use the authentication modes of the protocol.

The SSH protocol provides you with session protection from the following security threats:
- DNS spoofing
- Interception of passwords
- IP spoofing
- IP source routing
- Person-in-the-middle attacks (SSHv2 only)

Configuring SSH

The following procedure allows you to configure the Secure Shell (SSH) feature. To use SSH, enable it in the Enable/Disable SSH Service field. You do not need to configure other options or advanced options.

To enable SSH and configure SSH options:
1. Click Config on the home page.
2. Click the Secure Shell (SSH) link in the Security and Access Configuration section.
3. Click Yes in the Enable/Disable SSH Service field.

**Note**
The first time you enable SSH it generates both RSA v1, RSA v2, and DSA host keys. This process will take a few minutes.

4. Click Apply.

5. (Optional) In the Configure Server Access Control table, click the choice in the Permit admin user to login field.
   
The default is Yes, which allows the user to log in as admin by using SSH.

6. Click Apply.

7. (Optional) In the Configure Server Authentication of Users table, click Yes for each type of authentication to be used.

**Note**
You can authenticate SSH connections by using public keys (for RSA and DSA SSHv2), standard user and password information, rhosts files, and RSA keys (for SSHv1). You can permit any combination of these methods. In all cases the default is Yes, except for rhost and rhost with RSA authentication. The rhost authentication is insecure and Nokia does not recommend using it.

8. Click Apply.

9. (Optional) In the Configure Server Protocol Details field, click the version of SSH to be used. The default is both 1 and 2.

10. (Optional) To generate an RSA v1 host key (use with SSHv1), select the key size, listed in bits, from the Generate New RSA v1 Host Key drop-down list.

11. Click Apply.

12. (Optional) To generate an RSA v2 host key (use with SSHv2), select the key size, listed in bits, from the Generate New RSA v2 Host Key drop-down list.

13. Click Apply.

14. (Optional) To generate a DSA host key (use with SSHv2), select the key size, listed in bits, from the Generate New DSA Host Key drop-down list.
    
The recommend value is 1024 bits.

15. Click Apply.

16. Click Save to make your changes permanent.
**Configuring Advanced Secure Shell Server Options**

The advanced SSH Server Configuration page allows you to configure the Secure Shell (SSH) daemon settings, access methods, access filters, and logging behavior. These settings strictly control the SSH connections that the system accepts. These are optional settings. To use SSH, enable it in the Enable/Disable SSH Service text field. You do not need to configure other options or advanced options.

**To configuring advanced options**

1. Click Config on the home page.
2. Click the Secure Shell (SSH) link in the Security and Access Configuration section.
3. Click the Go to the advanced server options page link.
4. Click Yes in the Enable/Disable SSH Service field.

**Note**

The first time you enable SSH it generates both RSA and DSA host keys. This process takes a few minutes.

5. Click Apply.
6. (Optional) In the Configure Server Access Control table, enter the group and user names in the appropriate text boxes.

**Note**

If you specify users or groups, only those users and groups are allowed or forbidden. Group settings only apply to a user’s primary group—the Gid setting in the Voyager Password page. For more information on how to configure users and groups, see Adding Users and Managing Groups.

**Note**

You can use wild card characters when you specify multiple group or user names separated by spaces.

7. Click Apply.
8. Click the option to use in the Permit admin user to log in field.
   The default is Yes, which allows the user to log in as admin using SSH.
9. Click Apply
10. In the Configure Server Authentication of Users table, click Yes for each authentication option to be used.

**Note**
You can authenticate SSH connections by using public keys (for RSA and DSA SSHv2), standard user and password information, rhosts files, RSA keys (for SSHv1), or any combination of these methods. In all cases the default is Yes, except for rhost and rhost with RSA authentication. The rhost utility is insecure and Nokia does not recommend using it.

11. Click Apply
12. (Optional) In the Configure User Login Environment table, click Yes for each desired action.

   The default is Yes in the Print message of the day on login field. The default is No in the Use login(1) program for interactive logins field.

13. Click Apply
14. (Optional) In the Configure Server Protocol Details table, select the method of encryption (SSHv2), enter appropriate values in the text boxes, and click the choice to use in the Send keepalives to the other side and Protocol version(s) fields.

   The default settings are Yes and Both 1 and 2 in these fields respectively.

**Note**
The default setting in the Cipher to use field is all ciphers on. If you deselect all choices in this field, the setting reverts to the default setting.

15. Click Apply.
16. (Optional) In the *Configure Service Details* field, click the choices and enter appropriate values in the text boxes.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ALLOW REMOTE CONNECTIONS TO FORWARD PORTS</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>IGNORE USER’S OWN KNOWN_HOSTS FILE</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>IGNORE .RHOSTS AND .SHOSTS FILES</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>TIME (SECONDS) BEFORE REGENERATING SERVER KEY</strong></td>
<td>3600 seconds</td>
</tr>
<tr>
<td><strong>LOGIN GRACE TIME (SEC)</strong></td>
<td>600 seconds</td>
</tr>
<tr>
<td><strong>MAX UNAUTHORIZED CONNECTIONS</strong></td>
<td>10</td>
</tr>
</tbody>
</table>
17. Click Apply.

18. (Optional) In the Configure Server Implementation Details table, select the appropriate setting from the drop-down list, and click the choice.

   The default setting in the Message logging level field is INFO, and the default setting in the Strict checking of file modes field is Yes.

19. Click Apply.

20. Click Save to make your changes permanent.

### Configuring Secure Shell Authorized Keys

The Secure Shell (SSH) Authorized Keys feature lets you create clients that can access accounts on your system without using a password.

To configure an authorized key, you need to have information about the clients’ keys. For SSHv1 implementation, you need to enter the RSA key and such information as key size, exponent, and modulus. One commonly used file name on your SSH client that is used for storing this information is `identity.pub`. For SSHv2 implementations, you need to enter the RSA/DSA key. One commonly used file name on your SSH client that is used for storing this information is `id_dsa.pub`. For more information, consult your SSH client software documentation.

**To configure authorized keys**

1. Click Config on the home page.

2. Click the Secure Shell (SSH) link in the Security and Access Configuration section.

3. Click the Go to the authorized keys page link.

**Note**

If you previously configured authorized keys for user accounts, the information appears in the View/Delete Per-User Authorized Keys table. To delete the authorized key for each user click the Delete check box. Click Apply and then Save to make your changes permanent.

4. Select the user name from the Username drop-down list.

5. If you are adding an RSA authorized key to use in SSHv1, enter the key size, exponent, modulus, and an optional comment in the Add a New Authorized Key (RSA, for protocol version 1) table.

   Or

   If you are adding a RSA authorized key to use in SSHv2, enter the RSA key, in either OpenSSH format or SSHv2 format, depending on your client, and optional comment in the (RSA, for protocol version 2) table.

   Or

   or
If you are adding a DSA authorized key to use in SSHv2, enter the DSA key, in either OpenSSH format or SSHv2 format, depending on your client, and optional comment in the Add a New Authorized Key (DSA, for protocol version 2) table.

6. Click Apply.
7. Click Save to make your changes permanent.

Changing Secure Shell Key Pairs

The following procedure describes how to generate new RSA and DSA keys. When you generate new keys, you might need to change configurations of each client, or the client might return errors. For more information, see your SSH client documentation.

To configure key pairs
1. Click Config on the home page.
2. Click the Secure Shell (SSH) link in the Security and Access Configuration section.
3. Click the Go to the key pairs page link.
4. (Optional) To generate an RSA host key (to use with SSHv1), select the key size, listed in bits, from the Generate New RSA v1 Host Key drop-down list.

Note
The most secure value is 1024 bits. Values over 1024 bits cause problems for some clients, including those based on RSAREF.

5. Click Apply.
6. (Optional) To generate an RSA host key (to use with SSHv2), select the key size, listed in bits, from the Generate New RSA v2 Host Key drop-down list.
7. Click Apply.
8. (Optional) To generate a DSA host key (to use with SSHv2), select the key size, listed in bits, from the Generate New DSA Host Key drop-down list.
   The recommend value is 1024 bits.

9. Click Apply.
10. Click Save to make your changes permanent.

Note
Re-creating keys might cause problems with some clients, because the server use a key different from the one it used before. You can reconfigure the client to accept the new key.

Managing User RSA and DSA Identities

This procedure describes how to manage the public and private-key pairs of given users on your application platform.

To manage user identities
1. Click Config on the home page.
2. Click the Secure Shell link in the Security and Access Configuration section.
3. Click the Go to key pairs page link.
4. Click the View/Create Identity Keys for User ‘user name’ link for the appropriate user.
5. (Optional) To create an RSA identity to use with SSHv1, select the key length in the Generate key of size field in the Generate New RSA v1 Identity for user name.
6. Enter the passphrase in the Enter password field.
7. Enter the password again to verify it.
8. (Optional) To create an RSA identity to use with SSHv2, select the key length in the Generate key of size field in the Generate New RSA v2 Identity for user name.
9. Enter the passphrase in the Enter password field.
10. Enter the password again to verify it.
11. (Optional) To create a DSA identity to use with SSHv2, select the key length in the Generate key of size field in the Generate New DSA Identity for user name.
12. Enter the passphrase in the Enter password field.
13. Enter the password again to verify it.
14. Click Apply.
15. Click Save to make your changes permanent.

Tunneling HTTP Over SSH

To tunnel HTTP over SSH
1. Generate a key.
2. Put authorized public keys on the system.
3. Log in and redirect a port on your platform to the remote platform.

From a UNIX terminal do the following:

Use the -L option to redirect a port to port 80 on the remote platform. The following example redirects port 8000.

At the shell prompt, type:

```bash
ssh -l admin Nokia Platform.corp.com -L 8000:127.0.0.1:80
```
From a Windows terminal do the following:

Use the client to redirect port 8000.

1. When you open a connection, click Properties.
2. Select the Forward tab.
3. Enter a new local port-forwarding entry by clicking on new.
   The source port should be 8000. The destination host should be 127.0.0.1, and the destination port should be 80. For security reasons, check the allow local connections only box.
4. Click OK twice to return to the connection dialog box.
5. Press OK to connect to the remote host.

To redirect a port permanently, choose Save As in the File menu and save the configuration to a file. This allows you to redirect the same ports every time you create an HTTP tunnel over SSH.

Secure Socket Layer (SSL)

SSL Description

The secure socket layer (SSL) protocol gives you a secure way to connect to network appliances by using IPSO. SSL protocol is the industry standard for secure Web connections because the protocol uses a pair of asymmetric keys to establish Web sessions. Each pair of keys consists of a public key and a private key. Keeping the private key secret is critical to your security. When you use SSL, you reduce the risk of unauthorized parties tampering with your Network Voyager internet sessions.

Network Voyager lets you do the following:

- Enable SSL
- Generate certificate and private-key requests
- Install certificates and private keys

Enabling SSL Network Voyager Web Access

To enable SSL Web access and encryption by Voyager

1. Click Config on the home page.
2. Click the Voyager Web Access link in the Security and Access Configuration section.
3. Click yes in the Allow voyager web access field.
   The default is yes.
4. Enter the number of the port to activate in the Voyager SSL port number text box.
The default is port 443.

5. Click encryption-level appropriate for your security needs, for example, 40-bit key or stronger.
   The default is none, which disables SSL.

   **Note**
   When you enter the encryption level, you are entering the minimum level of encryption you require. You get stronger encryption by default if your Web browser supports it.

6. Click Apply.

   **Note**
   You must replace http://... with https://... in your browser window before you click Save because you are enabling a secured connection.

7. Click Save to make your changes permanent.

   **Note**
   IPSO includes a default sample certificate and private key in the files `/var/etc/voyager_ssl_server.crt` and `/var/etc/voyager_ssl_server.key` respectively. The certificate and private key are for testing purposes only and do not provide a secure SSL connection. You must generate a certificate, and the private key associated with the certificate, to create a secure connection by using SSL. See "Generating a Certificate and Private Key".

---

**Generating a Certificate and Private Key**

This procedure describes how to generate a certificate and its associated private key using Voyager. To better ensure your security, you should generate the certificate and private key over a trusted connection.

**To generate a certificate and private key**

1. Click Config on the home page.
2. Click the Certificate Tool link in the Security and Access Configuration section.
3. Click the Private Key Size appropriate for your security needs.
   The larger the bit size, the more secure the private key. The default is 1024 bits.
4. (Optional) Enter a passphrase in the Passphrase text box. The passphrase must be at least four characters long.
5. (Optional) Enter the passphrase in the Enter Passphrase Again text box to confirm the phrase.
Note
If you use a passphrase, you have to enter the phrase later when you install your new key.

6. Enter the two-letter code of the country in which you are located in the Country Name text box.

7. (Optional) Enter the name of your city in the Locality Name text box.

8. Enter the name of your state in the State or Province Name text box.

9. Enter the name of your organization in the Organization Name text box.
   If you are requesting a certificate from a certificate authority, the certificate authority might require the official, legal name of your organization.

10. (Optional) Enter the name of your department in the Organizational Unit Name text box.

11. Enter the fully qualified domain name of your host in the Common Name text box, for example www.ship.wwidgets.dom.

12. (Optional) Enter your email address in the Email Address text box.

13. Click Generate an X.509 certificate signing request (CSR) if you are requesting a certificate from a certification authority.
   or
   Click Generate a self-signed X.509 certificate to create a certificate which you can use immediately, but that is not validated by a certification authority.

14. Click Generate.
   If you generated a certificate signing request, a screen appears that contains a certificate request—New X.509 certificate signing request—and its associated private key—New private key.
   Send the New X.509 certificate signing request to your certification authority. Be sure to include the lines -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----.
   Store the New private key securely. You need to install the private key and the certificate you will receive from your certification authority.
   (See “Installing a Certificate and Private Key”.)
   If you generated a self-signed certificate, a screen appears containing the certificate—New X.509 certificate—and its associated private key—New private key.
   You must perform a cut-and-paste operation to move the certificate and the private key to the Voyager SSL Certificate page. (See “Installing a Certificate and Private Key”.)
Installing a Certificate and Private Key

To install a certificate and private key

1. Click Config on the home page.
2. Click the Voyager Web Access link in the Security and Access Configuration section.
3. Click the Configure SSL Certificate link.
4. Open the files that contain your certificate and private key.
5. Perform a cut-and-paste operation on your certificate to move it to the New server certificate text box in the Voyager SSL Certificate page.
   Be sure to include the lines -----BEGIN CERTIFICATE ----- and -----END CERTIFICATE ------.
6. Perform a cut-and-paste operation on your private key to move it to the Associated private key text box in the Voyager SSL Certificate page.
   Be sure to include the lines -----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----.
7. (Optional) If you entered a passphrase when you generated the certificate and private key, you must enter the passphrase in the Passphrase text box.
8. Click Apply.
9. Click Save to make your changes permanent.

Troubleshooting SSL Configuration

You might have problems accessing Voyager if SSL is not configured correctly. The following steps and suggestions can help you to recover Network Voyager:

1. Check that you are using the correct URL.
   Once you enabled SSL, you must use https rather than http when you connect through your Web browser.
2. Use the Network Voyager command line utility to turn off SSL and restart Network Voyager.
   To access this utility, log on to your network application platform (Nokia Platform) through your console terminal or the ssh client. Once you are logged on, enter the command:
   ```
   voyager -e 0 80
   ```
3. Check that you are using the correct PEM-encoded certificate and private key, and that they are installed properly with the dashed begin and end lines. (See “Installing a Certificate and Private Key”.) To view the certificate and private key, see /var/etc/voyager_ssl_server.crt and /var/etc/voyager_ssl_server.key respectively.
   To change or reenter the certificate and private key, first use step 2 to turn off SSL and restart Voyager. Then use Voyager to add the certificate and private key. (See “Installing a Certificate and Private Key”.)
4. Check the HTTP daemon error message log.
You can find the messages in the following logs:
/var/log/httpd_error_log and /var/log/ssl_engine_log. The messages might help you troubleshoot further and they might contain important information for customer support, should you contact them.

Authentication, Authorization, and Accounting (AAA)

Creating an AAA Configuration

Use this procedure to create an AAA configuration for a new service. A service is a name that is used by an application uses to invoking the Pluggable Authentication Module (PAM) Application Programming Interface (API) that is part of the AAA. The PAM mechanism provides for authentication, account management and session management algorithms that are contained in shared modules. The PAM infrastructure loads these modules when the application needs to access the algorithms.

To create an AAA configuration:
1. Click Config on the home page.
2. Click the AAA link in the Security and Access Configuration.
3. Create an AAA Configuration entry using one or more of the following elements:
   a. “Creating a Service Module Entry”
   b. “Creating a Service Profile”
   c. “Creating an Authentication Profile”
   d. “Creating an Accounting Profile”
   e. “Creating a Session Profile”

Which element to create depends on the needs of the service that uses AAA; at a minimum, a. and b. and one of c., d. or e. is needed before Apply is selected. If any items are to be configured individually, configure them in the following order:
   - e
   - d or c
   - b
   - a

The steps for configuring each of these elements is described in the following subsections.

**Note**
You can add an Authorization, Accounting, or Session profile without using any of them in a Service Profile.

4. Click Apply.
5. Click Save to make your changes permanent.

**Creating a Service Module Entry**

**To create a service module entry**

1. Enter the name of the service in the New Service text box under the Service Module Configuration table.

2. In the Profile text box under the Service Module Configuration table, enter either an existing Profile Name from the Service Profile table, if the requirements of the service match one of the existing profiles, or a unique profile name, if the requirements of the service do not match any of the existing profiles.

**Creating a Service Profile**

**To create a service profile**

1. Enter the name of the profile in the Service Profile text box under the Service Profile table; make sure that the name does not match any of the Profile Names in the Service Profile table.

2. In the Auth. Profile text box under the Service Profile table, enter either an existing item from the Auth. Profile table, if the service requirements match one of the existing authentication profiles, or a unique authentication profile name, if the service requirements do not match any of the existing authentication profiles. Leave the Auth. Profile text box blank if the service requirements do not include authentication services.

3. In the Acct. Profile text box under the Service Profile table, enter either an existing item from the Acct. Profile table, if the service requirements match one of the existing accounting profiles, or a unique accounting profile name, if the service requirements do not match any of the existing accounting profiles.

   Leave the Acct. Profile text box blank if the service requirements do not include accounting services.

4. In the Session Profile text box under the Service Profile table, enter either an existing item from the Session Profile table, if the service requirements match one of the existing session profiles.

   Leave the Session Profile text box blank if the service requirements do not include session services.

**Creating an Authentication Profile**

**To create an authentication profile**

1. Enter the name of the authentication profile in the New Auth. Profile text box under the Auth. Profile table; make sure that the name does not match any of the Names in the Auth. Profile table.

2. Select the item in the Type drop-down list that matches the service requirements.
For a description of the authentication algorithms that the list items represent, see “Authentication Profile Types.”

3. Select the item in the Control drop-down list that matches the service requirements. Values other than required are effective only when the service requires more than one Auth. Profile. For a description of the effect on result disposition and subsequent algorithm invocation that the list items represent, see “Profile Controls.”

Note
The Server/File field is unused.

Authentication Profile Types

The following table describes the authentication algorithms that the values represent in the Type drop-down lists under Auth. Profile.

Note
Modules in the MODULE column reside in the /usr/lib directory.

<table>
<thead>
<tr>
<th>Type</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>pam_httpd_auth.so.1.0</td>
<td>Uses the local password database to authenticate the user, using a special algorithm specifically for the Apache Web server. When the user requests a Network Voyager page, this module is called to authenticate the user, which, in turn, verifies the user name and password supplied during the Network Voyager login against the information in /etc/master.passwd. Then the module performs Lawful Interception Gateway processing to determine whether the user can access the indicated Network Voyager page.</td>
</tr>
<tr>
<td>PERMIT</td>
<td>pam_permit.so.1.0</td>
<td>Does not do any authentication. It returns a PAM_SUCCESS when invoked.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>pam_radius_auth.so.1.0</td>
<td>A client/server authentication system that supports remote administrator login to Network Voyager and command-line configuration, and selected management functions.</td>
</tr>
<tr>
<td>ROOTOK</td>
<td>pam_rootok_auth.so.1.0</td>
<td>Performs one task: If the user id is 0, it returns PAM_SUCCESS with the sufficient control flag. It can be used to allow password-free access to some services for root.</td>
</tr>
<tr>
<td>SECURETTY</td>
<td>pam_securety_auth.so.1.0</td>
<td>Allows root logins only if the user is logging in on a secure TTY.</td>
</tr>
</tbody>
</table>
Creating an Accounting Profile

To create an account profile

1. Enter the name of the accounting profile in the New Acct. Profile text box under the Acct. Profile table; make sure that the name does not match any of the Names in the Acct. Profile table.

2. Select the item in the Type drop-down list that matches the service requirements. (For a description of the accounting algorithms that the list items represent, see “Accounting Profile Types.”)

3. Select the item in the Control drop-down list that matches the service requirements. Values other than required are effective only when the service requires more than one Acct. Profile. (For a description of the effect on result disposition and subsequent algorithm invocation that the list items represent, see “Profile Controls.”)

Note
The Server/File field is unused.
Accounting Profile Types

The following table describes the account management algorithms that are represented by the values in the Type drop-down lists under Acct. Profile.

<table>
<thead>
<tr>
<th>Type</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMIT</td>
<td>pam_permit.so.1.0</td>
<td>Returns PAM_SUCCESS when invoked.</td>
</tr>
<tr>
<td>UNIX</td>
<td>pam_unix_acct.so.1.0</td>
<td>Provides the basic UNIX accounting mechanism by checking if the password is still valid. If the password is expired for some reason, this module logs in appropriate messages. This module also prompts for a password change if the password is going to expire soon.</td>
</tr>
</tbody>
</table>

Note
Modules in the Module column reside in the /usr/lib directory.

Creating a Session Profile

To create a session profile

1. Enter the name of the session profile in the New Sess. Profile text box under the Session Profile table; make sure that the name does not match any of the Names in the Session Profile table.

2. Select the item in the Type drop-down list that matches the service requirements.
   For a description of the session algorithms that the list items represent, see “Session Profile Types.”

3. Select the item in the Control drop-down list that matches the service requirements. Values other than required are effective only when the service requires more than one Session Profile. (For a description of the effect on result disposition and subsequent algorithm invocation that the list items represent, see Profile Controls.)

Session Profile Types

The following table describes the session management algorithms that the values represent in the Type drop-down lists under Session Profile.

<table>
<thead>
<tr>
<th>Type</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMIT</td>
<td>pam_permit.so.1.0</td>
<td>Returns PAM_SUCCESS when invoked.</td>
</tr>
<tr>
<td>UNIX</td>
<td>pam_unix_sess.so.1.0</td>
<td>Logs a message to indicate that a session has started or stopped.</td>
</tr>
</tbody>
</table>
Note
Modules in the Module column reside in the /usr/lib directory.

Profile Controls

Control values determine how the results of multiple authentication, accounting, or session algorithms are handled and when additional algorithms in a list are invoked. Specifies lists of algorithms by defining multiple entries under the Auth. Profile, Acct. Profile, and Session Profile columns of a Service Profile.

The following table describes these effects for algorithm invocation not at the end of the list.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>required</td>
<td>The result is retained and the next algorithm is invoked.</td>
</tr>
<tr>
<td>requisite</td>
<td>A result of failure is reported immediately and no further algorithms are invoked.</td>
</tr>
<tr>
<td>sufficient</td>
<td>If no previous algorithm reported failure, a result of success is reported immediately and no further algorithms are invoked; a result of failure for this algorithm is discarded; if a previous algorithm has reported failure or the result of this algorithm is failure, the next algorithm is invoked.</td>
</tr>
<tr>
<td>optional</td>
<td>A result of failure is ignored and a result of success is retained; the next algorithm is always invoked.</td>
</tr>
</tbody>
</table>

The following table describes these effects for algorithm invocation for a single item or an item at the end of the list.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>required</td>
<td>The result is combined with the results of previous algorithms such that any failure result causes failure to be reported.</td>
</tr>
<tr>
<td>requisite</td>
<td>The result is reported immediately.</td>
</tr>
<tr>
<td>sufficient</td>
<td>The result is reported immediately</td>
</tr>
<tr>
<td>optional</td>
<td>A result of success is reported.</td>
</tr>
</tbody>
</table>

Creating a Service Module Example

In creating a new service, there are unique requirements for authentication, accounting and session management, as follows:
The screens following graphic shows an example of creating a new service.

### Configuring RADIUS

RADIUS, or remote authentication dial-in user service, is a client and server-based authentication software system that supports remote-access applications. This service allows an organization to maintain user profiles in a centralized database that resides on an authentication server that can be shared by multiple remote access servers. A host contacts a RADIUS server, which determines who has access to that service. Beginning with IPSO 3.5, Nokia provides RADIUS client support only.

**To configure RADIUS servers for a single authentication profile**

1. Click Config on the home page.
2. Click the AAA link in the Security and Access Configuration section.
3. In the Auth. Profile section, enter a name for the RADIUS service in the New Auth. Profile text box. For more information, see “Creating an Authentication Profile.”
4. Click the Type drop-down list and select RADIUS as the type of service.
5. Click the Control drop-down list and select required, requisite, sufficient, optional or NOKIA-SERVER-AUTH-SUFFICIENT to determine the level of authentication to apply to a profile. For more information, see “Profile Controls.”

6. Click Apply, and then click Save to make your changes permanent.

The name of the RADIUS authentication profile appears in the Auth. Profile table.

7. You must now configure one or more servers to use in a single authentication profile. In the Auth. Profile table, click the Servers link in the row for the RADIUS authorization profile you configured. This action takes you to the AAA RADIUS Authorization Servers Configuration page.

8. In the RADIUS Servers for Auth. Profile table, enter a unique integer to indicate the priority of the server in the Priority text box. There is no default. You must enter a value in the Priority text box.

Note
You can configure multiple servers for a profile. The priority value determines which server to try first. A smaller number indicates a higher priority.

9. Enter the IP address of the RADIUS server in the Host Address text box.

RADIUS supports only IPv4 addresses.

10. Enter the port number of the UDP port to contact on the server host in the Port # text box.

The default is 1812, which is specified by the RADIUS standard. The range is 1 to 65535.

Caution
Firewall software often blocks traffic on port 1812. To ensure that RADIUS packets are not dropped, make sure that any firewalls between the RADIUS server and IPSO devices are configured to allow traffic on UDP port 1812.

11. Enter the shared secret used to authenticate the authorization profile between the RADIUS server and the local client in the Secret text box.

You must also configure this same value on your RADIUS server. Enter a text string without a backslash.

For more information see RFC 2865. The RFC recommends that the shared secret be at least 16 characters long. Some RADIUS servers limit the shared secret to 15 or 16 characters. Consult the documentation for your RADIUS server.

12. (Optional) Enter the number of seconds to wait for a response after contacting the server in the Timeout text box.

Depending on your client configuration, if the client does not receive a response, it retries the same server or attempts to contact another server. The default value is 3.

13. (Optional) Enter the maximum number of times to attempt to contact the server in the Max Tries text box.
If all the attempts do not make a reliable connection within the timeout period, the client stops trying to contact the RADIUS server. The default is 3.

**Note**  
The maximum tries value includes the first attempt. For example, a value of 3 means the client makes two additional attempts to contact the RADIUS server after the first attempt.

14. Click Apply, and then click Save to make your changes permanent.

**Note**  
Repeat steps 1 through 14 to configure additional RADIUS authentication profiles. You must configure a RADIUS authentication server for each profile even if you associate the new profile with a server that you previously configured for an existing RADIUS authentication profile.

**Note**  
Repeat steps 8 through 14 of this procedure to configure additional AAA RADIUS authentication servers only.

### Configuring TACACS+

The TACACS+ authentication mechanism allows a remote server that is not part of IPSO to authenticate users (checks passwords) on behalf of the IPSO system. TACACS+ encrypts transmitted passwords and other data for security.

In the IPSO 3.6 release, TACACS+ is supported for authentication only, and not for accounting. Challenge-response authentication, such as S/Key, over TACACS+ is not supported by IPSO at this time.

You can configure TACACS+ support separately for various services. The Network Voyager service is one of those for which TACACS+ is supported and is configured as the httpd service. When TACACS+ is configured for use with a service, IPSO contacts the TACACS+ server each time it needs to check a user password. For the Network Voyager service this occurs for each HTTP request (every page view). If the server fails or is unreachable, the password is not recognized and you are not allowed access. In Network Voyager, this denial is effective immediately. Before you change the Network Voyager configuration, confirm any new configuration.

**To configure TACACS+ servers for a single authentication profile**

1. Click Config on the home page.

2. Click the AAA link in the Security and Access Configuration section.

3. In the Auth. Profile section, enter a name for the TACACS+ service in the New Auth. Profile text box.
For more information, see “Creating an Authentication Profile.”

4. Click Type and select TACPLUS from the drop-down list as the type of service.

5. Click Control and select required, requisite, sufficient, optional or NOKIA-SERVER-AUTH-SUFFICIENT from the drop-down list to determine the level of authentication to apply to a profile.

For more information, see “Profile Controls.”

6. Click Apply, and then click Save to make your changes permanent.

The name of the TACACS+ authentication profile appears in the Auth. Profile table.

7. You must now configure one or more servers to use in a single authentication profile. In the Auth. Profile table, click the Servers link in the row for the TACACS+ authorization profile you configured. This action takes you to the AAA TACACS+ Authorization Servers Configuration page.

8. In the TACACS+ Servers for Auth. Profile table, enter a unique integer to indicate the priority of the server in the Priority text box. There is no default. You must enter a value in the Priority text box.

Note
You can configure multiple servers for a profile. The priority value determines which server to try first. A smaller number indicates a higher priority.

9. Enter the IP address of the TACACS+ Server in the Host Address text box. TACACS+ supports only IPv4 addresses.

10. Enter the port number of the TCP port to contact on the server host in the Port # text box.

The default is 49, which is specified by the TACACS+ standard. The range is 1 to 65535.

11. Enter the shared secret used to authenticate the authorization profile between the TACACS+ server and the local client in the Secret text box.

You must also configure this same value on your TACACS+ server. Enter a text string without a backslash.

12. (Optional) Enter the number of seconds to wait for a response after contacting the server in the Timeout text box. Depending on your client configuration, if the client does not receive a response, it retries the same server or attempts to contact another server. The default value is 3.

13. Click Apply, and then click Save to make your changes permanent.

Note
Repeat steps 1 through 13 to configure additional TACACS+ authentication profiles. You must configure a TACACS+ authentication server for each profile even if you associate the new profile with a server that you previously configured for an existing TACACS+ authentication profile.
Deleting an AAA Authentication Server Configuration

To delete an authentication server
1. Click Config on the home page.
2. Click the AAA link in the Security and Access Configuration section.
3. In the Auth. Profile table, click the Servers link in the row for the RADIUS or TACACS+ authentication profile.
   This action takes you to the page for AAA RADIUS or TACACS+ Authentication Servers Configuration.
4. In the RADIUS or TACACS+ Servers For Auth. Profile table, check the Delete check box next to the row for the RADIUS or TACACS+ server to disable.

Note
You must have at least one RADIUS or TACACS+ server configured to maintain RADIUS or TACACS+ service.

5. Click Apply, and then click Save to make your changes permanent.

Changing an AAA Configuration

To change an AAA configuration
1. Click Config on the home page.
2. Click the AAA link in the Security and Access Configuration section.
3. Change one or more of the following elements of an AAA Configuration:
   - Changing the Service Profile
   - Changing a Service Module Configuration
   - Changing an Authentication Profile Configuration
   - Changing an Accounting Profile Configuration
   - Changing a Session Profile Configuration
   - Deleting an Item in a Service Profile Entry
   The steps for changing each of these elements is described in the following subsections.
4. Click Apply.
5. Click **SAVE** to make your changes permanent.

### Changing the Service Profile

You can add one or more authentication, accounting, or session profiles to a service profile. Note that the authentication, accounting, and session profiles must exist before you can add them to the service profile.

**To add an authentication profile**

1. Enter the name of the service profile in the Service Profile text box; the name is shown in the Profile Name column of the Service Profile table.

2. Enter an authentication profile from the Name column of the Auth. Profile table into the Auth. Profile text box of the Service Profile table.

   If the requirements for the service do not match any of the entries in the Auth. Profile, create a new Auth. Profile using Creating an Authentication Profile and enter that name in the Auth. Profile text box.

---

**Note**

The algorithm is added to the end of the list. The order of algorithms in the list is the order that they are invoked. To change the order, delete the algorithms which are out of order by using [*Deleting an Item in a Service Profile Entry,*](#) and add them in the desired order using this procedure.

---

### Creating a Stacked Service Module

When you create a service, the requirement for multiple authentication algorithms is as follows.

<table>
<thead>
<tr>
<th>Service</th>
<th>Authentication Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>my_svc</td>
<td>requisite: SKEY</td>
</tr>
<tr>
<td></td>
<td>required: SECURETTY</td>
</tr>
</tbody>
</table>
The following graphic screens below show an example of how to create a service which has the requirement for multiple authentication algorithms. Only the portion of the page that has changes is shown here.

To add an accounting profile

1. Enter the name of the profile in the Service Profile text box; the name is shown in the Profile Name column of the Service Profile table.

2. Enter an item from the Name column of the Acct. Profile table into the Acct. Profile text box of the Service Profile table.

   If the requirements for the service do not match any of the entries in the Acct. Profile table, create a new Acct. Profile by using Creating an Accounting Profile and enter that new name in the Acct. Profile text box.

   **Note**

   The algorithm is added to the end of the list. The order of algorithms in the list is the order that they are invoked. To change the order, delete the algorithms which are out of order, using Deleting an Item in a Service Profile Entry, and add them in the desired order using this procedure.
To add a session profile

1. Enter the name of the profile in the Service Profile text box; the name is shown in the Profile Name column of the Service Profile table.

2. Enter an item from the Name column of the Session Profile table into the Session Profile text box of the Service Profile table.

If the requirements for the service do not match any of the entries in the Session Profile table, create a new Session Profile using Creating a Session Profile and enter the new name in the Session Profile text box.

Note
The algorithm is added to the end of the list. The order of algorithms in the list is the order that they are invoked. To change the order, delete the algorithms which are out of order, using "Deleting an Item in a Service Profile Entry," and add them in the desired order using this procedure.

Changing a Service Module Configuration

In the Service Module Configuration table enter the name of an existing Service Profile in the text box in the Profile column.

You can not assign a different service profile name to the following services:
- httpd
- snmpd

Changing an Authentication Profile Configuration

In the Auth. Profile table make one or more of the following changes to the Auth. Profile name in the Name column:
- Select a different item in the Type list that matches the new requirements of the service.
  For a description of the authentication algorithms that the list items represent, see Authentication Profile Types.
- Select a different item in the Control list that matches the new requirements of the service.
  Values other than required are effective only when the service requires more than one Auth. Profile. For a description of the effect on result disposition and subsequent algorithm invocation that the list items represent, see Profile Controls.

Note
The Server/File field is unused.
Changing an Accounting Profile Configuration

In the Acct. Profile table, make one or more of the following changes to the row where the service Acct. Profile name is in the Name column:

- Select a different item in the Type list that matches the new service requirements.
  For a description of the accounting algorithms that the list items represent, see Accounting Profile Types.
- Select a different item in the Control list that matches the new service requirements.
  Values other than required are effective only when the service requires more than one Acct. Profile. For a description of the effect on result disposition and subsequent algorithm invocation that the list items represent, see Profile Controls.

**Note**
The Server/File field is unused.

Changing a Session Profile Configuration

In the Session Profile table, make one or more of the following changes to the row where the service session profile name is in the Name column:

- Select a different item in the Type list that matches the new service requirements.
  For a description of the session algorithms that the list items represent, see Session Profile Types.
- Select a different item in the Control list that matches the new service requirements.
  Values other than required are effective only when the service requires more than one Session Profile. For a description of the effect on result disposition and subsequent algorithm invocation that the list items represent, see Profile Controls.

Deleting an Item in a Service Profile Entry

- Highlight one of the entries in the lists under the Auth Profile, Acct Profile or Session Profile column in the Service Profile table for the entry you want to change.
- Select the Delete check box of the same entry.

Deleting an AAA Configuration

To delete an AAA configuration

1. Click Config on the home page.
2. Click the AAA link in the Security and Access Configuration section.
3. Delete one or more of the rows of a table by selecting the check box in the Delete column of the table for that row.
Note
An item might not be deleted if it is referenced by another item; for example, a Service Profile might not be deleted if it is used in the Profile column of one of the rows in the Service Module Configuration table.

4. Click Apply.
5. Click Save to make your changes permanent.

You cannot delete the following services:
- httpd
- snmpd
- login
- sshd
- other

Encryption Acceleration

Encryption Acceleration Description

The Nokia encryption accelerator cards provide high-speed cryptographic processing that enhances the performance of virtual private network (VPN) tunnels. By taking over cryptographic processing, the cards allow the appliance CPU to perform other tasks.

These cards include the Nokia Encryption Accelerator Card and the Nokia Encrypt Card. For information on which security algorithms your encryption accelerator card supports, refer to the installation documentation for your card.

You can hot swap an encryption accelerator card—remove the card while your network application platform is running and then reinsert it or insert another accelerator card—on some appliances.

Enabling Encryption Acceleration Cards

If you do not intend to use SecureXL, you must manually enable the encryption accelerator card after you install it. If you enable SecureXL, the encryption accelerator card is automatically enabled—you do not need to perform any other software task to activate the card.

Note
You cannot enable the card before you install it. The options in Network Voyager for enabling the card do not appear until it is installed.
To enable the encryption accelerator card when you are using Check Point software to create and manage VPN tunnels, complete the following procedure.

**To enable the card for a Check Point VPN**

1. Start Network Voyager for your appliance.
2. On the Network Voyager home page, click Config.
3. Under Interfaces, click IPSec.
4. Scroll down and click IPSec Advanced Configuration.
5. At Hardware Device Configuration, click On.
6. Click Apply to enable the card.

You can also monitor encryption accelerator card interfaces with Network Voyager. For more information about accessing Network Voyager and locating relevant reference materials, see the *Network Voyager Reference Guide*.

**Monitoring Cryptographic Acceleration**

**To monitor the encryption accelerator cards**

1. Click Monitor on the home page.
2. Click the Cryptographic Accelerator Statistics link in the Hardware Monitoring section.

**IPSec Tunnels**

**Introduction**

Developed by the Internet Engineering Task Force (IETF), IPSec is the industry standard that ensures the construction of secure virtual private networks (VPNs). A VPN is a private and secure network implemented on a public and insecure network. Secure VPNs are as safe as isolated office LANs running entirely over private lines and much more cost effective.

**Note**

This feature is not supported on the IP2250. You cannot use Network Voyager or the IPSO CLI to create VPNs on this appliance.

The IPSec protocol suite provides three new protocols for IP:

- An authentication header (AH) that provides connectionless integrity and data origin authentication. The IP header is included in the authenticated data. It does not offer encryption services.
An encapsulation security payload (ESP) that provides authentication and confidentiality through symmetric encryption, and an optional anti-replay service. ESP does not include the IP header in the authentication/confidentiality.

A protocol negotiation and key exchange protocol (IKE) for easier administration and automatic secure connections. IKE introduces two negotiations. Phase 1 negotiation authenticates both peers and sets up the security for the Phase 2 negotiation. IPSec traffic parameters are negotiated in Phase 2.

Transport and Tunnel Modes

The basic building blocks of IPSec, AH and ESP, use symmetric cryptographic techniques for ensuring data confidentiality and data signatures for authenticating the data’s source. IPSec operates in two modes:

- Transport mode
- Tunnel mode

In transport mode the original IP header remains the outer header. The security header is placed between the IP header and the IP payload. This mode offers some light bandwidth savings, at the expense of exposing the original IP header to third party elements in the packet path. It is generally used by hosts—communication endpoints. This mode can be used by routers if they are acting as communication endpoints.

With IPSec transport mode:

- If AH is used, selected portions of the original IP header and the data payload are authenticated.

```
IP header   AH   Payload
```

- If ESP is used, no protection is offered to the IP header, but data payload is authenticated and can be encrypted.

```
IP header   ESP header   Payload   ESP trailer   ESP auth
```

`00126` `00127`
In tunnel mode, the original IP datagram is placed inside a new datagram, and AH or ESP are inserted between the IP header of the new packet and the original IP datagram. The new header points to the tunnel endpoint, and the original header points to the final destination of the datagram. Tunnel mode offers the advantage of complete protection of the encapsulated datagram and the possibility to use private or public address space. Tunnel mode is meant to be used by routers—gateways. Hosts can operate in tunnel mode too.

With IPSec tunnel mode:

- If AH is used, the outer header is authenticated as well as the tunneled packet:

```
New IP header       AH       Old IP header       Payload
                        --------      ---------
                        New IP header AH Old IP header Payload
```

- If ESP is used, the protection is offered only to the tunneled packet, not to the new outer IP header. By default, ESP, providing the highest level of confidentiality, is used in this release.

```
New IP header       ESP header Old IP header       Payload       ESP trailer       ESP auth
                                  --------      ---------     ------------       00128
                                  New IP header ESP header Old IP header Payload ESP trailer ESP auth
```

**Building VPN on ESP**

Tunneling takes the original IP header and encapsulates it within ESP. Then it adds a new IP header, containing the address of a gateway, to the packet. Tunneling allows you to pass nonrouteable and private (RFC 1918) IP addresses through a public network that otherwise would not be accepted. Tunneling with ESP using encryption also has the advantage of hiding the original source and destination addresses from the users on the public network, reducing the chances of traffic analysis attacks. Tunneling with ESP can conceal the addresses of sensitive internal nodes, protecting them from attacks and hiding its existence to outside machines.

**Protocol Negotiation and Key Management**

To successfully use the IPSec protocol, two gateway systems must negotiate the algorithms used for authentication and encryption. The gateway systems must authenticate themselves and choose session keys that will secure the traffic. The exchange of this information leads to the creation of a security association (SA). An SA is a policy and set of keys used to protect a one-
way communication. To secure bidirectional communication between two hosts or two security gateways, two SAs (one in each direction) are required.

Processing the IPSec traffic is largely a question of local implementation on the IPSec system and is not a standardization subject. However, some guidelines are defined to ensure interoperability between multivendor IPSec systems.

“Security Architecture for IP, RFC 240 defines a model with the following two databases:

- The security policy database that contains the security rules and security services to offer to every IP packet going through a secure gateway
- The SA database that contains parameters associated with each active SA. Examples are the authentication algorithms, encryption algorithms, keys, lifetimes for each SA (by seconds and bytes), and modes to use.

To offer a secure and automated IPSec SA negotiation, IETF added a new protocol. The Internet Key Exchange, (IKE, RFC 2409), based on ISAKMP (RFC 2408), is a more extended framework for SA authentication and key exchange. IKE is implemented on top of UDP, port 500. IKE provides authenticated secure key exchange with perfect forward secrecy (based on the Diffie-Hellman protocol) and mutual peer authentication using public keys or shared secrets. The IKE protocol defines two phases:

- Phase 1

In order to safely set an IPSec SA, the two peers first establish a secure channel, which is an encrypted and authenticated connection. The two peers agree on authentication and encryption methods, exchange keys, and verify each other’s identities. The secure channel is called ISAKMP Security Association. Unlike IPSec SAs, ISAKMP SAs are bi-directional and the same keys and algorithms protect inbound and outbound communications. IKE parameters are negotiated as a unit and are termed a protection suite. Mandatory IKE parameters are:

  a. Symmetric Encryption algorithm
  b. Hash function
  c. Authentication method: pre-shared key and X.509 certificates. See the following section on “Using PKI”.
  d. Group for Diffie-Hellman

Other optional parameters such as SA lifetime can also be part of the protection suite.

- Phase 2

IPSec SAs are negotiated once the secure ISAKMP channel is established. Every packet exchanged in phase 2 is authenticated and encrypted according to keys and algorithms selected in the previous phase.

The one method to complete phase 1 is Main Mode.

The Main Mode negotiation uses six messages, in a three two-way exchange. The messages containing the identity information are not authenticated nor encrypted.

One mode is defined for phase 2. This mode is called Quick Mode. Quick Mode uses three messages, two for proposal parameters and a third one to acquit the choice. With “perfect forward secrecy” enabled, the default value in Nokia’s configuration, a new Diffie-Hellman protocol...
exchange must take place during Quick Mode. Consequently, the two peers generate a new Diffie-Hellman key pair.

**Using PKI**

For Phase 1 negotiation of IKE, the IPSec systems can use X.509 certificates for authentication. X.509 certificates are issued by Certificate Authorities (CA). IPSO IPSec implementation supports Entrust VPN connector and Verisign IPSec on site services. Contact any of the listed CA vendors for certificate signing services.

To use the X.509 certificates, the IPSec system should follow these steps:

1. Install the trusted CA certificates (all, including yours) of all the peer IPSec systems.
2. Make a certificate request with all the information required to identify the system such as your IP address, a fully qualified domain name, organization, organization unit, city, state, country, and contact email address.
3. Forward the certificate request to the CA or corresponding RA (Registration Authority) using the Web interface or another file transfer mechanism. CA or RA verifies the identity of the IPSec system and generates the approved certificate. A certificate is valid only for a certain period of time.
4. Download and install the approved device certificate and the CA certificate on the IPSec system.
5. Link the certificate to an IPSec policy.

**Note**
The IPSO Web-based Network Voyager interface provides the mechanism you need to complete all the above steps.

**IPSec Implementation in IPSO**

**Note**
The IP2250 appliance does not support IPSO's implementation of IPSec.

The IPSO operating system provides a native IPSec implementation supporting ESP in tunnel mode. This implementation is compliant with the following RFCs:

- RFC 2401—Security Architecture for the Internet Protocol
- RFC 2402—IP authentication header
- RFC 2406—IP Encapsulating Security Payload (ESP)

Supports algorithms: 3DES, DES, and Blowfish for encryption and SHA-1 and MD5 for authentication.
The IPSec configuration in Network Voyager is based on three different IPSec objects: proposals, filters, and policies.

- Proposals define the combination of encryption and authentication algorithms that secure phase 1 negotiation (Main Mode) as well as phase 2 negotiations (Quick Mode) and IPSec packets.
- Filters determine which packets relate to certain proposals. The filters are matched against the source or destination fields in the packet header depending on whether the filters are used as source or destination filters. If applicable, Protocol and Port fields are also used.
- Policies link the type of IPSec security that proposals with traffic define. The traffic is defined by a list of filters specified for the source address and a second list specified for the destination address. If the source address of a packet matches a filter from the source filter list and the destination address matches a filter from the destination filter list, IPSec is applied to the traffic. Protocols and ports are used in the matching process, if applicable.

The kind of security applied to a defined traffic is specified by a list of proposals ordered by priority. This list is offered to the other peer beginning with the lowest priority value proposal.

Proposals and filters can be reused in different policies. Other elements defined in a policy are authentications methods (Preshared Keys or X.509 Certificates) and lifetime attributes.

**Miscellaneous Tunnel Requirements**

IPSec tunnels are defined by local and remote tunnel addresses. The tunnel requires a policy to define what traffic is encapsulated by the tunnel and what security to use in the encapsulation. The traffic that matches filters associated to the policy is encapsulated by using tunnel addresses. Policies can also be reused in different tunnels. An IPSec tunnel cannot function without an associated policy.

Native IPSO IPSec tunnels cannot coexist in the same machine with Check Point IPSec software. Before you use IPSO IPSec software, ensure that no Check Point software is running. Likewise, before you use Check Point IPSec software, ensure that no IPSO IPSec software is running.

You can create IPSec tunnel rules with or without a logical interface for all IPSO platforms except the IP3000 series. For the IP3000 series platform, you must create a logical interface with each tunnel rule. You can create tunnel rules without logical interfaces if you require a large number of tunnels. However, creating IPSec tunnels without interfaces can slow down non-IPSec traffic.
Phase 1 Configuration

For IPSO, the Phase 1 encryption and authentication algorithms are the same as those used in Phase 2. However, if Phase 2 encryption is NULL, such as with an AH proposal or NULL-encryption-ESP proposal, IPSO uses 3DES as Phase 1 for the encryption algorithm.

The values set in the Lifetime table are used as the hard lifetime of the Phase 2 SA. Phase 1 lifetimes are calculated as Hard Phase 1 lifetime (seconds) = 5* Hard Phase 2 lifetime (seconds). The soft limit value is approximately 80-90 percent of the hard-limit value, depending on whether the device is working as a session initiator or responder.

If you create tunnels between an IPSO platform and non-IPSO systems, configure the non-IPSO system so that the Phase 1 lifetime is five times the Phase 2 lifetime. Set the encryption to 3DES, and set the authentication so that it is the same as the Phase 2 algorithm.

Platform Support

IPSec is supported across all Nokia security appliances.

IPSec Parameters

The two IPSec peers should agree on authentication and encryption methods, exchange keys, and be able to verify each other’s identities. While you configuring the peer IPSec devices, consider the following:

- At least one proposal (encryption algorithm and hash function) should match on the peer devices. See “Proposal and Filters” in “Creating an IPSec Policy” for more information.

- Authentication method:
  - If you are using Shared Secret, both devices should have the same shared secret. See “Putting It All Together” in “Creating an IPSec Policy” for more information.
  - If you are using X.509 certificates, both devices should install all the trusted CA certificates in the trust hierarchy. See “Trusted CA Certificates” in “Creating an IPSec Policy” for more information.

- Some IPSec systems require that the SA lifetimes (seconds, as well as megabytes) match on both devices. See “Putting It All Together” in “Creating an IPSec Policy” for more information.

- IKE and PFS groups should match on both devices. See “Putting It All Together” in “Creating an IPSec Policy” for more information.

The Diffie-Hellman key exchange uses the IKE group during the establishment of Phase 1 ISAKMP SA. Value options are 1, 2, or 5; 2 is the default value.

The Diffie-Hellman key exchange uses the PFS group in Phase 2 to construct key material for IPSec SAs. The value options are 1, 2, 5, or none; 2 is the default. Setting the value to none disables PFS.
Creating an IPSec Policy

Choosing IPv4 or IPv6 General Configuration Page

To chose IPv4 or IPv6 general configuration pages
1. Click Config on the home page.
2. Access the appropriate IPSec General Configuration page.
   a. To display the IPv4 IPSec General Configuration page, click on the IPSec link
   b. To display the IPv6 IPSec General Configuration page, first click on the IPv6
      Configuration link; this takes you to the main IPv6 page. Next, click on the IPSec link;
      this takes you to the IPv6 IPSec General Configuration Page.
   c. If you are on the IPv4 General Configuration page, to move to the IPv6 General
      configuration page, scroll down to the bottom of the page and click the IPv6 IPSec
      General Configuration link.

Note
Application procedures are the same for both configuration page types. The primary
difference is the format of the IP addresses. IPv4 uses dotted quad format and IPv6 uses
canonical address format. Selected range values might be different; consult the inline Help
option for specifics.

The following sections describe how to create an IPSec policy.

Proposal and Filters
1. Under the Proposals table, enter a name for a new proposal in the New Proposal text box.
   Click either ESP or AH.

Note
If you click AH, the Encryption Alg (algorithm) must always be set to NONE. If this is not
done, an error message appears when you click Apply.

2. From the drop-down list in the Authentication Alg and Encryption Alg fields, select the
   necessary algorithms. Click Apply.
3. Under the Filters table, enter a new filter name in the New Filter text box for the subnetwork that you want to control.

4. Enter the subnet address and the mask length in the Address and Mask Length text boxes. Click Apply.

**Note**
Destination filters across multiple rules (tunnel or transport) should not overlap, although source filters can overlap.

After you click Apply, the new filter information is added to the Filters list. If needed, you can then define a protocol or a port. Defaults are assumed. Repeat this operation for as many networks you need.

**Note**
Each Network Voyager page displays a maximum of 10 proposals or 10 filters. If you create more than 10, they are continued on new pages. Access these pages by clicking the link directly below the appropriate section. The link to more pages appears only after you create more than 10 proposals or filters.

Skip to “Putting It All Together” if you do not plan to use a X.509 certificate and want to use shared secret for authentication.

**Trusted CA Certificates**

Trusted CA certificates are the publicly available certificates of the CAs.

**To select a trusted CA certificate**

1. Under the Trusted CA Certificates table, enter a name in the New CA text box. Click Apply.

2. An Apply Successful message appears and the name of the CA you just entered appears in the Trusted CA Certificates table.

3. Click on the new link with the same name that you entered in Step 1. This action takes you to the IPSec Certificate Addition page for that specific certificate.

4. On the Certificate Addition page, you have two choices:
   - If you have the PEM (base64) encoded certificate, select the Paste the PEM Certificate option.
   - If you know the URL to the certificate (including the local file), select the Enter URL to the Certificate option.

5. Click Apply.
Note
This action takes you to the next page that asks for the PEM encoded certificate or the URL information of the certificate. If you have the PEM encoded certificate, proceed to step 5; if you reach the URL to the certificate, skip to step 6.

6. If you are asked to enter the PEM coded certificate, use the copy and paste function of your browser to copy the PEM text of the certificate into the text box titled Paste the PEM Encoded Certificate; click Apply. This action should print a Success message. Click on the link titled IPSec General Configuration page to return to the main IPSec configuration page.

7. If you are asked to enter URL information of the certificate, enter the URL to the certificate. Examples are:
   - http://test.acme.com/dev1.cert
   - ftp://test.acme.com/dev1.cert
   - file://tmp/dev1.cert

   Enter the HTTP realm information (only for the HTTP protocol); enter the user name and password if needed to connect to the FTP/HTTP server.

8. Click Apply. This action should print a Success message. Click on the link titled IPSec General Configuration page to return to the main IPSec Configuration page.

Repeat the steps in this procedure for every trusted CA certificate that needs to be installed.

Note
On successful completion, a green button appears under the Certificate File column. The green button indicates that the certificate file is present on the machine and it is also a link to view the installed certificate.

Device Certificates
A device certificate is used to identify a particular IPSec system. Follow the steps below.

To enroll and install a device certificate

1. Under the Device Certificates table, enter a name in the New Certificate text box, then click Apply.

2. An Apply Successful message appears and the name of the CA you just entered appears in the Device Certificates table.

3. Click on the new link with the same name that you entered in step 1.

   This action takes you to the IPSec Certificate Enrollment page for that named item.

4. Enter all the fields on the page that identifies the IPSec system and click Apply.

   This action should take you to the page where a PEM-encoded certificate request is shown.
Note
Remember the passphrase that you entered for future reference.

5. Click on Save to avoid the risk of losing your private key.

6. If you have access to the CA/RA enrollment page, open the page in a separate browser window.
   Use the copy and paste function or your browser to paste the PEM certificate request into the CA/RA certificate enrollment page.

Note
Some CAs do not expect the header (----BEGIN CERTIFICATE REQUEST----) and the footer (----END CERTIFICATE REQUEST----) lines in the text.

Alternatively, you can copy the text in a file and send the file to the CA/RA by FTP or some other file transfer mechanism that is supported. Contact the CA for details.

7. If you could successfully make the certificate request select Completed the certificate request at the CA site option; otherwise, select the Will do it later option.

8. Click Apply.
   If you chose Completed the certificate request at the CA site, proceed to step 8. If you chose the Will do it later option, skip to step 10.

9. If you chose the Completed the request at the CA site, a new link Click here to install the Certificate appears towards the bottom of the page.
   To install the certificate, click the link to go to the page described in steps 3–6 under “Trusted CA Certificates.”

Note
Before you install the certificate, ensure that CA approved the certificate and that you know how to access the approved certificate. If you need to wait for the CA's approval, you can click on the link with the Certificate name in the IPSec General Configuration page to install the certificate.

10. If you chose Will do it later to make the certificate request, the link on the main IPSec General Configuration still points to the certificate request page.
    You can repeat steps 5 through 8 to install the certificate.

11. If you finished all the steps, two green buttons appear.
    You can click on the button under the Certificate column to view the certificate.
Advanced IPSec

The following options are available through the IPSec Advanced Configuration page; the link is at the bottom of the IPSec General Configuration Page:

- **Log Level**—IPSO IPSec provides three levels of message logging through the syslog subsystem:
  - **Error** (default value)—only error messages or audit messages are logged.
  - **Info**—provides minimum information about the successful connections to the system. Also includes error messages.
  - **Debug**—besides the informational messages, gives full details of the negotiations that the subsystem performs.

**Note**
In any of the log level options, confidential information (such as secrets or session keys) are not shown.

- **Allowing tunnels without logical interfaces**
  This option allows for the creation of IPSec tunnels that are not associated with a logical tunnel interface. You can create tunnels without logical interfaces if you want a greater number of tunnels and to achieve scalability. The Create a logical interface field appears only if the Allow tunnels without logical interface field is selected to On in the Advanced Configuration page.

**Note**
Enabling this option might slow down forwarding of non-IPSec packets.

- **LDAP servers**
  IPSO IPSec implementation supports automatic CRL retrieval following the LDAPv2/3 protocol specification (RFC 2251). To retrieve CRL automatically from the centralized directory enter the URL of the directory server.

  Because of different implementations, the internal configuration of the directory server might not be compatible with IPSO that has implemented LDAP query formats.

**Putting It All Together**

**To complete creating an IPSec policy**

1. Under the Policies table, enter a name for a new policy in the New Policy text box, then click Apply.
   An Apply Successful message appears and the policy name appears in the Policies table.
2. Click on the policy name in the Policies table.
   The IPSec Policy Configuration page for the name appears.
3. Under the Linked Proposals table, from the drop-down list in the Add a Proposal field, select the name of the proposal to use in this policy. Assign a priority in the Priority text box, then click Apply. Repeat this step for every proposal that must be offered to the other peer. The proposals are offered starting with the lowest priority value (one).

4. Select the authentication method (Pre-Shared Secrets or X.509 Certificates) needed in this policy, then click Apply.

**Note**
Only one method can be active at a time.

5. If you chose Pre-Shared Secret, enter the shared secret in the Enter Shared Secret text box. Enter the secret again, in the Shared Secret (Verify) text box, for verification.

6. Click Apply.
   If the secret has been entered correctly the red light of the Secret Status field turns green after you click Apply.

7. If you chose X.509 Certificates, select the certificate name from the list of device certificates that identifies this machine.

8. In the Lifetime table, if the default lifetime values are not appropriate, modify them in the Seconds and Megabytes text boxes.

**Note**
Lifetimes must be set to the same value between peers when negotiation is initiated. If they are not set the same, IPSO IPsec might deny the negotiation.

9. In the Diffie-Hellman Groups table, if the default values in the IKE Group and PFS Group text boxes are not appropriate, modify them, then click Apply.

**Note**
Each Network Voyager page displays a maximum of 10 policies. If you create more than 10 policies, they are continued on new pages. Access these pages by clicking the link directly below the policy section. The link to more pages appears only after you create more than 10 policies.

---

**Creating an IPsec Tunnel Rule**

**To create an IPsec tunnel rule**

1. Click Config on the home page.
2. Click the IPSec link.
3. Under the IPSec Tunnel Rules heading, enter a name in the New Tunnel text box.

4. If the Create a logical interface option appears and you want to create a logical interface, set the button to Yes.

5. Enter the IP address of the local end of the IPSec tunnel in the Local Address text box.
   The local address must be one of the system interface addresses and must be the remote endpoint configured for the IPSec tunnel at the remote gateway.

6. Enter the IP address of the remote interface to which the IPSec tunnel is bound in the Remote Address text box.
   The remote endpoint cannot be one of the system interface addresses and must be the local endpoint configured for the IPSec tunnel at the remote gateway.

7. Click Apply.
   An Apply Successful message appears and an entry for the new tunnel appears in the IPSec Tunnel Rules table.

8. Click on the new link with the name that you entered in the IPSec Tunnel Rules table.
   The IPSec Tunnel page appears.

9. (Optional) Activate Hello Protocol inside the tunnel, then click Apply.

Note
IPSO can support up to 1500 rules. However, each Network Voyager page displays a maximum of 10. If you create more than 10 rules, they are continued on new pages. Access these pages by clicking the link directly below the rule section. The link to more pages appears only after you create more than 10 rules.

10. (Optional) If the hello protocol is active, enter a value for the Hello Interval and Dead Interval text boxes, then click Apply.

   The Hello Interval text box specifies the interval (number of seconds) between the Hello packets being sent through the tunnel. The Dead Interval text box determines the interval (number of seconds) in which you do not receive an Hello packet before the link status changes to unavailable.

11. (Optional) Change the logical name of the interface to a more meaningful one by entering the preferred name in the Logical Name text box, then click Apply.
12. From the drop-down list in the Select Policy field, select the policy name that is needed, then click Apply.
   This action displays a new table, Linked Policy.

13. From the drop-down list in the Source Filters column, select a filter name that corresponds to the source of the traffic that this policy will protect, then click Apply.
   Repeat this operation to add as many filters as necessary. Click Apply after each selection.

**Note**
If there are 40 or more source or destination filters, they do not appear as a list on the Network Voyager page. To view a filter that is not displayed, type the name of the filter in the appropriate field.

14. From the drop-down list in the Destination Filters column, select a filter name that corresponds to the destination of the traffic that will be protected by this policy. Click Apply.
   Repeat this operation to add as many filters as necessary. Click Apply after each selection.

15. (Optional) In the Options table, select the option Include End-Points in the Filters, then click Apply.

16. Click Save to make your changes permanent.

**Transport Rule**

**To create a transport rule**

1. Click Config on the home page.
2. Click IPSec.
3. Click the IPSec Transport Rules Configuration link at the bottom of the page.
   The IPSec Transport Rules page appears. The structure of this page is common to both IPv4 and IPv6.
4. Enter the name of the new rule in the New Transport Rule field.
   In the Select a policy field select the desired option from the drop-down list, the click Apply.
   The new entry appears in the IPSec Transport Rules table.
5. (Optional) To change the policy entry without changing the name of the associated transport rule, perform the following steps:
   a. Click in the blank square next to the current policy entry. Click Apply. The policy name is removed.
   b. Under the Policy column, select a policy option from the drop-down list and click Apply.
      The new policy is entered without changing the associated transport rule.
6. From the drop-down list in the Source Filters column, select a filter name that corresponds to the source of the traffic that will be protected by this policy. Click Apply.
Repeat this operation to add as many filters as necessary.

7. Click Apply after each selection.

**Note**
Select as source filters only filters that present a single host but no subnet.

**Note**
If you have 40 or more source or destination filters, they are not displayed as a list on the Network Voyager page. To view a filter that is not displayed, type the name of the filter in the appropriate field.

8. From the drop-down list in the Destination Filters column, select a filter name that corresponds to the destination of the traffic to be protected by this policy.

9. Click Apply and then click Save to make your changes permanent.

10. To delete any entries, check the Delete check box and click Apply.
    
    Click Save to make delete permanent.

**Note**
Each Network Voyager page displays a maximum of 10 transport rules. If you create more than 10 rules, they are continued on new pages. Access the new pages by clicking the link directly below the rule section. The link to more pages appears only after you create more than 10 transport rules.
IPSec Tunnel Rule Example

The following steps tell how to configure a sample IPSec tunnel. The following figure below shows the network configuration for this example.

Configuring Nokia Platform 1

1. Click Config on the home page of the network application platform 1 (Nokia Platform 1).
2. Click the IPSec link.
3. Under the Proposals table, enter md5-des as a name for a new proposal in the New Proposal text box.
4. In the Type field, select the ESP button.
5. Select MD5 from the Authentication Alg drop-down list and DES from the Encryption Alg drop-down list. Click Apply.
6. In the Filters table, enter site_A as a new filter name in the New Filter text box. Enter 192.68.22.0 in the Address text box and 24 in the Mask Length text box. Click Apply.

The new entry appears in the Filters table.

7. In the Filters table, enter site_B as a new filter name in the New Filter text box. Enter 192.68.23.0 in the Address text box and 24 in the Mask Length text box. Click Apply.

Note
In this example, the authentication method is a preshared secret, so you don’t need to select a certificate.
8. (Optional) Click the IPSec Advanced Configuration link.

9. (Optional) From the drop-down list in the Log Level field, select Info. Click Apply.

10. (Optional) Click Up.

11. In the Policies table, enter **rule_1** as the name for a new policy in the New Policy text box. Click Apply.

12. In the policies table, click on **rule_1**.
    The corresponding Configuring Policy page appears to complete the missing parameters of the policy.

13. Select MD5-DES from the Add a Proposal drop-down list. Enter 1 in the Priority text box.

14. If no default is selected, select **PRE-SHARED SECRET** in the **AUTHENTICATION METHOD** field.

15. Enter a text string, such as **secret**, in the Enter Shared Secret text box and Shared Secret (Verify) text box. Click Apply.

16. Click Up to return to the IPSec General Configuration page.
    Under the IPSec Tunnel Rules table, enter **IPSec_tunn** in the New Tunnel field.

17. If Create a logical interface appears, select Yes.

18. Enter **192.68.26.65** in the Local Address text box.

19. Enter **192.68.26.74** in the Remote Address text box.
    Click Apply.

20. Click on the name in Tunnel Rules table.
    The IPSec Tunnel IPSec_tunn page appears.

21. (Optional) Click On to activate Hello Protocol.
    Click Apply. The Hello Interval and Dead Interval text boxes appear.

22. (Optional) Enter **60** as a value in the Hello Interval text box and enter 180 as a value for the Dead Interval text box.
    Click Apply.

23. From the drop-down list in the Select Policy field, select **rule_1**.
    Click Apply.
    A new table, Linked Policy, appears.

24. Select **site_A** from the Source Filters drop-down list.

25. Select **site_B** from the Destination Filters drop-down list.

26. Click Apply.

27. Click Save to make your changes permanent.
Configure Nokia Platform 2

Now set up network application platform 2 (Nokia Platform 2). Perform the same steps that you performed to configure Nokia Platform 1, with the following changes.

1. Step 18; enter 192.68.26.74 in the Local Address text box.
2. Step 19; enter 192.68.26.65 in the Remote Address text box.
3. Step 24; select SITE_B from the Source Filters drop-down list.
4. Step 25; select SITE_A from the Destination Filters drop-down list.

IPSec Transport Rule Example

The following procedure tells you how to configure a sample IPSec authentication connection. The following figure shows the network configuration for this example.

Configure Nokia Platform 1 (IPSO)

1. Click Config on the home page of the network application platform 1 (Nokia Platform 1, IPSO).
2. Click the IPSec link.
3. Under the Proposals table, enter ah-md5 as a name for a new proposal in the New Proposal text box.
4. In the Type field, click AH.
5. Select MD5 from the Authentication Alg drop-down list and None from the Encryption Alg drop-down list.
   Click Apply.
6. In the Filters table, enter local as a new filter name in the New Filter text box.
   Enter 192.68.26.65 in the Address text box and 32 in the Mask Length text box.
   Click Apply.
   The new entry appears in the Filters table.
7. In the Filters table, enter remote as a new filter name in the New Filter text box.
Enter 192.68.26.74 in the Address text box and 32 in the Mask Length text box. Click Apply.

**Note**
In this example, the authentication method is a preshared secret, so you do not need to select a certificate.

8. (Optional) Click the IPSec Advanced Configuration link.
9. (Optional) From the drop-down list in the Log Level field, select Info. Click Apply.
10. (Optional) Click Up.
11. In the Policies table, enter rule_2 as the name for a new policy in the New Policy text box. Click Apply.
12. In the policies table, click on rule_2.
    The corresponding Configuring Policy page appears to complete the missing parameters of the policy.
13. Select AH-MD5 from the Add a Proposal drop-down list.
    Enter 1 in the Priority text box.
14. If no default is selected, select Pre-Shared Secret in the Authentication Method field.
15. Enter secreted in the Enter Shared Secret text box and Shared Secret (Verify) text box. Click Apply.
16. Click Up to return to the IPSec General Configuration page.
17. Select IPSec Transport Rules Configuration link.
    The IPSec Transport Rules page appears.
18. In the New Transport Rule text box under the IPSec Transport Rules table, enter IPSec_trans.
19. In the Select a policy text box, select rule_2.
20. Select Apply.
    The new transport rule appears in the IPSec Transport Rules table.
21. Select local from the Source Filters drop-down list.
22. Select remote from the Destination Filters drop-down list.
23. Click Apply.
24. Click Save to make your changes permanent.
Configure PC1

You now need to set up PC1. Perform the same steps that you performed to configure Nokia Platform 1 (IPSO), with the following changes.

1. Step 6; for the local filter, enter 192.68.26.74 in the Address text box.
2. Step 7; for the remote filter, enter 192.68.26.65 in the Address text box.

Changing the Local/Remote Address or Local/Remote Endpoint of an IPSec Tunnel

1. Click Config on the home page.
2. Click the IPSec link.
   You are taken to the IPSec General Configuration page.
3. In the Name column, click the name link for which you want to change the IP address.
   Example: tun0c1
4. You are taken to the IPSec Tunnel page.
5. (Optional) Enter the IP address of the local end of the IPSec tunnel in the Local Address text box.
   The local address must be one of the system’s interfaces and must be the same as the remote address configured for the IPSec tunnel at the remote router.
6. (Optional) Enter the IP address of the remote end of the IPSec tunnel in the Remote Address text box.
   The remote address cannot be one of the system’s interfaces and must be the same as the local address configured for the IPSec tunnel at the remote router.
7. Click Apply.
8. To make your changes permanent, click Save.

Removing an IPSec Tunnel

Proposed New

1. Click Config on the home page.
2. Click the IPSec link.
   The IPv4 IPSec General Configuration page appears by default. If the IPv6 General Configuration page is desired, scroll to the bottom of the page and click on the IPv6 IPSec General Configuration link.
3. Under the IPSec Tunnel Rules heading, click in the Delete square of the tunnel name(s) you wish to delete.
4. Click Apply.
   An Apply Successful message appears and the tunnel(s) selected for deletion are removed from the IPSec Tunnel Rules table.

5. To make your changes permanent, click Save.

Miscellaneous Security Settings

Setting TCP Flag Combinations

Beginning with IPSO 3.8, the default behavior is for IPSO to drop TCP packets that have both SYN and FIN bits set. This change addresses a CERT advisory. For more information on that advisory, go to www.kb.cert.org/vul/id/464133. You must change the default configuration if you want your Nokia platform to accept packets that have both the SYN and FIN bits set. Complete the following procedure to configure your platform to accept packets that have both SYN and FIN bits set.

1. Click Config on the home page.
2. Click the Misc link in the Security and Access Configuration section.
3. Click the on button next to Allow TCP/IP (rfc1644) mode (SYN-FIN together).
4. Click Apply, and then click Save to make your change permanent.
   Click the off button to return to the default configuration if you have enabled your platform to accept packets that have both SYN and FIN bits set.

Network Voyager Session Management

Network Voyager Session Management Description

IPSO session management lets administrators prevent multiple users from making simultaneous configuration changes. This feature lets you acquire an exclusive configuration lock so that other users cannot make configuration changes to an appliance while you are logged into it. Sessions are logged out automatically after a time period that you can specify, and you can also manually log out from any configuration or monitoring screen. You can view the history of logins and logouts in the system logs.

Session management is enabled by default. You may disable this, in which case you will be asked to login with a window that asks only for your user name and password. To disable session management see “Disabling Network Voyager Session Management.”
Note
Network Voyager uses cookies to keep track of HTTP sessions. Network Voyager cookie based session management does not store user names or passwords in any form in the cookies. You should continue to access Network Voyager from a secure workstation.

If you acquire a configuration lock and then close your browser without logging out, the lock remains in effect. The lock does not expire until the session timeout elapses or someone manually overrides the lock.

If you acquire a lock while using Network Voyager, CLI users are also prevented from making changes (as well as other Network Voyager users). The reverse is also true—a lock acquired by a CLI user prevents Network Voyager users (and other CLI users) from making configuration changes on the appliance.

For instructions about how to override a configuration lock, see “Overriding Configuration Locks.”

Enabling Network Voyager Session Management

Note
Your browser must be configured to accept cookies.

Network Voyager session management is enabled by default.

To enable the feature if Network Voyager session management is disabled
1. Click Config on the home page.
2. Click the Voyager Web Access link in the Security and Access Configuration section.
3. Click Yes in the Enable cookie based session management field.
4. Click Apply.

A new login window opens. See “Logging In with Exclusive Configuration Lock” and “Logging In without Exclusive Configuration Lock.”

Disabling Network Voyager Session Management

To disable Network Voyager session management
1. Click Config on the home page.
2. Click the Voyager Web Access link in the Security and Access Configuration section.
3. Click No in the Enable cookie based session management field.
4. Click Apply.
A new login window opens. Log in with your user name and password and click Login.

Logging In with Exclusive Configuration Lock

When you log in with exclusive configuration lock, no other user can change the system configuration. Only users with read/write access privileges are allowed to log in with exclusive configuration lock (users with Uid 0 and Gid 0).

To log in with exclusive configuration lock
1. At the login, Enter your user name.
2. Enter your user password.
3. Click Yes in the Acquire Exclusive Configuration Lock field. This is the default.
4. Click Login.

Note
Enabling exclusive configuration lock in Network Voyager prevents you from using the IPSO command line interface to configure the system while the session is in progress.

Logging In without Exclusive Configuration Lock

To log in without exclusive configuration lock
1. At the login, enter your user name.
2. Enter your user password.
3. Click No in the Acquire Exclusive Configuration Lock field.
4. Click Login.

Overriding Configuration Locks

Note
Only users with read/write access privileges are allowed to override an exclusive configuration lock (users with Uid 0 and Gid 0).

To override a configuration lock
1. Click the Login with Advance Options link.
2. Make sure that Yes is selected in the Acquire Exclusive Configuration Lock field. This is the default choice.
3. Click **YES** in the **OVERRIDE LOCKS ACQUIRED BY OTHER USERS** field.
4. Enter your user name.
5. Enter your user password.
6. Click Login.

**Configuring Session Timeouts**

You can adjust the time interval which Network Voyager allows a user to be logged in without activity. If you close your browser without logging out, this interval is still in effect—that is, the lock remains in effect until the interval expires.

**To change session timeouts**

1. Click **Config** on the home page.
2. Click the **Voyager Web Access** link in the Security and Access Configuration section.
3. In the **Session timeout in minutes** text box, enter the time in seconds. The default is 20 minutes.
4. Click **Apply**.

**Virtual Tunnel Interfaces for Check Point Route-Based VPN**

**Virtual Tunnel Interfaces Description**

Virtual Tunnel Interfaces (VTI) support Check Point route-based VPN. A VTI is a virtual interface that can be used as a gateway to the encryption domain of the peer Gateway. Each VTI is associated with a single tunnel to a VPN-1 Pro peer gateway. As with domain-based VPNs, the tunnel and its properties is defined by a VPN community linking the two gateways. The peer gateway is also configured with a corresponding VTI. The native IP routing mechanism on each gateway can then direct traffic into the tunnel just as it would for any other type of interface and the traffic will be encrypted.

For more information about route-based VPN, see the Check Point *Virtual Private Networks* guide.

**Unnumbered VTIs**

Nokia IPSO supports only unnumbered VTIs. Local and remote IP addresses are not configured; instead, the interface is associated with a proxy interface from which it inherits an IP address. Traffic that is initiated by the gateway and routed through the VTI will have the proxy interface IP address as the source IP address.
If you want the source IP address to be an IP address not used on the system, you can create a loopback interface with the desired IP address and use it as the proxy interface.

Routing Traffic through the VTI

In route-based VPN, a packet is encrypted only if it is routed through the virtual tunnel interface. To make sure that the traffic is routed through the VTI, you have several options:

- You can make the VTI the default route. Make sure you also have a static or dynamic route that enables the gateway to reach the external interface of the peer gateway, and vice versa.
- You can add a specific static route to the intended network behind the peer gateway for which the next hop is the VTI.
- You can configure a dynamic routing protocol on the VTI. For example, you can enable OSPF on the VTI and redistribute the internal networks route to OSPF external. Or you can enable OSPF on both the VTI and its proxy interface.

VTIs appear in Nokia Network Voyager as unnumbered interfaces and are given logical names in the form tun0cn. You configure static or dynamic routes on VTIs the same way you configure them on other unnumbered interfaces. The dynamic routing protocols supported on VTIs are BGP4 and OSPFv2.

VRRP Support

VRRP HA mode is supported for OSPFv2 over virtual tunnels. Only active-passive mode is supported: that is, only one gateway can have the master state.

Because a VTI is an unnumbered interface, you cannot configure a virtual IP address on it. To run in VRRP mode across the tunnel, OSPF instead detects the presence of one or more VRRP virtual IP addresses on the system.

When configuring OSPF to run in VRRP mode, make sure that you:

- Configure OSPF identically on the VTI in both the master and backup.
- Turn on the Virtual Address option in the OSPF configuration for the VTI.

The OSPF protocol runs only on the VTI of the master gateway. If the master gateway fails, the OSPF protocol starts running on the VTI of the backup gateway. Because adjacency needs to be reestablished, there will be a temporary loss of routes.

Creating Virtual Tunnel Interfaces

To create a virtual tunnel interface, you:

1. Create a VPN community that contains the two gateways, using the SmartDashboard. The VPN community defines the virtual tunnel properties, such as the type of encryption used. Because encryption is determined by routing packets through the tunnel, no VPN domain is required. You must configure an empty VPN domain as described in the “To create the VPN community” procedure.
2. Create the virtual tunnel interface on each gateway, using either Nokia Network Voyager or the Check Point vpn shell. The procedure “To create the virtual tunnel interface” describes how to do so using Nokia Network Voyager.

To create the VPN community

In the Check Point SmartDashboard:

1. Create the peer gateway objects.

2. In the Topology tab of one gateway object, select the Manually defined option under VPN Domain and create a new group domain that has no members. Assign the second gateway also to this empty domain.

Note
If both domain-based VPN and route-based VPN are configured, then domain-based VPN takes priority. Configuring a VTI does not override the domain-based VPN. The only way to configure no VPN domain is to create an empty VPN domain group.
3. Create a VPN community and add both gateways to that community.
4. Create a security policy rule and install the policy on both gateways.

**To create the virtual tunnel interface**

In Nokia Network Voyager:

1. Click the Check Point Firewall-1 link under Security and Access Configuration. This link appears only if the Check Point VPN-1 Pro/Express package is enabled.
2. Click the FWVPN Configuration link.
3. Enter the name of the peer gateway in the Peer GW Object Name field. Use the same name you assigned the gateway when you created it in the SmartDashboard.
4. From the drop-down list, select the proxy interface. Because the proxy interface is used as the source IP address for the outbound traffic, you would normally choose an external interface for the proxy interface. You can also use a loopback interface.

5. Click Apply and then Save.

The new tunnel is added to the list of tunnels. If the status field shows a status other than OK, you can click on the tunnel interface name to display details about the VTI. The Description field contains information provided by the Check Point software about the status of the VPN tunnel.

**Note**

Both the Description and Status fields are read-only fields. Do not edit them.

Once created, a VTI is always up unless you administratively set it down.
8 Configuring Traffic Management

Chapter Contents

- Configuring Clustering in IPSO
  - Overview
  - IP Clustering Description
  - Upgrading IPSO in a Cluster
  - Creating and Configuring a Cluster
  - Adding a Node to a Cluster
  - Managing a Cluster
  - Synchronizing the Time on Cluster Nodes
  - Configuring VPN-1 NG for Clustering
  - Clustering Example (Three Nodes)
  - Clustering Example With Non-Check Point VPN

- Configuring Access Control Lists
  - Traffic Management Description
  - Packet Filtering Description
  - Traffic Shaping Description
  - Traffic Queuing Description
  - Creating an Access Control List
  - Deleting an Access Control List
  - Applying an Access Control List to an Interface
  - Removing an Access Control List from an Interface

- Configuring Access Control List Rules
  - Description of Access Control List Rules
  - Adding a New Rule to an Access Control List
  - Modifying a Rule
  - Deleting a Rule

- Configuring Aggregation Classes
  - Aggregation Class Description
  - Creating an Aggregation Class
Deleting an Aggregation Class
Associating an Aggregation Class with a Rule
Example: Rate Shaping

Configuring Queue Classes
Queue Class Description
Creating a New Queue Class
Deleting a Queue Class
Setting or Modifying Queue Class Configuration Values
Associating a Queue Class with an Interface
Example: Expedited Forwarding

Configuring ATM QoS
ATM QoS Description
Creating a New QoS Descriptor
Deleting an ATM QoS Descriptor
Associating an ATM QoS Descriptor with an Interface and a Virtual Channel

Configuring Common Open Policy Server
Common Open Policy Server Description
Configuring a COPS Client ID and Policy Decision Point
Configuring Security Parameters for a COPS Client ID
Assigning Roles to Specific Interfaces
Activating and Deactivating the COPS Client
Changing the Client ID Associated with Specific Diffserv Configuration
Deleting a Client ID

Configuring IP Clustering in IPSO

Overview
This section describes IPSO’s clustering feature and provides instructions for configuring clusters. It includes information about upgrading from IPSO 3.6 to IPSO 3.7 or later if you have a cluster configured with IPSO 3.6, and it also presents information about how to configure Check Point’s VPN-1 NG to work with an IPSO cluster.

IP Clustering Description
IPSO 3.6 and later lets you create firewall/VPN clusters that provide fault tolerance and dynamic load balancing. A cluster consists of multiple appliances (nodes) that share common IP addresses, and it appears as a single system to the networks connected to it.
A cluster continues to function if a node fails or is taken out of service for maintenance purposes. The connections being handled by the failed node are transferred to one of the remaining nodes.

IPSO clusters are also scalable with regard to VPN performance—as you add nodes to a cluster, the VPN throughput improves.

IPSO clusters support a variety of Check Point VPN-1 NG AI features, including:

- Synchronizing state information between firewalls
- Firewall flows
- Network address translation
- VPN encryption

**Note**
All cluster nodes must run the same versions of IPSO and VPN-1 NG.

**Note**
The IP2250 appliance does not support IP clustering.

**Example Cluster**

The following diagram shows a cluster with two nodes, firewall A and firewall B. The cluster balances inbound and outbound network traffic between the nodes. If an internal or external interface on one of the nodes fails, or if a node itself fails, the existing connections handled by
the failed node are not dropped—the other node processes them. The other node continues to function and handle all of the traffic for the cluster.

Routers connected to an IPSO cluster must have appropriate static routes to pass traffic to the cluster. In this example:

- The external router needs a static route to the internal network (192.168.1.0) with 192.168.2.10 as the gateway address.
- The internal router needs a static route to the external network (192.168.2.0) with 192.168.1.10 as the gateway address.

The IP addresses shown in boldface are cluster IP addresses, addresses shared by multiple interfaces in the cluster.

IPSO uses the cluster protocol networks shown in the diagram for cluster synchronization and cluster management traffic. If a primary cluster protocol interface fails on a node, the node uses its secondary cluster protocol interface, and service is not interrupted.

**Note**
Nokia recommends that these networks be dedicated to this purpose (as shown here). The ideal configuration is to physically separate the cluster protocol networks from the...
production networks. This configuration is preferable to using separate VLANs on one switch to separate them.

IPSO’s cluster management features allow you to configure firewall A and B as a single virtual device, and IPSO also lets you easily set up automatic configuration of cluster nodes.

In this and similar diagrams, switches and hubs are not shown for the sake of simplicity.

**Cluster Management**

You can manage all the nodes of a cluster simultaneously by using *Cluster Voyager*. This is a feature that lets you configure a cluster as a single virtual device. You can make configuration changes once and have them take effect on all the cluster nodes. You can also use the *Cluster CLI* (CCLI) to manage a cluster, and much of the information in this section applies to the CCLI as well. See the *CLI Reference Guide for IPSO* for more information about the CCLI.

The following list explains the difference between Voyager/CLI and Cluster Voyager/CCLI:

- Voyager and the CLI manage a single IPSO system.
- Cluster Voyager and the cluster CLI manage multiple clustered IPSO systems as if they are a single system.

This diagram illustrates the difference.

Any changes you make in Voyager or Cluster Voyager are immediately reflected in the CLI and CCLI. The reverse is also true—settings made in the CLI or CCLI are immediately reflected in Voyager or Cluster Voyager.

**Cluster Terminology**

This section explains the terms used in IPSO clustering. When applicable, it references the example cluster.

**CCLI:** Cluster CLI—A feature that lets you centrally manage all the nodes in a cluster as a single virtual system using one command-line session.
Cluster administrator: When you log into a Nokia appliance with the user name **cadmin**, you log in as a cluster administrator.

- If you are using a browser, the system displays Cluster Voyager.
- If you are using the command shell and enter **clish**, the system starts the CCLI.

Cluster ID: A user-specified number that uniquely identifies the cluster within the broadcast domain. Every node shares this ID number. The range is 0 to 65535.

If there is more than one cluster in the same network, each cluster must have a unique ID. In the example cluster, the ID is 10.

Cluster IP address: A unicast IP address that every node in the cluster shares. Each interface participating in a cluster must have an associated cluster IP address.

The example cluster has four cluster IP addresses:

- 192.168.1.10 is the cluster IP address of the internal interfaces.
- 192.168.2.10 is the cluster IP address of the external interfaces.
- 192.168.3.10 is the cluster IP address of the primary cluster interface.
- 192.168.4.10 is the cluster IP address of the secondary cluster interface.

Cluster MAC address: A MAC address that the cluster protocol installs on all nodes. Only the cluster master responds to ARP requests that routers send to cluster IP addresses. The cluster MAC address makes the cluster appear as a single device at the OSI layer two level.

Cluster master: The master node plays a central role in balancing the traffic among the cluster nodes. The cluster determines which node is the master according to the following criteria.

- In forwarding mode the master receives all the incoming packets and may forward them to the other nodes for processing.
  
  In this mode the master is the active node with the highest performance rating. If performance ratings are equal on all nodes, the master is the first node of the cluster.

- In the multicast modes, all the nodes receive all the incoming packets. The master determines which nodes should process each packet and provides that information to the other nodes. Nodes simply drop packets that they should not process.

  In these modes, the master is the node that joins the cluster first.

**Note**

See "Clustering Modes" for more information about this feature.

Cluster member: A cluster node that is not the master.

Cluster node: Any system that is part of a cluster, regardless of whether it is a member or the master.

Cluster protocol networks/interfaces: The cluster protocol networks are used for cluster synchronization and cluster management traffic. You create these networks by connecting cluster protocol interfaces. You must create a primary cluster protocol network, and Nokia recommends that you also create a secondary cluster protocol network for redundancy.
You specify which interfaces are cluster protocol interfaces by selecting from the configured Ethernet interfaces. (Only Ethernet interfaces can participate in a cluster.)

**Note**
These interfaces should be internal, and Nokia also recommends that you use separate networks to carry cluster protocol traffic and production traffic. The ideal configuration is to physically separate the cluster protocol networks from the production networks (connect them using different switches). This configuration is preferable to using separate VLANs on one switch to separate them and is the configuration shown in the example cluster.

The cluster protocol interfaces can also be used for VPN-1 NG synchronization traffic. For more information about how to configure VPN-1 NG for clustering, see “Configuring VPN-1 NG for Clustering.”

The following list explains the roles of primary and secondary cluster interfaces:

- **Primary cluster protocol network/interface:** Each node must be connected to the primary cluster protocol network. The interface a node uses to connect to this network is its primary cluster protocol interface. In the example cluster, the primary interface is eth-s3p1.

  If you do not use a dedicated network as the primary network—that is, if the primary network all carries data traffic, see “If You Do Not Use a Dedicated Cluster Protocol Networks” and “Configuring VPN-1 NG for Clustering” for configuration information.

  If the primary interface fails on a node and you have not configured a secondary network, the node is removed from the cluster. If it is the master, one of the remaining nodes becomes the new master.

- **Secondary cluster protocol network/interface:** Each node may also be connected to an (optional) secondary cluster protocol network. The interface a node uses to connect to this network is its secondary cluster protocol interface. In the example cluster, the secondary interface is eth-s4p1.

  If a primary interface fails on a member, the cluster synchronization and management traffic fails over to the secondary interface. In this event, the other nodes are not affected—they continue to use their primary interfaces to communicate with the master. If a primary interface fails on the master, all the other nodes must use the secondary protocol network to communicate with the master.

  If the primary and secondary cluster protocol interface fails on a node, the node is removed from the cluster. If it is the master, one of the remaining nodes becomes the new master.

**Cluster Voyager:** A feature that lets you centrally manage all the nodes in a cluster as a single virtual system using one browser session.

**Joining:** When becoming part of a cluster, a system can copy a variety of configuration settings from another cluster node (so you don’t have to configure these settings manually). This is called *joining*. When a system joins a cluster, it copies the configuration settings of the join-time shared features. Joining saves you time by allowing you to configure one node and then have the other nodes copy the appropriate configuration settings when they join the cluster.
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 can be configured this way are called join-time shared features, meaning that their configurations can be shared across cluster nodes during the joining process.

Clustering Modes

IPSO clusters have three modes of operation. Nokia provides this choice so that IPSO clusters can work in any network environment:

- In multicast mode each cluster node receives every packet sent to the cluster and decides whether to process it based on information it receives from the master node. If the node decides not to process the packet (because another node is processing it), it drops the packet. This mode usually offers better throughput because it uses the bandwidth of the production networks more efficiently.

  Multicast mode uses multicast MAC addresses for each of the nodes. If you use this mode, routers and servers adjacent to the cluster (either connected directly or through a switch or hub) must be able to accept ARP replies that contain a multicast MAC address. Switches connected directly to the cluster must be able to forward packets destined for a single (multicast) MAC address out multiple switch ports. See “Considerations for Clustering” for more information about the requirements for routers and switches when using multicast mode.

  When you use this mode, the cluster MAC addresses are in the form 01:50:5A:xx:xx:xx, in which the last three bytes are the last three bytes of the appropriate cluster IP address in hexadecimal.

- Multicast mode with IGMP offers the benefits of multicast mode with an additional improvement. When you use multicast mode (without IGMP), the switches connected to the cluster broadcast the data frames sent to the multicast MAC addresses of the cluster (unless they are configured not to do so). This means that any other devices attached to the same switches as the cluster also receive the traffic that is sent to the cluster. If the switches perform IGMP snooping (elicit or listen for IGMP messages), you can prevent this from happening by using multicast mode with IGMP.

  When you use this mode, each cluster interface joins an IP multicast group, and IPSO bases the cluster multicast MAC addresses on the IP multicast group addresses. The cluster MAC addresses are in the form 01:00:5E:xx:xx:xx, in which the fourth byte is the cluster ID and the last two bytes are the last two bytes of the multicast group address.

  You can change the default IP multicast group addresses assigned by IPSO. If you do so, the new addresses must be in the range 239.0.0.0 to 239.255.255.255. (See RFC 2365 for information about this range of addresses.)

- In forwarding mode the master cluster node initially receives all the packets sent to the cluster and decides which node should process the packet. If it decides that another node should handle the packet, it forwards the packet to that node. Otherwise, the master processes the packet itself.
Use forwarding mode if the routers and switches on either side of the cluster do not support multicast MAC addresses.

**Note**
All cluster nodes must use the same mode.

**Caution**
Avoid changing the cluster mode while a cluster is in service. If you change the cluster mode of a single node, the node leaves the cluster. If you change the mode on all the nodes (using Cluster Voyager or the CCLI), the cluster dissolves and reforms and is out of service temporarily.

### Considerations for Clustering

**Note**
For information about the requirements for using VPN-1 NG in an IPSO cluster, see “Configuring VPN-1 NG for Clustering.”

When you configure an IPSO cluster, take into account the considerations explained in the following sections.

#### Network Environment
- You can use static routing, OSPF, BGP, or PIM to forward traffic through a cluster.
  - If you use static routing, devices that need to send traffic through a cluster must have a static route that uses the appropriate cluster IP address (internal or external) for the route’s gateway address. For example, a router on the internal side of a cluster should use an internal cluster IP address as the gateway address.
  - You cannot use OSPFv3 in a cluster.
  - If you use OSPF, only the master exchanges OSPF messages with the external routers.
  - A cluster cannot use OSPF or BGP to forward traffic over VPN tunnels.
  - If you use PIM, see “PIM Support for IP Clustering” in the PIM documentation for details about how to configure it.
- The following items apply if you use BGP with a cluster:
  - BGP runs only on the master node. If a failover occurs, BGP stops running on the failed master and establishes its peering relationships on the new master.
  - You must configure a cluster IP address as a local address.
  - Nokia recommends that you configure BGP so that peer traffic does not run on the cluster protocol interfaces.
Caution
Nokia strongly recommends that you not configure a routing protocol on the primary or secondary cluster protocol interfaces.

- If you use a multicast mode, adjacent devices (either connected directly or through a switch or hub) must be able to accept ARP replies that contain a multicast MAC address. See “Changing ARP Global Parameters” in the information about configuring interfaces for instructions about how to configure a Nokia appliance to accept these replies.

Note
If there is no router between the cluster and host systems (PCs or workstations), the hosts must be able to accept ARP replies with multicast MAC addresses. You can avoid this requirement by adding a static ARP entry to each host that includes the cluster IP address and multicast MAC address of the internal cluster interface.

- If you use a multicast mode, the switches connected to the cluster nodes must be able to forward packets destined for a single (multicast) MAC address out multiple switch ports simultaneously. Many switches do this by default.
- If you use a two-node cluster, use switches (recommended) or hubs to connect the cluster protocol networks. This will ensure proper failover in the event that one of the nodes drops out of the cluster. Do not directly connect the cluster protocol interfaces using a crossover cable.
- For performance purposes, Nokia recommends that you do not use hubs to connect a cluster to user data networks. If possible, use switches for these connections. (If you need to troubleshoot a cluster that uses a multicast mode, you might want to temporarily replace switches with hubs to simplify your configuration.)
- You can create multiple clusters in the same LAN or VLAN (broadcast domain). The clusters are distinguished by their cluster IDs.

Other Considerations
- If a cluster will be in service as soon as it is activated, you should configure and enable VPN-1 NG on each node before they become part of the cluster. Add nodes to the Check Point cluster (using Check Point software) after they have successfully joined the IPSO cluster.
- Transparent mode is not supported on cluster nodes.
- Router services are not supported, with the exception of NTP.
- An IPSO system cannot participate in more than one cluster at one time.
- IPSO clusters support:
  - Multiple internal and external network connections
  - 10/100 mb or gigabit Ethernet LAN connections
  - The primary and secondary cluster protocol networks should have bandwidth of at least 100 mbps.
- IPSO clusters do not support network types other than Ethernet.
  All of the interfaces on a cluster node do not have to participate in the cluster. Interfaces that
do not participate in the cluster can be network types other than Ethernet.
- All the nodes must have the same number of interfaces participating in the cluster, and the
  cluster interfaces must be connected to the same networks.
- If you configure Gigabit Ethernet interfaces on different IP cluster nodes with different
  MTU values and also run OSPF in the cluster, OSPF routes are lost if a failover occurs
  between the nodes with different MTU values. To prevent this problem, make sure that the
  MTU values are the same on all cluster nodes with Gigabit Ethernet interfaces.

**If You Do Not Use a Dedicated Cluster Protocol Networks**

If you do not use separate networks for cluster protocol traffic and production traffic, IPSO’s
cluster protocol messages are propagated throughout the production networks. This happens
whenever you use the same physical links for cluster protocol traffic and production traffic—that
is, it occurs even if you use VLANs (trunking) to segregate the traffic. This is an unproductive
use of bandwidth because cluster protocol messages are used only by IPSO cluster nodes.

You can prevent the cluster protocol messages from being spread across the production networks
by using multicast mode with IGMP and connecting the networks with switches that use IGMP
snooping. You usually need to enable IGMP for specific switch ports or VLANs.

IPSO sends out IGMP membership reports for the cluster protocol multicast group. A switch
using IGMP snooping will then forward cluster protocol messages only to group nodes—that is,
the other cluster nodes. It will not forward the cluster protocol traffic to ports that are not
connected to cluster nodes.

**Note**

If you enable IGMP snooping on the switch, also enable IGMP queries and set a query
interval of 30 or fewer seconds. If you enable IGMP snooping but do not enable queries,
problems can occur when a system leaves and rejoins a cluster.

The ideal configuration is to physically separate the production and cluster protocol networks
(connect them using different switches). If you configure a cluster this way, the cluster protocol
messages will not appear on your production networks even if the switches on the data networks
do not support IGMP snooping. This configuration is preferable to using separate VLANs on
one switch to separate the networks.

**Upgrading IPSO in a Cluster**

**For All Upgrades**

When upgrading a cluster, make sure that all the nodes run the same versions of IPSO (and
VPN-1 NG, when appropriate). If you are upgrading both IPSO and VPN-1 NG, you should first
upgrade IPSO on all the nodes and then upgrade VPN-1 NG. This approach provides the best
continuity of service during the upgrade process.
Upgrading from IPSO 3.7 or Later

If you want to upgrade a cluster from IPSO 3.7 or later to a later version of IPSO, Nokia recommends that you use Cluster Voyager to upgrade the IPSO image on all the cluster nodes. See the instructions in “Installing IPSO images.”

The upgraded nodes retain any cluster configuration information that was created with the earlier version of IPSO.

The hash selection is not used by IPSO 3.8 and NG AI and no longer appears in the Clustering Setup Configuration page. Depending upon how you upgrade to IPSO 3.8 and NG AI, you might temporarily see this option. If you do you can safely ignore it. Once the upgrade is complete and IPSO has verified that NG AI is running, the option disappears.

Upgrading from IPSO 3.6

Upgrading a cluster from IPSO 3.6 to IPSO 3.7 or later requires a different process because IPSO 3.6 does not have cluster management functionality.

If you want to upgrade cluster nodes from IPSO 3.6 to IPSO 3.8, Nokia recommends that you first upgrade all the nodes to IPSO 3.7 and then upgrade to 3.8. Following this process allows the cluster to remain in service throughout the upgrade. The upgraded nodes retain any cluster configuration information that was created with the earlier version of IPSO.

Note
Make sure that you use a version of VPN-1 NG that is compatible with the IPSO version that you upgrade the cluster to. If you are using an incompatible version of VPN-1 NG, upgrade to a compatible version after you upgrade to the later version of IPSO. See the IPSO Release Notes and Getting Started Guide to find out which versions of VPN-1 NG are compatible with the version of IPSO you are installing.

A cluster functions if its master runs IPSO 3.6 and one or more nodes run IPSO 3.7 or later, but Nokia strongly recommends that you upgrade all the nodes of your IPSO 3.6 clusters. IPSO supports a 3.6 master with 3.7 or later members to allow a cluster to remain in service during an upgrade.

To upgrade IPSO on cluster nodes and ensure that there are the minimum number of master transitions, follow the steps below. This procedure assumes that you are upgrading a three-node cluster in which node C is the master. Under this procedure, two cluster nodes are in service at all times.

Note
You should upgrade the master last.

1. Upgrade node A and restart it.

   B and C continue to function as a 3.6 cluster. Node A (running the later version of IPSO) rejoins the cluster as a member.
2. Upgrade node B and restart it.
   Node C continues to function as a 3.6 cluster. Node B (running the later version of IPSO) rejoins the cluster as a member.

3. Make sure that nodes A and B have successfully restarted and rejoined the cluster.

   **Note**
   Performing this steps ensures that there will be no interruption in service when node C restarts.

4. Upgrade node C and restart it.
   When node C begins to restart, node A or B is selected as the new master and both nodes continue forwarding traffic. When node C completes the process of restarting, it joins the new cluster.

### Enabling Cluster Management

After you complete the upgrade process, the cluster is active but you cannot use Cluster Voyager or the CCLI until you create a password for the cadmin user on each of the cluster nodes. After you upgrade IPSO on the cluster nodes, perform the following procedure to create a password for the cadmin user on each of the nodes.

1. Click Config on the home page.
2. Click Clustering Setup in the Traffic Management section.
   The Clustering Setup Configuration page appears.
3. Click Change cadmin password.
   The Cluster Management Configuration page appears.
4. Enter a password for the user cadmin.

   **Note**
   You must use the same password on each node that you add to the cluster. This is also the password that you use to log into Cluster Voyager or the CCLI.

5. Enter the password for cadmin again (for verification).
6. Click Apply.
   The page displays fields for changing the cadmin password. Use this page if you want to change this password in the future.
7. Repeat this procedure on each of the other nodes that you upgraded from IPSO 3.6.
You can now manage the cluster using Cluster Voyager or the CCLI.
Creating and Configuring a Cluster

Configuration Overview

To create and configure a cluster, follow these basic steps:
1. Create a cluster on the first node.
2. Select the cluster mode.
3. Configure the cluster interfaces.
4. Enable or disable firewall monitoring, as appropriate:
   - If VPN-1 NG is running on the node, enable VPN-1 NG monitoring before you make the cluster active.
   - If VPN-1 NG is not running on the node, disable VPN-1 NG monitoring before you make the cluster active (so that the cluster can be initialized). After the cluster is active, enable the monitoring so that the cluster monitors the firewall and leaves the cluster if the firewall fails on the node.
5. Deselect any features that should not be cluster sharable.
6. Change the cluster state to up.
7. Save the cluster configuration to disk.
8. If you disabled firewall monitoring in step 4, re-enable it.
9. Create cluster configurations on the other nodes.
10. Join the other nodes to the cluster.

The failure interval and performance rating are set by default on each node and generally should not be changed. See “Configuring the Failure Interval” and “Configuring the Performance Rating” for more information about these features.

You must also configure the VPN-1 NG to work with the IPSO cluster. Use the Check Point client application to add a gateway object for the Nokia appliance. You also must create a gateway cluster object and add the gateway object to it. Refer to the Check Point documentation and “Configuring VPN-1 NG for Clustering” for details.

Creating a Cluster

1. Click Config on the home page.
2. Click Clustering Setup in the Traffic Management section. The Clustering Setup Configuration page appears.
3. Enter a cluster ID (0-65535).
4. Enter a password for the user cadmin.
   The password must have at least six characters.
Note
You must use the same password on each node that you add to the cluster. This is also the password that you use to log into Cluster Voyager or the CCLI.

5. Enter the password for cadmin again (for verification).
6. Click Apply.
7. Click Manually Configure IPSO Cluster.
   Configure the cluster as explained in the following sections.

Selecting the Cluster Mode
Select the cluster mode that is appropriate for your scenario:

- If the routers and switches on either side of the cluster support multicast MAC addresses, you can use multicast mode or multicast mode with IGMP. These modes usually offer better throughput because they make better use of the bandwidth of the production networks.
- If the routers or switches adjacent to the cluster do not support multicast MAC addresses, you must use forwarding mode.

Configuring the Work Assignment Method
A cluster initially balances its work load by automatically distributing incoming traffic between the nodes. Use the work assignment setting to govern whether the cluster can rebalance the load of active connections by moving them between nodes.

- For optimum load balancing, use the dynamic setting. This setting allows the cluster to periodically rebalance the load by moving active connections between nodes.
- Setting the work assignment to static prevents the cluster from moving active connections between nodes. Some Check Point applications and features require “bidirectional stickiness,” which means that all the packets for a given connection must be processed by the same node. If you use any of these applications and features, you must also set the work assignment to static for them to work properly. See Check Point’s document ClusterXL: NG with Application Intelligence for information about which applications and features require bidirectional stickiness. (Floodgate-1 and the Sequence Verifier feature of NG require this setting.)

You must use static work assignment if you are using IP pools with non-Check Point gateways or clients. See “Supporting Non-Check Point Gateways and Clients” for related information.

If any of the requirements for static work assignment apply to your cluster, you should use this setting. For example, you should use static work assignment if your cluster supports both of the following:

- VPNs with Check Point gateways (static work assignment not required)
- VPNs with non-Check Point gateways with IP pools (static work assignment required)
Configuring an Interface

To activate the cluster protocol, you must select at least two Ethernet interfaces. One of the two must be an internal or external interface (not a primary or secondary cluster interface). The other interface must be the primary interface.

**Note**
Nokia recommends that you select another interface as a secondary cluster protocol interface. Remember that the primary and secondary cluster protocol networks should not carry any production traffic.

The Interfaces Configuration table lists all the Ethernet interfaces on the system that are configured with IP addresses. The table displays the status and IP address of each interface. To add Ethernet interfaces to this list or to activate inactive interfaces, go to the Interface Configuration page.

**To include an interface in the cluster**

1. In the Select column, select Yes.
2. Enter the cluster IP address.
   The address must be in the same network as the IP address of the interface you are configuring. This is a common IP address that each node will share.
3. Repeat the above steps for the rest of the interfaces that will participate in the cluster.
4. For the interface that will serve as the primary cluster protocol interface for the node, click the Yes button in the Primary Interface column.
   The primary interfaces of all the cluster nodes must belong to the same network. This network should not carry any other traffic.
5. For the interface that will serve as the secondary cluster protocol interface for the node, click the Yes button in the Secondary Interface column.
   The secondary interfaces of all the cluster nodes must belong to the same subnet. This subnet should not carry any other traffic unless you use it to carry firewall synchronization traffic. (See “Configuring VPN-1 NG for Clustering” for information about selecting the firewall synchronization network.) Secondary interfaces are optional.
6. If you are using multicast with IGMP mode and do not want to use the default IP multicast group address, enter a new address in the range 239.0.0.0 to 239.255.255.255.
7. Click Apply.

**Configuring Firewall Monitoring**

Use the option Enable VPN-1 NG/FW-1 monitoring? in the firewall table to specify whether IPSO should wait for VPN-1 NG to start before the system becomes a node of a cluster—even if it is the only node of the cluster. (This is particularly relevant if a cluster node is rebooted while it is in service.) This option also specifies whether IPSO should monitor VPN-1 NG and remove the node from the cluster if the firewall stops functioning.
To enable firewall monitoring, click enable next to Enable VPN-1 NG/FW-1 monitoring? in the firewall table.

If VPN-1 NG is not running at the time you change the cluster state to up, click Disable next to Enable VPN-1 NG/FW-1 monitoring? If VPN-1 NG is not running and you do not disable firewall monitoring, you cannot initialize the cluster protocol.

**Note**
Be sure to enable firewall monitoring before you put the cluster into service (assuming that you are using VPN-1 NG).

**Supporting Non-Check Point Gateways and Clients**
If your IPSO cluster will create VPN tunnels with non-Check Point gateways or clients, Click the option for enabling non-Check Point gateway and client support on the Clustering Setup Configuration page and then perform the following procedure:

1. If you want to support non-Check Point clients, click the option for enabling VPN clients. This is all you have to do.
2. If you want to support non-Check Point gateways, enter the appropriate tunnel and mask information, as explained in “Configuring VPN Tunnels.”
3. If you want to support IP pools, follow the instructions in “Configuring IP Pools In Cluster Voyager.”

**Note**
If you want to support VPNs with remote non-Check Point gateways, do not check the “Support non-sticky connections” option for these connections in Check Point’s Smart Dashboard.

**Configuring VPN Tunnels**
If you want the cluster to support VPN tunnels in which non-Check Point gateways participate, you must configure the tunnels in Voyager (on the Clustering Setup Configuration page) as well as in VPN-1 NG. Perform the following procedure:

1. In the Network Address field under Add New VPN Tunnel, enter the remote encryption domain IP address in dotted-decimal format (for example, 192.168.50.0).
2. In the Mask field, enter the mask value as a number of bits. The range is 8 to 32.
3. In the Tunnel End Point field, enter the external address of the non-Check Point gateway.
4. Click Apply.
   The VPN Tunnel Information table appears and displays the information you configured.
5. If there is more than one network behind the non-Check Point gateway, repeat these steps for each network. In each case, enter the external address of the non-Check Point gateway as the
tunnel end point. If one of the networks behind a non-Check Point gateway is not encrypted (for example, a DMZ), set its end point to 0.0.0.0.

**Note**
See “Clustering Example With Non-Check Point VPN” for an example of configuring a cluster to support a VPN with a non-Check Point gateway.

**Using IP Pools**

IPSO clusters support the use of IP pools (address ranges), which are useful for solving certain routing problems. For example, you might want to use an IPSO cluster (and VPN-1 NG) to create a VPN but not want to route unencrypted traffic through the cluster. For this purpose, you can use a configuration similar to the one shown in the following diagram:

The purpose of this configuration would be to route the outgoing unencrypted traffic through the default gateway and route the outgoing encrypted traffic through the cluster. Traffic that passes through the cluster is NATed so that the source address of a packet is translated to one of the addresses in the IP pool of the cluster node that handles the connection.

How you configure IP pools depends on whether a non-Check Point gateway participates in the VPN:

- If the other end of the tunnel is also a Check Point gateway, you do not need to configure the IP pools in IPSO. Simply follow the instructions in “Using IP pools when only Check Point gateways are involved.”
If the other end of the tunnel is not a Check Point gateway, you must follow the instructions in “Using IP pools when only Check Point gateways are involved” and also configure the IP pools in IPSO, as explained in “Configuring IP Pools In Cluster Voyager.”

Using IP pools when only Check Point gateways are involved To set up the configuration shown in the previous diagram, you would:

- Configure the IP pools in VPN-1 NG.
- On the internal router:
  - create a default route to the Internet with 192.168.1.1 (the default gateway) as the gateway address.
  - create static routes to the IP pool networks with the internal cluster IP address (192.168.1.10) as the gateway address. Do not use the real IP addresses of the internal cluster interfaces (192.168.1.2 and 192.168.1.3) as gateway addresses. In the example network, the internal router has the following static routes:
    - route: 10.1.2.0/24, gateway: 192.168.1.10
    - route: 10.1.3.0/24, gateway: 192.168.1.10

Configuring IP Pools In Cluster Voyager If you want to use IP pools with a VPN in which a non-Check Point gateway participates, you must configure the pools in IPSO as well as in VPN-1 NG. You must configure all the pools on all the nodes, so it is easiest and less error prone to use Cluster Voyager (or the CCLI) for this task. To configure IP pools in Cluster Voyager, follow this procedure after you enable support for non-Check Point gateways:

1. In the Network Address field under Add New IP Pool, enter the network that the IP pool addresses will be assigned from.
   
   If you were configuring firewall A in the cluster shown in the previous diagram, you would enter 10.1.2.0.

   **Note**
   To ensure routing symmetry, the IP pool networks must be different on different cluster nodes.

2. In the Mask field, enter the appropriate subnet mask.
   
   If you were configuring firewall A in the cluster shown in the previous diagram, you would enter 24.

3. In the Member Address field, enter the real IP address of the primary cluster protocol interface.
   
   If you were configuring firewall A in the cluster shown in the previous diagram, you would enter 192.168.3.1.

Configuring 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 system joins (or rejoins) the cluster. In this case, the joining system receives the settings of the shared features.
- A new master is selected. In this case, all the members receive the settings of the shared features from the master. This occurs in either mode when the original master leaves the cluster (for example, if it is rebooted). It can also occur in forwarding mode if you manually adjust the performance rating or if a system with a higher rating becomes the new master. See “Configuring the Performance Rating” for more information.

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

The list of shared features should be specified *only* when you set up a cluster. Once the cluster is operational, you should avoid changing which features are cluster sharable. The basic approach to follow is:

1. Configure the first node.
2. Join the other systems to the first node so that they all copy the shared settings from the same source.

**What is Sharable?**

Join-time shared features are not directly related to clustering itself. They are features used on an IPSO system regardless of whether it is part of a cluster. For example, if you want each cluster node to have the same static routes, you configure the static routes on the first cluster node and make sure that static routes are selected as a sharable feature. When other nodes become part of the cluster, those routes are configured on them also.

If the system that is joining the cluster already has static routes configured, they are retained. The routes copied as a result of the joining process are added to the list of static routes.

**What if Settings Conflict?**

If there is a conflict between configuration settings on the existing node and the joining system, the settings on the joining system are changed to those of the master node. For example, assume that you have a cluster with nodes A (the master) and B in which DNS is a shared feature and the domain name on node A is company-name.com. If a third node (C) joins the cluster and its domain name is foobar.com before it joins, foobar.com is replaced by company-name.com during the joining process.

If you change the domain name on node C back to foobar.com, the domain name remains foobar.com unless any of the following occurs:

- node C leaves and rejoins the cluster
- node B becomes the master
- a *cadmin* user changes the domain name (while logged into any node)
In the first two situations, node C will once again copy the settings for all the join-time shared features, and company-name.com will replace foobar.com as the domain name. In the third situation, the domain name is changed on all the nodes.

If you want to be able to easily reset the configuration of node C to what you had configured manually, simply save the desired configuration on C. If the active configuration changes because of join-time sharing, you can reload the desired configuration on C from the saved configuration file. See “Managing Configuration Sets” for information about saving and loading configuration files.

If node C becomes the master in the previous example, then its settings for join-time shared features are copied to the other nodes. For example, foobar.com would replace company-name.com on nodes A and B.

---

**Caution**

Be aware that if node C becomes the master in this scenario, its settings override conflicting settings on the other nodes, which could result in configuration issues. The best practice is to avoid conflicts in the configurations of join-time shared features.

---

If a feature on a joining system has a setting and the feature is not configured on the master, the joining system retains its setting. For example, assume that you have a two node cluster in which DNS is a shared feature but no domain name is configured on the master. If a third system joins the cluster and its domain name is foobar.com before it joins, it retains that domain name after it joins.

**Configuring Features for Sharing**

Follow these steps to ensure that the appropriate configuration settings are identical on each cluster node:

1. After you create a cluster configuration on the first node, make sure all the relevant settings are correct (on the Clustering Setup Configuration page).
2. Scroll to the bottom of the Clustering Setup Configuration page and click No next to any features that should not share settings across the cluster.

---

**Caution**

After you click Apply (the next step), you cannot conveniently make features sharable again if you make them unshared in this step. Make sure that the settings are correct before you proceed.

---

3. Click Apply.

If you want to make more features unshared after you click Apply, simply click No next to them and click Apply again. If you change your mind and want to share features that you previously chose not to share, you must delete the cluster and create a new one with the desired settings.
Once the cluster is active, you see the following message each time you log into a cluster node as admin and navigate to a configuration page of a feature that is cluster sharable:

This feature is associated with cluster id 10.

Any changes made would be local to this cluster node only.

The changes may be overwritten by cluster configuration.

This message alerts you that settings for this feature can be changed by a cluster administrator.

**After You Create a Cluster**

Whenever you use Cluster Voyager (or the CCLI), you can remove features from the list of ones that are cluster sharable. You can do this on any node. However, Nokia recommends that you avoid doing this. You should set up the appropriate feature sharing when you create a cluster and then leave it unchanged.

If a feature is shared and you want to reconfigure it on all the cluster nodes, use Cluster Voyager or the CCLI. Any changes you make are implemented on all the nodes automatically.

**Making the Cluster Active**

Nokia recommends that you configure a firewall and or VPN on the node before you activate the cluster. For more information, see Check Point FW-1 documentation and “Configuring VPN-1 NG for Clustering.”

---

**Note**

If you do not configure a firewall on the node before you activate the cluster, you must click disable next to Enable monitoring of FW-1/VPN-1 NG? before you activate the cluster. After the cluster is active, change this setting to enable. When this is set to ENABLE, the cluster monitors the firewall. If the firewall fails on a node, that node drops out of the cluster and stops forwarding traffic.

Before you activate the cluster, click Save to store all the cluster configuration settings in the configuration database on the hard disk.

To make the cluster active, click Up in the Cluster State field of the Cluster Status table.

You can make the cluster active only if the node has:

- No VRRP or router services
- At least two configured interfaces participating in the cluster, including one primary interface

You receive error messages if the node does not meet these requirements.

**Adding a Node to a Cluster**

It is very easy to add Nokia appliances to an existing cluster. There are two methods you can use:

- Joining (automatic configuration). This is the recommended method because:
The only tasks you must do on the joining systems are:

- Configure interfaces with IP addresses in each of the networks the cluster will connect to
- Supply an IP address (a real addresses or a cluster IP address) that is already part of the cluster when joining the cluster

Manual configuration. If you use this method, you must supply more information so that the system can join the cluster. Manually adding nodes is very similar to the process of creating a cluster configuration on the first node, and you must make sure to enter the appropriate settings identically to how you entered them on the first node.

If you add a node manually, do not make any changes under Join-Time Shared Feature Configuration.

You might want to add a node manually if both of the following conditions are true:

- The existing nodes are running VPN-1 NG and firewall monitoring is enabled on them.
- VPN-1 NG is not running on the system you are adding.

If you try to add the system to the cluster using the join method under these conditions, it will not join because VPN-1 NG is not running on it. In this situation you could manually add the system to the cluster by disabling its firewall monitoring.

Caution
For security reasons, you should never add a system that is not running VPN-1 NG to a cluster that is in service. This should only be done in a test environment.

Recommended Procedure

Nokia recommends that you follow this general procedure when building a cluster:

1. Fully configure the first cluster node and make sure that all the appropriate features are cluster sharable.
2. Make sure that all of the join-time shared features are configured appropriately on the first node.
   Remember that joining nodes inherit the configuration settings for each cluster sharable feature.
3. Create a cluster on another system.
4. Join the other system to the cluster.

Note
This is the most efficient approach to building a cluster and will configure all the cluster nodes consistently.
Joining a System to a Cluster

To join a system to a cluster, perform this simple procedure:

1. On the main configuration page, click Interfaces to display the Interface Configuration page.
2. Configure interfaces with IP addresses in each of the networks used by the cluster and activate the interfaces.
3. Click Top.
4. Under Traffic Management Configuration, click Clustering Setup to display the Clustering Setup Configuration page.
5. Enter the ID of the existing cluster.
6. Enter the password for the user cadmin in both password fields.

Note
This must be the same password that you entered for cadmin when you created the cluster on the first node.

7. Click Apply
8. In the Cluster node address field, enter an IP address that meets the following criteria:
   - You should use an address of an interface on the cluster node that you configured first.

Note
Using an interface on the first system that you configured for clustering each time you join another system will make sure that all nodes are configured appropriately.

- The interface must be one of the cluster interfaces.
- You should use the “real” address of the interface—not its cluster IP address. (If the cluster is in forwarding mode and you supply a cluster IP address for joining purposes, the joining system will copy configuration settings from the master node, which might not be the one you want to copy the settings from.)

9. Click Join.
   - If the node successfully joins the cluster, Voyager displays a number of new fields.
   - If the node does not successfully join the cluster, you see a message indicating why. Correct the problem and attempt the join again.

Managing a Cluster

You can choose between two different approaches to making configuration changes on cluster nodes:
You can make changes that are implemented on all the nodes simultaneously. To make changes in this way, you use Cluster Voyager or the CCLI. (See the IPSO CLI Reference Guide for information about using the CCLI.)

**Note**
Nokia recommends that you use Cluster Voyager or the CCLI to change cluster settings or to make changes to join-time shared features.

You can make configuration changes on individual nodes. If you want to make the same changes on other nodes, you must log into them (as admin) and make the same changes. There are some features that can be modified only by logging into individual nodes as admin. These are explained in “Removing a Node from a Cluster,” “Changing Cluster Interface Configurations,” and “Deleting a Cluster Configuration.”

**Caution**
If a feature has been specified as cluster sharable and you change its configuration while logged into a node as admin, the change is implemented on that node only. Making changes this way can lead to confusing or inconsistent configurations.

### Using Cluster Voyager

#### Starting Cluster Voyager

**To start Cluster Voyager**

1. In your browser’s address or URL field, enter an IP address of a system that is participating in the cluster or the appropriate shared cluster IP address (for example, the internal cluster IP address).

   If you enter a shared cluster IP address, the master node responds.

2. Enter the user name cadmin and the password for cadmin.

**Note**
If you forget the cadmin password, follow the instructions in “If you forget the cadmin password.”

If either of the following conditions are true, you can log into Cluster Voyager, but you cannot make configuration changes unless you break the configuration lock:

- Someone else is logged into one of the cluster nodes as admin (using Voyager or the CLI) and has acquired an exclusive configuration lock
- Someone else is logged into Cluster Voyager or the CCLI and has acquired an exclusive configuration lock
If someone else has acquired an exclusive configuration lock when you attempt to log in and acquire a lock, Voyager will display a “permission denied” message and ask you to log in again. If you want to break the lock acquired by the other user, see “Network Voyager Session Management Description” in the information about configuring security and access for more information.

**If you forget the cadmin password** If you forget the password for the cadmin user, you are not able to start Cluster Voyager. To recover from this situation, follow these steps:

1. Log into one of the cluster nodes as admin using a command line session.
2. Start the CLI by entering `clish`
3. Enter `set user cadmin oldpass "" newpass new_password`
   The new password must have at least six characters.
4. Log out of the CLI by entering `exit`
5. Repeat step 1 through step 4 on the other cluster nodes.
6. Log into Cluster Voyager using the new password.

**Monitoring a cluster**

If you click Monitor on the Cluster Voyager home page, you see a number of links to pages that you can use to monitor the status of the cluster. These pages present status information for all the nodes. For example, the IPSO Cluster Process Utilization page shows the status of processes on each node.

**Configuring the Failure Interval**

The failure interval is used to determine whether a node should leave the cluster because it cannot synchronize quickly enough with the other nodes. If a node does not receive cluster protocol information (over the primary or secondary cluster protocol network) for this length of time, it leaves the cluster and attempts to rejoin it. You might need to adjust this value if congestion on the primary or secondary network causes nodes to repeatedly leave and rejoin the cluster (though the cluster protocol attempts to prevent this situation by sending data at shorter intervals if it detects delays).

To change the number of milliseconds the node waits before assuming cluster breakup, enter a number in the Failure Interval field, then click Apply and Save.

**Configuring the Performance Rating**

The performance rating is a measure of a cluster member's throughput and performance capabilities. The higher the rating, the more work a cluster member is capable of doing.

In forwarding mode, cluster members use the performance rating to elect the best performing system as the master. The cluster master receives all the packets for the cluster first, so the
performance of the master affects the performance of the whole cluster. If a joining system has a higher rating than the other nodes, it becomes the master. If more than one system have the same performance rating, the first system to join the cluster is the master.

The cluster master takes the performance rating of the members into account when assigning workload (in all modes). Nodes with higher performance ratings receive a larger share of the workload than lower performing nodes.

The default performance rating for a system reflects its performance relative to that of other Nokia platforms. You can adjust the performance rating to change the amount of work a system is assigned relative to other members. If a cluster uses forwarding mode, you can adjust the performance rating to force a particular node to be the master (which will also have the effect of giving that node a larger share of work).

To change the performance rating, enter a number in the Performance Rating field (the range of values is 0 through 65535), then click Apply and Save.

If you change the master by adjusting the performance rating, or if the master changes because a joining system has a higher rating than the other nodes, the settings of join-time shared features are propagated across the cluster at that point. The settings on the new master are replicated on the other nodes.

**Note**

Do not change the performance rating of the master to 0. This will cause the traffic load to be distributed unequally across the cluster.

**Note**

After you click Apply, you might see a message that reads Joining in progress. If so, refresh your browser. The message disappears and you can proceed by clicking click Apply and then Save.

**Managing join-time shared features**

You can change the configuration settings of join-time shared features while logged in as admin or cadmin, but the results are different:

- When you log in as cadmin (and use Cluster Voyager or the CCLI) and change a setting of a shared feature, the change is made on all the nodes.

  For example, if static routes are shared and you add a static route while logged in as cadmin, the route is added to all the cluster nodes.

- When you log in as admin and change a configuration setting of cluster shareable feature, the change is implemented on the node you are logged into but not implemented on the other nodes. This is true even if you are logged into the master node.

  For example, if static routes are shared and you add a static route while logged in as admin, the route is added to the node you are logged into but not the other cluster nodes.
Changes made as `cadmin` overwrite any conflicting settings made by someone logged into an individual cluster node as `admin`. However, nonconflicting changes made as `admin` are not overwritten. For example, if you configure static routes on a node while logged in as `admin` and later add static routes as `cadmin`, the latter routes are added to the list of routes on that node. The original routes are unchanged.

**Note**
Nokia recommends that you do not make changes to cluster settings or join-time shared features on individual nodes—use Cluster Voyager or the CCLI to make these changes. This will help you ensure that all the nodes are configured consistently.

When you log in as `cadmin` and change a setting of a join-time shared feature, the change is made across the cluster *even if you did not share the feature when you created the cluster*. However, systems that join the cluster later do not copy the configuration settings for that feature.

When you make changes to features that you removed from the list of join-time shared features, you see the following message:

*This feature is not associated with cluster xxx.*

Any changes made would be propagated to all the cluster nodes.

This message is alerting you to the fact that the change will be implemented on all the current nodes but systems that join later will not implement the change.

**Note**
Some settings of cluster shareable features cannot be configured as `cadmin`. For example, you cannot use Cluster Voyager to set SSH host and identity keys. To configure these settings, you must log into the individual cluster nodes as `admin`.

### Installing IPSO images

**Note**
You cannot upgrade a cluster directly from IPSO 3.6 to IPSO 3.8 or later. You must upgrade from IPSO 3.6 to IPSO 3.7 and then upgrade to 3.8 or later.

If you want to upgrade a cluster from IPSO 3.7 or later to a later version of IPSO (or revert to the earlier version), Nokia recommends that you use Cluster Voyager to change the IPSO image on all the cluster nodes. To download and install an image in a cluster, follow these steps:

1. On the Cluster Configuration page, click *Install New IPSO Image (Upgrade)*.
2. Use the Cluster New Image Installation (Upgrade) page to download the new IPSO image.
If you specify an invalid FTP server or an invalid path to a valid server as the source of the image, Cluster Voyager does not respond with an error message and displays the following messages instead:

New Image installation in progress
Please don't perform a cluster reboot until all nodes have finished the upgrade.

If IPSO does not also display additional messages indicating that the download is proceeding (there might be a short delay), the FTP information might be incorrect. Correct the FTP information if required and begin the download again.

3. After the new image has been successfully installed on all the nodes, you need to reboot the nodes so that they will run the new image. When the system prompts you to reboot the cluster, click Manage IPSO images (including REBOOT).

4. On the IPSO Cluster Image Management page, click the Reboot button at the bottom of the page.

**Note**
Clicking this button allows you to perform a cluster safe reboot, which ensures that no traffic is dropped while the cluster reboots (see “Rebooting a cluster”). If you manually reboot each node by clicking the Reboot buttons associated with the individual nodes, there might be a period in which all the nodes are out of service.

5. On the Cluster Safe Reboot page, click Apply.

The upgraded nodes retain any cluster configuration information that was created with the previous version of IPSO.

**Rebooting a cluster**

When you click Reboot, Shut Down System on the main configuration page in Cluster Voyager, you see the Cluster Reboot, Shut Down System page. At the bottom of this page is the Cluster Traffic Safe Reboot link. If you click this link and then click Apply, the cluster nodes are rebooted in a staggered manner. The process is managed so that only one node is out of service at a time. For example, if you reboot a three-node cluster, one of the nodes controls the rebooting of the other nodes. This node is called the *originating node*.

The originating node reboots each of the other nodes in order. It waits until each node has successfully rebooted and rejoined the cluster before rebooting the next node. Once all the other nodes have rebooted and rejoined, the originating node reboots itself.

**Note**
The originating node is the node that you are logged into. It might not be the cluster master.
The following is an illustration of this process in a three node cluster with nodes A, B, and C, in which C is the originating node.

1. If the node A restarts successfully and rejoins the cluster, node B restarts.

   If node A does not reboot and rejoin the cluster successfully, the cluster reboot process is halted and the remaining two nodes continue functioning. You should investigate and resolve the problem that prevented node A from restarting and rejoining the cluster.

2. If node A successfully restarts and rejoins the cluster but node B does not complete the process, the cluster reboot process stops and nodes A and C continue functioning as a cluster.

3. If the nodes A and B complete the process, the node C restarts. As soon as it does, one of the other nodes becomes the originating node and the cluster continues to function.
   - If the node C restarts successfully, it rejoins the cluster.
   - If the node C does not restart successfully, the other two nodes continue to function as a cluster.

**Note**
Your Cluster Voyager session stays active throughout the process of rebooting the cluster. You can monitor the process by clicking Cluster Safe Reboot Status.

---

**Caution**
Do not log out of Cluster Voyager, end your browser session, or otherwise break your connection with the cluster while a cluster safe reboot is in progress. Doing so causes the nodes that you are not logged into to leave the cluster. (If you logged into Cluster Voyager using a cluster IP address, you are logged into the master.) If this occurs, manually rejoin the systems to the cluster.

You can also reboot all the cluster nodes simultaneously. In this case, your Cluster Voyager session does not stay active throughout the reboot process. To reboot all the nodes simultaneously:

1. On the main configuration page in Cluster Voyager, click Reboot, Shut Down System.
2. Click Reboot (do not click Cluster Traffic Safe Reboot).

**Removing a Node from a Cluster**

If you want to remove a node from a cluster, you must log into the individual node as `admin`.

1. On the Clustering Setup Configuration page, change the cluster state to down.
2. Click Apply.
   - The node leaves the cluster, but the cluster configuration information is saved.
3. To rejoin the node to the cluster, simply click Join.
Changing Cluster Interface Configurations

If you want to change the cluster interface configuration of a node—for example, if you want to change the primary interface—you must log into the node as admin. You cannot use Cluster Voyager or the CCLI.

Note
Any time you make a change to the cluster interface configuration, the node leaves and attempts to rejoin the cluster.

1. Log into the Voyager on the node as admin.
2. Display the Clustering Setup Configuration page.
3. To add an interface to the cluster, click Yes in the Select column.
4. To change the primary interface, click a button in the Primary Interface column.
   You can select only one primary interface for each node, and the interface you select should be on a dedicated or internal network. Click Apply and Save.
5. To change the cluster IP address for an interface, enter a new IP address in the Cluster IP Address field for that interface, then click Apply and Save.

Deleting a Cluster Configuration

If you want to delete all the cluster configuration information and remove a node from a cluster, you must log into the node as admin. On the Clustering Setup Configuration page, click Delete.

Synchronizing the Time on Cluster Nodes

You probably want to keep the times on the cluster nodes synchronized. If you run Check Point’s VPN-1 NG, be sure to do so to prevent problems with firewall synchronization.

To make sure that the time is synchronized on cluster nodes you must:

- assign the same time zone to each node
- configure NTP so that each node gets its time from the same time server

Assigning the Time Zone

To conveniently assign the same time zone to each node, follow these steps:

1. Log into Cluster Voyager
2. Under System Configuration, click Local Time Setup
3. Select the appropriate time zone.
4. Click Apply.
   All the cluster nodes are now set to the time zone you specified.
Configuring NTP

There are two approaches to configuring NTP in a cluster:

- Using a device outside the cluster as the NTP server.
  In this case you use the IP address of the server when configuring NTP on the cluster nodes.

- Using the cluster master node as the NTP server.
  In this case you use one of the cluster IP addresses when configuring NTP on the cluster nodes. If the master node fails and another node becomes the master, the new master becomes the time server.

**Caution**
Do not assign a specific node to be the time server for the cluster. If you configure NTP this way and the master node fails, the other nodes will not get their time from another server. This situation could lead to problems with firewall synchronization.

The most convenient way to set up NTP in a cluster is to use Cluster Voyager (or the CCLI) because you need to perform the configuration steps only one time instead of performing them on each node individually. The instructions provided in the following sections assume that you are using Cluster Voyager.

**Note**
Nokia recommends that you keep NTP as a cluster sharable feature (the default setting) so that if a node leaves and rejoins the cluster it will automatically obtain the proper NTP settings.

NTP server outside the cluster

If you use a device outside the cluster as the NTP server, do the following steps on the NTP configuration page (you must enable NTP before you can access this page):

1. Log into Cluster Voyager.
2. Under System Configuration, click NTP.
3. Enable NTP.
   After you enable NTP, you see, you see additional options.
4. Enter the IP address of the NTP server under NTP Servers.
5. Make sure that the NTP Master choice is set to No.
6. Click Apply.
   All the cluster nodes will now learn their time from the time server you specified.
7. Allow NTP traffic in the appropriate firewall rule.
Using the master node as the NTP server

To configure the cluster master as the NTP server, do the following steps on the NTP configuration page:

1. Log into Cluster Voyager.
2. Under System Configuration, click NTP.
3. Enable NTP.
   
   After you enable NTP, you see, you see additional options.
4. Enter one the cluster IP addresses under NTP Servers.
   
   The cluster IP addresses are the addresses that are shared by the interfaces participating in the cluster.
5. Make sure that the NTP Master choice is set to Yes.
6. Click Apply.

Configuring VPN-1 NG for Clustering

If the cluster will be in service as soon as it becomes active, you should configure and enable VPN-1 NG before making the cluster active. You must configure VPN-1 NG appropriately.

Follow the guidelines below when configuring VPN-1 NG to work with an IPSO cluster. Refer to the Check Point documentation for details.

- Each cluster node must run exactly the same version of VPN-1 NG.
- You must install and enable exactly the same Check Point packages on each node. In other words, each node must have exactly the same set of packages as all the other nodes.
- When you use Check Point’s cpconfig program (at the command line or through the Voyager interface to this program), follow these guidelines:
  - You must install VPN-1 NG as an enforcement module (only) on each node. Do not install it as a management server and enforcement module.
  - After you choose to install VPN-1 NG as an enforcement module, you are asked if you want to install a Check Point clustering product. Answer yes to this question.
  - After you choose to install a Check Point clustering product (and reboot the system when prompted to do so, you should resume using the cpconfig program to finish the initial configuration of VPN-1 NG. One of the options available to you at this point is to enable CheckPoint SecureXL. Do not enable SecureXL.
- Create and configure a gateway cluster object:
  - Use the Check Point Smart Dashboard application to create a gateway cluster object.
  - Set the gateway cluster object address to the external cluster IP address (that is, the cluster IP address of the interface facing the Internet).
  - Add a gateway object for each Nokia appliance to the gateway cluster object.
  - In the General Properties dialog box for the gateway cluster object, do not check ClusterXL.
Configure state synchronization:

- Enable state synchronization and configure interfaces for it.
- The interfaces that you configure for state synchronization should not be part of a VLAN or have more than one IP address assigned to them.

- Enable antispoofing on all the interfaces in the cluster, including those used for firewall synchronization and cluster synchronization.

- Set the options the 3rd Party Configuration tab as follows:
  - Set the Availability Mode of the gateway cluster object to Load Sharing. Do not set it to High Availability.
  - In the pull-down menu, select Nokia IP Clustering.
  - Check all the available check boxes.

- Enable automatic proxy ARP on the NAT Global Properties tab.

- Add the cluster IP addresses in the Topology tab of the Gateway Cluster Properties dialog box.

- If you want to support VPNs with remote non-Check Point gateways, do not check the “Support non-sticky connections” option for these connections.

- You can configure firewall synchronization to occur on either of the cluster protocol networks, a production network (not recommended), or a dedicated network (avoid using a production network for firewall synchronization). If you use a cluster protocol network for firewall synchronization, Nokia recommends that you use the secondary cluster protocol network for this purpose.

Note
The firewall synchronization network should have bandwidth of 100 mbps or greater.

- Connection synchronization is CPU intensive, and Nokia recommends that you carefully choose which traffic should have its connections synchronized. For example, you might choose to not synchronize HTTP traffic.

- If a cluster can no longer synchronize new connections because it has reached its limit, it can fail. If you see a large number of firewall synchronization error messages (indicating that the cluster has reached the limit of connections it can synchronize), you can configure VPN-1 to drop connections that exceed the limit by entering the following commands at the console:
  
  ```
  fw ctl set int fw_sync_block_new_conns 0
  fw ctl set int fw_sync_ack_seq_gap 128
  ```

  Entering these commands configures the cluster to give preference to maintaining the synchronization state of the existing connections over establishing new connections.

- If you use sequence validation in VPN-1 NG, you should be aware that in the event of a cluster failover, sequence validation is disabled for connections that are transferred to another cluster member. Sequence validation is enabled for connections that are created after the failover.
To enable sequence validation in the Check Point management application and IPSO, follow these steps:


b. On the Advanced System Tuning page, click the button to enable sequence validation.

c. Enable sequence validation in the Check Point management application.

d. Push the new policy to the IPSO appliance.

**Clustering Example (Three Nodes)**

This section presents an example that shows how easy it is to configure an IPSO cluster. The following diagram illustrates the example configuration:

This example cluster has three firewall nodes: A, B, and C. To the devices on either side of the cluster, A, B, and C appear as a single firewall.

The following sections explain the steps you would perform to configure this cluster.

**Configuring the Cluster in Voyager**

1. Using Voyager, log into node A.

2. Click Config.
3. On the main configuration page, click Interfaces to display the Interface Configuration page.
4. Configure interfaces with IP addresses in each of the networks shown in the example and activate the interfaces.
   For example, the IP address for interface eth-s1p1 would be 192.168.1.1.
5. Click Top.
6. Under Traffic Management Configuration, click Clustering Setup to display the Clustering Setup Configuration page.
7. Enter ID 10 for the cluster.
8. Enter a password for cadmin twice.
9. Click Apply.
10. Set the cluster mode to multicast with IGMP.
    This example assumes that you want to use multicast with IGMP mode to achieve the maximum throughput. See “Clustering Modes” for more information about this feature.
11. Configure the cluster interfaces.
    a. Click Yes in the Select column of the Interfaces Configuration table for each appropriate interface.
    b. Enter each cluster IP address in the appropriate field:
       ■ For eth-s1p1, enter 192.168.1.10.
       ■ For eth-s2p1, enter 192.168.2.10.
       ■ For eth-s3p1, enter 192.168.3.10.
       ■ For eth-s4p1, enter 192.168.4.10.

   **Note**
   The cluster IP address must be in the same subnet as the real IP address of the interface.

12. In the Primary Interface column, click Yes for eth-s3p1 to make it the primary cluster protocol interface for the node.
13. In the Secondary Interface column, click Yes for eth-s4p1 to make it the secondary cluster protocol interface for the node.
14. Under FireWall Related Configuration, set the firewall check so that IPSO does not check to see if Firewall-1 is running before it activates the cluster.
    This example assumes that you have not enabled Firewall-1 before configuring the cluster.
15. Make sure that are selected to be shared across the cluster.
16. Change the cluster state to On.
17. Click Apply.
18. Click Save.
19. Configure static routes from this node to the internal and external networks using 192.168.1.5 and 192.168.2.5 as gateway addresses (next hops).

20. On nodes B and C, configure interfaces with real IP addresses in each of the four networks shown in the example.

21. Join nodes B and C to the cluster.

These nodes will copy the configuration information you entered on node A, including the static routes to the internal and external networks.

Configuring the Internal and External Routers

You would also need to perform the following tasks on the routers facing the cluster:

1. Because the cluster is using multicast mode with IGMP, configure the internal and external routers to accept multicast ARP replies for unicast IP addresses. (This is not necessary if you use forwarding mode.)

2. Configure static routes to the cluster:
   - On the internal router, configure a static route for 192.168.2.0 (the external network) using 192.168.1.10 (the internal cluster IP address) as the gateway address.
   - On the external router, configure a static route for 192.168.1.0 (the internal network) using the cluster IP 192.168.2.10 (the external cluster IP address) as the gateway address.
Clustering Example With Non-Check Point VPN

This section presents an example that shows how easy it is to configure an IPSO cluster to support a VPN with a non-Check Point gateway. The following diagram illustrates the example configuration:

This example cluster is very similar to the previous example. The additional elements are:

- Hosts in the 10.1.1.0 network (the remote encryption domain) use a VPN tunnel to access the 192.168.1.x network (connected to the internal router).
- The VPN tunnel end points are the external cluster IP address and the external address of the remote non-Check Point VPN gateway.

Here are the steps you would perform to configure the tunnel:

1. Follow the steps under “Configuring the Cluster in Voyager.”
2. Log into the cluster using Cluster Voyager.
3. Click the option for enabling non-Check Point gateway and client support on the Clustering Setup Configuration page.
4. In the Add New VPN Tunnel section, enter 10.1.1.0 in the Network Address field.
5. In the Mask field, enter 24.
6. In the Tunnel End Point field, enter 10.1.2.5.
7. Click Apply.
8. Click Save.
9. Configure the same tunnel in VPN-1 NG.

For more information, see “Configuring VPN-1 NG for Clustering” and the Check Point documentation.

Configuring Access Control Lists (ACL)

Traffic Management Description

The traffic management software allows packet streams to be filtered, shaped, or prioritized. The prioritization mechanisms conform to RFC 2598, the Expedited Forwarding specification of the IETF DiffServ Working Group.

Traffic is separated into discrete streams, or classified, through an Access Control List (ACL). Traffic is metered to conform to throughput goals with an Aggregation Class (AGC). The combination of these control blocks form the basis of the filtering, shaping, and prioritization tools. A queue class is used to implement an output scheduling discipline to prioritize traffic.

Logically, the ACLs and the AGCs are placed inline to the forwarding path. You can configure ACLs and AGCs to process all incoming traffic from one or more interfaces, or to process all outgoing traffic from one or more interfaces. IPSO supports ACLs for both IPv4 and IPv6 traffic.

Packet Filtering Description

Traffic that is classified can be filtered immediately. The actions for filtering are:

- Accept—The accept action forwards the traffic.
- Drop—The drop action drops the traffic without any notification.
- Reject—The reject action drops the traffic and sends an ICMP error message to the source.

For information on how to configure a packet filter, see “Description of Access Control List Rules”.

Traffic Shaping Description

Traffic that is classified can be shaped to a mean rate. The shaper is implemented using a token bucket algorithm; this means that you can configure a burstsize from which bursts can "borrow." Measured over longer time intervals, the traffic will be coerced to the configured mean rate.
Over shorter intervals, traffic is allowed to burst to higher rates. This coercion is accomplished by adding delay to packets that must wait for more tokens to arrive in the bucket. When more bursts arrive than can be accommodated by the shaping queue, then that traffic is dropped. Both outgoing and incoming traffic streams can be shaped.

To configure a shaper, see “Description of Access Control List Rules”. Select shape as the action for one or more rules. See “Creating an Aggregation Class” for information about creating AGC meters. You should associate the AGC with the shaping rule(s) of the ACL.

Traffic Queuing Description

Traffic that is classified by an Access Control List (ACL) rule can be given preferential treatment according to RFC 2598. Higher-priority traffic must be policed to prevent starvation of lower-priority service traffic. Traffic that conforms to the configured policing rate is marked with the Differentiated Services codepoint (DSCP). When such traffic is processed by the output queue scheduler, it receives favorable priority treatment.

Some traffic is generated by networking protocols. This traffic should be given the highest queuing priority; otherwise, the link may become unstable. For this reason, the Queue Class (QC) configuration provides an internetwork control queue by default; some locally sourced traffic is prioritized to use that queue.

Prioritization is only relevant for outgoing traffic. Incoming traffic is never prioritized.

Use the DSfield in the Access Control List (ACL) to set the value for marking traffic that matches a given ACL rule. The QueueSpec is used to map a flow with the output queue.

To configure EF, see “Description of Access Control List Rules” for information about creating ACL rules. Choose prioritize as the action for one or more rules. Enter the appropriate values in the DSfield and QueueSpec edit boxes. See “Creating an Aggregation Class” for information about creating Aggregation Class meters. You should associate the AGC with the prioritize rule(s) of the ACL.

Creating an Access Control List

To set up an Access Control List (ACL), you must configure the interface(s) with which you want to associate the ACL and the Bypass option. IPSO supports both the IPv4 and IPv6 protocols. To configure an interface, see “Applying an Access Control List to an Interface”. The Bypass option denotes that the entire packet stream flowing out of the selected interfaces should not be classified, policed, or marked. Instead, the output queue scheduler should use the...
supplied IP TOS as an output queue lookup. Use the Bypass option to circumvent the classifier and policer for selected interfaces.

1. Click Config on the home page.
2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.
3. Enter a name for the ACL in the Create a New Access List edit box. Click Apply. The Access Control List name, Delete check box, and Bypass this Access List field appear.
4. To make your changes permanent, click Save.

Deleting an Access Control List

1. Click Config on the home page.
2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.
3. Click the Delete check box next to the Access Control List you want to delete. Click Apply. The Access Control List name disappears from the Access List Configuration page.
4. To make your changes permanent, click Save.

Applying an Access Control List to an Interface

1. Click Config on the home page.
2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.
3. Click the link for the appropriate Access Control List in the ACL Name field. This takes you to the page for that Access Control List.
4. Select the appropriate interface from the Add Interfaces drop-down window.
5. Select either Input or Output from the Direction drop-down window. Click Apply.
Note
You can apply the same interface with the same direction to an IPv4 Access Control List and to an IPv6 Access Control List. You cannot apply the same interface with the same direction to more than one IPv4 Access Control List to more than one IPv6 Access Control List.

Note
Selecting the "input" direction for a Access Control List with a rule whose action is set to "prioritize" is equivalent to setting the action to "skip."

The new interface appears in the Selected Interfaces section.

Note
Only the default rule appears in the Access Control List until you create your own rule.

6. To make your changes permanent, click Save.

Removing an Access Control List from an Interface

1. Click Config on the home page.
2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.
3. Click the link for the appropriate Access Control List in the ACL Name field. This takes you to the page for that Access Control List.
4. Click the Delete check box next to the interface (to the right) under the Selected Interfaces section that you want to remove. Click Apply. The interface disappears from the Selected Interfaces section.
5. To make your changes permanent, click Save.

Configuring Access Control List Rules

Description of Access Control List Rules

An Access Control List (ACL) is a container for a set of rules, and traffic is separated into packet streams by the Access Control List. The content and ordering of the rules is critical. As packets
are passed to an ACL, the packet headers are compared against data in the rule in a top-down fashion. When a match is found, the action associated with that rule is taken, with no further scanning done for that packet.

The following actions can be associated with a rule that is configured to perform packet filtering:

- Accept
- Drop
- Reject

The following additional actions can also be associated with a rule:

- Skip—skip this rule and proceed to the next rule
- Prioritize—give this traffic stream preferential scheduling on output
- Shape—coerce this traffic’s throughput according to the set of parameters given by an aggregation class

Rules can be set up to match any of these properties:

- IP source address
- IP destination address
- IP protocol
- UDP/TCP source port
- UDP/TCP destination port
- TCP establishment flags—When selected, traffic matches this rule when it is part of the initial TCP handshake.
- Type of Service (TOS) for IPv4; Traffic Class for IPv6

The following values can be used to mark traffic:

- DiffServ codepoint (DSfield)
- Queue Specifier (QueueSpec)

**Note**
The DSfield and QueueSpec field are used to mark and select the priority level.

Masks can be applied to most of these properties to allow wildcarding. The source and destination port properties can be edited only when the IP protocol is UDP, TCP, or the keyword "any."

All of these properties are used to match traffic. The packets that match a rule whose action is set to "prioritize" are marked with the corresponding DSfield and sent to the queue set by QueueSpec field. The DSfield and QueueSpec field can only be edited when the Action field is set to "prioritize."
Adding a New Rule to an Access Control List

1. Click Config on the home page.
2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.
3. Click the link for the appropriate Access Control List in the ACL Name field.
   This takes you to the page for that Access Control List.
4. Click the Add New Rule Before check box. Click Apply.
   This rule appears above the default rule.
   After you create more rules, you can add rules before other rules. If you have four rules—rules 1, 2, 3, and 4—you can place a new rule between rules 2 and 3 by checking the Add Rule Before check box on rule 3.
   To make your changes permanent, click Save.

Modifying a Rule

1. Click Config on the home page.
2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.
3. Click the link for the appropriate Access Control List in the ACL Name field.
   This takes you to the page for that Access Control List.

The following items can be modified:

- Action
- Aggregation Class
- Bypass this Access List
- Source IP Address
- Source Mask Length
- Destination IP Address
- Destination Mask Length
- Source Port Range
Note
You can specify the Source Port Range only if the selected protocol is either "any," 6, TCP, 17, or UDP.

- Destination Port Range

Note
You can specify the Destination Port Range only if the selected protocol is either "any," 6, TCP, 17, or UDP.

- Protocol
- TCP-Establishment flag—When it is selected, traffic matches this rule when it is part of the initial TCP handshake. This option applies only to IPv4 ACLs.

Note
You can specify the TCP Establishment flag only if the selected protocol is TCP, 6, or "any."

- Type of Service (TOS) for IPv4; Traffic Class for IPv6
- DiffServ codepoint (DSfield)

Note
RFC 791 states that the least significant two bits of the DiffServ codepoint are unused. Thus, the least significant two bits for any value of the DSfield that you enter in the ACL rule will be reset to 0. For example, if you enter 0xA3, it will be reset to 0xA0 and the corresponding packets will be marked as 0xA0 and not 0xA3.

- Logical Queue Specifier (QueueSpec)

Note
The DSfield and QueueSpec field can be configured only when the rule’s action is set to "prioritize."

To modify the Aggregation Class, go to “Associating an Aggregation Class with a Rule.”

4. Modify the values in one or more of the edit boxes or drop-down window or (de)select a radio button. Click Apply.
5. To make your changes permanent. Click Save.
Deleting a Rule

1. Click Config on the home page.
2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.
3. Click the link for the appropriate Access Control List in the ACL Name field.
   This takes you to the page for that Access Control List.
4. Click the Delete check box next to the rule that you want to delete. Click Apply.
5. To make your changes permanent, click Save.

Configuring Aggregation Classes

Aggregation Class Description

An Aggregation Class (AGC) is used to determine whether the traffic stream meets certain throughput goals. Traffic that meets these goals is conformant. Traffic that does not meet these goals is non-conformant. Depending on the configuration of the classifier rules, non-conformant traffic may be delayed, policed, that is dropped, or marked. An Aggregation Class groups traffic from distinct rules and measures its throughput.

You can configure an Aggregation Class with two parameters: meanrate and burstsize. The meanrate is the rate, in kilobits per second (kbps), to which the traffic rate should be coerced when measured over a long interval. The burstsize is the maximum number of bytes that can be transmitted over a short interval.

When you initially create an AGC, a burst of traffic is conformant—regardless of how quickly it arrives—until the size of the burst (in bytes) is equal to or larger than the burstsize you configured for the AGC. When the burst reaches the configured burstsize, traffic is non-conformant, but the AGC increases the rate at which traffic is transmitted based on the configured meanrate. Traffic that arrives consistently at a rate less than or equal to the configured meanrate will always be marked conformant and will not be delayed or dropped in the respective shaper or policer stages.

Creating an Aggregation Class

1. Click Config on the home page.
2. You can reach the Aggregation Class Configuration page in two ways. Either click the Aggregation Class Configuration link under the Traffic Management section, or click the
IPv6 link and then click the Aggregation Class Configuration link under the Traffic Management section.

3. Enter the name of the aggregation class in the Name edit box in the Create a New Aggregation Class section.

4. Enter the bandwidth in the Mean Rate (kbps) edit box.

5. Enter the burstsize in the Burstsize (bytes) edit box.

6. Click Apply.

   The aggregation class you have just created appears in the Existing Aggregation Classes section.

7. To make your changes permanent, click Save.

### Deleting an Aggregation Class

1. Click Config on the home page.

2. You can reach the Aggregation Class Configuration page in two ways. Either click the Aggregation Class Configuration link under the Traffic Management section, or click the IPv6 link and then click the Aggregation Class Configuration link under the Traffic Management section.

3. Click the Delete check box next to the aggregation class that you want to delete. Click Apply.

   This aggregation class disappears from the Existing Aggregation Classes section.

4. To make your changes permanent, click Save.

### Associating an Aggregation Class with a Rule

1. Click Config on the home page.

2. IPSO supports both the IPv4 and IPv6 protocols.
   a. For IPv4 ACLs, click the Access List Configuration link under the Traffic Management section.
   b. For IPv6 ACLs, click the IPv6 link. This takes you to the IPv6 page. Click the Access List Configuration link under the Traffic Management section.

3. Click the link for the appropriate Access Control List in the ACL Name field.

   This takes you to the page for that Access Control List.

4. Select Shape or Prioritize from the Action drop-down window. Click Apply.

5. Select an existing aggregation class from the Aggregation Class drop-down window. Click Apply.
Note
If there is no aggregation class listed, you need to create an aggregation class. Go to "Creating an Aggregation Class."

Note
A rule treats traffic as if it were configured for "skip," if the traffic matches a rule whose action has been set to "prioritize" or "shape" and no Aggregation Class is configured.

6. To make your changes permanent, click Save.

Configuring Queue Classes

Queue Class Description

Queue classes (QCs) are used to instantiate a framework, or template, for output queue schedulers. Like Access Control Lists (ACLs) they are created and configured and then associated with an interface.

There are a maximum of 8 priority-level queues for a QC. You can configure the size (in packets) of each queue level as well as the queue specifier. The queue specifier is a tag assigned by the classifier and is used as a key to look up the proper queue level. Three queue levels are pre-defined: the Internetwork Control (IC), Expedited Forwarding (EF), and Best Effort (BE) queues. The remaining queues can be assigned any name and QueueSpec you want. The table below shows the values that correspond to these queue values:

<table>
<thead>
<tr>
<th>Name of Queue Level</th>
<th>Priority</th>
<th>IETF DiffServ Codepoint</th>
<th>Queue Specifier Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internetwork Control</td>
<td>0</td>
<td>0xc0</td>
<td>7</td>
</tr>
<tr>
<td>Expedited Forwarding</td>
<td>1</td>
<td>0xb8</td>
<td>6</td>
</tr>
<tr>
<td>Best Effort</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

When you configure an ACL rule to use the priority action, you must configure an Aggregation Class (AGC). This AGC will function as a policer, that is, non-conforming traffic will be dropped. You should configure the AGCs so that the aggregate of the NC and EF flows consumes no more than 50% of the output link bandwidth. This action prevents lower-priority traffic from being starved. See RFC 2598 for more information. The other policers should also be configured to prevent the lower-priority queue from being starved.
Internetwork Control traffic, such as routing messages and keepalives, should be configured to use the IC queue so that it receives precedence over regular IP traffic. Note that locally originated internetwork control traffic is automatically sent through this queue. See RFC 791 for more information about Internetwork Control traffic.

A queue class can be configured to maximize device throughput or to minimize prioritized traffic latency. The QoS functionality is not achieved without a cost. The choice of QoS with minimal latency is the most costly in terms of forwarding performance, but it allows the least amount of head-of-line blocking for high priority traffic.

Creating a New Queue Class

1. Click Config on the home page.
2. You can reach the Queue Class Configuration page in two ways. Either click the Queue Class Configuration link under the Traffic Management section, or click the IPv6 link and then click the Queue Class Configuration link under the Traffic Management section.
3. To create a new queue class, enter its name in the Create a New Queue Class edit box. The new queue class appears in the Existing Queue Classes field.
4. Click Apply, and then click Save to make your change permanent.

Deleting a Queue Class

1. Click Config on the home page.
2. You can reach the Queue Class Configuration page in two ways. Either click the Queue Class Configuration link under the Traffic Management section, or click the IPv6 link and then click the Queue Class Configuration link under the Traffic Management section.
3. Click the Delete check box in the Existing Queue Classes field next to the name of the Queue class you want to delete. The queue class disappears from the Existing Queue Classes field.
4. Click Apply, and then click Save to make your change permanent.

Setting or Modifying Queue Class Configuration Values

1. Click Config on the home page.
2. You can reach the Queue Class Configuration page in two ways. Either click the Queue Class Configuration link under the Traffic Management section, or click the IPv6 link and then click the Queue Class Configuration link under the Traffic Management section. Click the Queue Class Configuration link under the Traffic Management section.
3. Enter a name for each queue you want to configure in the Logical Name edit box. This name appears on the queue monitoring page.
4. To modify an existing queue class, in the Existing Queue Classes field, click on the name of the queue class you want to edit.

**Note**
Choose a name (with no spaces) that will allow you to identify the queue's purpose.

---

**Note**
Each queue class can have up to eight queues. Three queues are reserved for internetwork control, expedited forwarding, and best effort traffic.

---

5. Enter an integer for the logical identifier used to address each queue you configure within a queue class in the Queue Specifier edit box.

6. For each queue, enter a value for the maximum number of packets that can be queued before packets are dropped in the Max Queue Length edit box. A value of zero (0) is used to disable a queue. Neither the network control nor the best effort queue can be disabled.

7. Click Apply, and then click Save to make your changes permanent.

8. To change the name of any of the queue levels 3-7, enter the new name in the Logical Name edit box. This name appears in the queue monitoring page.

**Note**
Choose a name (with no spaces) that will allow you to identify the queue’s purpose.

---

9. Click Apply, and then click Save to make your changes permanent.

### Associating a Queue Class with an Interface

1. Click Config on the home page.

2. You can reach the Queue Class Configuration page in two ways. Either click the Queue Class Configuration link under the Traffic Management section, or click the IPv6 link and then click the Queue Class Configuration link under the Traffic Management section.

3. To associate a queue class with an interface, click on the appropriate physical interface in the List of Available Physical Interfaces field.

4. You are now in the physical interface page for the interface you selected. To enable QoS queuing, select either Max Throughput or Min QoS Latency from the Queue Mode drop-down window in Queue Configuration field.

5. Click Apply.

6. Select the configured queue class you want to associate with the interface from the Queue Class drop-down window in the Queue Configuration field.
Note
If you do not select a queue class, the default class will be used. The default queue class has two queues, Internetwork Control and Best Effort.

7. Click Apply.
8. Click Save to make your changes permanent.

Configuring ATM QoS

ATM QoS Description

ATM networks can provide different quality of service for network applications with different requirements. Unspecified Bit Rate (UBR) service does not make any traffic related guarantees. It does not make any commitment regarding cell loss rate or cell transfer delay. Constant Bit Rate (CBR) service provides continuously available bandwidth with guaranteed QoS.

The implementation supports CBR channels through a mechanism on an ATM network interface card (NIC) that limits the cell rate for each virtual channel you configure. The CBR feature limits the peak cell rate for each CBR channel in the output direction only. Each ATM port supports up to 100 CBR channels with 64 kbits/sec of bandwidth resolution.

See “Queue Class Description” for more information about queue classes.

Creating a New QoS Descriptor

1. Click Config on the home page.
2. Click the ATM QoS Descriptor Configuration link in the Traffic Management section.
3. To create an ATM QoS Descriptor, enter its name in the Create a New ATM QoS Descriptor edit box.
   The category for any new ATM QoS Descriptor that you configure is set to constant bit rate (CBR).
   CBR limits the maximum cell output rate to adhere to the requirements on CBR traffic imposed by the network.

Note
The default ATM QoS Descriptor is set to unspecified bit rate; this descriptor cannot be modified.

4. Enter a value for the maximum cell rate to be used in the output direction on a CBR channel in the Peak Cell Rate edit box.
The Peak Cell Rate is rounded down to a multiple of 64 kilobits/sec. One cell per second corresponds to 424 bits/sec.

**Note**
You can configure no more than 100 CBR channels per interface. The sum of the Peak Cell Rate of all the CBR channels on an interface cannot exceed 146Mbs.

5. Click Apply.
   The new ATM QoS Descriptor appears in the Existing ATM QoS Descriptors field.
6. Click Save to make your changes permanent.

### Deleting an ATM QoS Descriptor

1. Click Config on the home page.
2. Click the ATM QoS Descriptor Configuration link in the Traffic Management section.
3. In the Existing ATM QoS Descriptors field, click the Delete check box next to the name of the ATM QoS Descriptor that you want to delete.

**Note**
You can delete an existing ATM QoS Descriptor only after you dissociate it from an existing permanent virtual channel (PVC). See the steps below.

4. Click Apply.
5. The ATM QoS Descriptor disappears from the Existing QoS Descriptors field.
6. Click Save to make your changes permanent.

If the ATM QoS Descriptor that you want to delete is associated with an existing PVC complete the steps below.
1. Click Config on the home page.
2. Click Interfaces link.
3. Click the appropriate ATM interface link in the Physical field.
4. You are now in the physical interface page for the interface you selected. Click the ATM QoS Configuration link. You are now in the ATM QoS Configuration page for the physical interface you selected. In the QoS Configured PVCs field, click the QoS Descriptor dropdown window and select Default (UBR).
5. Click Apply, and then click Save to make your changes permanent.
6. Click the ATM QoS Descriptors link.
7. In the Existing ATM QoS Descriptors field, click the Delete check box next to the name of the ATM QoS Descriptor that you want to delete.
8. Click Apply.
9. The ATM QoS Descriptor disappears from the Existing QoS Descriptors field.
10. Click Save to make your changes permanent.

**Associating an ATM QoS Descriptor with an Interface and a Virtual Channel**

1. Click Config on the home page.
2. Click the Interfaces link.
3. To associate an ATM QoS Descriptor with an interface, click the appropriate interface link in Physical field.
4. You are now in the physical interface page for the interface you selected. Click the ATM QoS Configuration link. You are now in the ATM QoS Configuration page for the physical interface you selected. In the Configure a New PVC field, enter the virtual path identifier/virtual channel identifier (VPI/VCI) of the permanent virtual channel (PVC) you want to configure, in the VPI/VCI edit box.
5. In the Configure a New PVC field, click the QoS Descriptor drop-down window and select the QoS descriptor with which you want to associate the PVC you configured.

**Note**

You cannot delete or modify a QoS Descriptor that has been associated with a permanent virtual channel (PVC). You must first disassociate the PVC from the QoS descriptor. See "Deleting an ATM QoS Descriptor" for more information.

**Note**

You can change the QoS configuration of a PVC while it is being used. However, doing so results in a short break in traffic because the PVC is closed while QoS configuration values change. Afterward, the system reopens the PVC.

6. Click Apply.

The name of the new PVC and ATM QoS Descriptor with which you associated the PVC appear in QoS Configured PVCs field.
7. Click Save to make your changes permanent.
Configuring Common Open Policy Server

Common Open Policy Server Description

The Common Open Policy Server (COPS) provides a standard for exchanging policy information in order to support dynamic Quality of Service (QoS) in an IP (Internet Protocol) network. This information is exchanged between PDPs (Policy Decision Points) and PEPs (Policy Enforcement Points). The PDPs are network-based servers that decide which types of traffic (such as voice or video) receive priority treatment. The PEPs are routers that implement the decisions made by the PDPs. In the Nokia implementation, the Nokia platform functions as a PEP.

Configuring a COPS Client ID and Policy Decision Point

You must configure at least one COPS Client ID and a corresponding policy decision point, that is, policy server, for the COPS Policy Module to function.

1. Click either Config on the Voyager home page or click the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. In the Configured COPS Modules section click the Diffserv PIB link. This action takes you to the COPS Diffserv specific configuration page.
4. In Diffserv PIB specific configuration section, enter the name of the new client ID in the Create a new Client ID edit box. Click Apply. To view the new client ID, click on the Client ID drop-down window. The name of the new COPS client appears in a Client ID list in the COPS Security configuration section.

Note
You can configure multiple client IDs. Only one client ID can be active at a time.

5. To configure a COPS client, click on the Client ID drop-down window and select a client name. Click Apply.
6. Enter either the IP address or domain name the server to act as the Policy Decision Point (PDP) in the Primary PDP edit box.
7. (Optional) Enter the IP address or domain name of the server to act as the secondary Policy Decision Point (PDP) in the Secondary PDP edit box. Click Apply.
8. Click Save to make your changes permanent.
Configuring Security Parameters for a COPS Client ID

The Nokia implementation lets you configure send and receive key IDs for each COPS Client ID to authenticate sessions with the PDP, or policy server.

1. Click either Config on the Voyager home page or click the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. In the Configured COPS Modules section click the DiffServ PIB link. This action takes you to the COPS DiffServ specific configuration page.
4. In the COPS security configuration section, click on the link for the name of the COPS Client ID for which you want to configure security. This action takes you to the COPS Security Configuration page for that client.
5. In the Sequence Number edit box, enter a value between 1 and 2147483647 to define the sequence number used for the COPS protocol. Click Apply.
6. In the Key ID field, enter a value between 1 and 2147483647 in the Send edit box to define the send key ID used for the COPS protocol.
7. In the Key field, enter a string value of up to 64 characters in the edit box next to the Send Key ID value. This value defines the key used for the COPS protocol. Use alphanumeric characters only. Click Apply.
8. In Key ID field, enter a value between 1 and 2147483647 in the Recv edit box to define the receive key ID used for the COPS protocol.
9. In the Key field, enter a string value of up to 64 characters in the edit box next to the Recv Key ID value. This value defines the key used for the COPS protocol. Use alphanumeric characters only. Click Apply.

Note
You can configure up to 5 receive key IDs.

10. Click Save to make your changes permanent.

Assigning Roles to Specific Interfaces

The Nokia COPS implementation lets you assign roles to specific interfaces. A role refers to a logical name assigned to a group of objects within a network. The role name lets you group objects to which you want to assign a particular policy. You can also assign a combination of roles to a particular logical interface. You then apply policies to role(s) and not just to a single object.

1. Click either Config on the Voyager home page or the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. In the Interface Role Combinations section, enter the name for a role in the edit box next to the appropriate logical interface name. The role name can be up to 31 characters long. Use alphanumeric characters, the period, hyphen or underscore symbols only. Do not begin a role name with the underscore symbol.

4. Click Apply.

**Note**
You can assign multiple roles to each interface.

**Note**
You can assign different roles to different interfaces on the same system.

5. Click Save to make your changes permanent.

### Activating and Deactivating the COPS Client

You must activate the COPS client to implement the COPS module you configure. You can deactivate the COPS client to halt the COPS module implementation.

1. Click either Config on the Voyager home page or the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. Click the Start button in the COPS client field. Click Apply.
4. Click Save to make your change permanent.

Perform the following steps to deactivate the COPS client. You can maintain any existing module and role configuration. This configuration remains available if you reactivate the COPS client.

1. Click either Config on the Voyager home page or the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. Click the Stop button in the COPS client field. Click Apply.
4. Click Save to make your change permanent.
Changing the Client ID Associated with Specific Diffserv Configuration

You can change a client ID on a running system. Typically, each client ID refers to a specific policy or set of policies.

1. Click either Config on the Voyager home page or the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. Click the Diffserv PIB link in the Configured COPS Module section. This action takes you to the COPS Diffserv specific configuration page.
4. In the Diffserv PIB specific configuration section, click the Client ID drop-down window and select the client ID name you now want to run. Click Apply. The name of the client ID you selected now appears in the Client ID field.

Note
A list of all existing Client IDs appears in the COPS Security configuration section.

5. Click Save to make your change permanent.

Deleting a Client ID

Before you delete a Client ID, make sure that it is not active. Perform the following steps to deactivate a client ID before you delete it.

1. Click either Config on the Voyager home page or the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. Click the Diffserv PIB link in the Configured COPS Module section. This action takes you to the COPS Diffserv specific configuration page.
4. Click the Client ID drop-down window in the DiffServ PIB specific configuration section and select either another existing client ID name or none.
5. Click Apply.

You can now delete the client ID you disabled.

1. Click either Config on the Voyager home page or the Traffic Management link on the home page.
2. Click the COPS link in the Traffic Management section.
3. Click the Diffserv PIB link in the Configured COPS Module section. This action takes you to the COPS Diffserv specific configuration page.
4. In the COPS security configuration section, click the Delete check box next to the name of the client ID you want to delete.
5. Click **APPLY**, and then click **SAVE** to make your change permanent.

**Example: Rate Shaping**

The following example shows you how to limit ftp data traffic to 100 kilobits per second (kbps) with a 5000 byte burstsize on output interface eth-s2p1c0.

First, you create an Access Control List.

1. Click on **Config** in the home page.
2. Click on the Access List Configuration link under the Traffic Management section.
3. To create the Access Control List, enter its name in the Create a New Access List edit box.
4. Click **Apply**.
5. Click the Add Rule Before check box next to the last rule.
6. Click **Apply**.
7. Enter tcp in the Protocol edit box and enter 20 in both the Source or Destination Port Range edit box.
8. Click **Apply**.
9. Select **Shape** from the Action drop-down window.
10. Click **Apply**.

Second, you create an Aggregation Class.

1. Click on the Aggregation Class Configuration link on the Access Control List Configuration page.
2. Enter the name of the new Aggregation Class in the Name edit box in the Create a New Aggregation Class section.
3. Click **Apply**, and then click **Save** to make your change permanent.
4. Enter 100 in the Meanrate (Kbps) edit box.
5. Enter 5000 in the Burstsize (bytes) edit box.
6. Click **Apply**, and then click **Save** to make your changes permanent.

Third, you associate the Aggregation Class with the rule you set when you created the Access Control List.

1. Click on the Access List Configuration link on the Aggregation Class Configuration page.
2. For the rule you set up when you created the Access Control List, select the aggregation class you created from the Aggregation Class drop-down window.
3. Click **Apply**.
4. Select eth-s2p1c0 from the Add Interfaces drop-down window, and select **Output** from the Direction drop-down window.
5. Click **Apply**.
6. Click **Save** to make your changes permanent.
Example: Expedited Forwarding

This example illustrates the combined use of the Access Control List, Traffic Conditioning, and Queuing features.

This example demonstrates how to improve the response time to Telnet sessions between client and server systems over a private WAN connection within a corporate intranet as shown in the diagram below. The WAN interfaces for Network Application Platform (Nokia Platform) A and for Network Application Platform (Nokia Platform) B are ser-s3p1. The following configuration is done both on Nokia Platform A and Nokia Platform B.

1. Save the current configuration on each Nokia Platform before you set up QoS. Doing so allows you to compare the relative performance of the QoS and non-QoS configurations.
   a. Click on Config on the home page.
   b. Click on the Manage Configuration Sets link under the System Configuration section.
   c. Enter `pre-QoS` in the Save Current State to New Configuration Database edit box.
   d. Click Apply, and then click Save to make your change permanent.

2. Create an Aggregation Class
   a. Click Config on the home page.
   b. Click on the Aggregation Class Configuration link under the Traffic Management section.
   c. Enter `wan_1_ef` in the Name edit box in the Create a New Aggregation Class section.
   d. Enter `100` in the Mean Rate (Kbps) edit box.
   1. Enter `5000` in the Burstsize (bytes) edit box.
   e. Click Apply, and then click Save to make your changes permanent.

2. Create a Queue Class
   a. Click Config on the home page.
   b. Click the Queue Class Configuration link under the Traffic Management section.
   c. Enter `wan_1_ef` in the Create a New Queue Class edit box.
d. Click on the link to \textit{wan\_1\_ef} in the Existing Queue Classes section to view existing queue class values.

\textbf{Note}

The queue specifier associated with expedited forwarding queue is 6.

3. Associate the \texttt{wan\_1\_ef} queue class with the appropriate interface.
   a. Click Config on the home page.
   b. Click the Interfaces link.
   c. Click on ser-s3p1 in the Physical column.
   d. In the Queue Configuration field, select Max Throughput from the Queue Mode drop-down window.
   e. Click Apply.
   f. In the Queue Configuration field, select \texttt{wan\_1\_ef} from the Queue Class drop-down window.
   g. Click Apply.
   h. Click Save to make your changes permanent.

4. Create a new Access Control List rule to classify, condition, and prioritize telnet traffic.
   a. Click Config on the home page.
   b. Click on the Access List Configuration link under the Traffic Management section.
   c. Enter \texttt{wan\_1\_telnet} in the Create a New Access List edit box.
   d. Click Apply.
   e. Select ser-s3p1 from the Add Interfaces drop-down window.
   f. Select Output from Direction drop-down window.
   g. Click Apply.
   h. In the Existing Rules for \texttt{wan\_1\_telnet} section, click on the Add New Rule Before check box.
   i. Click Apply.
   j. Select prioritize from the Action drop-down window, and then click Apply.
   k. Select \texttt{wan\_1\_ef} from the Aggregation Class drop-down window, and then click Apply.
   l. For Nokia Platform A, enter 23 in the Destination Port Range edit box, and for Nokia Platform B, enter 23 in the Source Port Range edit box.

\textbf{Note}

The telnet port number is 23.
m. Enter tcp in the Protocol edit box; enter 0xB8 in the DSfield edit box; and enter 6 in the QueueSpec edit box.

Note
0xB8 is the IETF differentiated-services codepoint (in hexadecimal) for expedited forwarding traffic.

n. Click Apply, and then click Save to make your changes permanent.

To test the configuration:
1. Start a telnet session between the client and server.
2. Check the statistics on Nokia Platform A and Nokia Platform B
   a. Click Config on the home page.
   b. Click on the Interfaces link.
   c. Click on the link for ser-s3p1 in the Physical column.
   d. Click on the Interface Statistics link.
   e. Scroll down to view statistics for Queue Class wan_1_ef.
      You should see values other than zero on both Nokia Platform A and Nokia Platform B for the Packets Passed and Bytes Passed counters in the Expedited Forwarding row.
3. Use the telnet session to generate traffic, and then check each Nokia Platform’s interface statistics.
   a. Click Config on the home page.
   b. Click on the Interfaces link.
   c. Click on the link for ser-s3p1 in the Physical column.
   d. Click on the Interface Statistics link.
   e. Examine the statistics for input and output traffic and compare them to the statistics for Expedited Forwarding traffic.
4. Start an ftp session to create heavy (non-telnet) background traffic over the WAN. Note that the telnet session remains responsive. Use a text editor to examine a file.
5. Save the QoS routing configuration (See Step 1 in the instructions for how to configure this example), and restore the non-QoS configuration. Compare the difference in responsiveness when there is heavy WAN traffic both with and without QoS routing.
Chapter Contents

- Overview
  - SNMP Description
  - SNMP Proxy Support for Check Point MIB
- Configuring SNMP v1 and v2
  - Enabling and Disabling the SNMP Daemon
  - Setting an SNMP Agent Address
  - Setting the SNMP Version
  - Setting Community Strings
  - Disabling Community Strings
  - Sending SNMP Traps to a Network Management System
  - Enabling SNMP Traps
  - Setting the SNMP Trap Agent Address
  - Entering SNMP Location and Contact Information
- Interpreting SNMP
  - SNMP Error Messages
- Configuring SNMP v3
  - Using Enhanced Security
  - Adding a User-based Security Model User
  - Deleting a User-Based Security Model User
  - Modifying a User-based Security Model User Entry
  - Changing a User-based Security Model User Permissions
Overview

SNMP Description

**Caution**
If you use SNMP, Nokia strongly recommends that you change the default community strings for security purposes. If you do not use SNMP, you should disable the community strings.

SNMP, as implemented on Nokia platforms, supports the following:

- getRequest, getNextRequest, getBulkRequest, and a select number of traps. The Nokia implementation also supports SetRequest for three attributes only: sysContact, sysLocation, and sysName. See “Setting Community Strings.” You must configure a read-write community string to enable set.
- SNMP v1, v2, and v3. For more information about SNMP v3, see “Adding a User-based Security Model User.”

**Note**
The Nokia implementation of SNMPv3 does not yet support SNMPv3 traps.

- Other public and proprietary MIBs as follows.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Source</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate-Shape MIB</td>
<td>proprietary</td>
<td>Monitoring rate-shaping statistics and configuration. Monitoring system-specific parameters.</td>
</tr>
<tr>
<td>IPSO System MIB</td>
<td>proprietary</td>
<td>Defines the system MIB for IPSO. The IPSO chassis temperature, fan group, and power-supply group function only on certain firewalls.</td>
</tr>
<tr>
<td>IPSO Registration MIB</td>
<td>proprietary</td>
<td>Defines the object ID (OID) prefixes.</td>
</tr>
<tr>
<td>OID Registration MIB</td>
<td>proprietary</td>
<td>Defines the object ID (OID) prefixes.</td>
</tr>
<tr>
<td>Unit Types MIB</td>
<td>proprietary</td>
<td>Contains OID values for the different types of circuit cards used in Nokia equipment.</td>
</tr>
<tr>
<td>TCP MIB</td>
<td>RFC 2012</td>
<td>Provides management information of TCP implementations.</td>
</tr>
<tr>
<td>EtherLike MIB</td>
<td>RFC 1650</td>
<td>Generic objects for Ethernet-like network interfaces.</td>
</tr>
<tr>
<td>Host Resources MIB</td>
<td>RFC 1514</td>
<td>Provides information about the system, such as hardware, software, processes, CPU utilization, disk utilization and so on.</td>
</tr>
<tr>
<td>MIB</td>
<td>Source</td>
<td>Function</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IANAifType MIB</td>
<td>IANA</td>
<td>Defines the IANAifType textual convention, including the values of the ifType object defined in the MIB-II ifTable.</td>
</tr>
<tr>
<td>IF MIB</td>
<td>RFC 2233</td>
<td>Describes generic objects for network interface sublayers.</td>
</tr>
<tr>
<td>IP MIB</td>
<td>RFC 2011</td>
<td>Provides management information for IP and ICMP implementations.</td>
</tr>
<tr>
<td>IP Forwarding MIB</td>
<td>RFC 2096</td>
<td>Displays CIDR multipath IP routes.</td>
</tr>
<tr>
<td>ISDN MIB</td>
<td>RFC 2127</td>
<td>Describes the management of ISDN interfaces.</td>
</tr>
</tbody>
</table>

**Note**
The isdnMibCallInformation trap is not supported by IPSO.

| VRRP MIB                  | RFC 2787    | Provides dynamic failover statistics.                                                                                                     |
| RIP MIB                   | RFC 1724    | Describes RIP version 2 protocol.                                                                                                          |
| SNMP Framework MIB        | RFC 2571    | Outlines SNMP management architecture.                                                                                                     |
| SNMP MPD MIB              | RFC 2572    | Provides message processing and dispatching.                                                                                               |
| SNMP User-based SM MIB    | RFC 2574    | Provides management information definitions for SNMP User-based Security Model                                                           |
| SNMPv2 MIB                | RFC 1907    | Defines SNMPv2 entities.                                                                                                                   |
|                           |             | **Note:** The warmStart trap is not supported.                                                                                             |
| SNMPv2 SMI                | RFC 2578    |                                                                                                                                            |
| SNMPv2 TC                 | RFC 854     | Defines textual conventions for various values reported in OIDs and Traps.                                                                 |
| Dial-Control MIB          | RFC 2128    | Describes peer information for demand access and other kinds of interfaces.                                                              |
|                           |             | **Note:** The dialCtlPeerCallInformation and dialCtlPeerCallSetup traps are not supported by IPSO.                                         |
| Entity MIB                | RFC 2737    | Represents the multiple logical entities that a single SNMP agent supports.                                                               |
|                           |             | IPSO does not support the entConfigChange trap is not supported by IPSO.                                                                     |
| Tunnel-MIB                | RFC 2667    | Provides statistics about IP tunnels.                                                                                                       |
| UDP-MIB                   | RFC 2013    | Provides statistics about UDP implementations.                                                                                              |
| Frame Relay DTE MIB       | RFC 2115    | Keeps statistics and errors in one or more circuits of a device implementing Frame Relay.                                                |
Both the proprietary MIBs and the public MIBs are supplied with the system. To view more detailed information about the MIBs, see the /etc/snmp/mibs directory.
Note
The SNMPv2-CONF MIB resides in the /etc/snmp/mibs/unsupported directory.

The SNMP agent implemented in Nokia IPSO enables an SNMP manager to monitor the device and to modify the sysName, sysContact and sysLocation objects only.

Note
You must configure an SNMP string first to configure sysContact and sysLocation.

Use Nokia Voyager to perform the following tasks:
- Define and change one read-only community string.
- Define and change one read-write community string.
- Enable and disable the SNMP daemon.
- Enable and disable USM users.
- Modify USM user access privileges, that is, change permissions from read-only to read-write and the reverse.
- Add or delete trap receivers.
- Enable or disable the various traps.
- Enter the location and contact strings for the device.

SNMP Proxy Support for Check Point MIB

Beginning with Nokia IPSO 3.7, IPSO supports the use of a proxy for SNMP GetRequest and SNMP GetNextRequest for Check Point objects. The following are guidelines and limitations you should be aware of.

Using the Check Point MIB

You must use the Check Point version of the Check Point MIB (CP-MIB) text file in $FWDIR/lib/snmp of your network management tool. Do not use the CheckPoint-MIB.txt included in releases before Nokia IPSO 3.7.

Whenever IPSO SNMPd is started or restarted, it searches for the CheckPoint-MIB.txt. The following is an example of a message you may see as a result of the search:

```
IP650 [admin]# Jan 31 12:17:19 IP650 [LOG_ERR] snmpd: Cannot find module (CheckPoint-MIB) : At line 1 in (none)
```

You can ignore this message.

Any SNMP requests to the CP-MIB when the Check Point SNMPd (CP-SNMPd) is not running time out. (The IPSO SNMPd does not respond.)
The SNMP Proxy support is hard-coded to work only with the CP-SNMPd. It is not a generic proxy that you can use for accessing other MIBs. If you change the following default configurations, the SNMP Proxy for the CP-MIB does not work:

- CP-SNMPd must continue to run on port 260.
- CP-SNMPd must continue to accept SNMPv1 and have a read community set to “public.”
- CP-SNMPd must continue to be accessible through “localhost” on the Nokia IPSO device.

The SNMP Proxy is not a trap proxy and only proxies SNMP Get and SNMP GetNext requests. When simultaneous SNMP queries arrive, the SNMP Proxy sreturn valid values to only one request.

Because Nokia IPSO uses a proxy to support the Check Point MIB, reference the Check Point documentation for any limitations of the CP-SNMPd.

### Using cpsnmp_start

You must run the `cpsnmp_start` script to make sure that CP-SNMPd is running on Check Point versions NG FP1, FP2, and FP3. You do this by first enabling the IPSO SNMMPd from Nokia Network Voyager and then enabling the CP-SNMPd by using `/bin/cpsnmp_start` on the command line.

**Note**

Whenever you use the `cprestart` or `cpstop;cpstart` commands, you must run the `cpsnmp_start` script to restart the CP-SNMPd when you are using NG FP3.

**Note**

Using FloodGate with Check Point NG FP1, FP2, and FP3 causes SNMP query operations to fail, even on non-FloodGate CheckPoint MIB objects. You must restart the CP-SNMPd to have SNMP query operations. On NG FP2, just disabling FloodGate might not enable SNMP query operations. In this case, you might have to delete the FloodGate package from your system.

### Configuring SNMP v1 and v2

#### Enabling and Disabling the SNMP Daemon

1. Click Config on the home page.
2. Click the SNMP link.
3. To enable the SNMP daemon, click Yes in the Enable SNMP daemon field. Click Apply.
Caution
To run the Check Point and SNMP daemons simultaneously, you must start the Check Point SNMP daemon after you start VPN-1/Firewall NG. If you start the Check Point SNMP daemon before you start VPN-1/FireWall-1 NG, the IPSO daemon does not start.

All possible configuration options appear, which allow you to enter the necessary values.

4. To disable the SNMP daemon, click No in the Enable SNMP daemon field. Click Apply. The configuration options disappear.

5. To make your changes permanent, click Save.

Setting an SNMP Agent Address

1. Click Config on the home page.
2. Click the SNMP link.
3. To configure a specific IP address on which the agent responds to requests, enter the valid IP address of a configured interface in the Agent New Address text box. Click Apply. The IP address and its current status appears on the Network Voyager page.
4. Click Save to make your change permanent.

Note
The default is for the protocol to respond to requests from all interfaces.

5. To delete a configured IP address, click off button next to the entry for the address. Click Apply. The entry for the address disappears.

6. Click Save to make your change permanent.

Setting the SNMP Version

The Nokia implementation of SNMP lets you select whether to allow SNMPv3 access only. Selecting SNMPv3 access limits community access. Only requests from users with enabled SNMPv3 access are allowed. All other requests are rejected. To continue to allow community names, select v1/v2/v3 as the SNMP version. This option is the default.

1. Click Config on the home page.
2. In the SNMP version drop-down list, select either v1/v2/v3 or v3-Only. Click Apply. The default is v1/v2/v3.
3. Click Save to make your change permanent.
Note
To enable specific SNMPv3 users, click the Add USM Users link at the bottom of the SNMP Network Voyager page, which takes you to the Network Voyager page that lets you configure users for SNMPv3. For more information, see "Adding a User-based Security Model User."

Setting Community Strings

⚠️ Caution
Nokia strongly recommends that you change or disable the community strings.

1. Click Config on the home page.
2. Click the SNMP link.
3. (Optional) To enable or change the read-only community string, enter the name of the new string in the Read-only community string text box.
   Use alphanumeric characters without spaces. Click Apply.
   The default read-only community string is public.
4. (Optional) To enable or change a read-write community string, enter the name in the Read-write community string text box.
   Use alphanumeric characters without spaces. Click Apply.
   The name of the new read-write community string appears in the current read-write community string field.
5. To make your changes permanent, click Save.

Disabling Community Strings

1. Click CONFIG on the home page.
2. Click the SNMP link.
3. To disable a read-only community string, check the disable check box in the CURRENT READ-ONLY COMMUNITY STRINGS field.
   Click Apply.
4. To disable a read-write community string, check the disable check box in the CURRENT READ-WRITE COMMUNITY STRINGS field.
   Click Apply.
5. Click Save to make your changes permanent.
Sending SNMP Traps to a Network Management System

1. Click Config on the home page.
2. Click the SNMP link.
3. Enter the IP address (or the hostname if DNS is set) of a new receiver that will accept traps from this device in the Add New Trap Receiver text box. Click Apply.
4. (Optional) Enter the community string, using alphanumeric characters (do not use spaces), for the specified receiver in the Community String for New Trap Receiver text box. Click Apply. The default is community string for the trap receiver is public.
5. To delete an existing receiver, click Off radio button in the Status field. Click Apply.
6. To make your changes permanent, click Save.

Enabling SNMP Traps

The system traps are defined in the Nokia-IPSO-System-MIB. The ifLinkUpDown trap is defined in the IF-MIB. The clustering traps are defined in the Nokia-IPSO-LBCluster-MIB. The Disk Mirror traps are defined in the Nokia-IPSO-System-MIB. The text files that define the MIBs are located in the /etc/snmp/mibs directory.

Below is a list of the objects associated with individual traps.

The systemTrapConfigurationChange, systemTrapConfigurationFileChange, and systemTrapConfigurationSaveChange traps are associated with the ipsoConfigGroup objects. These objects include ipsoConfigIndex, ipsoConfigFilePath, ipsoConfigFileDateAndTime, ipsoConfigLogSize, ipsoConfigLogIndex, and ipsoConfigLogDescr.

The systemTrapDiskMirrorSetCreate, systemTrapDiskMirrorSetDelete, systemTrapDiskMirrorSyncFailure, and systemTrapDiskMirrorSyncSuccess traps are associated with the ipsoDiskMirrorGroup objects. These objects include ipsoTotalDiskMirrorSets, ipsoMirrorSetIndex, ipsoMirrorSetSourceDrive, ipsoMirrorSetDestinationDrive, ipsoMirrorSetSyncPercent.

The linkUp and linkDown traps are associated with the ifIndex, ifAdminStatus, and ifOperStatus objects.

Table 9 lists the types of SNMPv1 and SNMPv2 traps which IPSO supports.

Note
The Nokia implementation of SNMPv3 does not yet support SNMPv3 traps.
<table>
<thead>
<tr>
<th>Type of Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coldStart</td>
<td>Supplies notification when the SNMPv2 agent is reinitialized.</td>
</tr>
<tr>
<td>linkUp/linkDown</td>
<td>Supplies notification when one of the links, which is administratively up, either comes up or is lost.</td>
</tr>
<tr>
<td>lmemberActive</td>
<td>Supplies notification when a port is added to a link aggregation group.</td>
</tr>
<tr>
<td>lmemberInactive</td>
<td>Supplies notification when a port is removed from a link aggregation group.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Supplies notification when an SNMP operation is not properly authenticated.</td>
</tr>
<tr>
<td></td>
<td>Although all implementation of SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap is generated.</td>
</tr>
<tr>
<td>vrrpTrapNewMaster</td>
<td>Supplies notification when a new VRRP master is elected.</td>
</tr>
<tr>
<td>vrrpTrapAuthFailure</td>
<td>Supplies notification when a VRRP hello message is not properly authenticated.</td>
</tr>
<tr>
<td>systemTrapConfigurationChange</td>
<td>Supplies notification when a different configuration file is selected.</td>
</tr>
<tr>
<td>systemTrapConfigurationFileChange</td>
<td>Supplies notification when a different configuration file is selected.</td>
</tr>
<tr>
<td>systemTrapConfigurationSaveChange</td>
<td>Supplies notification when a permanent change to the system configuration occurs.</td>
</tr>
<tr>
<td>systemTrapLowDiskSpace</td>
<td>Supplies notification when space on the system disk is low. This trap is sent if the disk space utilization has reached 80 percent or more of its capacity. If this situation persists, a subsequent trap is sent after 15 minutes.</td>
</tr>
<tr>
<td>systemTrapNoDiskSpace</td>
<td>Supplies notification when the system disk is full. This trap is sent if 2 percent or less of the disk space remains available, or if the remaining disk space is equal to or less than 1 MB. If this situation persists, a subsequent trap is sent after 15 minutes.</td>
</tr>
<tr>
<td>systemTrapDiskFailure</td>
<td>Supplies notification when a particular disk drive fails. Note: The systemTrapDiskFailure applies only to the IP740 and IP530 Nokia platforms.</td>
</tr>
<tr>
<td>systemTrapDiskMirrorSetCreate</td>
<td>Supplies notification when a system disk mirror set is created.</td>
</tr>
<tr>
<td>systemTrapMirrorSetDelete</td>
<td>Supplies notification when a system disk mirror set is deleted.</td>
</tr>
</tbody>
</table>
To enable or disable traps

1. Click Config on the home page.
2. Click the SNMP link.
3. To enable any type of trap, click On next to the name of the trap and click Apply.
4. To disable any type of trap, click Off next to the name of the trap and click Apply.
5. To make your changes permanent, click Save.
Setting the SNMP Trap Agent Address

1. Click Config on the home page
2. Click the SNMP link.
3. (Optional) To specify the IP address to be used for sent trap PDU, enter the IP address in the Trap PDU Agent Address field, and then click Apply.

Note
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 Nokia IPSO, the default was to use the IP address of the first valid interface.

The Network Management System uses the agent address to identify the network element that generated the trap. This address must belong to one of the interfaces.

4. To make your changes permanent, click Save.

Entering SNMP Location and Contact Information

1. Click Config on the home page.
2. Click the SNMP link.
3. (Optional) In the SNMP Location String text field, enter the actual location of the device. Click Apply.
4. (Optional) In the SNMP Contact String text field, enter the name of department or person who has administrative responsibility for the device. Click Apply.
5. To make your changes permanent, click Save.

Interpreting SNMP Messages

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.

The following table lists 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>Error status code</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>1</td>
<td>tooBig</td>
</tr>
<tr>
<td>2</td>
<td>NoSuchName</td>
</tr>
<tr>
<td>3</td>
<td>BadValue</td>
</tr>
<tr>
<td>4</td>
<td>ReadOnly</td>
</tr>
<tr>
<td>5</td>
<td>genError</td>
</tr>
<tr>
<td>6</td>
<td>noAccess</td>
</tr>
<tr>
<td>7</td>
<td>wrongType</td>
</tr>
<tr>
<td>8</td>
<td>wrongLength</td>
</tr>
<tr>
<td>9</td>
<td>wrongEncoding</td>
</tr>
<tr>
<td>10</td>
<td>wrongValue</td>
</tr>
<tr>
<td>11</td>
<td>noCreation</td>
</tr>
<tr>
<td>12</td>
<td>inconsistentValue</td>
</tr>
<tr>
<td>13</td>
<td>resourceUnavailable</td>
</tr>
<tr>
<td>14</td>
<td>commitFailed</td>
</tr>
<tr>
<td>15</td>
<td>undoFailed</td>
</tr>
<tr>
<td>16</td>
<td>authorizationError</td>
</tr>
<tr>
<td>17</td>
<td>notWritable</td>
</tr>
<tr>
<td>18</td>
<td>inconsistentName</td>
</tr>
</tbody>
</table>

**Note**
You might not 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 following table describes each element.

<table>
<thead>
<tr>
<th>Variable-bindings element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>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 table lists possible value field sets in the response PDU or error-status messages when performing a GetRequest:

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

**GetNextRequest**

The only values that can be returned 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 is the index of the problem object in the variable-bindings field.

Configuring SNMP v3

Using Enhanced Security

IPSO supports the User-based Security Model (USM) component of SNMP v3 to provide message-level security. To use USM, you create a USM user account. When you do so, the system uses the user’s password as a passphrase to generate authentication and encryption keys for that user. These keys are then automatically used to protect communication between the Nokia system and the SNMP manager.

The system uses the MD5 hashing algorithm to provide authentication and integrity protection and DES to provide encryption (privacy). Nokia recommends that you use both authentication and encryption, but you can employ them independently by specifying one or the other with your SNMP manager requests. The Nokia system responds accordingly.

Note
Nokia systems do not protect traps with authentication or encryption.

You must configure your SNMP manager to specify the security you want. If you are using a UCD-SNMP/Net-SNMP based manager, here are the security-related options you can use in request messages:

- `-u name` Specifies the user name.
- `-a MD5` Use MD5 hashing for authentication.
- `-x DES` Use DES for encryption.
- `-A password` Specifies the user’s password/passphrase. Use for authentication. The password/passphrase must have at least 8 characters.
For example, to send an snmpwalk request from your manager with full protection you would enter:

```
snmpwalk -v 3 -u username -a MD5 -A password -x DES -X password -l authPriv system_name OID
```

For more information about USM, see RFC 3414.

### Adding a User-based Security Model User

**To add a USM user**

1. Click Config on the home page.
2. Click the SNMP link. You are now in the SNMP page. Click the Add USM Users link.
3. In the Add New User text field, enter a login name for the user in the Username text box. The range for a new user name is 1 to 8 alphanumeric characters with no spaces.
4. In the Add New User text field, enter a numeric value for the User ID in the Uid text box. The range is 0 to 65535. There is no default.
5. Enter the name of the user's home directory in the Home Directory text box. Enter the full Unix pathname of the directory where the user will be placed after login. If the home directory does not exist, the system creates it.
6. Click Apply. An entry for the new user and his/her profile appears. The default shell is /bin/csh. The default page refers to the user's default page when he/she logs in. The default page is set to the home page.
7. (Optional) To modify the shell, enter the new shell path name in the Shell text box. Consult the file /etc/shells for valid login shells.
8. (Optional) To modify the default page, enter the name of the new default page in the Default Page text box.
9. Enter the new user's password in the New Password edit box. Leave the Old Password edit box empty.
10. Enter the same password that you entered in the New Password text box in the New Password (Verify) text box.
**Note**
The password of an SNMP USM user must be at least 8 characters long.

11. Click Apply, and then click Save to make your changes permanent.
A table appears on the SNMP page with the name of each user and his/her permissions.

### Deleting a User-Based Security Model User

This procedure describes how to delete a User-based Security Model (USM) user.

1. Click Config on the home page.
2. Click the SNMP link.
   You are now on the SNMP page. Click the Add USM Users link.
3. You can either delete a user completely or remove a user’s SNMPv3 functionality but keep that user as an IPSO user.
   a. To delete a user, click OFF next to the name of each user to delete. Click Apply.
      The name of each user and his/her entry disappears from the SNMPv3 Users list on the SNMP page.
   b. To remove a user’s SNMPv3 functionality but keep that user’s entry, change the user’s password to one that has fewer than eight characters but at least six characters. Enter the user’s current password in the Old Password text box. Enter a new password that is fewer than eight characters long but at least six characters long in the New Password edit box. Enter the same password that you entered in the New Password text box in the New password (verify) edit box. Click Apply.
      The name of the user and his/her entry disappears from the SNMPv3 Users list on the SNMP page. The name of any user whose password you change to one that has fewer than 8 characters but has at least 6 characters continues to appear on the Password Setting page. To reach that page, click Config on the home page and then click the Users link in the Security and Access Configuration section.
      Click Apply.
4. Click Save to make your changes permanent.

### Modifying a User-based Security Model User Entry

To modify a User-based Security Model (USM) user entry

1. Click Config on the home page.
2. Click the SNMP link.
   You are now on the SNMP page. Click the Add USM Users link.
3. Go the entry for the user whose profile you want to modify.
   Click the text boxes that you want to change.
   Enter the new value or name.

4. Click Apply, and then click Save to make your changes permanent.

Changing a User-based Security Model User Permissions

This procedure describes how to change read and write permissions for a User-based Security Model (USM) user.

1. Click Config on the home page.

2. Click the SNMP link.
   You are now on the SNMP page.

3. Go the SNMPv3 USM USERS table. Find that user for which you would like to change read or write permissions. Click button that corresponds to the type of permission you want for that user in the Permission column.

4. Click Apply, and then click Save to make your changes permanent.
Chapter Contents

- Configuring DHCP
  - Introduction to DHCP
  - Enabling DHCP Clients
  - Configuring the DHCP Server
  - Enabling the DHCP Server Process
  - Disabling the DHCP Server Process
  - Adding DHCP Address Pools
  - Enabling DHCP Address Pools
  - Disabling DHCP Address Pools
  - Assigning a Fixed-IP Address to a Client
  - Creating DHCP Client Templates
  - Configuring Dynamic Domain Name System Service
  - Configuring Dynamic Domain Name System Zones
- DNS Hostname Procedure
  - Selecting a DNS Server to Resolve for Hostnames
- Configuring Disk Mirroring
  - Introduction to Disk Mirroring (RAID Level 1)
  - Creating a Mirror Set
  - Deleting a Mirror Set
- Using an Optional Disk (Diskless Systems Only)
  - Installing an Optional Disk
  - Removing an Optional Disk
- Mail Relay
  - Mail Relay Description
  - Configuring Mail Relay
  - Sending Mail
- System-Failure Notification
  - Setting System-Failure Notification
- Time and Date Procedures
  - Setting the System Time
- Static Host Procedures
  - Adding a Static Host
  - Deleting a Static Host
- System Logging
  - Disk-Based Systems Only
  - Diskless Systems Only
  - All Systems
- Remote Core-Dump Server (Diskless Systems Only)
  - Configuring an Application Core-Dump Server
- Hostname Procedure
  - Changing the Hostname
- Managing Configuration Sets
  - Saving the Current Configuration as a New Configuration Set
  - Creating a Factory Default Configuration Set
  - Loading a Configuration Set
  - Deleting a Configuration Set
- Backing Up and Restoring Files
  - Description of Creating Backup Files
  - Creating a Backup File Manually
  - Creating a Regularly Scheduled Backup File
  - Automatically Transferring Backup Files to a Remote Server
  - Manually Transferring Backup Files to a Remote Server
  - Restoring Files from Locally Stored Backup Files
  - Restoring Files from Backup Files Stored on a Remote Server
  - Deleting Locally Stored Backup Files
- Scheduling Jobs Through the Crontab File
  - Configuring Scheduled Jobs
  - Deleting Scheduled Jobs
- Managing Nokia IPSO Images
  - Selecting Nokia IPSO Images
  - Testing Nokia IPSO Images
  - Deleting Nokia IPSO Images
  - Upgrading the Nokia IPSO Image
  - Downgrading Nokia IPSO Images
- Installing New Nokia IPSO Images
  - Upgrading the Nokia IPSO Image
Configuring DHCP

Introduction to DHCP

Dynamic Host Configuration Protocol (DHCP) for Nokia IPSO provides complete DHCP client and DHCP server capabilities for your Nokia appliance. DHCP gives you the ability to provide network configuration parameters, through a server, to clients which need the parameters to operate on a network. DHCP eliminates the need for you to configure each client manually and thus reduces configuration errors.

DHCP for Nokia IPSO support includes the following:

- Enabling the DHCP client
- Configuring the DHCP client interface
- Dynamic and fixed IP address allocation from the DHCP server.
- Automatic Domain Name System (DNS) server updates from the DHCP server.
- The ability to specifies various client parameters including which servers are available for services such as DNS, NTP, TFTP, and SMTP. You can also configure NetBIOS over TCP/IP which includes identifying WINS and Datagram Distribution servers available to clients.
- Support for VLAN clients.

**Note**
If you enable the IPSO DHCP server, the appliance receives and accepts DHCP requests even if there is a firewall rule blocking DHCP requests. Although requests are shown as blocked in the firewall logs, the IPSO DHCP server still provides addresses to clients that request them. If you don’t need the DHCP server, leave it disabled (the default option). If you enable the DHCP server but do not want DHCP requests from the outside to be accepted, enable it only on internal interfaces.
Enabling DHCP Clients

To enable the DHCP client process
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click Client next to the logical interface link to be configured as a DHCP client in the DHCP Interface Configuration table.
4. In the DHCP Client Configuration table, click enable.

Note
The Ethernet interface must be enabled before you enable the client. For more information on how to configure Ethernet interfaces see Configuring Ethernet Interfaces.

5. Enter a host name in the Host Name text box.
6. Click Apply.
7. Click Save to make your changes permanent.

Configuring DHCP Client Interfaces

To configure the DHCP client interface
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click the logical interface link in the DHCP Interface Configuration table to be configured.

Note
The logical interface must be enabled. It is enabled if the link-state indicator is green. For more information on how to configure Ethernet interfaces see Configuring Ethernet Interfaces.

4. (Optional) Enter a unique name in the Client ID text box. The name will be used in request packets instead of the MAC address of the interface.
5. Enter a value, in seconds, in the Timeout text box. If you do not enter a value, the configuration will default to 60 seconds.
6. Enter a value, in seconds, in the Retry text box. If you do not enter a value, the configuration will default to 300 seconds.
7. Enter a value, in seconds, in the Lease text box for the length of time the IP address will be leased to the interface.
8. Enter a value, in seconds, in the Reboot text box for the client to reacquire an expired lease address before it attempts to discover a new address

9. Click Apply.

10. Click Save to make your changes permanent.

**Configuring the DHCP Server**

**To configure the DHCP server process**

1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click Server in the DHCP Service Selection box.
4. Click Apply.

**Note**
You must configure an Ethernet interface and enter the subnet address and the subnet mask length on which the interface is listening in the Subnet text box (see steps 6 and 7) before you enable the DHCP Server Process. For more information on how to configure Ethernet interfaces see Configuring Ethernet Interfaces.

5. Click the Add a new Subnet Entry link.
6. Enter the subnet address of the Ethernet interface you have configured for the DHCP server process in the Subnet text box.
7. Enter the mask length for the subnet in the Mask Length text box.
8. (Optional) Enter the lease length, in seconds, for client IP addresses in the Default Lease text box. This would be applied only if clients do not request a specific lease time. If you do not enter a value, the configuration will default to 43,200 seconds.
9. (Optional) Enter the maximum lease length, in seconds, for client IP addresses in the Maximum Lease text box. This would be the longest lease the server would allow. If you do not enter a value, the configuration will default to 86,400 seconds.
10. Enter the range of IP addresses the server will assign to clients in the Start and End text boxes respectively in the New Pool field.

**Note**
Make sure that Enabled is selected in the State field. This is the default selection.

**Note**
If you are configuring a large number of VLANs, you might experience a delay in having IP addresses assigned to VLAN interfaces.
11. (Optional) Enter the Trivial File Transfer Protocol (TFTP) server clients will use in the TFTP text box.

12. (Optional) Enter the file name where diskless clients will find the boot file in the File Name text box.

13. (Optional) Enter a path for clients to get additional configuration options in the Extensions Path text box.

**Note**
You must configure the TFTP option to use the Extension Path option since clients will use TFTP to transfer the configuration options from the server.

14. (Optional) Enter the root path where diskless clients mount a network file system (NFS) in the Root Filename text box.

15. Enter the IP address of the default router clients will use in the Router text box.

16. (Optional) Enter the domain name you want clients to use in the Domain text box.

17. (Optional) Enter the time offset for clients in the Time Offset text box.

18. (Optional) Enter the IP address or the name of the swap server diskless clients will use in the Swap Server text box.

19. Enter the Domain Name System (DNS) server clients will use to resolve domain names in the DNS Servers text box.

20. Enter the Network Time Protocol (NTP) servers clients will use in the NTP Servers text box. Enter the servers you want clients to use in the order of preference separated by commas.

21. Enter the Simple Mail Transfer Protocol (SMTP) servers available to clients, separated by commas, in the SMTP Servers text box.

22. If you configure NetBIOS, enter the Windows Internet Naming Servers (WINS) available to clients in the WINS text box.

23. If you configure NetBIOS, enter the Datagram Distribution (DD) servers available to clients, separated by commas, in the DD Servers text box.

24. If you configure NetBIOS, enter the node type that the client will configure itself as in the Node Type text box.

25. If you configure NetBIOS, enter the scope for the client in the Scope text box.

26. Click Apple.

27. Click Save to make your changes permanent.
Enabling the DHCP Server Process

**To enable the DHCP server process**
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click Server in the DHCP Service Selection box.
4. Click Apply.

**Note**
You must configure an Ethernet interface and enter the subnet address and the subnet mask length on which the interface is listening before you enable the DHCP Server Process. See Configuring the DHCP Server, steps 5, 6, and 7. For more information on how to configure Ethernet interfaces, see Configuring Ethernet Interfaces.

5. Click Enable in the DHCP Server Process box.
6. Click Apply.
7. Click Save to make your changes permanent.

Disabling the DHCP Server Process

**To disable the DHCP server process**
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click Disable in the DHCP Server Process box.
4. Click Apply.
5. Click Save to make your changes permanent.

Changing DHCP Service

**To change the DHCP service**
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click the Change DHCP Service link.
4. Click the service for which you would like to configure your appliance in the DHCP Service Selection box.
5. Click Apply.
6. Click Save to make your changes permanent.
Adding DHCP Address Pools

To add additional IP address ranges to an exiting DHCP server configuration
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click the IP address link for which you would like to add additional address ranges in the DHCP Server Subnet Configuration box.
4. Enter the range of IP addresses the server will assign to clients in the Start and End text boxes respectively in the New Pool field.

Note
Make sure that Enabled is selected in the State field. This is the default selection.

Note
If you are configuring a large number of VLANs, you might experience a delay in having IP addresses assigned to VLAN interfaces.

5. Click Apply.
6. Click Save to make your changes permanent.

Enabling DHCP Address Pools

To enable an existing IP address pool
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click enable next to the subnet IP address link in the DHCP Server Subnet Configuration box.
4. Click Apply.
5. Click Save to make your changes permanent.

Disabling DHCP Address Pools

To disable an existing IP address pool
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click disable next to the subnet IP address link in the DHCP Server Subnet Configuration box.
Assigning a Fixed-IP Address to a Client

To assign a fixed-ip address to a client
1. Click Config on the home page.
2. Click the DHCP link in the System Configuration section.
3. Click the Add a new Fixed-IP Entry link in the Fixed-IP Address Client Configuration.
4. (Optional) Enter a host name that will be assigned to the client in the Host Name text box. If you do not enter a host name, the server will assign the IP address of the client as the host name.

Note
Check the State field to make sure that Enabled is selected. Enabled is the default.

5. Enter a client identification in the Client ID text box or enter the MAC address of the client in the Client MAC Address text box.
6. Enter the IP address you want to assign the client in the IP Address text box.
7. (Optional) Enter the Trivial File Transfer Protocol (TFTP) server clients will use in the TFTP text box.
8. (Optional) Enter the file name where diskless clients will find the boot file in the File Name text box.
9. (Optional) Enter a path for clients to get additional configuration options in the Extensions Path text box.

Note
You must configure the TFTP option to use the Extension Path option since clients will use TFTP to transfer the configuration options from the server.

10. (Optional) Enter the root path where diskless clients mount a network file system (NFS) in the Root Filename text box.
11. Enter the IP address of the default router clients will use in the Router text box.
12. (Optional) Enter the domain name you want clients to use in the Domain text box.
13. (Optional) Enter the time offset for clients in the Time Offset text box.
14. (Optional) Enter the IP address or the name of the swap server diskless clients will use in the Swap Server text box.
15. Enter the Domain Name System (DNS) server clients will use to resolve domain names in the DNS Servers text box.

16. Enter the Network Time Protocol (NTP) servers clients will use in the NTP Servers text box. Enter the servers you want clients to use in the order of preference separated by commas.

17. Enter the Simple Mail Transfer Protocol (SMTP) servers, separated by commas, available to clients in the SMTP Servers text box.

18. If you configure NetBIOS, enter the Windows Internet Naming Servers (WINS), separated by commas, available to clients in the WINS text box.

19. If you configure NetBIOS, enter the Datagram Distribution (DD) servers, separated by commas, available to clients in the DD Servers text box.

20. If you configure NetBIOS, enter the node type that the client will identify itself as in the Node Type text box.

21. If you configure NetBIOS, enter the scope for the client in the Scope text box.

22. Click Apply.

23. Click Save to make your changes permanent.

Creating DHCP Client Templates

This procedure describes how to create a template for subnet and fixed-ip entries. After creating a template, you will have the ability to configure server and clients quickly and with fewer errors because you will only have to enter IP address information when you configure subnets or fixed-ip entries.

1. Click Config on the home page.

2. Click the DHCP link in the System Configuration section.

3. Click the Template for adding new client entries link.

4. (Optional) Enter the Trivial File Transfer Protocol (TFTP) server clients will use in the TFTP text box.

5. (Optional) Enter a path for clients to get additional configuration options in the Extensions Path text box.

Note
You must configure the TFTP option to use the Extension Path option since clients will use TFTP to transfer the configuration options from the server.

6. (Optional) Enter the root path where diskless clients mount a network file system (NFS) in the Root Filename text box.

7. (Optional) Enter the file name where diskless clients will find the boot file in the File Name text box.

8. (Optional) Enter the domain name you want clients to use in the Domain text box.
9. (Optional) Enter the time offset for clients in the Time Offset text box.

10. (Optional) Enter the IP address or the name of the swap server diskless clients will use in the Swap Server text box.

11. Enter the Domain Name Servers (DNS) clients will use to resolve domain names in the DNS Servers text box.

12. Enter the Network Time Protocol (NTP) servers clients will use in the NTP Servers text box. Enter the servers you want clients to use in the order of preference separated by commas.

13. Enter the Simple Mail Transfer Protocol (SMTP) servers available to clients, separated by commas, in the SMTP Servers text box. If you configure NetBIOS, enter the Windows Internet Naming Servers (WINS), separated by commas, available to clients in the WINS text box.

14. If you configure NetBIOS, enter the Datagram Distribution (DD) servers, separated by commas, available to clients in the DD Servers text box.

15. If you configure NetBIOS, enter the node type that the client will identify itself as in the Node Type text box.

16. If you configure NetBIOS, enter the scope for the client in the Scope text box.

17. Click Apply.

18. Click Save to make your changes permanent.

---

### Configuring Dynamic Domain Name System Service

This procedure describes how to configure the Dynamic Domain Name System (DDNS) feature. DDNS gives you the ability to configure your DHCP server to automatically update DNS servers on your network.

1. Click Config on the home page.

2. Click the DNS link in the System Configuration section.

3. Click the DDNS Configuration link.

4. Check that enable is selected.

5. Select a style in the Update Style box.

6. Enter a key name in the Key Name text box and click the enable button next to the name.

7. Enter the secret key to be matched by the DNS server in the Key Secret text box.

8. Click Apply.

9. Click Save to make your changes permanent.

To add more keys, complete steps 6 through 9 for each new key.

---

### Configuring Dynamic Domain Name System Zones

This procedure describes how to configure Dynamic Domain Name System (DDNS) zones.
Note
Before you can configure DDNS zones, you must have created DDNS keys. See “Configuring Dynamic Domain Name System Service.”

1. Click Config on the home page.
2. Click the DNS link in the System Configuration section.
3. Click the DDNS Configuration link.
4. Enter the zone identifier in the Zone text box.
5. Check that enable is selected next to the Zone text box.
6. Select a key to associate with the zone in the Key drop-down box.
7. Enter the IP address of the primary DNS server in the Primary text box.
8. (Optional) Enter the IP address of the secondary DNS server in the Secondary text box.
9. Click Apply.
10. Click Save to make your changes permanent.

To add more zones, complete steps 4 through 9 for each new zone.

DNS Hostname Procedures

Selecting a DNS Server to Resolve for Hostnames

To select a DNS server
1. Click Config on the home page.
2. Click the DNS link in the System Configuration section.
3. Enter the new domain name in the Domain name text box.
4. Enter the IP address of the primary DNS in the Primary name server box; then click Apply.
5. (Optional) Enter the IP address of the secondary DNS in the Secondary name server box; then click Apply.
6. (Optional) Enter the IP address of the tertiary DNS in the Tertiary name server box; then click Apply.
7. Click Save to make your changes permanent.
Configuring Disk Mirroring

Introduction to Disk Mirroring (RAID Level 1)

The Nokia disk mirroring feature protects against downtime in the event of a hard-disk drive failure in your appliance (for platforms that support the feature). You must have a second hard disk drive installed on your appliance.

Disk mirroring gives you the ability to configure a mirror set composed of a source hard disk drive and a mirror hard disk drive that uses Network Voyager. The hard disk drive in which you installed IPSO is your source hard disk drive. When you configure a mirror set, and the hard disk drives are synchronized (source hard disk drive is fully copied to the mirror hard disk drive), all new data written to your source hard disk drive is also written to your mirror hard disk drive. If your source hard disk drive fails, your mirror hard disk drive automatically replaces your source hard disk drive without interrupting service on your appliance.

The source and mirror hard disk drives can be warm swapped on appliances other than IP500 Series appliances, which means, you can replace a failed hard disk drive without shutting down your appliance.

In addition to being able to configure a mirror set, you can monitor the status of a mirror set, synchronization time, and system log entries.

Note
See Important Information Regarding Disk Mirroring for information on creating a mirror set when you install IPSO.

Creating a Mirror Set

To create a mirror set
1. Click Config on the home page.
2. Click the Disk Mirroring link in the System Configuration section.
3. Select the Create check box in the Create Mirror Set table.

Note
The source hard disk drive and the mirror hard disk drive should have identical geometries. You can view hard-disk drive geometry in the Drivers Information table.

4. Click Apply. Text at the top of the Network Voyager window with a message indicates a mirror set was created, numbers indicates which hard disk drive is the source and which hard disk drive is the mirror, and that mirror synchronization is in progress.
Note
The synchronization percent value in the Mirror Set table indicates the percentage of synchronization zones that are copied from the source disk to the mirror disk. A sync zone is equivalent to contiguous disk sectors. When all synchronization zones are copied to the mirror disk, the synchronization percent value reads 100 percent and your platform is protected from a disk failure. Synchronization time is approximately 20-30 minutes for a 20 GB disk. No mirror set is created if the synchronization operation is not successful.

Deleting a Mirror Set

To delete a mirror set
1. Click Config on the home page.
2. Click the Disk Mirroring link in the System Configuration section.
3. Select the Delete check box in the Mirror Sets table.
4. Click Apply.

Note
You can only delete a mirror set that is 100-percent synchronized.

Using an Optional Disk (Diskless Systems Only)

Installing an Optional Disk
You can add PC card flash memory in diskless 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.

When you insert a PC card into a diskless platform and select the card as an optional disk, any existing data on the card is erased. If you remove a PC card that contains log files and want to permanently store the data, insert the card into a PC or other computer and save the data to that system before reinserting the card into a Nokia diskless platform.

Note
PC card memory smaller than 512 megabytes are not recognized by the IP2250. Use a card that has at least this much storage capacity.
To install and configure PC card flash memory
1. Insert the card into one of the PC card slots in the front of the system. Make sure that the card is fully inserted.
2. On the Network Voyager home page, click System Configuration.
3. Click Optional Disk.
   Network Voyager displays information about the card you inserted. If you do not see this information, verify that the card has at least one gigabyte of storage and is fully inserted into the slot.
4. Choose the card by clicking in the CHOOSE column.
5. Wait until you see a message indicating that you should reboot the system. There is a short delay before the message appears.
6. When the message appears, click the link Reboot, Shutdown System.
7. Reboot the system.

Storing Log Files on a PC Card

To configure the system to store log files on the PC card
1. Wait until the system reboots.
2. Log into the system using Network Voyager.
3. On the Network Voyager home page, click System Logging
4. Next to Logging to Optional Disk, click ON.

Removing an Optional Disk

If you want to stop using PC card flash memory, follow these steps:
2. Click Optional Disk.
3. Deactivate the card by clicking in the unselect column.
4. Wait until you see a message indicating that you should reboot the system. There is a short delay before the message appears.
5. When the message appears, click the link Reboot, Shutdown System.
6. Reboot the system.
Mail Relay

Mail Relay Description

Email relay allows you to send email from the firewall. You can send email interactively or from a script. The email is relayed to a mail hub that then sends the email to the final recipient.

Mail relay is used as an alerting mechanism when a Check Point FireWall-1 rule is triggered. It is also used to email the system administrator the results of cron jobs.

Features Supported

- Presence of a mail client or Mail User Agent (MUA) that can be used interactively or from a script
- Presence of a sendmail-like replacement that relays mail to a mail hub by using SMTP
- Ability to specify the default recipient on the mail hub

Features not Supported

- Support for incoming email
- Support for mail transfer protocols other than outbound SMTP
- Ability to telnet to port 25
- Support for email accounts other than admin or monitor

Configuring Mail Relay

To configure mail relay for your firewall

1. Click Config on the home page.
2. Click the Mail Relay link in the System Configuration section.
3. Enter either the IP address or hostname of the email server that relays outgoing email in the Mail Server text box.
4. Enter the username on the mail server to which mail addressed to admin or monitor is sent in the Remote User text box; then click Apply.
5. To make your changes permanent, click Save.
Sending Mail

This procedure describes how to send mail from the firewall.

1. Log in to the firewall by using either your admin or monitor account.
2. At the prompt, type the mail command, followed by a space, and the username of the recipient:
   
   mail username@hostname

3. Type the subject of your message at the subject prompt; then press Enter.
4. Type your message; then press Enter.
5. When you finish typing your message, type a period on an empty line; then press Enter.
   
   Your message is sent.

Failure Notification

Setting System-Failure Notification

This procedure describes how to set your system to send email to one or more people when a system failure occurs. Separate multiple email addresses by spaces.

1. Click Config on the home page.
2. Click the System Failure Notification link in the System Configuration section.
3. Click On next to Enable Failure Notification.
4. Click Apply.
5. Enter the email address of the people who want to be notified in the event of a system failure, and then click Apply.

   Examples of a system failure include crashing daemons (snmpd, ipsrd, ifm, xpand) and a system reboot that results from a fatal error.

   In a system failure notification, the following information appears:
   
   • System information
   • Image information
   • Crash information
   • Crash trace

6. To make your changes permanent, click Save.
Time and Date Procedures

Setting the System Time

The default time is set to GMT.

To set the system time to another time zone
1. Click Config on the home page.
2. Click the Local Time Setup link in the System Configuration section.
3. Click the appropriate time zone in the Time Zone drop-down list.
4. Enter the appropriate information in each text box and then click Apply.
5. To make your change permanent, click Save.

Static Host Procedures

Adding a Static Host

To add a static host entry
1. Click Config on the home page.
2. Click the Host Address Assignment link in the System Configuration section.
3. Enter the new hostname in the Add new hostname text box; then click Apply.
4. Enter the IP address of the new host in the IP address text box; then click Apply.
5. To make your changes permanent, click Save.

Deleting a Static Host

To delete a static host
1. Click Config on the home page.
2. Click the Host Address Assignment link in the System Configuration section.
3. Click off next to the host to delete, then click Apply.
4. To make your changes permanent, click Save.
System Logging Procedures

Disk-Based Systems Only

This section describes how to configure system logging on disk-based appliances.

Accepting Log messages

This procedure describes how to set the system to accept unfiltered syslog messages from a remote machine.

1. Click Config on the home page.
2. Click the System Logging link in the System Configuration section.
3. Click Yes to accept syslog messages.
4. To make your changes permanent, click Save.

Logging to a Remote System

To send a syslog message to a remote machine

1. Click Config on the home page.
2. Click the System Logging link in the System Configuration section.
3. Enter the IP address of the host machine to which you are sending syslog messages.
4. Click Apply.
5. Click the Added Security Level drop down window to select at least one severity level.
   Specifying a particular severity level means that all messages at least that severe are sent to the associated remote host.
   The choices are Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug, All.
   If you specify more than one severity level, all messages that are least as severe as the lowest severity level you select are sent to the remote host.

Note
You must select at least one severity level for this option to function. The system will not send syslog messages to the remote host if you do not configure at least one severity level.

6. Click Apply.
   The name of each severity level appears in Log at or above severity field.
7. To disable any of the severity levels, click No next to the name of the severity level you want to delete.
8. Click Apply.
9. To make your changes permanent, click Save.

Diskless Systems Only

On diskless systems, log files are not persistent across system reboots unless they are stored on an appropriate device. You can store log files on either or both of the following:

- remote log servers (primary and secondary)
- PC card flash memory in the diskless system

If you decide to use remote systems, you must configure them to store the log files. If you decide to use PC card flash memory, you must install and configure it before you set up the system logging. (For information about installing a flash memory card, see “Installing an Optional Disk”.)

Caution

When you insert a PC card into a diskless platform and select the card as an optional disk, any existing data on the card is erased. If you remove a PC card that contains log files and want to permanently store the data, insert the card into a PC or other computer and save the data to that system before reinserting the card into a Nokia diskless platform.

Log messages are temporarily stored in system memory and are stored to remote log servers and/or PC card flash memory according to a schedule that you can configure. Messages are stored in the following files:

- Most log messages are stored in /tmp/tmessages (in memory) and also in /var/log/messages when PC card flash memory is installed. (Messages stored in http_error_log or httpd_access_log on other platforms are stored in the messages files on diskless systems.)
- Messages about shell logins and logouts are stored in /var/log/wtmp. When PC card flash memory is installed, /var/log/wtmp is automatically stored on the drive.

Using Remote Log Servers

To configure a diskless system to use a remote log server

2. Click System Logging.
3. Next to Network Logging, click On.
4. Enter the IP address of the primary remote log server. Make sure that the diskless system has connectivity to the remote server.
5. If you want to use a secondary remote log server, enter its IP address.

If the primary log server is unreachable for any reason, the system sends its log files to the secondary log server. Make sure that the system has connectivity to the secondary server. If the primary log server is unreachable, there is a several minute delay before log messages
are sent to the secondary server. The messages are stored in a buffer during this time and are sent when connectivity is established with the secondary server.

6. Set the threshold level for saving log messages to the remote server.

diskless systems can hold 512 log messages in a specific memory buffer. Use this configuration 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.

7. Use the Flush Frequency option as an additional control for saving messages.

When the Flush Frequency interval expires, log messages are transferred to the remote server and the log buffer is cleared regardless of how many messages are in the buffer.

**Using an Optional Disk**

If PC card flash memory is installed and enabled, you can configure the system to save log files on it by enabling the local logging option. If you enable local logging, log messages are saved in /var/log/message and /var/log/wtmp on the memory card. The messages are saved to the card according to the setting of the Flush Frequency option.

You can save log files to a remote log server and PC card flash memory simultaneously.

If the flash memory is full, the system displays a console message to that effect and stops saving log messages to the card. Messages that have been previously saved on the card are not affected. If you have configured the system to send messages to remote log server, it continues to do so. (If you use SNMP, the system sends SNMP traps when the flash memory file system is full 90 percent and 95 percent full to alert you of the impending issue.)

To delete log files stored in PC card flash memory so that new messages can be stored, you can use the `rm` command to delete files in /var/log/.

**All Systems**

**Setting the System Configuration Auditlog**

Use this feature to set the system to log transient and permanent configuration changes. You can view the syslog messages to determine whether authorized users only are making configuration changes to the system.

1. Click Config on the home page.
2. Click the System Logging link in the System Configuration section.
3. To log transient configuration changes only, click the Logging of transient changes button in the System Configuration Auditlog field.

Transient changes refer to changes that apply only to the currently running system. Transient changes are equivalent to clicking the Apply button only in Network Voyager. Reboot the system to restore the previous configuration.
4. Click Apply.

5. To log both transient and permanent configuration changes, click the Logging of transient and permanent changes button in the System Configuration Auditlog field. Permanent changes remain active after the system is rebooted. These changes are equivalent to clicking the Save button in Network Voyager after you apply a configuration change. Click Apply.

6. If you are using a system with a hard disk, a Destination Log Filename text box appears after you enable the system configuration auditlog. The box contains the name of the file to which syslog messages for this feature are sent. The default is /var/log/messages. To change the file, enter the new file name in the Destination Log Filename text box. (On diskless systems, you cannot save the messages to another file.)

7. Click Apply.

8. If you are using a system with a hard disk, a Destination Log Filename text box appears after you enable the system configuration auditlog. The box contains the name of the file to which syslog messages for this feature are sent. The default is /var/log/messages. To change the file, enter the new file name in the Destination Log Filename text box. (On diskless systems, you cannot save the messages to another file.)

**Note**

You must enter a destination file name to view log messages in the Management Activity Log. The default destination file logs messages in the standard system log file.

To access the Management Activity Log page, click Monitor on the Home page in Network Voyager and then click the Management Activity Log link in the System Logs section. For more information, see “Monitoring System Logs.”

9. Click Apply.

10. Click Save to make your changes permanent.

### Setting the Nokia Network Voyager AuditLog

Use this feature to set the system to log all Apply and Save actions to the Network Voyager pages. If you enable this feature, each time the Apply or Save button is pressed, the log records the name of the user, the name of the Network Voyager page, and the name of the button that was pressed. The log records these actions whether or not the operation succeeded.

To view the log, click the Monitor button on the Network Voyager home page, and then click the System Message Log link to view system messages. For more information on viewing the system message log, see the Monitoring System Logs section.

**Note**

For Nokia Network Voyager configuration pages, such as image.tcl, that do not include Apply and Save buttons, the log records the relevant action, such as when you press the Reboot button.

1. Click Config on the home page.
2. Click the System Logging link in the System Configuration section.
3. In the Voyager Auditlog field, click the Enabled button to have the system log all Apply and Save actions to Network Voyager.
4. Click Apply.
5. Click Save to make your change permanent.

Note
The Voyager AuditLog feature does not record any operations performed using the command-line interface (CLI).

Disabling the System Configuration Auditlog
1. Click Config on the home page.
2. Click the System Logging link in the System Configuration section.
3. In the System Configuration Auditlog field, click Logging disabled button to disable the System Configuration Auditlog feature.
4. Click Apply.
5. Click Save to make your change permanent.

Disabling the Nokia Network Voyager AuditLog
1. Click Config on the home page.
2. Click the System Logging link in the System Configuration section.
3. In the Voyager Auditlog field, click the Disabled button to stop having the system log all Apply and Save actions to Network Voyager.
4. Click Apply.
5. Click Save to make your change permanent.

Remote Core-Dump Server (Diskless Systems Only)

Configuring an Application Core-Dump Server

Note
This feature does not apply to Nokia 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.

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.

**Note**
You must also configure the remote system (FTP or TFTP server) appropriately.

To configure a diskless system to transfer application core files to a remote server, follow these steps:

1. On the Core-Dump Server Configuration page, enter the IP address of the remote server.
2. Choose whether to use FTP or TFTP for the transfer protocol.

**Caution**
The TFTP option 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.

If you choose FTP, make sure that your server accepts anonymous FTP logins. You cannot use non-anonymous FTP logins to transfer application core files.

3. Indicate where the core files should be stored on the remote server by entering the appropriate path and directory.
4. Click apply.
5. Click save to make your changes permanent.

### Hostname Procedure

#### Changing the Hostname

**To change the hostname (system name) of the firewall**

1. Click Config on the home page.
2. Click the Change Hostname link in the System Configuration section.
3. Enter the new hostname in the Change it to field.
4. Click Apply.
5. To make your changes permanent, click Save.

**Note**
Host address assignments must match an IP address.
Managing Configuration Sets

Saving the Current Configuration as a New Configuration Set

To save the current configuration into a new configuration database file
1. Click Config on the home page.
2. Click the Manage Configuration Sets link in the System Configuration section.
3. Enter the name of the new configuration file in the Save current state to new configuration database field.
4. Click Apply.

The current configuration is saved in the new file, and the file appears in the list of database files on this page. Subsequent configuration changes are saved in the new file.

Creating a Factory Default Configuration Set

To create a new configuration database file that does not contain user configuration information
1. Click Config on the home page.
2. Click the Manage Configuration Sets link in the System Configuration section.
3. Enter the name of the factory default configuration database file in the Create a new factory default configuration field.
4. Click Apply.

The new file appears in the list of database files on this page, but it is not selected as the current configuration database. The factory default configuration has not been loaded.

Note
Loading this configuration set will cause all system configurations to be deleted from the system. You cannot configure the system through Network Voyager until you configure an IP address through the system console.

Loading a Configuration Set

To switch a currently active database
1. Click Config on the home page.
2. Click the Manage Configuration Sets link in the System Configuration section.
3. Click the button next to the database, click Apply.
4. To make your changes permanent, click Save.

Deleting a Configuration Set

To delete unwanted configuration database files
1. Click Config on the home page.
2. Click the Manage Configuration Sets link in the System Configuration section.
3. Click the Delete Configuration Databases link.
4. For each database file to delete, click its Delete button in the table.
5. Click Apply.
6. Click Up to return to the Configuration Database Management page.

Backing Up and Restoring Files

Description of Creating Backup Files
You can configure your Nokia appliance to perform manual or regularly scheduled backups. By default, the backup file contains all of the configuration (/config), cron (/var/cron), etc (/var/etc), and IPSec files (/var/etc/IPSec). Export versions of Nokia IPSO do not include IPSec files. You can also choose to back up the home directories, which are stored in the /var/admin and /var/monitor directories and the log files, which are stored in the /var/logs directory.

Creating a Backup File Manually
1. Click Config on the home page.
2. Click the Configuration Backup and Restore link in the System Configuration section.
3. In the Manual Backup field, enter a file name for your backup file in the Backup File Name text box.

Note
If you do not enter a name, the backup file is not created.

4. (Optional) Click the Yes button in the Backup home directories field to include home directories in the backup file.
5. (Optional) Click the Yes button in the Backup log files field to include your log files in the backup file.
6. (Optional) To include package files in your backup file, click Yes next to the name of each package to back up in the Backup /opt fields.
7. Click Apply.
8. To make your changes permanent, click Save.

Creating a Regularly Scheduled Backup File

1. Click Config on the home page.
2. Click the Backup and Restore link in the System Configuration section.
3. In the Scheduled Backup field, in the Frequency drop-down list select Daily, Weekly, or Monthly to configure how often to perform a regular backup.
4. (Optional) If you selected Monthly in the Frequency drop-down list, click the Date drop-down list and select the date on which to schedule the monthly backup.
5. (Optional) If you selected Weekly in the Frequency drop-down list, click the Day drop-down list and select the day on which to schedule the weekly backup.
6. Click the Hour drop-down list to select the specific time of day for the system to perform a regular backup.
7. Click the Minute drop-down list and select 00, 15, 30, or 45 to specify the minute of the hour for the system to perform the regular backup.
8. Enter a name of the backup file in the Backup file name text box.

**Note**
If you do not enter a name, the backup file is not created.

9. (Optional) Click Yes in the Backup home directories field to include home directories in the backup file.
10. (Optional) Click Yes in the Backup log files field to include your log files in the backup file.
11. (Optional) To include package files in your backup file, click Yes next to the name of each package to back up in the Backup/opt fields.
12. Click Apply.
13. To make your changes permanent, click Save.

Automatically Transferring Backup Files to a Remote Server

To configure the system to automatically transfer backup files to a remote server on an hourly schedule

1. Click Config on the home page.
2. Click the Backup and Restore link in the System Configuration section.
3. Under Automatic Transfer of Archive File, choose whether to use FTP or TFTP as the file transfer protocol.
Note
If you choose FTP, make sure that your server accepts anonymous FTP logins. You cannot use non-anonymous FTP logins to automatically transfer backup files.

Caution
The TFTP option does not work with TFTP servers running on many Unix-based operating systems if there is not a file in the target directory on the remote server that has the same name as the backup file that is being transferred. 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.

4. Enter the IP address of the remote server.
5. If you chose FTP as the transfer protocol, indicate where the core files should be stored on the remote server by entering the appropriate path and directory.
6. Click apply.
7. To make your changes permanent, click Save.

Manually Transferring Backup Files to a Remote Server

1. Click Config on the home page.
2. Click the Backup and Restore link in the System Configuration section.
3. Under Manual Transfer of Archive File, enter the IP address of the FTP server in the FTP site text box.
4. Enter the path to the directory on which to save the backup files in the FTP dir text box.
5. Enter the name of the user account for connecting to the FTP server in the FTP user text box.
6. Enter the name of the password to use when connecting to the FTP server in the FTP password text box.

Note
You must change the password if you change the FTP server, FTP directory, or FTP user.

Note
The password is not stored in the database. Enter the password each time you want to transfer files to remote server even if you are using the same FTP server.

7. (Optional) Click Yes in the Backup home directories field to include home directories in the backup file.
8. (Optional) Click Yes in the Backup log files field to include your log files in the backup file.
9. (Optional) To include package files in your backup file, Click Yes next to the name of each package you want to back up in the Backup/opt field.

10. Click either the Manual backup file drop-down list or the Scheduled backup file drop-down list to select the backup files you want to transfer to the FTP server.

11. Click Apply.

12. To make your changes permanent, click Save.

Restoring Files from Locally Stored Backup Files

This procedure describes how to restore your files to the system from locally stored backup files. You must first create backup files. See “Creating a Backup File Manually” or “Creating a Regularly Scheduled Backup File”. You can restore files either from locally stored backup files or from files stored on a remote server. To store backup files on a remote server, see “Manually Transferring Backup Files to a Remote Server”.

Restoring Files from Locally Stored Files

1. Click Config on the home page.

2. Click the Backup and Restore link in the System Configuration section.

3. In the Restore from Local field, click either the Manual backup file drop-down window or the Scheduled backup file window to select the name of the backup file from which to restore. Manually backed-up files are in the /var/backup directory, and scheduled backup files are in the /var/backup/sched directory.

   The drop-down windows contain lists of all the files in the var/backup or /bar/backup/sched directory but some of the files might not be backup files.

4. Click Apply.

   Repeat the previous two steps for each file you want to restore.
5. Do not click Save. Ignore any Unsaved changes will be lost messages.
6. Click the Reboot link near the bottom of the page and wait for the system to reboot.

**Note**
You must reboot your system after restoring from backup files.

---

### Restoring Files from Backup Files Stored on a Remote Server

This procedure describes how to restore your files to the system from backup files stored on a remote server. You must first create backup files and then transfer the files to a remote server. See “Creating a Backup File Manually” or “Creating a Regularly Scheduled Backup File”. To store backup files on a remote server, see “Manually Transferring Backup Files to a Remote Server”.

1. Click Config on the home page.
2. Click the Backup and Restore link in the System Configuration section.

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

**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).

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

3. In the Restore from Remote field, enter the IP address of the FTP server on which the backup files are stored in the FTP site text box.
4. In the Restore from Remote field, enter the path to the directory on which the backup files are stored in the FTP dir text box.
5. In the Restore from Remote field, enter the user name for connecting to the FTP server in the FTP user text box.
6. In the Restore from Remote field, enter the password for connecting to the FTP server in the FTP password text box.
7. Click Apply.
8. A list of available files in the directory you specify appears. Select the backup files you want to restore.
9. Click Apply.
10. Do not click Save. Ignore any **Unsaved changes will be lost** messages.
11. Click the Reboot link at the bottom of the page and wait for the system to reboot.

**Note**
You must reboot your system after restoring from backup files.

---

### Deleting Locally Stored Backup Files

1. Click **Config** on the home page.
2. Click the **Backup and Restore** link in the System Configuration section.
3. In the **Delete Backup Files** field, click the Delete button next to the name of each backup file that you want to delete.
4. Click **Apply**, and then click **Save** to make your changes permanent.

### Scheduling Jobs Through the Crontab File

#### Configuring Scheduled Jobs

This procedure describes how to use Network Voyager to access the crontab file and schedule regular jobs. The cron daemon executes jobs at dates and times you specify through this procedure.

1. Click **Config** on the home page.
2. Click the **Job Scheduler** link the System Configuration section.
3. Enter a name for a job you want the cron daemon to execute in the **Job Name** text box. Use alphanumeric characters only, and do not include spaces.
4. Enter the name of the command you want the cron daemon to execute in the **Command name** text box. The command can be any Unix command.
5. To configure how often to execute the job, click the **Repeat** drop-down window and select **Daily**, **Weekly**, or **Monthly**. Click **Apply**.
6. To configure the Timezone, click the **Timezone** drop-down window and select **Local** or **Universal** to execute the timezone for the job.
7. (Optional) If you selected to execute the job monthly, click the **Date** drop-down window and select the date of the month to execute the job.
8. (Optional) If you selected to execute the job weekly, click the **Day** drop-down window and select the day of the week to execute the job.
9. Click the **Hour** drop-down window to select the hour of the day to execute the job.
10. Click the Minute drop-down window and select, 00, 15, 30, or 45 to select the minute of the day to execute the job.

11. Click Apply. If your configuration is successful, the job appears in the Scheduled Jobs table. To make your changes permanent, click Save.

12. To receive mail addressed to the admin or monitor regarding your scheduled jobs, enter your email address in the email address text box. Click Apply, and then click Save to make your changes permanent.

13. Repeat steps 1 through 10 to add new scheduled jobs.

Deleting Scheduled Jobs

1. Click Config on the home page.
2. Click the Job Scheduler link in the System Configuration section.
3. In the Scheduled Jobs table, click the Delete button next to the name of each job you want to delete.
4. Click Apply, and then click Save to make your changes permanent.

Managing Nokia IPSO Images

Selecting Nokia IPSO Images

To select an Nokia IPSO image
1. Click Config on the home page.
2. Click the Manage IPSO Images link in the System Configuration section.
3. Click the IPSO Image button in front of the image you want to select.
4. Click Reboot to activate the new image. The system will take a few minutes to reboot.

Testing Nokia IPSO Images

To test an Nokia IPSO image before permanently activating the image
1. Click Config on the home page.
2. Click the Manage IPSO Images link in the System Configuration section.
3. Click the Nokia IPSO Image button in front of the image you want to select.
4. Click the Test Boot button activate the new image. The system takes a few minutes to reboot.
5. Click Top.
6. Click the Manage IPSO Images link in the System Configuration section.
7. (Optional) Click the Commit testboot button to use the image you are testing.
8. (Optional) Click the Revert to previous image and Reboot button to use the original image.
9. Click Apply.
10. To make your changes permanent, click Save.

Deleting Nokia IPSO Images

To delete an Nokia IPSO image
1. Click Config on the home page.
2. Click the Manage IPSO Images link in the System Configuration section.
3. Click the Delete IPSO images link.
4. Click the delete button next to the image you want to delete; then click Apply.
5. To make your changes permanent, click Save.

Installing New Nokia IPSO Images

Upgrading the Nokia IPSO Image

This procedure describes how to use Network Voyager to upgrade the Nokia IPSO image. You can also upgrade the image from the command line. See the latest version of Nokia IPSO Release Notes, which is available on the Nokia customer support site: https://support.nokia.com for more information. To upgrade the image from Network Voyager, you must first install the image that is on the Nokia CD on an http server, ftp server, or file server.

Note
Diskless systems can store a maximum of two Nokia IPSO images.

1. Click Config on the home page.
2. Click the Install New IPSO Image link in the System Configuration section.
3. Enter the universal resource location (URL) or IP address of the ftp, http, or file server on which the Nokia IPSO image is installed in the Enter URL to the image location text box.

**Note**
If you enter a URL, the system must be configured to use a valid DNS server. You can use the DNS Configuration page to configure which DNS servers the system will use.

**Note**
If you enter the absolute path to an image on an FTP site, you must type a double slash (//) after the domain name. For example:

```
ftp://test.acme.com//tmp/ipso.tgz
```

If you enter a path that is relative to the home directory of the user whose name and password you enter in step 5 and step 6, use the standard URL format. For example:

```
ftp://test.acme.com/tmp/ipso.tgz
```

4. (Optional) If the HTTP site on which the Nokia IPSO image is stored requires authentication, enter the HTTP realm to which authentication is needed in the Enter HTTP Realm (for HTTP URLs only) text box.

5. (Optional) If the server on which the Nokia IPSO image is stored requires authentication, enter the user name in the Enter User Name text box.

6. (Optional) If the server on which the Nokia IPSO image is stored requires authentication, enter the password in Enter Password text box.

7. Specify whether the installed packages (such as VPN-1/FireWall-1 packages) start automatically after the system is rebooted with the new image.

8. Click Apply.
   A message appears that tells you that the upgrade process could take a long time if the network is slow.

9. Click Apply again.
   The system downloads the specified image file.

10. To see messages about the status of the download and installation process, click New image installation status.

11. When you see the following message at the bottom of the list of messages, the download and installation process is complete:

    ```
    To install/upgrade your packages run /etc/newpkg after REBOOT
    ```

12. If you made configuration changes, click Save.

13. Click Manage IPSO images (including REBOOT and Next Boot Image Selection).

14. Under Select an image for next boot, select the image you just installed.

15. Select one of the following options for rebooting the system:
    - To reboot with the newly installed image, click Reboot.
To test boot the new image, click Test Boot.

**Note**
When you click Test Boot, the system tests the new image for five minutes. If you let the five-minute test period expire without committing to the new image, the system automatically reboots and reverts to the previous image.

A new page appears, and you see a message telling you that the system will be rebooted. Do not click anything on this page.

If you did not choose the test boot option, the upgrade is complete after the appliance reboots. You do not need to do anything else.

If you chose the test boot option and want the system to continue with the new image, you have five minutes after the system restarts to perform the following steps. If you do not perform these steps within five minutes, the system automatically reboots the previous image.

1. Log in to the system.
   The Nokia IPSO Image Management page appears.
2. Click Testboot Commit.
   The new image is now the default image.

### Upgrading Nokia IPSO Images for a Cluster

You can use Cluster Voyager to upgrade the Nokia IPSO image on all the cluster nodes. After you see that the new image is successfully installed on all of the nodes, you need to reboot them so that they will run the new image. For more information about Cluster Voyager, see “Managing a Cluster” in the section on configuring traffic management.

### Rebooting a cluster

When you click Reboot, Shut Down System on the main configuration page in Cluster Voyager, you see the Cluster Traffic Safe Reboot link. If you click this link, the cluster nodes are rebooted in a staggered manner. The process is managed so that at least one node is always operational. For example, if you reboot a two-node cluster, one node restarts first. The second node waits for the first node to restart successfully and rejoin the cluster before it reboots. If the first node does not successfully rejoin the cluster, the first node does not reboot.

### Downgrading Nokia IPSO Images

When you downgrade an IPSO image, the system behaves differently depending on whether the version you are downgrading to was previously installed on the appliance:

- When you revert to a previously installed IPSO version, the system accesses and uses the network connectivity information configured for that version.
When you downgrade to an earlier IPSO version that has never been installed on your appliance, the system carries over the configuration information related to basic connectivity. This functionality allows you to perform this type of downgrade over a network connection.

If you are using IPSO 3.9, you can use this method to downgrade only to IPSO 3.8, 3.7, or 3.6.

Only when you are downgrading to a version that was never on your appliance is the connectivity information from the already installed IPSO version carried over to the less recent version that you are installing. The configuration information carried over includes:

- Interface configurations
- Passwords
- SNMP user information
- Hostname
- Default gateway
- DHCP
- SSH
- Modem and TTY

Other configuration information is not carried over and all other parameters are set to factory defaults. When you downgrade to a previously-installed IPSO version, no information is carried over—all configurations, including connectivity information from the previous version is retained and used.

When you install a new image for a previous version that was never on your appliance, the following message is displayed:

WARNING: Configuration set for <target release> does not exist. Will attempt to create a new configuration set with connectivity only information. All other configuration changes will be lost.

You are also instructed to perform a test boot, just as you would with any other fresh install.

**Note**
If you downgrade to IPSO 3.6 and it was not previously installed on the appliance, users with RSA authorization might lose connectivity. This is because the SSH configuration for IPSO 3.6 might not be fully compatible with later IPSO version, and the RSA keys might not be carried over.
Managing Packages

Installing Packages

**Note**
You can install a maximum of two versions of Check Point's VPN-1/FireWall-1 on IP2250 systems. The only packages you can install are
* VPN-1/FireWall-1 NG with Application Intelligence (R55) for Nokia IPSO 3.8 (or later)
* SVN Foundation
* Policy Server

To install a package

1. Click Config on the home page.
2. Click the Manage Installed Packages link in the System Configuration section.
3. Click the FTP and Install Packages link.
4. Enter the hostname or IP address of the FTP site where the packages are located.
5. Enter the FTP directory where the packages reside at the FTP site.
6. (Optional) Enter the user account and password to use when connecting to the FTP site. If you leave these fields empty, the anonymous account is used.

**Note**
If you specify a user account and password, you must re-enter the password whenever you change the FTP site, FTP directory, or FTP user on future requests.

7. Click Apply.

**Note**
A list of files ending with extensions .tgz, .Z, and .gz in the specified FTP directory appears in the Site Listing field.

8. Select a package to download from the Site Listing field, then click Apply.
   The selected package is downloaded to the local Nokia IPSO system. After the download is complete, the package appears in the Unpack New Packages field.
9. Select the package in the Unpack New Packages field, then click Apply.
   The package is unpacked into the local file system.
10. Click the **Click here to install/upgrade [file name]** link.
11. (Optional) Click Yes next to **Display all packages**, then click Apply to display all of your installed packages.
12. (Optional) Click Yes next to Install, then click Apply to perform a first-time installation.
13. (Optional) Click Yes next to Upgrade.
14. (Optional) Click the button of the package from which you want to upgrade under Choose one of the following packages to upgrade from.
15. Click Apply.
16. Click Save to make your changes permanent.

**Enabling Packages**

**To enable a package**
1. Click Config on the home page.
2. Click the Manage Installed Packages link in the System Configuration section.
3. Click On next to the package you want to enable, then click Apply.
4. Click Save.

**Disabling Packages**

**To disable a package**
1. Click Config on the home page.
2. Click the Manage Installed Packages link in the System Configuration section.
3. Click Off next to the package to disable, then click Apply.
4. To make your changes permanent, click Save.

**Deleting Packages**

**To delete a package**
1. Click Config on the home page.
2. Click the Manage Installed Packages link in the System Configuration section.
3. Click the Delete Packages link.
4. Click Delete next to the package you want to delete, then click Apply.
5. To make your changes permanent, click Save.

**Advanced System Tuning**

The configurations in this section are intended for specific purposes, and, under most circumstances, you should not change any of the default settings.
Tuning the TCP/IP Stack

When a TCP connection is established, both ends of the connection announce their TCP maximum segment size (MSS). The MSS setting is the value that your system advertises, and you can change the value to tune TCP performance by allowing your system to receive the largest possible segments without their being fragmented.

This MSS configuration is subject to the following:

- It is only applicable to TCP.
- It sets the TCP MSS for packets that this system generates (as well as packets it receives). If a remote terminating node advertises an MSS higher than the MSS configured on this system, this system will send packets that have the segment size configured with this feature. For example, if you set this value to 512 and a remote system advertises 1024, this system sends packets with a TCP segment size of 512.
- It is only relevant to Check Point security servers or similar products that require the Nokia appliance to terminate the connection.
- Only the remote terminating node responds to the MSS value you set; that is, intermediate nodes do not respond. Generally, however, intermediate notes can handle 1500-byte MTUs. Your system advertises the MSS value you set, and remote terminated nodes respond by sending segments in packets that do not exceed your advertised value. This segment size your system advertises should be 40 bytes less than the smallest MTU between your system and the outgoing interface. The 40-byte difference allows for a 20-byte TCP header and a 20-byte IP header, which are included in the MTU.

To set the TCP MSS

1. Click Config on the home page.
2. Click the Advanced System Tuning link in the System Configuration section.
3. Enter the value you will use for your MSS.
   - The range for this value is 512 through 1500, and the default value is 1024. If you enter a value outside of this range, an out-of-range error is generated.
4. Click Apply.
5. Click Save to make your changes permanent.

Router Alert IP Option

You can use this feature 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.)
Chapter Contents

- Overview
  - IPv6 Description
- Interfaces
  - Configuring IPv6 Logical Interfaces
  - Deleting an IPv6 Address
  - Disabling IPv6 on an Interface
  - Configuring Neighbor Discovery
- IPv6 and IPv4 Compatibility
  - Configuring IPv6 in IPv4 Tunnels
  - Configuring IPv6 to IPv4
  - Configuring IPv6 over IPv4
  - Configuring IPv4 in IPv6 Tunnels
  - Configuring an IPv6 Default Route
  - Creating an IPv6 Static Route
- Routing Configuration
  - Configuring OSPFv3
  - Configuring RIPng
  - Creating IPv6 Aggregate Routes
  - Creating Redistributed Routes
  - Redistributing Static Routes into RIPng
- Router Discovery
  - Configuring ICMPv6 Router Discovery
- VRRP for IPv6
  - Configuring VRRP for IPv6
  - Creating a Virtual Router for an IPv6 Interface Using VRRPv3
  - Creating a Virtual Router to Back Up Another VRRP Router Addresses Using VRRPv3
  - Monitoring the Firewall State
  - Setting a Virtual MAC Address for a Virtual Router
Overview

IPv6 Description

IPv6 is the next generation IP protocol and is expected to replace IPv4, the current IP protocol. The Internet Engineering Task Force (IETF) formally began to work on the new protocol in 1994. IPv6 enhances IPv4 in many ways including:

- Expanded addressing capabilities
- Simplified header format
- Improved support for extensions and options
- Flow-labeling capability
- Plug and play autoconfiguration

The IPv6 implementation includes basic features specified in IPv6 RFCs and features that support IPv6-capable hosts in a network.

IPv6 includes a transition mechanism that allows users to adopt and deploy IPv6 in a diffuse way and provides direct interoperability between IPv4 and IPv6 hosts.

IPSO supports the following features as specified in the corresponding RFCs:

- IPv6 Specification (RFC 2460)
- ICMP v6 (RFC 2463)
- Neighbor Discovery (RFC 2461, router only)
- Basic IPv6 Socket Interface (RFC 2553), except the following features:
  - Compatibility with IPv4 nodes
  - Translation of nodename to address
  - Translation of address to nodename
  - Socket address structure to nodename and service name
- IPv6 Addressing Architecture (RFC 2373)
- IPv6 Aggregatable Global Unicast Address Format (RFC 2374)
- IPv6 UDP support
- IPv6 TCP support
- IPv6 over IPv4 Tunnel (RFC 2185)
- IPv6 over Ethernet (RFC 2464)
- IPv6 over FDDI (RFC 2467)
- IPv6 over PPP (RFC 2472)
- IPv6 over ATM (RFC 2492, PVC only)
- IPv6 over ARCNET (RFC 2497)
- IPv6 over Token Ring (RFC 2470)
- IPv6 over IPv4 (RFC 2529)
- IPv6 to IPv4 (Internet Draft)
- Generic Packet Tunneling (RFC 2473, IPv4 through IPv6 only)
- RIPng for IPv6
- Static Routes
- Route Aggregation
- Route Redistribution
- IPv6 inetd
- IPv6 telnet client and server
- IPv6 FTP client and server
- Utilities (ping, netstat, tcpdump, ndp)

**Interfaces**

**Configuring IPv6 Logical Interfaces**

1. Click Config on the home page.
2. Click the IPv6 Logical Interfaces link in the IPv6 section.
3. Click the logical interface link to configure in the Logical column.
   
   **Example:** eth-slplc0

4. Enter the IP address prefix in the New IP Address text box and the mask length (in bits) in the New Mask Length text box.
   The default mask length is 64.
5. Click Apply.
6. Click Save to make your changes permanent.
7. Click Up at the top of the page to take you back to the IPv6 Logical Interfaces page.
8. To enable the IPv6 address, click On in the IPv6 Active field.
9. Click Apply.
10. Click **SAVE** to make your change permanent.

**Deleting an IPv6 Address**

1. Click **Config** on the home page.
2. Click the IPv6 Logical Interfaces link in the IPv6 section.
3. Click the logical interface link to configure in the Logical column for which you want to delete an IPv6 address.
   
   **Example:** eth-s1p1c0
4. Check the delete box next to the IPv6 address you want to delete.
   
   Click **Apply**.
5. Click **Save** to make your changes permanent.

**Disabling IPv6 on an Interface**

1. Click **Config** on the home page.
2. Click the IPv6 Logical Interfaces link in the IPv6 section.
3. To disable IPv6 on a specific logical interface, click off in the IPv6 active field next to the name of that 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, Network Voyager 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.

4. Click **Apply**.
   
   The list of addresses in the IPv6 address field for the specified logical interface disappear.
5. Click **Save** to make your changes permanent.

**Configuring Neighbor Discovery**

1. Click **Config** on the home page.
2. Click the Neighbor Discovery link in the IPv6 section.
3. In the Global Neighbor Discovery Settings field, enter the value for the queue limit in the Queue Limit text box.
   
   This value represents the maximum number of output packets to be queued while the link-layer destination address is being resolved.
4. In the Global Neighbor Discovery Settings field, enter the value for the unicast retry limit in the Unicast Retry Limit text box.
   This value represents the number of times to retry Unicast Neighbor Discovery requests.
5. In the Global Neighbor Discovery Settings field, enter the value for the multicast retry limit in the Multicast Retry Limit text box.
   This value represents the number of times to retry Multicast Neighbor Discovery requests.
6. In the Global Neighbor Discovery Settings field, enter the value for the duplicate address detection retry limit in the Duplicate Address Detection Retry Limit text box. This value represents the number of times to retry Duplicate Address Detection Neighbor Discovery requests.
7. In the Permanent Neighbor Discovery Entries field, enter the permanent IPv6 address for the permanent neighbor discovery destination in the New Permanent Neighbor Discovery Entry text box.
8. Click Apply.
9. Click Save to make your changes permanent.
10. To flush current dynamic Neighbor Discovery entries, click Flush in the Dynamic Neighbor Discovery Entries field.
11. Click Apply.

**IPv6 and IPv4 Compatibility**

**Configuring IPv6 in IPv4 Tunnels**

If your IPv6 traffic needs to travel through IPv4 networks to reach its destination, you need to set up a virtual link by configuring a tunnel.

1. Click Config on the home page.
2. Click the IPv6 in IPv4 Tunnels link in the IPv6 section.
3. Enter the IPv4 address of the local tunnel endpoint in the Local IPv4 Address text box.
4. Enter the IPv4 address of the remote tunnel endpoint in the Remote IPv4 Address text box.

**Note**
The local address must be the address of another interface configured for the router.

5. (Optional) Enter the IPv6 link-local address of the local tunnel endpoint in the Local IPv6 Link Local text box.
   If you do not specify an address a default will be configured.
6. (Optional) Enter the remote IPv6 link-local address of the remote tunnel endpoint in the Remote IPv6 Link Local text box.
7. (Optional) Enter a value in the Time to Live text box for the Time to Live (TTL) packets sent on the tunnel.
8. Click Apply.
9. Click Save to make your changes permanent.

Configuring IPv6 to IPv4

This feature allows you to connect an IPv6 domain through IPv4 clouds without configuring a tunnel.

1. Click Config on the home page.
2. Click the IPv6 to IPv4 link in the IPv6 section.
3. In the Enable IPv6 to IPv4 field, click Yes.
4. In the Active field, just below the Logical Interface field, click On to enable the logical interface.

This value represents the pseudo-interface that is associated with this feature. It does not correspond to a specific physical device.
5. Enter the IPv4 address of the local interface in the Local IPv4 Address text box.

Note
This address must be the address of another interface configured for the router.

6. (Optional) Enter a value in the Time to Live text box for the Time to Live (TTL) packets sent.
7. Click Apply.
8. Click Save to make your changes permanent.

Configuring IPv6 over IPv4

This feature allows you to transmit IPv6 traffic through IPv4 domains without configuring a tunnel.

1. Click Config on the home page.
2. Click the IPv6 over IPv4 link in the IPv6 section.
3. In the Enable IPv6 over IPv4 field, click Yes.
4. In the Active field, just below the Logical Interface field, click On.

This value represents the pseudo-interface that is associated with this feature. It does not correspond to a specific physical device.
5. Enter the IPv4 address of the local interface in the Local IPv4 Address text box.
6. (Optional) Enter a value in the Time to Live text box for the Time to Live (TTL) packets sent.
7. Click Apply.
8. Click Save to make your changes permanent.

Configuring IPv4 in IPv6 Tunnels

This feature allows you to set up a point-to-point link to permit traffic from IPv4 domains to travel through IPv6 domains.

1. Click Config on the home page.
2. Click the IPv4 in IPv6 Tunnels link in the IPv6 section
3. Enter the IPv6 address of the local tunnel endpoint in the Local IPv6 Address text box.
4. Enter the IPv6 address of the remote tunnel endpoint in the Remote IPv6 Address text box.
5. (Optional) Enter a value in the Hop Limit text box for the maximum number of hops the packets sent on the tunnel can take to reach their destination.
6. Click Apply.
7. Click Save to make your changes permanent.

Configuring an IPv6 Default Route

1. Click Config on the home page.
1. Click the Static Routes link in the IPv6 section.
2. To enable a default route, click On in the Default field, and click Apply.
3. Enter the IPv6 address of the gateway router in the Next Hop text box.
4. Select the type of next hop the static route will take from the Next Hop Type drop-down list. The options are normal, reject, and black hole.
5. Select the interface that the static route will use to reach the gateway in the Interface field.

Note
This interface must be specified only if the gateway is a link local address.

6. To specify the order in which next hops are selected, enter a value from one to eight in the Preference text box. 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.

The preference option also supports equal-cost multipath routing. For each preference 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.

7. Click Apply.
8. Click Save to make your changes permanent.

Creating an IPv6 Static Route

1. Click Config on the home page.
2. Click the Static Routes link in the IPv6 section.
3. Enter the IPv6 address prefix in the New Static Route text box.
4. Enter the mask length (number of bits) in the Mask Length text box.
5. Click Apply.
6. Enter the IPv6 address of the gateway router in the Next Hop text box.
7. Select the type of next hop the static route will take from the Next Hop Type drop-down list.
8. Select the interface the static route will take to reach the gateway in the Interface field.
9. To specify the order in which next hops are selected, enter a value from one to eight in the Preference text box.
   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.
   The preference option also supports equal-cost multipath routing. For each preference 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.
10. Click Apply.
11. Click Save to make your changes permanent.

Routing Configuration

Configuring OSPFv3

IPSO supports OSPFv3, which supports IPv6 addressing and is based on RFC 2740. OSPFv3 has essentially the same configuration parameters as OSPFv2, except that you enter them from the Network Voyager page that you access by clicking Config (on the home page) > IPv6 Configuration > OSPFv3 (in the Routing Configuration section). For more information, see “OSPF Description” on page 171 and “Configuring OSPF” on page 173.
Configuring RIPng
1. Click Config on the home page.
2. Click the RIPng link in the IPv6 section.
3. To enable RIPng, click On next to the logical interface on which you want to run RIP, and then click Apply.
4. Enter a value in the Metric text box for the RIPng metric to be added to routes that are sent by way of the specified interface.
5. Click Apply.
6. Click Save to make your changes permanent.

Creating IPv6 Aggregate Routes
1. Click Config on the Home Page.
2. Click the IPv6 Route Aggregation link in the IPv6 section.
3. Enter the IPv6 prefix for the new aggregate route in the Prefix for New Aggregate text box.
4. Enter the mask length (number of bits) in the Mask Length text box.
5. Click Apply.
6. Scroll through the New Contributing Protocol List click the protocol you want to use for the new aggregate route.
7. Click Apply.
8. Click Save to make your changes permanent.
9. Click On in the Contribute All Routes from <Protocol> field.
10. (Optional) To specify an IPv6 prefix, enter the IPv6 address and mask length in the text boxes in the Prefix for New Contributing Route from <Protocol> field.
11. Click Apply, and click Save to make your changes permanent.

Creating Redistributed Routes

Redistributing Static Routes into RIPng
1. Click Config on the home page.
2. Click the Route Redistribution link in the IPv6 section.
3. Click the Static Routes link.
4. To redistribute all currently valid static routes into RIPng, click the On button in the Distribute all Statics in the RIPng field.
5. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.
6. Click Apply.
7. Click Save to make your changes permanent.
8. To redistribute a specific static route or routes into RIPng, click On next to the IPv6 interface for the static route to redistribute to RIPng.
9. Enter a value in the Metric text box for the metric cost that the created RIPng route(s) will have.
10. Click Apply.
11. Click Save to make your changes permanent.

Redistributing Aggregate Routes in RIPng

1. Click Config on the home page.
2. Click the Route Redistribution link in the IPv6 section.
3. Click the Aggregate Routes link.
4. To redistribute all currently valid aggregate routes into RIPng, click On in the Redistribute all Aggregates into RIPng field.
5. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.
6. Click Apply.
7. Click Save to make your changes permanent.
8. To redistribute a specific aggregate route or routes into RIPng, click On next to the IPv6 interface for the aggregate route to redistribute into RIPng.
9. Enter a value in the Metric text box for the metric cost that the created RIPng route will have.
10. Click Apply.
11. Click Save to make your changes permanent.

Redistributing Interface Routes into RIPng

1. Click Config on the home page.
2. Click the Route Redistribution link in the IPv6 section.
3. Click the Interface Routes link.
4. To redistribute all currently active interface routes into RIPng, click On in the Export all Interfaces into RIPng field.
5. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.
6. Click Apply.
7. Click Save to make your changes permanent.
8. To redistribute a specific interface route or routes into RIPng, click On next to the IPv6 interface for the route to redistribute into RIPng.

9. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.

10. Click Apply.

11. Click Save to make your changes permanent.

Router Discovery

Configuring ICMPv6 Router Discovery

The ICMPv6 Router Discovery Protocol allows hosts running an ICMPv6 router discovery client to locate neighboring routers dynamically as well as to learn prefixes and configuration parameters related to address autoconfiguration. Nokia implements only the ICMPv6 router discovery server portion, which means that the Nokia platform can advertise itself as a candidate default router, but it will not adopt a default router using the router discovery protocol.

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. When VRRP failover occurs, the new master begins to send out router discovery advertisements. For more information about configuring VRRP for IPv6 interfaces, see “Configuring VRRP for IPv6.”

1. Click Config on the home page.

2. Click the ICMPv6 Router Discovery link in the IPv6 section.

3. To enable ICMPv6 router discovery, click On next to the interface on which you want to run the protocol.

4. Click Apply.

5. (Optional) To enable the managed address configuration flag in the router advertisement packet, click Yes in the Managed Config Flag field.

   This flag enables hosts to perform stateful autoconfiguration to obtain addresses.

6. (Optional) To enable the other stateful configuration flag in the router advertisement packet, click Yes in the Other Config Flag field.

   This flag enables hosts to perform stateful autoconfiguration to obtain information other than addresses.

7. (Optional) To enable the MTU options field in the router advertisement packet, click Yes in the Send MTU Option field.
8. (Optional) Enter a value (in seconds) in the Min Adv Interval text box for the minimum time between which unsolicited multicast ICMPv6 router advertisements are sent on the interface.

9. (Optional) Enter a value (in seconds) in the Max Adv Interval text box for the maximum time between which unsolicited multicast ICMPv6 router advertisements are sent on the interface in the Max Adv Interval text box.

Whenever an unsolicited advertisement is sent, the timer is set to a value between the maximum advertisement interval and the minimum advertisement interval.

10. (Optional) Enter a value (in seconds) in the Router Lifetime text box for a router advertisement packets router lifetime field.

A value of zero indicates that the router is not to be used as a default router.

11. (Optional) Enter a value in the Reachable Time text box for the router advertisement packets reachable time field.

The value represents the time that a node assumes a neighbor is reachable after having received a reachability confirmation.

12. (Optional) Enter a value (in seconds) in the Retransmission Timer text box for the router advertisement packets retransmission timer field.

This value represents the time between which neighbor solicitation messages are retransmitted if the node doesn’t receive a response.

13. (Optional) Enter a value in the Cur Hop Limit text box for the router advertisement packets hop limit field.

14. (Optional) To specify that the IPv6 prefix can be used for on-link determination, click Yes in the Onlink Flag field.

15. (Optional) To specify that the IPv6 prefix can be used for autonomous address configuration, click Yes in the Autonomous Flag field.

16. (Optional) Enter a value (in seconds) in the Prefix Valid Lifetime text box for the prefix information options valid lifetime field.

This value represents the length of time—relative to the time the packet is sent—that the prefix is valid for the purpose of on-link determination.

17. (Optional) Enter a value (in seconds) in the Prefix Preferred Lifetime text box for the prefix information options preferred lifetime field.

This value represents the length of time—relative to the time the packet is sent—that addresses that are generated by the prefix through stateless autoconfiguration remain preferred.

18. Click Apply.

19. Click Save to make your changes permanent.
VRRP for IPv6

Configuring VRRP for IPv6

Beginning with IPSO 3.8.1, Nokia supports VRRP configuration for IPv6 interfaces. Nokia supports VRRP version 3, which is based on VRRP version 2 as defined for IPv4 in RFC 3768, and Monitored Circuit.

Unlike VRRP version 2, VRRP version 3 does not support authentication, and the advertisement interval in the VRRP packet is 12 bits rather than eight bits. Also, for both VRRP version 3 and Monitored Circuit for IPv6 interfaces, the hello interval is measured in centiseconds rather than seconds. In version 3, the first address in the packet must be an IPv6 link-local address. For more general information about VRRP, see “Understanding VRRP.”

For more information about how to configure Check Point NG with Application Intelligence for VRRP for IPv6 see, “Configuring Check Point NGX with Application Intelligence for VRRP.”

Note
Check Point NG with Application Intelligence does not support user, session, or client authentication for IPv6 interfaces.
Also, Check Point NG does not support state synchronization for IPv6 interfaces. When a master router of a VRRP pair fails, and the backup router becomes the new master, all previously established connections are lost because state synchronization does not occur.

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. When VRRP failover occurs, the new master begins to send out router discovery advertisements. For more information about configuring Router Discovery for IPv6 interfaces, see “Configuring ICMPv6 Router Discovery.”

Creating a Virtual Router for an IPv6 Interface Using VRRPv3

You must configure a virtual router on an interface to enable other routers to back up its addresses.

1. Click Config on the home page.
2. Click IPv6 Configuration link.
3. Click the VRRP for IPv6 link.
4. Click VRRPv3 button next to the interface for which to enable VRRP. Click Apply.
5. Enter a value from 1 to 255 in the Own VRID text box to specify a virtual router ID for the virtual router. Click Apply.

Additional configuration options appear on the Network Voyager page after you click Apply.
Note
Other routers on the LAN use the virtual router ID to back up the addresses of this router. No other router on the LAN can use this value to configure VRRP for its own addresses.

6. From the Address drop-down list select an IP address to specify a virtual IPv6 address for the virtual router. Click Apply. You must configure at least one virtual address, and at least one virtual IPv6 address must be the link-local address for the interface. To remove a virtual IP address, click off next to the entry for the IPv6 address.

7. (Optional) In the Hello Interval text box, enter a value from 1 to 4095 to specify the interval, in centiseconds, that is, 1 one-hundredth of a second, between VRRP advertisement transmissions. This value should be the same on all the routers with this virtual router configured. The default is 100 centiseconds, that this 1 second. Click Apply.

8. To make your changes permanent, click Save.

Creating a Virtual Router to Back Up Another VRRP Router Addresses Using VRRPv3

Note
Do not turn on the VRRP backup router before the VRRP master is configured. This leads to a service outage because the VRRP backup router takes over the IP address while the master is still active with that IP address. To configure the master router, see “Creating a Virtual Router for an IPv6 Interface Using VRRPv3.”

Use this procedure to configure virtual routers to back up the addresses of other routers on a shared media network.

1. Click Config on the home page.
2. Click the IPv6 Configuration link.
3. Click the VRRP for IPv6 link.
4. Click VRRPv3 button next to the interface for which to enable VRRP. Click Apply.
5. In the Backup Router with VRID text box, enter a value of from 1 to 255 to specify a virtual ID for the virtual router used to back up the IP addresses of another system. The router you are backing up must also have this virtual router configured for its addresses. Click Apply. Additional configuration options appear that let you enter the IPv6 addresses of the router you are backing up.
6. (Optional) Enter a value from 1 to 254 in the Priority text box to specify the priority of this router during contention for the IP addresses of a failed router. Of the routers backing up the
failed router, the one with the priority of highest value take overs the addresses. The default value is 100.

7. (Optional) In the Hello Interval text box, enter a value from 1 to 4095 to specify the interval, in centiseconds, that is, 1 one-hundredth of a second, between VRRP advertisement transmissions. This value should be the same on all the routers with this virtual router configured. The default is 100 centiseconds, that is, 1 second.

8. (Optional) Click Disabled next to Preempt Mode if you do not want a virtual router with a higher priority to preempt the current master router and become the new master. The default value is Enabled, which means that a virtual router with a higher priority than the current master preempts the master and becomes the new master router.

9. (Optional) Click Enabled next to Accept Mode if you want the virtual router when it is in a master state to accept and respond to IP packets sent to virtual IPv6 addresses. The VRRP protocol specifies not to accept or respond to such IP packets, so the default is Disabled.

10. Enter an IPv6 address for this virtual router in the Backup Address text box. The first backup address you configure must be a link-local address. Any link-local address must belong to the fe80::/64 subnet, and global addresses must belong to the subnet of the interface.

11. (Optional) If the router you are backing up had more than one IP address, repeat step 10.

12. Click Apply, and then click Save to make your changes permanent.

**Monitoring the Firewall State**

You can configure the system 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.

This option does not affect the functioning of your system if a firewall is not installed.

1. Click Config on the home page.
2. Click the IPv6 Configuration link.
3. Click the VRRP for IPv6 link.
4. Click Enabled in the Monitor Firewall State field.
5. To disable this option, if you have enabled it, click Disabled. The default is Enabled.
6. Click Apply, and then click Save to make your changes permanent.

**Setting a Virtual MAC Address for a Virtual Router**

This feature allows you to set a virtual MAC (VMAC) address for a virtual router by using one of three options. The implementation continues to support the default selection of a VMAC through the method outlined in the VRRP protocol specification. All three modes are useful for
Virtual LAN deployments, which forward traffic based on the VLAN address and destination MAC address.

- The Interface mode selects the interface hardware MAC address as the VMAC.
- In the Static mode, you specify fully the VMAC address.
- In the extended mode, the system dynamically calculates three bytes of the interface hardware MAC address to extend its range of uniqueness.

**To set the virtual MAC address**

1. Click Config on the home page.
2. Click the IPv6 Configuration link.
3. Click the VRRP for IPv6 link.
4. You can set the VMAC option for an interface on which you enable VRRP or Monitored Circuit
   a. To enable VRRP, click the VRRPv3 button next to the interface for which to enable VRRP, and then click Apply.
      To specify the virtual router ID for the virtual router used to back up the local interface address(es) of the interface, enter a value of from 1 to 255 in the Own VRID text box. Click Apply.
      To specify the virtual router ID for the virtual router used to back up IP address(es) of another system, enter a value of from 1 to 255 in the Backup Router with VRID edit box. Click Apply.
      A Backup Address text box appears that allows you to add an IP address for this virtual router.
   b. To enable Monitored Circuit, click the Monitored Circuit button next to the interface for which to enable Monitored Circuit, and then click Apply.
      To specify the virtual router ID for the virtual router to be used to back up the local interface address(es), enter a value of from 1 to 255 in the Create Virtual Router text box. Click Apply.
      Enter the IP address you want to assign to the virtual router back up in the Backup Address edit box. Click Apply.

**Note**
The IP address(es) associated with the monitored circuit virtual router must not match the real IP address of any host or router on the network of the interface.

5. To set a VMAC address, click the VMAC Mode drop-down list and select either Interface, Static, or Extended. VRRP is the default. If you select Static, you must enter the VMAC address that you want to use in the Static VMAC text box. Click Apply, and then click Save to make your changes permanent.
Note
If you set the VMAC mode to interface or static, you will get syslog error messages when you reboot, or at failover, indicating duplicate IP addresses for the master router and backup router. This is expected behavior since both the master router and the backup router will be using the same virtual IP address temporarily until they resolve into master and backup.

Changing the IP Address List of a Virtual Router in VRRPv3

You must configure at least one virtual address for a virtual router. Addresses already configured are displayed in the List of IPv6 addresses field. Addresses that belong to the interface but not selected for the virtual router are displayed in the Addresses drop-down list.

1. Click Config on the home page.
2. Click the IPv6 Configuration link.
3. Click the VRRP for IPv6 link.
4. Locate the virtual router and the interface with the IP address to change.
   You can locate the virtual router information by using the VRID value displayed in the Router with VRID field.
5. To remove an IP address from the list, in the List of IPv6 addresses field, click Off next to the address you want to delete.
   Click Apply.
6. To add an IP address, select an address from the Address drop-down list.
   Click Apply.
7. To add a backup IP address, enter the IP address in the Backup Address text box.
   Click Apply.
8. To make your changes permanent, click Save.

Removing a Virtual Router in VRRPv3

When you disable a virtual router, the VRRP operation terminates, and the configuration information no longer appears on the VRRP for IPv6 Configuration page in Network Voyager. Failover of the default router no longer occurs. When you disable a virtual router, you must first remove the VRRP configuration for that virtual router from all of the backup routers.

You must not delete the virtual router on the default router first, as it stops sending VRRP advertisements. This results in the backup routers assuming that the default router has failed, and one of the backup routers automatically adopts the backup address of the default router. This situation results in two routers having the address of the default router configured.

1. Click Config on the home page.
2. Click the IPv6 Configuration link.
3. Click the VRRP for IPv6 link.
4. Locate the virtual router to remove.
   a. To locate a virtual router used to back up the local interface IP addresses, find the correct virtual ID in the Own VRID field.
   b. To locate a virtual router used to back up the IP addresses of another router, find the correct virtual ID in the Router with VRID field.
5. Click off next to the entry for the VRID of the virtual router you want to remove.
6. Click Apply.
   All the information about that specific virtual router disappears from the Network Voyager configuration page.
7. To make your changes permanent, click Save.

Creating a Virtual Router in Monitored Circuit Mode for IPv6

The monitored circuit feature makes the election of the virtual master router dependent on the current state of the access link. You can select which interfaces on which to associate dependency and configure a priority delta for each interface you select. The up and down status of each interface is monitored, and the election of the VRRP master dynamically adapts to the current state of each interface selected for dependency. For specific information on configuring specific interfaces on which to associate dependency, see “Setting Interface Dependencies for a Monitored Circuit Virtual Router for IPv6.”

The IPv6 address associated with a monitored circuit virtual router must not match the actual IPv6 address of the host or router on the network of the interface. The first address you configure must be a link-local address.

1. Click Config on the home page.
2. Click the IPv6 Configuration link.
3. Click the VRRP for IPv6 link.
4. To enable Monitored Circuit, click the Monitored Circuit button next to the interface for which to enable Monitored Circuit, and then click Apply.
5. To specify the virtual router ID for the virtual router to be used to back up the local interface address(es), enter a value of from 1 to 255 in the Create Virtual Router text box. Click Apply.
6. (Optional) In the Hello Interval text box, enter a value from 1 to 4095 to specify the interval, in centiseconds, that is, 1 one-hundredth of a second, between VRRP advertisement transmissions. This value should be the same on all the routers with this virtual router configured. The default is 100 centiseconds, that is, 1 second.
7. (Optional) Click Disabled next to Preempt Mode if you do not want virtual router with a higher priority to preempt the current master router and become the new master. The default is Enabled, which means that a virtual router with a higher priority than the current master preempts the master and becomes the new master router.
8. (Optional) Click Enabled next to Accept Mode if you want to a virtual router in a master state to accept and respond to IP packets sent to virtual IPv6 addresses. The VRRP protocol specifies not to accept or respond to such IP packets, so the default is Disabled.

9. Enter an IPv6 address for this virtual router in the Backup Address text box. The IPv6 address associated with a monitored circuit virtual router must not match the actual IPv6 address of any host or outer on the network of the interface. The first back-up address you configure must be a link-local address. Any link-local address must belong to the fe80::/64 subnet, and global addresses must belong to the subnet of the interface.

10. (Optional) If the router you are backing up has more than one IP address, repeat step 10.

11. (Optional) Click Enabled in the Auto-deactivation field to set the minimum value for the effective priority of the virtual router to zero (0). The default is Disabled, 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. Click Apply.

12. (Optional) To configure a virtual MAC (VMAC) address for the virtual router, see “Setting a Virtual MAC Address for a Virtual Router.”

13. Click Apply, and then click Save to make your changes permanent.

**Setting Interface Dependencies for a Monitored Circuit Virtual Router for IPv6**

The Monitored Circuit feature lets you select one or more interfaces with which to associate dependencies. The up and down status of each interface is monitored, and the election of the VRRP master dynamically adapts to the current state of each interface selected for dependency.

Follow this procedure after you create a monitored circuit virtual router. For more information, see “Creating a Virtual Router in Monitored Circuit Mode for IPv6.”

1. Click Config on the home page.

2. Click the IPv6 Configuration link.

3. Click the VRRP for IPv6 link.

4. Click the Monitor Interface drop-down list for the specific virtual router entry and select the interface you want to monitor.

5. In the Priority Delta text box, enter a value of from 1 to 254 to specify 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.
**Note**
You must enter a priority delta value for each interface you select to monitor. If you do not enter a priority delta value, Network Voyager displays an error message.

6. Click Apply.

7. Repeat steps 4 and 5 for each interface you want to monitor.

8. To remove a specific monitored interface dependency, click off next to the name of the interface you want to remove from the monitored list. Click Apply.

   The name of the interface disappears from the list of monitored interfaces

9. Click Save to make your changes permanent.

**Changing the List of Addresses in a Monitored Circuit Virtual Router for IPv6**

1. Click Config on the home page.

2. Click the IPv6 Configuration link.

3. Click the VRRP for IPv6 link.

4. Locate the virtual router and the interface with the IP address to change.

   You can locate the virtual router information by using the Virtual Router ID value displayed in the Virtual Router field.

5. To remove an IP address from the list, click Off next to the address you want to delete. Click Apply.

6. To add an IP address to the list, enter the IP address in the Backup Address text box. Click Apply.

   The first back-up address you configure must be a link-local address. Any link-local address must belong to the fe80::/64 subnet, and global addresses must belong to the subnet of the interface.

7. To make your changes permanent, click Save.

**Traffic Management**

**Traffic Management Overview and Configuration**

Click the links below to view documentation on Traffic Management features and how to configure them.

“Configuring IP Clustering in IPSO”

“Packet Filtering Description”
Security and Access Configuration

Configuring IPv6 Network Access and Services

Enabling FTP Access

1. To enable IPv6 FTP access, click Yes in the Allow Ipv6 FTP Access field.
2. Click Apply.
3. Click Save to make your changes permanent.

Enabling Telnet Access

1. To enable IPv6 Telnet access, click Yes in the Allow IPv6 Telnet Access field.
2. Click Apply.
3. Click Save to make your changes permanent.
12 Configuring Asset Management

Chapter Contents

- Asset Management Summary
  - Asset Management Summary Description
  - Viewing the Asset Management Summary

Asset Management Summary

Asset Management Summary Description

The asset management summary page provides a summary of all system resources, including hardware, software and the operating system. The hardware summary includes information about the CPU, Disks, Bios, and motherboard, including the serial number, model number, and capacity, or date, as appropriate. The summary also displays the amount of memory on the appliance.

The Check Point FireWall summary lists information about the host and policy installed and the date on which the FireWall policy was installed. The summary also describes which version of the FireWall is running and license information.

The operating system summary lists which software release and version of that release is running on the system.

Viewing the Asset Management Summary

1. Click Config on the home page.
2. Click the Asset Management Summary link. This action takes you to the asset management summary page.
3. The page separates information into three tables: Hardware, FireWall Package Information, and Operating System.
4. Click the Up button to return to the main configuration page.
Chapter Contents

- IPSO Process Management
  - Overview of Nokia IPSO Process Management
  - Process Monitoring Details

Nokia IPSO Process Management

Overview of Nokia IPSO Process Management

The process monitor (PM) monitors critical Nokia IPSO processes. The PM is responsible for:

- Starting and stopping the processes under its control
- Automatically restarting the processes if they terminate abnormally

The Nokia IPSO processes that the PM monitors are listed in the following table. In addition, the PM might also monitor application package processes, such as IFWD, FWD, CPRID.

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inetd</td>
<td>Internet daemon. This daemon helps manage Internet services on IPSO by monitoring port numbers and handling all requests for services.</td>
</tr>
<tr>
<td>ipsrd</td>
<td>Routing daemon. This daemon is a user-level process that constructs a routing table for the associated kernel to use for packet forwarding. With a few exceptions, IPSRD completely controls the contents of the kernel forwarding table. This daemon factors out (and separately provides) functionality common to most protocol implementations. This daemon maintains and implements the routing policy through a database.</td>
</tr>
<tr>
<td>ifm</td>
<td>Interface management daemon. This daemon sends and receives information to and from the kernel to verify the integrity of the interface configuration.</td>
</tr>
</tbody>
</table>
Process Monitoring Details

The PM frequently checks the status of the processes it monitors and typically takes less than a second to notice if a process has terminated abnormally. It then attempts to restart the process. If the process fails to start, the PM continues to try to restart it at regular intervals, with each interval increasing by a factor of two (for example, 2 seconds, 4 seconds, 8 seconds, 16 seconds, and so on). If the PM fails to start the process after 900 seconds, it stops trying. Each unsuccessful attempt is logged in the system message log. The process monitoring behavior the PM is not user configurable.

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xntpd</td>
<td>Network time protocol daemon. This daemon sets and maintains a UNIX system time-of-day in compliance with Internet standard time servers.</td>
</tr>
<tr>
<td>monitord</td>
<td>System monitor daemon. This daemon monitors system health, collects and stores statistical information, and displays the data on request.</td>
</tr>
<tr>
<td>httpd</td>
<td>Web server daemon.</td>
</tr>
<tr>
<td>sshd</td>
<td>Secure shell daemon.</td>
</tr>
<tr>
<td>xpand</td>
<td>Configuration daemon (also called configd). This daemon processes and validates all user configuration requests, updates the system configuration database, and calls other utilities to carry out the request.</td>
</tr>
<tr>
<td>snmpd</td>
<td>SNMP agent.</td>
</tr>
</tbody>
</table>
ADSL

Asymmetric Digital Subscriber Line. A modem technology that converts existing twisted-pair telephone lines into an access path for multimedia and high-speed data communications. Download speeds can be as high as 6 Mbps.

ARP

Address Resolution Protocol. A protocol that relates (fixes) an IP address to a hardware address. It allows a host to find a physical address of a node on the same network when it only knows the target’s logical address. ARP is used on a single network and is limited to hardware-type broadcasting.

AS

Autonomous System. A group of networks and routers controlled by a single-administrative authority. An unique number identifying an Internet-connected network that has routing policies distinct from upstream connections.

ATM

Asynchronous Transfer Mode. A technology that transmits all voice, video, and data in packets as small 53-bit cells (5-bit header, 48-bits data). ATM is capable of high-speed routing up to 622 Mbps and is not packet-switched.

Bandwidth

The transmission width or capacity, usually measured in bits per second, of a network. Analog bandwidth is measured in Hertz or cycles per second. Digital bandwidth is the amount or volume of data that may be sent through a channel, measured in bits per second, without distortion. Bandwidth should not be confused with the term band, such as a wireless phone that operates on the 900 MHz band. Bandwidth is the space it occupies on that band. The relative importance of bandwidth in wireless communications is that the size, or band-width, of a channel will impact transmission speed. A lot of data flowing through a narrow channel takes longer than the same amount of data flowing through a broader channel.
BGP

Border Gateway Protocol. An inter-domain routing protocol for communications between a router in one autonomous system and routers in other autonomous systems.

CIDR

Classless Inter-domain Routing. A routing technique that allows routers to group routes together to reduce the quantity of routing information carried by core routers. CIDR uses a group of contiguous class-C addresses in place of one, different-sized class-B address.

CPDS

Connectionless Packet-Delivery Service. A form of packet-switching that relies on the global addresses in each packet rather than on predefined virtual circuits. All address information is contained in the message itself.

CRC

Cyclic Redundancy Check. A method used to check the transmission accuracy of a communications link. A sending computer performs a calculation on the data and attaches the result, and the receiving computer performs the same calculation and compare its result to the attached value. If they do not match, a transmission error is returned with a retransmission request.

CSU/DSU

Channel Service Unit/Data Service Unit. A service that connects an external digital circuit to a digital circuit on a customer's premises. The DSU converts data into the correct format, and the CSU terminates the line, conditions the signal, and participates in remote testing of the connection.

DES

Data Encryption Standard. A 56-bit, U.S. National Bureau of Standard method of data encryption. It's limited to 40 bits outside of U.S.

DCE

Data Communications Equipment. Switching equipment that forms a packet-switched network, versus computers or terminals connected to the network. See DTE.

DHCP

Dynamic Host Configuration Protocol. A protocol that is used to lessen the administrative burden of manually configuring TCP/IP hosts on a network.
DLCI
Data Link Connection Identifier. A frame relay value that identifies a logical connection.

DTE
Data Terminal Equipment. A terminal or computer that functions as a source or destination of network communication; end-user equipment. See DCE.

DVMRP
Distance Vector Multicast Routing Protocol. A protocol that is used to propagate membership information among multicast-capable routers.

E1
Transmission rate. A 2.048 Mbps (at 32 discrete channels) digital network system. Also called CEPT.

E3
Transmission rate. Generally, the highest (34 Mbps) transmission rate in a European digital infrastructure.

EGP
Exterior Gateway Protocol. A protocol that is used by a router in one autonomous system to advertise the IP addresses of networks in its autonomous systems to a router in another autonomous system. Handles load balancing.

Firewall
A system of hardware and software that enforces a boundary between two or more networks in accordance with a local security policy. Nokia technology combines a firewall with a router.

FDDI
Fiber Distributed Data Interface. LAN technology for data transfer (up to 100 Mbps) on a dual, counter-rotating, fiber-optic cable, token ring.

Frame Relay
A packet-based protocol that supports multiple logical channels over a single link. Frame Relay is more efficient than X.25 and is generally considered a replacement. Frame Relay defines the interface between user equipment and a WAN; it does not define internal operation of the network, or the interfaces, or protocols used within the WAN. For this reason, the term Frame Relay cloud is often used to describe the internal operation of a WAN that has a Frame Relay interface.
FTP

File Transport Protocol. A TCP/IP protocol for transferring files between different systems. A method of retrieving files to a home directory or directly to a computer using SLIP/PPP. There are thousands of FTP sites on the Internet offering files and programs of all kinds.

GSM

Global System for Mobile Communication. The digital wireless-transmission technique used in Europe and supported in North America for Personal Communication Service. GSM uses 900 MHz and 1800 MHz in Europe. In North America, GSM uses 1900 MHz.

HDLC

High-level Data Link Control. A popular ISO standard that is a bit-oriented, link-layer protocol derived from Synchronous Data Link Control (SDLC). HDLC specifies a method of encapsulating data on synchronous serial-data links.

Hop

The transition between two networks via a router. The next hop is defined as the IP address of the next router port encountered while traveling to a destination IP (host). Cost is the number of routers encountered along a route (series of hops) to a destination IP.

HSSI

High-speed Serial Interface. A network standard for high-speed (up to 52 Mbps) serial communications over WAN links.

ICMP

Internet Control Message Protocol. The standard error and control message protocol for Internet systems. Defined in RFC 792. The most well-known ICMP messages is the Echo Request - Echo Reply sequence used by ping.

IDR

Inter-domain Routing Protocol. An OSI protocol that specifies how routers communicate with routers in different domains.

IGP

Interior Gateway Protocol. Any protocol that propagates network accessibility and routing information within an autonomous system. The Routing Information Protocol (RIP) is one IGP.

IGMP

Internet Group Management Protocol. Protocol that runs between hosts and their next-hop, multicast routers; the mechanisms of the protocol allow a host to inform its local router that it
wishes to receive transmissions addressed to a specific multicast group. Based on group membership information learned from the IGMP, a router is able to determine which, if any, multicast traffic needs to be forwarded to each of its leaf subnetworks.

**IGRP**

**Interior Gateway Routing Protocol.** A widely used interior gateway protocol that uses distance vectors. Like RIP, IGRP allows multiple paths to a single destination, thus providing load sharing and stability during topology changes.

**IPSO**

**Nokia (Ipsilon) Router Operating System.** An UNIX-like operating system based on FreeBSD that runs Nokia's firewalls in conjunction with Check Point's FireWall-1 software.

**IPSRD**

**Nokia (Ipsilon) Software Routing Daemon.** Nokia software that computes routes using resident-database information, which is configured and maintained by Nokia Network Voyager. A **daemon** is a dormant, background process (in a UNIX environment) that waits to perform tasks.

**ISDN**

**Integrated Digital Service Network.** The recommendation published by CCITT for private or public digital telephone networks where binary data, such as graphics and digitized voice and data transmission, pass over the same digital network that carries most telephone transmissions today. ISDN provides 128 kbits bi-directional data capacity.

**LAPB**

**Link Access Procedure, Balanced.** Derived from HDLC, a CCITT X.25 version of a bit-oriented data link protocol.

**LLC**

**Logical Link Control.** The upper portion of the datalink layer, as defined in IEEE 802.2. The LLC sublayer presents a uniform interface to the user of the datalink service, usually the network layer.

**LMI**

**Local Management Interface.** In frame relay, a specification that defines a method of exchanging status information between devices such as routers. The routers learn which Data Link Connection Identifier is defined, its current status, and then use it.
MAC

**Media Access Control.** The lower physical portion of the datalink layer. MAC differs for various physical media. It controls access to a transmission medium such as Token Ring, CSMA/CD, Ethernet, FDDI, etc. The term *MAC address* is often used as a synonym for a physical address.

MIB

**Management Information Base.** A database that a SNMP router maintains to hold information about all resources managed by a network management system.

MIME

**Multipurpose Internet Mail Extensions.** An extension to Internet Email that provides the ability to transfer non-textual data, such as graphics, audio, video, and fax images.

MTU

**Maximum Transfer Unit.** The largest frame length (largest possible unit of data) that may be sent on a given physical medium.

NAP

**Network Application Platform.** A term describing the Nokia hardware chassis and software that routes network traffic and operates network applications. Nokia NAPs provide a full range of networking capabilities, including IP routing, combined with state-of-the-art security applications, virus detection, and intrusion detection.

NMS

**Network Management System.** A generic term describing most elements of network management.

Octet

An octet is 8 bits. This term is used in networking, rather than byte, because some systems have bytes that are not 8 bits long.

OPSEC

**Open Platform for Secure Enterprise Connectivity.** A level of certification applicable to products that are deemed compatible with OPSEC standards. OPSEC-certified products guarantee interoperability at the policy level between Checkpoint's FireWall-1 and leading security applications. OPSEC Alliance members cover the broad range of enterprise network security technologies, including authentication, encryption, content security, networking infrastructure, application software, and managed service providers.
OSPF

Open Shortest Path First. Similar to RIP, except that OSPF broadcasts when a new router is on the network or a route changes. OSPF also considers factors such as line capacity, delay, and security restrictions, as well as Hop count when calculating a route. OSPF is a link state, as opposed to distance vector, routing protocol. It calculates routes based on least hops, speed of transmission lines, and congestion delays.

OSI

Open Systems Interconnection. A set of international, openly developed and accepted standards created by the ISO and CCITT (now ITU-T) for data networking.

PDU

Protocol Data Unit. A data object exchanged by protocol machines within a given layer of the OSI Reference model, which contains both protocol-control information and user data.

PIM

Protocol Independent Multicast. A routing protocol that provides scalable (Sparse or Dense modes) of inter-domain, multicast routing across the Internet.

PPP

Point-to-Point Protocol. A protocol that provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. Used by Internet Service Providers. Allows dial-up networks. PPP is the successor to SLIP (IP over Serial lines, such as telephone circuits or RS-232 cables).

Protocol

The rules of communication that describe how a computer responds when a message arrives, and how a computer handles errors. Protocols allow a computer-communication discussion independent of the hardware.

PSN

Packet-switching Node. Replaced Internet Message Processor (IMP) as a term. In packet switching, all the data coming out of a host is broken into chunks (packets), each chunk has the address of where it came from and where it is going. This enables packets of data from many different sources to co-mingle on the same lines, and be sorted (at nodes) and directed to different routes.

PVC

Permanent Virtual Circuit. A virtual circuit (X.25), virtual connection (Frame Relay), or virtual-channel connection (ATM) that is established by administrative means, much like a leased or dedicated real circuit.
**RFC**

*Request for Comments.* A series of notes (standards and specifications) recording proposed techniques, ideas, and includes accepted TCP/IP standards. RFCs are continually emerging.

**RIP**

*Routing Information Protocol.* Network Layer protocol that runs on routers. Routers maintain their routing tables by broadcasting their tables to their neighbors. This makes RIP an insecure protocol, inviting hackers to capture these frequent broadcasts. Networks are then navigated using fewest hops possible.

**RSA**

RSA is a public key or asymmetric, encryption scheme invented by and named for 3 mathematicians, Ron Rivest, Adi Shamir, and Len Adleman. The theoretical background to RSA is that it's very difficult to find factors of a very large number that is the product of 2 prime numbers. RSA has been analyzed closely and is considered very secure provided a sufficiently long key is used.

**SDLC**

*Synchronous Data Link Control.* A bit-synchronous link-layer protocol that has spawned numerous similar protocols, including HDLC and LAPB.

**SLIP**

*Serial Line Internet Protocol.* Internet protocol used to run IP over serial lines such as telephone circuits or RS-232 cables interconnecting two systems. SLIP is now being replaced by PPP.

**SMI**

*Structure of Management Information.* Based on RFC 1155, which specifies rules used to define managed objects in a management information base (MIB).

**SMTP**

*Simple Mail Transfer Protocol.* A standard TCP/IP protocol that transfers electronic mail from one machine to another. SMTP specifies how two mail systems interact and the format of the messages they exchange.

**SNMP**

*Simple Network Management Protocol.* As a standard method of managing and monitoring network devices on a TCP/IP-based internet, it allows network administrators to connect, setup, and maintain a network.
SSH

Secure Shell. A program to log into another computer over a network that allows execution of commands and to movement of files. Intended as a replacement for rlogin, rsh, and rcp, it provides strong authentication and secure communications over channels that are not secure.

Symbol

A 4-bit unit.

T1

A transmission rate. An AT&T term for a formatted digital signal, level-1 being transmitted at a rate of 1.544 Mbytes using 24 discrete channels.

TCP/IP

Transmission Control Protocol/Internet Protocol. A suite of Internet protocols. Separately, they are defined as:

TCP - Transmission Control Protocol. A protocol that ensures that connections are made and maintained, which allows a process running on one computer to send a data stream to another computer. TCP is a reliable, full-duplex, connection-oriented transport (verifying connection) service. TCP works with IP to move packets through an inter-network.

IP - Internet Protocol part of the TCP/IP protocol that defines the IP datagram as the unit of information passed on a network. IP includes the Internet Control Message Protocol.

TRPB

Truncated Reverse-Path Broadcasting. An algorithm used by multicast routing protocols to determine the group memberships on each leaf of a subnetwork, which avoids forwarding datagrams onto a leaf subnetwork that does not have a member of the destination group. Prunes multicast distribution trees to a minimum.

TTL

Time to Live. The time allowed before an endlessly looping packet is discarded. TTL was originally intended to be a measure of the time in seconds a datagram was allowed to be in transit across a network. In practice, however, datagrams traverse routers in less than a second, so usage was changed. Now as a datagram is forwarded, its TTL is decrements by one. Thus, TTL actually represents the maximum number of Hops that a datagram can make before being discarded.

UDP

User Datagram Protocol. A protocol that allows an application on one machine to send a short datagram to an application on another machine. UDP contains an exact-port address.
Voyager

Nokia Voyager software. Nokia’s Voyager software that communicates with its routing software element, Ipsilon Routing Daemon (IPSRD) to configure interface hardware, set routing protocols and routing policies, and monitor routing traffic and protocol performance.

VPI / VCI

Virtual Path Identifier/Virtual Circuit Identifier. Two fields (eight-bit identifiers) used in an Asynchronous Transfer Mode packet to distinguish a semi-permanent connection destination.

VRRP

Virtual Router Redundancy Protocol. A means by which a router can automatically assume responsibility for forwarding IP traffic that was sent to a default router's address when the default router fails.
A
AAA 322
  Account Profile
    Changing a Configuration 336
    Creating 325
    Types 326
  Changing a Configuration 332
  Creating a Configuration 322
  Deleting a Configuration 336
  Deleting an Authentication Server Configuration 332
  Profile Controls 327
  Service Module 323, 327
  Service Profile 323
  Session Profile 326
  Stacked Service Module 333
Access and Security Configuration 507
Access Control List
  Adding a New Rule 410
  Applying to an Interface 407
  Creating 406
  Deleting 407
  Modifying a Rule 410
  Removing 408
  Rules 408
access control list (ACL) 409
Access Control List Rules
  Configuring 408
Access Control Lists
  Configuring 405
access control lists
  VRRP 292
access list
  adding rules 410
  applying to an interface 407
  configuring 407
  deleting 407
  deleting rules 412
  modifying rules 410
  removing from an interface 408
ACL, see also Access Control List
Active status monitor
  changing settings 139
  adding
    users 299
Aggregate Routes
  Creating 216
  Removing 216
aggregate routes
  configuring 216
  removing 216
Aggregation Class 412
  Creating 412
  Deleting 413
Aggregation Class, Associating with a Rule 413
Aggregation Classes
  Configuring 412
aggregation classes
  associating rules 413
  configuring 412
  deleting 413
Apply button 10
ARP
  adding a permanent table entry 153
Address Resolution Protocol 46
Changing Global Parameters 152
changing global parameters 152
Configuring for the ATM Interface 155
deleting a permanent table entry 154
Deleting a Static Entry 154
Deleting Dynamic Entries 154
deleting dynamic table entries 154
Flushing All Dynamic Entries 154
flushing dynamic entries 154
Proxy, Adding an Entry 153
Static, Adding an Entry 153
Table Entries 152
table entries 152
Viewing Dynamic Entries 154
viewing dynamic entries 154
ARP for ATM
  Adding a Static Entry 155
Changing Global Parameters 155
Deleting a Static Entry 156
Index - 524

Nokia Network Voyager for IPSO 3.9 Reference Guide

Viewing and Deleting Dynamic ARP Entries 156
AS, see also autonomous system
ASPATH Regular Expressions 263
Asset Management 509
Asset Management Summary 509
  Viewing 509
ATM
  changing IP address 97
  Changing the IP Address of an Interface 97
  Changing the IP Address of an LIS Interface 102
  Changing the IP MTU of an Interface 98, 102
  Changing the VPI/VCI of an Interface 96
  Changing the VPI/VCes of an LIS Interface 101
  configuring 95
  Configuring a Logical IP Subnet (LIS) Interface 100
  Configuring an Interface 95
  Configuring ARP 155
  Configuring QoS 417
  Deleting a QoS Descriptor 418
  Example 98
  example 98
  Removing an Interface 98, 103
ATM Example 98
ATM QoS 417
ATM QoS Descriptor
  Associating with an Interface and a Virtual Channel 419
Auditlog, Disabling 469
Authentication
  Profile Types 324
  authentication
    VRRP 276, 279
Authentication Profile
  Changing a Configuration 335
  Creating 323
Authentication, Authorization, and Accounting (AAA) 322
Authentication, MD5 228
  auto-deactivation 282
  auto-negotiation
    enabling 48
  autonomous system (AS)
    BGP 223
      description 168
      auto-summarization
        configuring 183
B
Back button 11
Backing Up and Restoring Files 472
backup address, VRRP 277, 279
Backup Files 472, 477
  Manually Creating 472
  Regularly Scheduled 473
  Restoring 475, 476
  Transferring to a Remote Server 474
backup state, VRRP 289
Backup Static Route 215
Backup Static Routes 214
Bellman Ford algorithm 168
BGP 169, 220
  Adjusting Timers 251
  AS Path Filtering 263
  Communities 224, 246
  Confederation 226, 240
  IGP Interactoins 223
  Inbound Route Filters 42, 223
  Memory Requirements 230
  Multi-Exit Discriminator (MED) 222
  Neighbors 231
  Neighbors, Verification 235
  Path Attributes 221
  Path Filtering Based on Communities 235
  Path Selection 254
  Redistributing Routes 169
  Redistribution 224
  Route Dampening 253
  Route Dampening, Verification 253
  Route Inbound Policy 261
  Route Redistribution 255
  Sessions (Internal and External) 221
  Tables 230
  VRRP 272
BGP MED
  Configuring 236
  Local Preference 238
  Values
    Configuring 237
    Configuring for all Peers of AS200 236
    Configuring per External BGP 237
  Verification 238
BGP, see also Border Gateway Protocol
Bootp Relay 266
  Disabling on an Interface 267
  Enabling on an Interface 266
  Bootp Relay (Bootp)
    description 266
    disabling 267
    enabling 266
  Bootstrap Protocol Relay 266

Index - 524
Border Gateway Protocol 220
Border Gateway Protocol (BGP)
autonomous system (AS) 223
communities 224
confederations 226
external session (EBGP) 221
importing 223
internal session (IBGP) 221
Multi-Exit Discriminator (MED) 221
overview 169
path attributes 221
redistributing 169, 224
route reflection 225

C
CA Certificates 346
Call Traces, ISDN 83
Candidate Bootstrap and Candidate Rendezvous Point
Configuring Router 193
Cause Codes
Troubleshooting 86
Certificate and Private Key
Generating 319
Installing 321
Chargen Service 310
Check Point NG
configuring for VRRP 285
Cisco
HDLC
Changing the IP Address 135
Cisco HDLC 134
changing IP address 135
changing keepalive interval 134
Changing the Keepalive Interval 134
Configuring a Serial Interface 104
Configuring a T1 Interface 110
Configuring an E1 Interface 118
Configuring an HSSI Interface 125
configuring for HSSI 125
configuring for T1 110, 118
configuring for V.35 104
configuring for X.21 104
clearing
disk cache 11
memory cache 11
CLI interface, described 9
CLI Over HTTP 304
CLI Over HTTPs 304
CLI Reference Guide
accessing 11
Cluster Management 371
Cluster Voyager 391
Clustering
Active 388
Adding a node to a cluster 388
Changing Interface Configurations 397
Cluster Mode 381
Cluster Terminology 371
Cluster Voyager 391
Configuring 368
Configuring for NAT 399
Configuring in Voyager 401
Configuring VPN-1/FireWall-1 399
Creating a Cluster 380
Deleting a Configuration 397
Displaying Cluster Status and Members 26
Example 401
Example Cluster 369
Example With a VPN Tunnel 404
FP4 400
Internal and External Routers 403
Joining a System 390
Managing 390
Modes 371
New Cluster 380
No Dedicated Network 399
Rebooting a Cluster 481
Recommended procedure for creating 389
Removing a Node 396
Synchronizing the Time 397
Transparent Mode 157, 164
Upgrading from IPSO 3.6 378
Enabling cluster management 379
Upgrading IPSO Images 481
Clustering Description 368
COM2
Configuring a Modem 305, 306
COM2 Login 305
COM3 Login 305
COM4 (PCMCIA)
Configuring a Modem 307
Command-line Utility Files 13
commands, routing daemon (iclid) 29
Common Open Policy Server Description 420
communities (BGP) 224
Community Strings
Disabling 436
Setting 436
confederations (BGP) 226
Config button 10
Configuration Lock 361
Configuration Locks
   Overriding 361
Configuration Overview 380
Configuration Set
   Deleting 472
   Factory Default 471
   Loading 471
   Managing Multiple 471
   Saving the Current as New 471
configuring
   aggregate routes 216
   ATM 95
   auto-summarization 183
   backup static routes 214
   default route 210
   DVMRP 206
   Ethernet 47
   HSSI for Frame Relay 128
   HSSI for PPP 126
   IGRP 203
   interfaces 39
   IP addresses 44
   IP Broadcast Helper 268
   loopback 141
   mail relay 462
   multicast tunnels 142
   network devices 43
   NTP 293
   OSPF 132, 173, 489
   RIP 181
   route rank 219
   routing 165, 487
   S/key 300
   Secure Shell (SSH) 311, 313, 315, 316, 317
   static route 211
   T1 110, 118
   T1 for PPP 112
   V.35 107
   X.21 107
Contents button 10
COPS 420
   Activating and Deactivating the Client 422
   Client ID
      Configuring Security Parameters 421
      Deleting 423
   Configuring 420
   Configuring a Client ID and Policy Decision Point 420
   Expedited Forwarding 425
   Rate Shaping 424
   cron jobs, scheduled times 293
   Crontab File, Scheduling Jobs 477
   Cryptographic Acceleration 337
   Displaying States 28
   Internet Key Exchange Protocol (IKE) 337
   Monitoring 338
   CSU/DSU, T1 Interfaces 110

D
   Data Collection Events, Configuring 16
   Date and Time 464
   date/time setting 464
   Daytime Service 310
   DDR List
      Adding a New Rule 78
      Applying to an Interface 80
      Creating 78
      Deleting 78
      Removing from an Interface 80
   Default Route
      Configuring 210
      default route
         configuring 210
      Defer Apply button 10
      deleting
         IP address, VRRP considerations 280
      Deleting IPSO 479
      Deleting Locally Stored 477
   Dense-Mode PIM
      Setting Advanced Options 189
   Dense-Mode PIM (PIM-DM), Configuring 188
   DHCP, see Dynamic Host Configuration Protocol (DHCP)
   Dial-on-Demand Routing Lists 77
   Diffserv
      Changing the Client ID Associated with a Specific Configuration 423
   disabling
      aggregate route 216
      Bootp Relay (Bootp) 267
      DHCP 267
      IP Broadcast Helper 269
      router discovery 271
      static route 214
      Discard Service 309
      disk cache, clearing 11
      Disk Mirroring 459
      Disk Mirroring (RAID Level 1) 459
      displaying
kernel forwarding table 27
routing daemon status (iclid) 28
routing protocol information 27
Distance Vector Multicast Routing Protocol 205
Distance Vector Multicast Routing Protocol (DVMRP)
configuring 206
description 205
overview 169
DLCI, changing in Frame Relay 138
DNS Hostname 458
DNS Server, Selecting to Resolve for Hostnames 458
Doc button 10
DSA and RSA
Managing User Identities 317
duplex mode
setting ethernet interface 48
duplex settings
changing FDDI 66
duplicate IP addresses error message 278
DVMRP 169, 205, 206
DVMRP Tunnel
Configuring 150
Creating 149
Removing 150
DVMRP Tunnels 47, 149, 150
DVMRP, see also Distance Vector Multicast Routing Protocol
Dynamic Host Configuration Protocol (DHCP)
disabling 267
enabling 266
Dynamic Monitoring 16

E
E1
CSU/DSU 118
EBGP
Configuring 234
Load Balancing 247, 249
Load Balancing, Verification 251
Multihop Support 227
Echo Service 309
effective priority, VRRP 274
enabling
Bootp Relay (Bootp) 266
DHCP 266
router discovery 270
error messages
duplicate IP addresses 278
Ethernet
configuring 47

Ethernet Interface
Configuring 47
Exclusive Configuration Lock
Login With 361
Login Without 361
extended mode, VMAC 278

F
Factory Default Configuration Set 471
Failure Notification 463
FDDI 65, 67
changing duplex setting 66
changing IP address 67
FDDI Interface
Changing the Duplex Setting 66
Changing the IP Address 67
Configuring 65
Features
Not Supported 462
Supported 462
Feedback button 10
Files, Backup and Restore 472
Files, Restoring 475
Filters, Inbound Route 259
firewall policies
VRRP 291
firewall state, monitoring for VRRP 290
FireWall-1, see also Check Point FireWall-1
Forward button 11
Forward Nonlocal, IP Broadcast Helper 268
Frame Relay 137
changing active status monitor settings 139
changing LMI parameters 138
Changing the Active Status Monitor Setting 139
Changing the DLCI 138
changing the DLCI 138
Changing the Interface Type 139
changing the interface type 139
Changing the IP Address 140
Changing the Keepalive Interval 137
changing the keepalive interval 137
Changing the LMI Parameters in 138
Configuring a Serial Interface 107
Configuring a T1 Interface 114
Configuring an E1 Interface 122
Configuring an HSSI Interface 128
configuring for HSSI 128
configuring for T1 114
configuring for V.35 107
configuring for X.21 107
interface mode, VMAC 277
Interface type
   Frame relay type change 139
Interface type, changing in Frame Relay 139
Interfaces
   Assigning Roles 421
   Associating a Queue Class 416
   Changing an Unnumbered to a Numbered Interface 131
   Configuring 39, 382
   Creating a Logical 70
   Displaying Settings 28
   E1 (with built-in CSU/DSU) 118
   FDDI 65
   ISDN 69
   Serial 109
   T1 110, 116
   Token Ring 90
   Types 12
   Unnumbered 130
   Virtual LAN 62
interfaces
   enabling Ethernet 48, 56
   logical 44
   loopback 46
   overview 42
   prefixes 43
   see also Ethernet
   see also FDDI
   see also HSSI
   see also loopback
   see also T1
   see also V.35
   see also x.21
types 42
interfaces, ethernet
   adding an identifying string 48, 57
   setting duplex mode 48
   setting speed 48
Interfaces, HSSI 125
Inter-Gateway Routing Protocol 199
Interior Gateway Routing Protocol (IGRP)
   configuring 203
   overview 168
   redistributing 170
Internet Group Management Protocol 207
Internet Group Management Protocol (IGMP) 207
IP Addresses
   Configuring 44
IP addresses
   adding to a loopback 141
changing ATM 97
changing FDDI 67
changing in Cisco HDLC 135
changing in PPP 137
changing loopback 141
configuring 44
IP Broadcast Helper 267
   configuring 268
Configuring Services 268
description 267
disabling 269
Disabling Services 269
Forward Nonlocal 268
IP over ATM (IPoA) 100, 100
   Example 103
IP2250
   Support of transparent mode 157
IP330
   Configuring to Place an Outgoing Call 81
IP650
   Configuring to Handle an Incoming Call 82
IPsec 349
   Creating a Policy 345
   Creating a Tunnel Rule 350
   Device Certificates 347
   Implementation in IPSO 342
   Parameters 344
   Phase 1 Configuration 344
   Platforms 344
   Policies 349
   Proposal and Filters 345
   Protocol Negotiation and Key Management 340
   Removing a Tunnel 358
   Transport mode 339
   Transport Rule 352
   Tunnel mode 339
   Tunnel Rule Example 354
   Tunnels 338
IPsec Transport Rule Example 356
IPsec Tunnel
   Configuring 358
Ipsilon Routing Daemon (IPSRD)
   description 167
   overview 9
IPSO 9
   deleting images 479
   overview 9
   selecting images 478
IPSO Image
   Upgrading 479
IPSO Images
Deletions 479
Installing 479
Managing 478
Selecting 478
Testing 478
IPSRD, see also Ipsilon routing Daemon
IPv4 in IPv6 Tunnels 493
IPv4 or IPv6, Choosing the General Configuration
Page 345
IPv6 488
Configuring 487
Creating a Static Route 494
Creating an Aggregate Routes 495
Description 488
Displaying Running States 28
Interfaces 489
Logical Interfaces 489
Neighbor Discovery 490
Network Access and Services 507
Router Discovery 497
Routing Configuration 494
Traffic Management 506
IPv6 and IPv4 Compatibility 491
IPv6 Default Route 493
IPv6 in IPv4 Tunnels 491
IPv6 over IPv4 492
IPv6 to IPv4 492
IRP, see also Interior Routing Protocols
ISDN 69
Bearer-Capable Values 90
Call Traces 83
Cause Code Fields 86
Cause Values 87
Deleting a Logical Interface
76
Incoming Number 75
Interfaces 69
Logical Interface 70
Network Configuration Example 81
Place and Receive Calls
76
Receive Calls
73
Removing an Incoming Number
75
Tracing Traffic 86
Troubleshooting 85
ISDN Calling Line-Identification Screening 74

J
Job Scheduling, Crontab File 477
Join-Time Shared Features, Configuring 385

K
keepalive
changing interval for Cisco HDLC 134
changing interval in Frame Relay 137
changing interval in PPP 136
maximum failures 136
kernel forwarding table 27
Kernel Forwarding Table, Displaying 27

L
link recognition delay 48
link speed
setting interface 48
LMI, changing parameters 138
Load Balancing, Controlling 399
Logging
Setting Log Level 85
Logical Interface
Creating 70
Login 305, 361
login
network 305
Login/Logout Activity 25
loopback
adding an IP address 141
changing IP address 141
interfaces 46
Loopback Interface 141
Adding an IP Address 141
Changing the IP Address 141
Using 46

M
MAC address
VRRP 277
Mail Relay 462
Configuring 462
mail relay
configuring 462
description 462
features 462
sending mail 463
Mail, Sending 463
Management Activity Log 25
master state, VRRP 289
MED 236
memory cache, clearing 11
Memory Size 230
Message Log, Viewing 85
metric, description 169
Mirror Set
   Creating 459
   Deleting 460
Modern Configuration 305, 306, 307
Monitor button 10
monitor interface parameter 282
monitored-circuit VRRP
   configuring overview 280
Monitoring
   Dynamic and Static 16
monitoring (SNMP) 434, 436
MTU
   setting for GigE Interfaces 56
multicast routers 207
multicast tunnels
   changing endpoint address 143
   configuring addresses 206
   creating 142
   removing 145
Multi-Exit Discriminator (MED)
   autonomous system (AS) 221
   Border Gateway Protocol (BGP) 221
Multi-Exit Discriminator 236
Multiple Static Routes
   Configuring 212

N
NAT, see also Network Address Translation
Network Access 303
Network Access, Services 309
Network Devices
   Configuring 43
   network devices, configuring 43
   network interface card (NIC) 43
Network Voyager
   described
   network, login 305
Notification, System Failure 463
NTP 293
   Configuring 293
   configuring 293
   description 293
   Peers 293
   Servers 293
   NTP Description 293

O
Online Help
   Viewing 11
Open Shortest Path First 171
Open Shortest Path First (OSPF)
   configuring 132, 173, 489
   overview 168
   redistributing 170
operating system (IPSO) 9
OSPF 168, 171
   Configuring 173, 178
   Description 171
   Redistributing Routes 170
   Unnumbered Interface 133
   Virtual Links 133
   VRRP 272
OSPF, see also Open Shortest Path First
Outgoing Call
   Configuring the IP330 81
   Overriding Configuration Locks 361

P
Packages
   Deleting 484
   Disabling 484
   Enabling 484
   Installing 483
   Managing 483
   packages
   disabling 484
   enabling 484
Packet Filtering 405
Password Procedures 299
   passwords
      S/key 302
   Passwords, Changing 299
   path attributes (BGP)
      definitions 222
      description 221
      local preference 221
Physical Interface 70
   physical interfaces 43
PIM 184
   Debugging 198
   Disabling 189
   High-Availability Mode 192
   VRRP 272
PIM-DM
   Configuring 188
PIM-SM 191
Index - 532

Nokia Network Voyager for IPSO 3.9 Reference Guide

PIM-SM Static Rendezvous Point 195
PKI, Using 342
PM (Process Monitor) 511
Point-to-Point
   changing IP address 137
   changing keepalive interval in PPP 136
   changing keepalive maximum failures in PPP 136
Point-to-Point Link over ATM 95
Point-to-Point Protocol 136
PPP 136
   changing keepalive failures in Point-to-Point 136
   changing keepalive interval in Point-to-Point 136
   Changing the IP Address 137
   Changing the Keepalive Interval 136
   Changing the Keepalive Maximum Failures 136
   Configuring a Serial Interface 106
   Configuring a T1 Interface 112
   Configuring an E1 Interface 120
   Configuring an HSSI Interface 126
   configuring for HSSI 126
   configuring for T1 112
   preempt mode 282
   priority
      VRRP parameter 272
   priority delta, VRRP 276, 279
   priority, VRRP 275, 279
   Process, Management 511
   Protocol-Independent Multicast 184

Q
QoS Descriptor
   Creating 417
Queue Class 414
   Configuration Values 415
   Creating 415
   Deleting 415
Queue Classes
   Configuring 414

R
RADIUS
   Configuring 328
Rate Shaping Bandwidth
   Displaying 18
   Report 17
Redistributed Routes 495
   redistributing
      BGP 169, 224
      IGRP 170
      OSPF 170
RIP 170
   Redistributing Routes 169
      BGP 169
      OSPF 170
      OSPF to BGP 259
      OSPF to RIP 258
      RIP and IGRP 170
      RIP to OSPF 256
      RIP to OSPF External 257
   refreshing pages 11
   Reload button 11
   reloading pages 11
Remote System Logging 465
   Reset Routing button 10
   Resource
      Displaying Settings 27
      Restoring Files 475
      Remote Server 476
RIP 168, 179
   Auto Summarization 180, 183
   Configuring 181
   Configuring Timers 183
   VRRP 272
   RIP 1 180
      Enabling on an Interface 184
   RIP 1, Network Mask 180
   RIP 2 179
      Authentication 180
      Enabling on an Interface 184
      Network Mask 180
   RIP, see also Routing Information Protocol
RIPng
      Configuring 495
      Redistributing Aggregate Routes 496
      Redistributing Interface Routes 496
      Redistributing Static Routes 495
Route
   Displaying Settings 27
   Rank Assignments 218
   route
      aggregation 215
      configuring rank 219
      filter 169
      precedence 218
      rank 218
      redistribution 169, 170, 171
      reflection (BGP) 225
   Route Aggregation 215
   Route Dampening 228
   Route Rank 218
   Setting 219
Route Redistribution 254
Route Redistribution Between Protocols 171
Route Reflection 225
Router Discovery 269
router discovery
  disabling 271
  enabling 270
Router Discovery Server 269
Router Discovery Services
  Disabling 271
  Enabling 270
Router Services
  Configuring 265
Routes
  Redistributing All 256
  Redistributing One 256
Routers, Redistributed 495
Routing 12
  Configuring 165
  Protocol Rank 219
routing
  configuring 165, 487
  creating a default route 210
  creating a static route 211
  disabling a static route 214
  enabling auto-summarization 183
  features 205
  IGRP 203
  OSPF 132, 173, 489
  removing an aggregate route 216
  RIP 181
Routing Daemon
  Displaying Status 28
routin daemon (iclid)
  commands 29
  displaying status 28
  help 29
routing domain (RD) 226
routing domain identifier (RDI) 226
Routing Information Protocol 179
Routing Information Protocol (RIP) 181
  auto-summarization 183
  configuring 181
  overview 168
  redistributing 170
routing protocol information, displaying 27
Routing Protocols 167
Routing Subsystem 167
RSA and DSA
  Managing User Identities 317
Rule
Deleting 79, 412
Modifying 79
  rules
  adding 410
  associating aggregation classes 413
  deleting 412
  modifying 410
S
S/Key
  Configuring 300
  Disabling 302
  Using 301
S/key
  configuring 300
  password 302
  using 301
S/Key Password 302
Save button 10
Scheduled Jobs
  Configuring 477
  Scheduled Jobs, Deleting 478
Secure Shell 311
  Authorized Keys 315
  Changing Key Pairs 316
  Server Options 313
Secure Shell (SSH) 311
  configuring 311, 313, 315, 316, 317
  description 311
  features 311
Secure Socket Layer 318
Secure Socket Layer (SSL) 318
Security and Access Configuration 507
Security Model
  Modifying a User-based User Entry 445
Serial Interfaces 104
Service Module Configuration
  Changing 335
Service Profile Entry
  Deleting an Item 336
Session Management
  Enabling 360
Session Profile Configuration
  Changing 336
Session Profile Types 326
Session Timeouts
  Configuring 362
setting time/date 464
Settings
  Interface 28
show mcvr 289
show vrrp 289
Simple Network Management Protocol (SNMP)
  description 430
  enabling traps 437, 439
  entering contact information 440
  entering location 440
  monitoring 434, 436
  traps 437
Slot
  Displaying Statistics 28
SNMP 430
  Agent Address 435
  Configuring 429
  Enabling and Disabling the Daemon 434
  Entering Location and Contact Information 440
  Sending Traps to a Network Management
    System 437
    Trap Agent Address 440
    Traps 437
    USM 443
    Version 435
SNMP, see also Simple Network Management Protocol
Software 9
spanning tree protocol 292
Sparse-Mode PIM
  Configuring 191
  Setting Advanced Options 195
SSH 311
  Configuring 311
SSH, see also Secure Shell
SSL 318
  Enabling Voyager Web Access 318
  Troubleshooting 321
states, virtual router 289
Static Host 464
  Deleting 464
static host
  adding 464
  deleting 464
static mode
  VMAC 278
Static Monitoring 26
Static Route
  Backup 214
  Configuring over an Unnumbered Interface 132
  Creating 211
Static Route, Backup 215
Static Routes 169, 210
  Backup 214
Configuring for an IBGP Session 239
  Rank 212, 220
static routes
  configuring 211
  description 210
  disabling 214
  mask length 211
Statistics
  Interface Linkstate 21
  Interface Throughput 19, 22, 23
Subsystem, Routing 167
  Support button 10
System
  Displaying Status 28
System Configuration Auditlog
  Setting 467
System Configuration Auditlog, Deleting 469
System Functions
  Configuring 447
System Health
  Monitoring 23, 24
System Logging 465
  Remote 465
System Logs, Monitoring 24
  system name, see hostname
System Resources, Monitoring and Configuring 15
System Utilization, Displaying Statistics 16
System-Failure Notification, Setting 463
T
T1
  configuring for Cisco HDLC 110, 118
  configuring for Frame Relay 114
  configuring for PPP 112
  example 116
T1 Interface 110, 116
T1 Interface Example 116
T1(with built-in CSU/DSU) Interfaces 110
TACACS+
  Configuring 330
TCP MD5 Authentication 228, 252
TCP/IP stack
  Tuning 485
tcpdump, Using with ISDN 86
Telnet
  Enabling Access 507
Telnet Access 304
Time and Date 464
  Time Service 310
time/date setting 464
Token Ring Interface 90, 93
  Changing 92
  Configuring 90
  Deactivating 91
  Top button 10
Traffic Management 405
  Configuring 367
Traffic Queuing 406
Traffic Shaping 405
Transparent Mode 157
  Configuring 157
  Functionality 160
  Group Configuration 157
  Limitations 157
  Neighbor Learning 158
  Receive Processing 158
  VPN Support 159
  VRRP Support 159
Transparent Mode Group
  Adding an Interface 162
  Creating 161
  Deleting 162
  Enabling 163
  Enabling VRRP 163
Transparent Mode Groups
  Monitoring 164
Trusted CA Certificates 346
Tunnel Interfaces, Configuring 46
Tunnel Requirements 343
Tunneling HTTP Over SSH 317

U
Unnumbered Interface 130
Unnumbered Interfaces 130
Up button 10
User
  Removing 300
User-based Security Model User 444
  Deleting 445
  Permissions 446
Users
  Adding 299
  adding 299

V
V.35 104
  configuring for Cisco HDLC 104
  configuring for Frame Relay 107
  example 109
  virtual IP address, VRRP 277
Virtual LAN 62
Virtual Router Redundancy Protocol 271
VLAN 62
  Configuring an Interface 63
  Deleting an Interface 64
  Example Topology 64
  Maximum Number 64
VMAC 277
VMAC mode 279
Voyager
  Enabling Session Management 360
  interfaces 206
  overview 10
Voyager See Network Voyager
Voyager Session Management 359
  Disabling 360
Voyager Web Access 303
VPN
  Building on ESP 340
  Configuring Tunnels 383
  Tunnels 47
VRID 271
  selecting 279
VRRP 271
  active-active configuration 273
  advertisements 272
  authentication 279
  authentication method 276
  auto-deactivation 282
  backup address 277, 279
  changing backup address 283
  Check Point configuration rules 287
  Check Point NG 285
  CLI commands 289
  configuring VRRPv2 284
  deleting IP address from interface 280
  effective priority 274
  election protocol 271
  Enabling for a Transparent Mode Group 163
  established master vs. equivalent priority 276
  firewall state 290
  full method 280
    adding virtual router 283
    deleting virtual router 283
  hello interval 276, 279
  hello messages 272
  IPv6 support 271
  link aggregation 288
  load sharing 273
  location 289
monitored circuit
  described 274
  full method 274
  simplified method 274
monitoring 289
overview 271
preempt mode 276, 282
priority 272
priority delta 276, 279
priority parameter 275, 279
providing redundancy 273
removing VRRPv2 virtual router 284
RFC 271
routing protocols 272
simplified method 280
  adding virtual router 280
  deleting virtual router 281
  reconfiguring virtual router 281
stats 290
switched environments 292
troubleshooting failover 291
virtual IP address 277
VMAC mode 277, 279
VRID 279
VRRP, see also Virtual Router Redundancy Protocol

X
X.21 104
  configuring for Cisco HDLC 104
  configuring for Frame Relay 107
  example 109