Contents

Chapter 1

About Network Voyager
   Software Overview ................................................................. 12
   Logging In to Network Voyager ........................................... 13
   Logging Off .......................................................................... 14
   Obtaining a Configuration Lock ......................................... 14
   Navigating in Network Voyager ........................................ 16
   Reloading Pages .................................................................. 17
   Accessing Documentation and Help .................................. 17
   Viewing Hardware and Software Information for Your System 19

Chapter 2

Configuring Interfaces
   Interface Overview ............................................................... 22
   Configuring Network Devices ............................................. 22
   Configuring IP Addresses .................................................. 22
   Interface Status .................................................................... 23
   Configuring Tunnel Interfaces ........................................... 24
   Ethernet Interfaces ............................................................. 25
   Configuring Ethernet Interfaces ......................................... 25
   Link Aggregation ................................................................. 30
      Supported Standards ......................................................... 31
      Upgrading IPSO with Link Aggregation ......................... 31
      Managing Link Aggregation Using SNMP .................. 31
      Configuring Switches for Link Aggregation ................. 32
      Configuring Link Aggregation ....................................... 33
   Link Redundancy ................................................................. 38
      If You Use Link Redundancy Before Upgrading to 6.1 ........ 39
      Configuring Link Redundancy Groups ......................... 39
   Gigabit Ethernet Interfaces ................................................ 41
   Virtual LAN Interfaces ........................................................ 43
      VLAN Example Topology ............................................... 45
   Loopback Interfaces ............................................................ 46
   GRE Tunnels ........................................................................ 48
      Configuring GRE Tunnels ............................................... 48
      GRE Tunnel Example ..................................................... 51
      High Availability GRE Tunnels ...................................... 52
      HA GRE Tunnel Example .............................................. 53
   DVMRP Tunnels ................................................................. 56
      DVMRP Tunnel Example ................................................ 58
   ARP Table Entries ............................................................... 60
   Transparent Mode ................................................................. 63
      Limitations ...................................................................... 63
      Transparent Mode Processing Details ....................... 64
<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Configuring System Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuring Banner and Login Messages</td>
</tr>
<tr>
<td></td>
<td>Configuring DHCP</td>
</tr>
<tr>
<td></td>
<td>Configuring DHCP Client Interfaces</td>
</tr>
<tr>
<td></td>
<td>DHCP Client Configuration</td>
</tr>
<tr>
<td></td>
<td>Configuring the DHCP Server</td>
</tr>
<tr>
<td></td>
<td>DHCP Server Configuration</td>
</tr>
<tr>
<td></td>
<td>Changing the DHCP Service</td>
</tr>
<tr>
<td></td>
<td>Adding DHCP Address Pools</td>
</tr>
<tr>
<td></td>
<td>Enabling or Disabling DHCP Address Pools</td>
</tr>
<tr>
<td></td>
<td>Assigning a Fixed-IP Address to a Client</td>
</tr>
<tr>
<td></td>
<td>Creating DHCP Client Templates</td>
</tr>
<tr>
<td></td>
<td>Configuring Dynamic Domain Name System Service</td>
</tr>
<tr>
<td></td>
<td>Configuring the Domain Name Service</td>
</tr>
<tr>
<td></td>
<td>Configuring Disk Mirroring/RAID</td>
</tr>
<tr>
<td></td>
<td>Mail Relay</td>
</tr>
<tr>
<td></td>
<td>System Failure Notification</td>
</tr>
<tr>
<td></td>
<td>Configuring Mail Relay</td>
</tr>
<tr>
<td></td>
<td>Sending Mail</td>
</tr>
<tr>
<td></td>
<td>Configuring System Time</td>
</tr>
<tr>
<td></td>
<td>Setting System Time</td>
</tr>
<tr>
<td></td>
<td>Configuring Daylight Savings Time</td>
</tr>
<tr>
<td></td>
<td>Configuring Host Addresses</td>
</tr>
<tr>
<td></td>
<td>Using an Optional Disk (Flash-Based Platforms Only)</td>
</tr>
<tr>
<td></td>
<td>Configuring System Logging</td>
</tr>
<tr>
<td></td>
<td>Configuring Logging on Disk-Based Systems</td>
</tr>
<tr>
<td></td>
<td>Configuring Logging on Flash-Based Systems</td>
</tr>
<tr>
<td></td>
<td>Configuring Audit Logs</td>
</tr>
<tr>
<td></td>
<td>Using a Core Dump Server with Flash-Based Systems</td>
</tr>
<tr>
<td></td>
<td>Changing the Host Name</td>
</tr>
<tr>
<td></td>
<td>Managing Configuration Sets</td>
</tr>
<tr>
<td></td>
<td>Scheduling Jobs</td>
</tr>
<tr>
<td></td>
<td>Backing Up and Restoring Files</td>
</tr>
<tr>
<td></td>
<td>Creating Backup Files</td>
</tr>
<tr>
<td></td>
<td>Transferring Backup Files</td>
</tr>
<tr>
<td></td>
<td>Restoring Files from Locally Stored Backup Files</td>
</tr>
<tr>
<td></td>
<td>Managing Check Point IPSO Images</td>
</tr>
<tr>
<td></td>
<td>Changing Current Image</td>
</tr>
<tr>
<td></td>
<td>Deleting Images</td>
</tr>
<tr>
<td></td>
<td>Installing New Images</td>
</tr>
</tbody>
</table>
Testing a New Image ................................................................. 129
Upgrading Check Point IPSO Images for a Cluster .......................... 130
Downgrading Check Point IPSO Images ....................................... 131
Configuring Monitor Reports ....................................................... 133
Managing Packages ...................................................................... 135
Installing and Enabling Packages .............................................. 135
Advanced System Tuning ............................................................ 137
Controlling SecureXL ............................................................... 137
Router Alert IP Option ............................................................. 138

Chapter 4
High Availability Solutions
Using an External Load Balancer .................................................. 141
Configuring the Firewall for a Load Balancer ................................ 141
HA Voyager .............................................................................. 143
Configuring the Firewall for HA Voyager .................................... 144
Creating an HA Configuration ................................................... 144
Adding and Configuring HA Members ........................................ 145
Configuring VRRP with HA Voyager ......................................... 147
Rebooting an HA Configuration Group ....................................... 148
HA Voyager Configuration Example .......................................... 149
VRRP Overview ................................................................. 154
How VRRP Works ...................................................................... 155
Configuring Network Switches .................................................. 158
Use Port Fast with Spanning Tree Protocol ................................. 158
Do Not Cascade Switches ........................................................ 158
Before You Configure VRRP .................................................... 159
Configuring VRRP ..................................................................... 160
Choosing Global Settings ......................................................... 161
Choosing a VRRP Method ........................................................ 162
Selecting Node Parameters ....................................................... 164
Configuring Monitored-Circuit VRRP ....................................... 169
Configuring VRRPv2 ............................................................... 175
Configuring the Check Point Security Gateway for VRRP ............ 177
Configuring VRRP Rules for the Check Point Security Gateway .... 179
Monitoring VRRP ...................................................................... 181
Monitoring the Firewall State .................................................... 182
Troubleshooting VRRP ............................................................ 183
General Configuration Considerations ....................................... 183
Firewall Policies ........................................................................ 184
Access Control Lists ............................................................... 184
Switched Environments ........................................................... 185

Chapter 5
Configuring SNMP
SNMP Overview ................................................................. 188
SNMP Proxy Support for Check Point MIB ................................. 193
Using the Check Point MIB ....................................................... 193
Enabling SNMP and Selecting the Version ................................. 194
Configuring the System for SNMP ........................................... 196
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting an Agent Address</td>
<td>196</td>
</tr>
<tr>
<td>Configuring Traps</td>
<td>196</td>
</tr>
<tr>
<td>Interpreting Error Messages</td>
<td>203</td>
</tr>
<tr>
<td>Configuring SNMPv3</td>
<td>206</td>
</tr>
<tr>
<td>Request Messages</td>
<td>206</td>
</tr>
<tr>
<td>Managing SNMP Users</td>
<td>207</td>
</tr>
<tr>
<td><strong>Chapter 6</strong></td>
<td></td>
</tr>
<tr>
<td>Configuring IPv6</td>
<td></td>
</tr>
<tr>
<td>IPv6 Overview</td>
<td>212</td>
</tr>
<tr>
<td>Interfaces</td>
<td>214</td>
</tr>
<tr>
<td>IPv6 and IPv4 Compatibility</td>
<td>217</td>
</tr>
<tr>
<td>Configuring IPv6 in IPv4 Tunnels</td>
<td>217</td>
</tr>
<tr>
<td>Configuring IPv6 to IPv4</td>
<td>217</td>
</tr>
<tr>
<td>Configuring IPv6 over IPv4</td>
<td>218</td>
</tr>
<tr>
<td>Configuring IPv4 in IPv6 Tunnels</td>
<td>219</td>
</tr>
<tr>
<td>Configuring an IPv6 Default or Static Route</td>
<td>219</td>
</tr>
<tr>
<td>Routing Configuration</td>
<td>221</td>
</tr>
<tr>
<td>Configuring OSPFv3</td>
<td>221</td>
</tr>
<tr>
<td>Configuring RIPng</td>
<td>221</td>
</tr>
<tr>
<td>Creating IPv6 Aggregate Routes</td>
<td>222</td>
</tr>
<tr>
<td>Creating Redistributed Routes</td>
<td>222</td>
</tr>
<tr>
<td>Router Discovery</td>
<td>225</td>
</tr>
<tr>
<td>Configuring ICMPv6 Router Discovery</td>
<td>225</td>
</tr>
<tr>
<td>VRRP for IPv6</td>
<td>227</td>
</tr>
<tr>
<td>Configuring VRRP for IPv6</td>
<td>227</td>
</tr>
<tr>
<td>Creating a Virtual Router for an IPv6 Interface Using VRRPv3</td>
<td>227</td>
</tr>
<tr>
<td>Creating a Virtual Router to Back Up Another VRRP Router Addresses Using VRRPv3</td>
<td>228</td>
</tr>
<tr>
<td>Monitoring the Firewall State</td>
<td>230</td>
</tr>
<tr>
<td>Setting a Virtual MAC Address for a Virtual Router</td>
<td>230</td>
</tr>
<tr>
<td>Changing the IP Address List of a Virtual Router in VRRPv3</td>
<td>232</td>
</tr>
<tr>
<td>Removing a Virtual Router in VRRPv3</td>
<td>232</td>
</tr>
<tr>
<td>Creating a Virtual Router in Monitored Circuit Mode for IPv6</td>
<td>233</td>
</tr>
<tr>
<td>Setting Interface Dependencies for a Monitored Circuit Virtual Router for IPv6</td>
<td>235</td>
</tr>
<tr>
<td>Changing the List of Addresses in a Monitored Circuit Virtual Router for IPv6</td>
<td>237</td>
</tr>
<tr>
<td>Traffic Management</td>
<td>237</td>
</tr>
<tr>
<td>Security and Access Configuration</td>
<td>238</td>
</tr>
<tr>
<td><strong>Chapter 7</strong></td>
<td></td>
</tr>
<tr>
<td>Managing Security and Access</td>
<td></td>
</tr>
<tr>
<td>Password and Account Management</td>
<td>241</td>
</tr>
<tr>
<td>Configuring Password Strength</td>
<td>241</td>
</tr>
<tr>
<td>Configuring Password History Check</td>
<td>244</td>
</tr>
<tr>
<td>Configuring Mandatory Password Change</td>
<td>245</td>
</tr>
<tr>
<td>Denying Account Access After Failed Login Attempts</td>
<td>249</td>
</tr>
<tr>
<td>Denying Access to Unused Accounts</td>
<td>251</td>
</tr>
<tr>
<td>Changing Passwords</td>
<td>252</td>
</tr>
<tr>
<td>Managing User Accounts</td>
<td>253</td>
</tr>
<tr>
<td>Adding and Deleting Users</td>
<td>256</td>
</tr>
</tbody>
</table>
Managing and Using S/Key .............................................................. 257
Managing Groups ........................................................................... 257
Role-Based Administration ............................................................... 262
Managing Roles ............................................................................. 262
Assigning Roles and Access Mechanisms to Users ......................... 264
Creating Cluster Administrator Users .............................................. 265
Configuring Network Access and Services .................................. 266
Configuring Network Voyager Access ......................................... 269
Configuring Basic Network Voyager Options .............................. 269
Generating and Installing SSL/TLS Certificates .......................... 270
Secure Shell (SSH) ......................................................................... 274
Initial SSH Configuration ................................................................. 274
Configuring Advanced Options for SSH ....................................... 276
Configuring Secure Shell Authorized Keys .................................... 278
Changing Secure Shell Key Pairs .................................................... 279
Managing User RSA and DSA Identities ......................................... 280
Tunneling HTTP Over SSH ............................................................. 280
Network Voyager Session Management ...................................... 282
Enabling or Disabling Session Management ................................. 282
Configuring SessionTimeouts ......................................................... 282
Authentication, Authorization, and Accounting (AAA) .................. 284
Configuring AAA Service Modules ............................................... 284
Configuring RADIUS ................................................................. 289
Configuring TACACS+ ................................................................. 294
Encryption Acceleration ................................................................. 300
Enabling Encryption Accelerator Cards ....................................... 300
Monitoring Cryptographic Acceleration ....................................... 300

Chapter 8

Configuring Routing
Routing Overview .......................................................................... 302
Routing Protocols .......................................................................... 302
Route Maps .................................................................................. 304
OSPF ........................................................................................ 306
Types of Areas ........................................................................... 306
Area Border Routers .................................................................... 307
High Availability Support for OSPF ............................................. 308
Configuring OSPF ...................................................................... 309
RIP .......................................................................................... 321
RIP 2 ...................................................................................... 321
RIP 1 ...................................................................................... 322
Virtual IP Address Support for VRRP .......................................... 322
Configuring RIP ........................................................................ 323
Configuring RIP Timers .............................................................. 325
Configuring Auto-Summarization ................................................. 325
RIP Example ............................................................................. 326
PIM ......................................................................................... 327
Configuring Virtual IP Support for VRRP .................................... 328
PIM Support for IP Clustering ...................................................... 328
Chapter 9

Configuring Traffic Management
Traffic Management with Differentiated Services .................................................. 434
Performance Considerations ............................................................................. 434
Configuring Access Control Lists .................................................................. 435
Configuring ACL Rules .................................................................................. 437
Configuring Aggregation Classes ................................................................... 444
Configuring Queue Classes ............................................................................ 446
Example: Rate Shaping ................................................................................... 452
Example: Expedited Forwarding ...................................................................... 453
Configuring Policy Based Routing .................................................................. 457
Combining PBR with Other Routing ................................................................. 457
Creating a PBR Table ....................................................................................... 458
Deleting a PBR Table ...................................................................................... 461
Configuring an Access Control List for PBR .................................................. 461
Using PBR with VRRP and IP Clustering ......................................................... 462
Configuring Netflow Services ......................................................................... 463
Defining Flows ................................................................................................ 463
Flow Records .................................................................................................. 464

Chapter 10

Configuring Router Services
BOOTP/DHCP Relay ....................................................................................... 468
Configuring BOOTP/DHCP Relay ................................................................ 468
IP Broadcast Helper ....................................................................................... 471
Router Discovery ............................................................................................. 473
Router Discovery Overview ............................................................................ 473
Configuring Router Discovery ........................................................................ 474
Chapter 11

Using Voyager Tools

Migrating a System Configuration......................................................... 482
Acquiring Configuration Information............................................... 483
Migrating Configuration Information............................................... 484
Exporting Configuration Information............................................. 487
Using the Enhanced Configuration Summary Tool ......................... 488
Running ECST Using Network Voyager.......................................... 489
Running ECST from the IPSO Shell............................................... 490
Tuning the Check Point Firewall Kernel.......................................... 491

Chapter 12

Monitoring System Configuration and Hardware

Viewing Performance Information ................................................... 494
Connection Dashboard................................................................. 494
Connection Map Dashboard.......................................................... 495
Traffic Dashboard......................................................................... 495
Forwarding Dashboard................................................................. 496
Interface Dashboard.................................................................. 496
System Dashboard................................................................. 496
ADP Dashboard............................................................ 497
Custom Dashboard................................................................. 497
Viewing System Utilization Statistics............................................. 498
CPU-Memory Live Utilization......................................................... 498
Disk and Swap Space................................................................. 498
Monitoring Process Utilization.................................................... 499
IPSO Process Management........................................................... 500
Generating Monitor Reports........................................................... 502
Monitoring System Health............................................................. 505
Monitoring System Logs............................................................... 507
Viewing Cluster Status and Members............................................ 509
Viewing Routing Protocol Information.......................................... 510
Displaying the Kernel Forwarding Table....................................... 510
Displaying Route Settings............................................................. 510
Displaying Interface Settings....................................................... 511
Hardware Monitoring................................................................. 512
Preventing Full Log Buffers and Related Console Messages.......... 514
Chapter 1

About Network Voyager

This chapter provides an overview of Network Voyager, the Web-based interface that you can use to manage Check Point IPSO systems.

Network Voyager is a Web-based interface that you can use to manage IPSO systems from any authorized location. Network Voyager comes packaged with the IPSO 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 for the version of IPSO you are running.

In This Chapter

- Software Overview
- Logging In to Network Voyager
- Software Overview
- Viewing Hardware and Software Information for Your System
Software Overview

Check Point firewalls on IP Appliance platforms function with the help of several software components:

- **Operating System**—Check Point IPSO is a UNIX-like operating system based on FreeBSD. IPSO is customized to support Check Point’s enhanced routing capabilities and 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 Check Point’s routing software. The routing policy implemented by IPSRD resides in a database. Network Voyager (see below) configures and maintains the routing software and database.

- **Check Point FireWall-1**—FireWall-1 consists of two major components: (1) the Security Gateway, which implements the security policy, and (2) the Security Management server, which can run either on the same machine as the Security Gateway, or on another machine. Use the Security Management server to define and maintain the security policy.

- **Network Voyager**—Network 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. Network Voyager also provides online documentation. Network Voyager itself runs on a remote machine as a client application of the Check Point routing software and is HTML based.
Logging In to Network Voyager

When you log in to Network Voyager, the navigation tree you see depends on the role or roles assigned to you. If the roles assigned to your user account do not include access to a feature, you will not see a link to the feature in the tree. If they have read-only access to a feature, you will see a link and be able to access the page, but all the controls will be disabled. For more information on role-based administration, see “Role-Based Administration” on page 204.

Note - The system logs messages about both successful and unsuccessful attempts by users to log in. These are stored in the /var/log/messages file.

To open Network Voyager

1. Open a Web browser on a computer with network connectivity to the IPSO system.

2. In the Location or Address text box, enter the IP address of the initial interface you configured for the appliance.

   You are prompted to enter a username and password. If this is the first login, enter the Admin username and the password you entered when you performed the initial configuration.

   You can select to log in with or without an exclusive lock on configuration changes. For more information, see “Obtaining a Configuration Lock” on page 14.

For information about initial configuration, see the Getting Started Guide and Release Notes for IPSO.

Note - If the login screen does not appear, you might not have a physical network connection between the host and your appliance, or you might have a network routing problem. Confirm the information you entered during the initial configuration and check that all cables are firmly connected.
Logging Off

When you are finished with your Network Voyager session, or if you need to log in to a new session, log out by clicking **Log Off** at the top of the Network Voyager window.

**Note** - The Log Off link does not appear if you disabled session management. For information about session management, see “Network Voyager Session Management” on page 220.

Obtaining a Configuration Lock

When you log in with exclusive configuration lock, no other user will be able to change the system configuration. Only users with read/write access privileges are allowed to log in with exclusive configuration lock.

If you acquire a configuration lock and then close your browser without logging out, the lock remains in effect until the session time-out elapses or someone manually overrides the lock. For instructions about how to override a configuration lock, see “To override a configuration lock”

Users who have one or more read/write access privileges (as defined by the administrator under role-based administration) acquire configuration locks unless they uncheck the **Acquire Exclusive Configuration Lock** check box when they log in. However, their read/write access is limited to the features assigned by the administrator even though the configuration lock is in effect for all features.

**To log in with exclusive configuration lock**

1. At the login, enter your user name.
2. Enter your password.
3. Check the Acquire Exclusive Configuration Lock check box. This is the default.
4. Click Log In.

**Note** - Enabling the exclusive configuration lock in Network Voyager prevents you or other users from using the CLI to configure the system while your browser session is active.

**To log in without exclusive configuration lock**

1. At the login, enter your user name.
2. Enter your password.
Obtaining a Configuration Lock

3. Uncheck the Acquire Exclusive Configuration Lock check box.
4. Click Log In.

To override a configuration lock

Note - Only users with read/write access privileges are allowed to override an exclusive configuration lock.

1. From the login page, click Log In with Advanced Options.
2. Verify that the Acquire Exclusive Configuration Lock check box is checked. This is the default choice.
3. Check the Override Locks Acquired by Other Users check box.
4. Enter your user name and password.
5. Click Log In.
Navigating in Network Voyager

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

<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>Help</td>
<td>Displays help for all elements of the page.</td>
</tr>
<tr>
<td>Reset</td>
<td>Restarts the routing daemon.</td>
</tr>
<tr>
<td>Routing</td>
<td></td>
</tr>
<tr>
<td>Save</td>
<td>Saves the current (running) configuration file to disk.</td>
</tr>
</tbody>
</table>

Use the navigation tree in the left pane to navigate in Network Voyager. In particular:

- 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.

- Avoid entering a page’s URL in the browser address/location bar as a way to navigate to that page.

- Avoid using bookmarks as a way of navigating to Network Voyager pages.

To prevent an exploit known as cross-site request forgery, all URLs in Network Voyager contain a random secret that is generated for each authenticated session. Any request made without this secret will be considered a breach and the user will be redirected to the login page. When the user logs off or the authenticated session times out, the URL random string becomes invalid.

The secret is not displayed in the browser address bar. Because of this, you will be returned to the login page if you attempt to navigate with the following methods:

- Click the refresh button
- Entering a page’s URL
- Use a bookmark for a Network Voyager page
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 Check Point 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 Check Point Network Voyager Reference Guide for IPSO, is the comprehensive reference source for IPSO 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 Documentation link in the tree view.
- Check Point support site (http://support.checkpoint.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.

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>italic text</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>
Accessing Documentation and Help

<table>
<thead>
<tr>
<th>Type of Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>typewriter text</td>
<td>Indicates a UNIX command, program, file name, or path name.</td>
</tr>
<tr>
<td>bold typewriter</td>
<td>Indicates text to be entered verbatim by you.</td>
</tr>
<tr>
<td>text</td>
<td>Represents the name of a key on the keyboard, of a button displayed on your</td>
</tr>
<tr>
<td></td>
<td>screen, or of a button or switch on the hardware. For example, press the</td>
</tr>
<tr>
<td>&lt;bracketed&gt;</td>
<td>Return key.</td>
</tr>
<tr>
<td>LinkText</td>
<td>Indicates a hypertext link.</td>
</tr>
<tr>
<td>- OR -</td>
<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.
Viewing Hardware and Software Information for Your System

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.

To view the asset management summary

1. Click Asset Management under Configuration in the tree view.
   The asset management summary page appears.
2. The page separates information into three tables: Hardware, FireWall Package Information, and Operating System.
3. Click the Up button to return to the main configuration page.
Chapter 2
Configuring Interfaces

This chapter describes how to configure and monitor the various types of interfaces supported by Check Point IP security platforms, as well as other topics related to physical and logical interfaces, such as how to aggregate Ethernet ports and configure GRE and DVMRP tunnels and use transparent mode to allow your IPSO appliance to behave like a Layer 2 device.

In This Chapter

Interface Overview ....................................................... page 22
Ethernet Interfaces .................................................... page 25
Link Aggregation ....................................................... page 30
Link Redundancy ...................................................... page 38
Gigabit Ethernet Interfaces ........................................ page 41
Virtual LAN Interfaces ................................................ page 43
Loopback Interfaces .................................................... page 46
GRE Tunnels ............................................................ page 48
DVMRP Tunnels ........................................................ page 56
ARP Table Entries ..................................................... page 60
Transparent Mode ..................................................... page 63
Virtual Tunnel Interfaces (FWVPN) for Route-Based VPN page 74
Interface Overview

Check Point IPSO supports the following interface types.
- Ethernet/Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet
- VPN Tunneling

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 appliance. 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 appliance.
- \(<port>\) is the port number of the NIC. 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 loopback interface also has a physical interface named loop0.

Use Network Voyager to set attributes of interfaces. 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.

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:
Interface Status

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

where

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

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

For logical interfaces created automatically, the channel number is always zero. For example, the logical interface of a physical interface \(eth-s2p1\) is called \(eth-s2p1c0\).

Once a logical interface exists for a device, you can assign an IP address to it. 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.

**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.

---

### Interface Status

The configuration and status of removable-interface devices are displayed. Interfaces can be changed while they are offline. Table 2-1 describes the interface status indicators.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>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.</td>
</tr>
<tr>
<td>Blue</td>
<td>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.</td>
</tr>
</tbody>
</table>
Events that can affect the status of interfaces:

- 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.

### 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.
Ethernet Interfaces

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

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

Configuring Ethernet Interfaces

Table 2-2 describes the configuration settings for an Ethernet interface.

<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.</td>
</tr>
<tr>
<td></td>
<td>These selections appear on both the main Interface Configuration page and</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>interface. Default is On for all physical interfaces.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Select 100 Mbit/sec or 10 Mbit/sec.</td>
</tr>
<tr>
<td></td>
<td>This setting must be the same for all hosts on the network to which the</td>
</tr>
<tr>
<td></td>
<td>device connects.</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Select Full or Half.</td>
</tr>
<tr>
<td></td>
<td>This setting must be the same for all hosts on the network to which the</td>
</tr>
<tr>
<td></td>
<td>device connects. When connecting to a hub, configure use half duplex.</td>
</tr>
<tr>
<td></td>
<td>If you set the interface to full duplex, the link will come up but many</td>
</tr>
<tr>
<td></td>
<td>collisions will occur, which could cause the link to flap or fail.</td>
</tr>
<tr>
<td>Rx Ring Size</td>
<td>Specify the receiving side descriptor ring size.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 128-512, and should be divisible by 8</td>
</tr>
<tr>
<td>Tx Ring Size</td>
<td>Specify the transmitting side descriptor ring size.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 128-512, and should be divisible by 8</td>
</tr>
</tbody>
</table>
Configuring Ethernet Interfaces

Table 2-2  Physical and Logical Interface Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Control</td>
<td>Select on or off to enable or disable flow control. Enabling flow control can reduce receiving-buffer overflows and therefore reduce the number of dropped packets. If you enable flow control option, interfaces can send flow-control packets and respond to received packets. This option is not available for all Ethernet interfaces.</td>
</tr>
<tr>
<td>Autoadvertise</td>
<td>Select on or off to enable or disable autoadvertising. 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>UDLD</td>
<td>Select on or off to enable or disable the Unidirectional Link Detection (UDLD) protocol. Enable UDLD to improve the way IPSO detects partial failure of fiber-optic links. This option is available only for fiber interfaces. For more information, see “Using UDLD” on page 27.</td>
</tr>
<tr>
<td>ARP Mirroring for HA</td>
<td>If you enable VRRP on this interface, specify whether it should learn the same ARP information as the master if is on a backup router. Enabling this option can speed VRRP failovers because the new VRRP master does not need to learn the MAC addresses that correspond to its next hop IP addresses before it can forward traffic.</td>
</tr>
<tr>
<td>MSS Clamping</td>
<td>Configure the maximum segment size (the largest chunk of data to send) that this system advertises. Default is 536; range is 536-65535. See “Using MSS Clamping” on page 28 for more information.</td>
</tr>
<tr>
<td>IP address &amp; Mask length</td>
<td>You can add multiple IP addresses. <strong>Note</strong> - 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 Network Voyager browser.</td>
</tr>
<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>
Configuring Ethernet Interfaces

**To configure an Ethernet interface**

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. Click the name of the physical interface you want to configure.
   
   Example: eth-s2p1

3. Specify the configuration parameters for speed add duplex mode.
4. 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.
7. 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.
9. Click Apply.
10. (Optional) Add a comment to further define the logical interfaces function in the Comments text box.
   
   Click Apply.
11. Click Up to go to the Interface Configuration page.
12. Click On button that corresponds to the logical interface you configured.
   
   Click Apply.
   
   The Ethernet interface is now available for IP traffic and routing.
13. To make your changes permanent, click Save.

**Using UDLD**

Check Point systems sometimes do not properly detect partial link failures in fiber-optic connections. When this occurs, the system continues trying to send traffic over links that are not completely functional. For example, if the transmit side of a fiber interface installed in a Check Point platform fails, IPSO might not
Configuring Ethernet Interfaces

detect the failure. In that case, it continues trying to send traffic through that interface. The same problem can occur if there is a partial interface failure at the other end of the link.

IPSO includes an implementation of the Cisco Unidirectional Link Detection (UDLD) protocol to improve its detection of partial failures in fiber links (regardless of whether the problem occurs in the Check Point platform or at the other end of the link). If a partial failure is detected, IPSO deactivates the Check Point interface.

**Note** - You must also enable UDLD on the other end of the link.

If a fiber interface fails completely—that is, the interface cannot transmit or receive, IPSO detects the failure properly regardless of whether UDLD is enabled.

**Warning** - A problem can occur with UDLD if the platform receives very heavy traffic. Under this condition, some UDLD packets might get dropped, which causes IPSO to see the link as unidirectional and deactivate the interface. If IPSO deactivates a UDLD interface, a connected Cisco switch also deactivates the corresponding port and does not reactivate that port without user intervention unless configured to do so.

**Using MSS Clamping**

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.

The MSS Clamping setting is subject to the following:

- It is only applicable to TCP.
- The MSS size that the Check Point system advertises should be at least 40 bytes less than the MTU of the appropriate interface. The 40-byte difference allows for a 20-byte TCP header and a 20-byte IP header (which are included in the MTU).
- The Check Point system advertises the MSS value you set, and remote terminated nodes respond by sending segments in packets that do not exceed your advertised value.
- When the Check Point system originates packets, it will send packets that have the segment size configured with this option or the advertised MSS of the remote terminating node, whichever is lessor. For example:
Configuring Ethernet Interfaces

- If you set this value to 536 and a remote system advertises 1024, the Check Point system sends packets with a TCP segment size of 536.
- If you set the MSS clamping value to 1500 and the remote system advertises an MSS of 1024, the Check Point system sends packets with a TCP segment size of 1024.
- Only the remote terminating node responds to the MSS value you set; that is, intermediate nodes do not respond. Generally, however, intermediate nodes can handle 1500-byte MTUs.
Link Aggregation

Check Point 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 logical interface continues to function. If you use static link aggregation, 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. If you use dynamic link aggregation, IPSO offers several transmit options.

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

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 reinsert the NIC, the appropriate ports rejoin the aggregation group and resume forwarding traffic automatically.

**Note** - You can include aggregated Ethernet interfaces in transparent mode groups and link redundancy groups.
You can view statistical information about link aggregation groups and the individual interfaces in the groups by clicking Configuration > Monitor > System Health > Interface Traffic Statistics > Link Aggregation Statistics.

**Supported Standards**

IPSO supports the IEEE 802.3ad standard for static link aggregation and the 802.3ad Link Aggregation Control Protocol (LACP) for dynamic link aggregation. Choose static or dynamic aggregation to match the setting on the device at the other end of the link.

Regardless of whether you use static or dynamic link aggregation, you must configure the physical interface settings for both ends of the link identically.

IPSO does not completely implement dynamic link aggregation. The IPSO implementation differs from the standard in that:

- You must create a link aggregation group on your IPSO platform and assign it an IP address even when using LACP because the firewall requires an IP address for the group.
- You must add ports to the group manually.

See “Configuring Dynamic Link Aggregation” for more information.

**Upgrading IPSO with Link Aggregation**

IPSO 4.2 and later requires aggregated interfaces to use full duplex duplicity. Previous versions of IPSO allow aggregated interfaces to be half duplex. If you have a group with half duplex interfaces on a system running a previous version of IPSO and upgrade to 4.2 or later, the group is active after the upgrade and continues to forward traffic. However, both of the following are true:

- You cannot add any interfaces to the original group.
- If you create a new link aggregation group on a system running IPSO 4.2 or later, you cannot include half duplex interfaces in the new group.

**Managing Link Aggregation Using SNMP**

Check Point IPSO systems use a proprietary SNMP MIB to manage link aggregation. To incorporate link aggregation into your SNMP-based management, perform the following tasks:
Configuring Switches for Link Aggregation

- Copy the file CheckPoint-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

Note - 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 Check Point appliance:

- You must configure the appropriate switch ports to use link aggregation. (On Cisco switches, this means you must enable EtherChannel.) That is, if you aggregate four ports into one group on your Check Point appliance, the four switch ports that they connect to must use 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 you configure it to use the destination MAC address to distribute the load, all the traffic flowing from the switch to the IPSO system over the aggregated link will be 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 Check Point 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:
Configuring Link Aggregation

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

### Configuring Link Aggregation

To set up link aggregation in Network Voyager:

1. Physically configure the interfaces.
2. Create the aggregation group.
3. Logically configure the aggregation group.

These steps are explained in the following sections.

#### 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.

Interfaces in a link aggregation group must:

- not have an IP address
- use full duplex duplicity

Interfaces that do not meet these requirements are not available to be added to a link aggregation group.

**Warning** - Previous versions of IPSO allow aggregated interfaces to be half duplex. If you have a group with half duplex interfaces and upgrade to IPSO 4.2, the group is inactive after the upgrade and does not forward traffic until you change the interfaces to full duplex.

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.
Configuring Link Aggregation

Because the management port is now part of an aggregation group, Network Voyager and the CLI identify it using the format \( aexxx \), in which xxx is the group ID.

To physically configure the interfaces you will aggregate
1. Click Interfaces under Configuration > Interface Configuration in the tree view.
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.

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.

If you use VRRP on the Check point Security Gateway, you can run firewall synchronization traffic over an aggregated link, regardless of which ports participate in the link.

To configure link aggregation groups
1. Click Link Aggregation under Configuration > Interface Configuration in the tree view.
2. In the New Group ID field, enter a numeric value to identify the group of aggregated interfaces.
3. Click Apply.
   An entry for the new group appears under Existing Link Aggregation Groups.
4. Use the Primary Port pull-down menu to select a port for the aggregation group.
Configuring Link Aggregation

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.

5. 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.

6. Add other ports to the group by selecting other interfaces from the Add Port menu and clicking Apply.

7. Specify the minimum number of physical port that must be active for the aggregation group (logical interface) to remain active.

   If the number of active ports becomes less than this number, the logical interface is deactivated.

   **Note** - Network Voyager’s display of the aggregated bandwidth does not reflect whether any of the ports are physically up or logically active.

8. Select a method for distributing outgoing traffic between the aggregated interfaces under Aggregate Tx Policy for Group. The choices are:

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

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

9. Click Apply.
Configuring Link Aggregation

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 aexxxc0. 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, you cannot configure it logically.

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, click Delete 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.

Configuring Dynamic Link Aggregation
Use dynamic link aggregation if the Link Aggregation Control Protocol (LACP) is enabled on the device at the other end of the link.

To configure dynamic link aggregation
1. To enable LACP, select an LACP mode.
   • Select Active if you want the interfaces in the aggregation group to send LACP control traffic repeatedly. Check Point recommends that you use this setting.
   • Select Passive if you want the interfaces in the aggregation group to send LACP control traffic only in the following circumstances:
     • An interface needs to provide information about itself to the other end of the link (as happens when a Check Point interface becomes active and receives a packet).
     • When a configuration setting changes on the Check Point interface.
2. Select an option for the LACP timer. IPSO uses this option to detect if a link is active and determine whether to drop inactive interfaces from a link aggregation group.
Configuring Link Aggregation

- Short: IPSO expects to receive an LACP control packet every 30 seconds on each physical interface in the link aggregation group. If it does not receive a control packet on an interface within 30 seconds, it drops the interface from the group.

- Long: IPSO expects to receive an LACP control packet every 90 seconds on each physical interface in the link aggregation group. If it does not receive a control packet on an interface within 90 seconds, it drops the interface from the group.

**Warning** - When an aggregated interface receives more traffic than it can process, it might drop LACP control packets. This can cause IPSO to remove the interface from the aggregation group. When the dropped interface starts receiving control packets again, it rejoins the aggregation group.

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

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

5. Click Apply.
Link Redundancy

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

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

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

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

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

By using a Check Point high-availability solution and connecting redundant interfaces to redundant switches, you can create highly resilient network configurations. For example, if you use VRRP, you can set up redundant switches by using a configuration such as the following:

1. Using internal interfaces, create a link redundancy group on each system (platforms A and B).
2. On platform A:
   1. Connect the primary redundant interface to redundant switch A.
   2. Connect the secondary redundant interface to redundant switch B.
3. On platform B:
If You Use Link Redundancy Before Upgrading to 6.1

1. Connect the primary redundant interface to redundant switch B.
2. Connect the secondary redundant interface to redundant switch A.
4. If there are VLANs configured on the switches, put all the switch ports you used in steps 2 and 3 in the same VLAN.
5. If necessary, connect the switches with a trunk link (to support VLANs, for example).
6. Repeat this procedure using external interfaces on your Check Point platforms and additional switches.

By deploying a configuration such as this you can eliminate a single switch as a single point of failure and extend your high availability configuration on both sides of your firewall.

If You Use Link Redundancy Before Upgrading to 6.1

If you create a link redundancy group with IPSO 6.1, the maximum number of ports in the group is two. However, this constraint does not apply if you have a link redundancy group with more than two ports in IPSO 4.x and upgrade to IPSO 6.1 by adding the 6.1 image. In this case, all the ports work after the upgrade but you cannot add any more ports to the group.

Configuring Link Redundancy Groups

Perform the steps in the following section to create a group of redundant interfaces.

To configure redundant interfaces
1. Click Link Redundancy under Configuration > Interface Configuration in the tree view.
2. In the New Group ID field, enter a numeric value to identify the group of redundant interfaces.
3. Click Apply.

An entry for the new group appears under Existing Link Redundancy Groups.
4. Use the Bonded Port pull-down menu to select the primary port for the group.

Because this is the default interface, you should probably choose the fastest of the available interfaces.
5. Click Apply.
6. Use the Bonded Port pull-down menu to select another interface.
7. Click Apply.
8. (Optional) Add additional interfaces to the group.
9. Click Save.

**Logical Configuration**

When you have completed the redundancy 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 rexxxc0. For example, the logical name of a redundancy group with the ID 100 is re100c0.

If you create a link redundancy group but do not add any interfaces to it, you cannot configure it logically.

**Deleting Link Redundancy Groups**

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

You cannot remove the primary port from a 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

You can configure the parameters listed in Table 2-3 for each Gigabit Ethernet interface.

For information on how to complete the configuration of a Gigabit Ethernet interface, see “To configure an Ethernet interface” on page 27.

Table 2-3 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>You can implement flow control 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.</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 interfaces that have the capability of transmitting jumbo frames. Default is 1500; range is 1500-16,000.</td>
</tr>
<tr>
<td>IP Address &amp; Mask Length</td>
<td>You can add multiple IP addresses. 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 Network browser.</td>
</tr>
<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>
To configure a Gigabit Ethernet interface

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. Click the physical interface link to configure. *Example: eth-s5p1.*
3. Set flow control to On.
4. Click Apply.
5. Click the name of the logical interface in the logical interfaces table.
   The Logical Interface page is displayed.
6. (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.
7. Enter the IP address and subnet mask length for the device in the appropriate text fields.
8. 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.
9. (Optional) Change the interface 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. Click Up to go to the Interface Configuration page.
12. 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.
13. To make your changes permanent, click Save.

*Note -* Link speed is fixed and duplex mode is set to full at all times for Gigabit Ethernet interfaces.
Virtual LAN Interfaces

Check Point IPSO 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 Check Point implementation of VLAN supports adding a logical interface with a VLAN ID to a physical interface. In a VLAN packet, the OSI Layer 2 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 Check Point 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 Check Point appliance can receive and generate fully conformant IEEE 802.1Q tags. The IEEE802.1Q standard defines the technology for virtual bridged networks. The Check Point implementation is completely interoperable as a router, not as a switch.

IPSO supports a maximum of 1015 VLAN interfaces. However, if you do not explicitly configure the system to support this number (in the Maximum Number of VLANs Allowed text box), the default maximum is 950 VLAN interfaces. This is system limit and not limited to specific interface.

To configure a VLAN Interface

1. Click Interfaces under Interface Configuration in the tree view.
2. Click the link to the physical Ethernet interface for which you want to enable a VLAN interface.
   - The physical interface page for that interface is displayed.
3. 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.
4. Click Apply.
Virtual LAN Interfaces

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 2 through 4 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.

7. Click Apply.

8. 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.

9. Click Apply.

10. Click Save to make your change permanent.

Note - You can assign multiple IP addresses to each logical VLAN interface.

To delete a VLAN Interface

1. Click Interfaces under Configuration > Interface Configuration in the tree view.

2. 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.

3. In the Logical Interface table, click Delete in the row for the logical VLAN interface to delete.

4. Click Apply.

5. Click Save to make your change permanent.

   The entry for the logical VLAN interface disappears from the Logical Interfaces table.

To define the maximum number of VLANs
1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. Enter a number in the Maximum Number of VLANs Allowed text box. The maximum value is 1015.
3. Click Apply.
4. Click Save to make your change permanent.

**VLAN Example Topology**

The following topology represents a fully redundant firewall with load sharing and VLAN. Each 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.
Loopback Interfaces

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.

To add 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 Interfaces under Configuration > Interface Configuration in the tree view.
2. Click the loopback logical interface link in the Logical column (loop0c0).
3. 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.
4. Click Save to make your changes permanent.

To change the IP Address of a loopback interface

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. Click the loopback logical interface link in the Logical column (loop0c0).
3. To remove the old IP address, click the Delete check box that corresponds to the address to delete.
   Click Apply.
4. To add the new IP address, enter the IP address for the device in the New IP address text box.
   Click Apply.
Loopback Interfaces

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. Click Save to make your changes permanent.
GRE Tunnels

GRE tunnels encapsulate IP packets by using Generic Routing Encapsulation (GRE) with no options. The encapsulated packets appear as unicast IP packets. GRE tunnels can provide a redundant configuration between two sites for high availability.

For each GRE 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. The remote router must also support GRE encapsulation and must be configured with a tunnel interface to the local router.

Configuring GRE Tunnels

To create a GRE tunnel

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. Click Tunnels in the Physical column.
3. Click the drop-down window in the Create a new tunnel interface with encapsulation field and select GRE.
4. Click Apply.
   
   Each time you select a tunnel encapsulation and click Apply, the new tunnel appears in 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 for the specified tunnel. Example: tun0c1.
6. 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.
7. 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.
8. 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.
Configuring GRE Tunnels

9. 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.

10. 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.

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 a custom value from the TOS value drop-down window, enter a value in the range of 0-255.

Click Apply.

13. (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.

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

Click Apply.

Note - If the local endpoint is a loopback address, you must set this option to Off to allow traffic to egress through the tunnel.
15. Click Save to make your changes permanent.

**To change the local or remote address or endpoint of a GRE tunnel**

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. In the Logical column, click the Logical Interface link for which to change the IP address.
   
   Example: tun0c1
3. (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.
4. (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.
5. (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.
6. (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.
7. Click Save to make your changes permanent.

**To change IP TOS value of a GRE tunnel**

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. In the Logical column, click the Logical Interface link of the item for which to change the TOS. Example: tun0c1.
3. 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.

4. (Optional) If you selected custom value from the TOS value drop-down window, enter a value in the range of 0-255.

Click Apply.

5. Click Save to make your changes permanent.

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 Interfaces under Configuration > Interface Configuration in the tree view.
2. Click Tunnels in the Physical column.
3. Click the drop-down window in the Create a new tunnel interface with encapsulation field and select GRE.
4. Click Apply.
5. From the Interface column on the Logical interfaces table, select tun01.
6. Enter 10.0.0.1 in the Local address text box.
7. Enter 10.0.0.2 in the Remote address text box.
8. Enter 192.68.26.65 in the Local endpoint text box.
10. (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.
11. (Optional) If you selected custom value from the TOS value drop-down window, enter a value in the range of 0-255.
    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. Click Save.

High Availability GRE Tunnels

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.

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.
HA GRE Tunnel Example

1. Perform the steps as presented in the *To create 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:

1. 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.

2. 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.

3. 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.

4. 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`

3. VRRP provides redundancy in case one of the firewalls is lost. Perform the steps as presented in “Configuring VRRP” on page 130. 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
HA GRE Tunnel Example

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

DVMRP Tunnels

DVMRP (Distance Vector Multicast Routing Protocol) tunnels encapsulate multicast packets IP unicast 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.

To create a DVMRP tunnel

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. Click Tunnels in the Physical column.
3. From the pulldown menu in the Create a new tunnel interface with encapsulation, select DVMRP.
4. Click Apply.
   Each time you select a tunnel encapsulation and click Apply, a new tunnel appears in the table.
5. 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.
6. 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.
7. Enter the IP address of the remote end of the DVMRP tunnel in the Remote Address text box.
DVMRP Tunnels

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.

8. (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.

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

10. 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.

To change the local or remote addresses of a DVMRP tunnel

1. Click Interfaces under Configuration > Interface Configuration in the tree view.

2. In the Logical column, click the Logical Interface link on the tunnel that is to have the IP address changed.
   Example: tun0c1

3. (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.

4. (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.

5. Click Apply.

6. Click Save to make your changes permanent.

   Note - When the tunnel interface has been created, set all other DVMRP configuration parameters from the DVMRP page.
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 it 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. IP Appliance 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 Check Point Platform A points to 22.254/24.

1. Initiate a Network Voyager session to Platform A. In this example, we use Platform A as the starting point.
2. Click Interfaces under Configuration > Interface Configuration in the tree view.
3. Click Tunnels in the Physical column.
4. From the pulldown menu in the Create a new tunnel interface with encapsulation, select DVMRP.
DVMRP Tunnel Example

4. Click Apply.
   Each time you select a tunnel encapsulation and click Apply, a new tunnel appears in the table.

5. 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

6. Enter the following in the Local IP Address text box:
   192.168.22.1

7. Enter 192.168.22.254 in the Remote IP Address text box

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

9. Click Apply.

10. 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.

11. Click DVMRP under Configuration > Routing in the tree view.

12. For each interface to configure for DVMRP, click On for the interface.

13. Click Apply.

14. (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.

15. (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.

16. Click Apply.

17. 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.

18. 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

The Address Resolution Protocol (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.

To change ARP global parameters

1. Click ARP under Configuration > Interface Configuration in the tree view.

2. 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).

3. 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.

4. 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 that uses a multicast mode. Because all the nodes of a multicast mode 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.

5. Enable ARP Mirroring for HA to cause the VRRP-enabled interfaces on VRRP backup routers to have the same ARP information as the master. Enabling this option can speed VRRP failovers because the new VRRP master does not need to learn the MAC addresses that correspond to its next hop IP addresses before it can forward traffic.

6. Click Apply.

7. Click Save to make your changes permanent.

To add a static ARP entry

1. Click ARP under Configuration > Interface Configuration in the tree view.
To add 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 ARP under Configuration > Interface Configuration in the tree view.
2. Enter the new IP address in the IP Address field in the Add a New Proxy ARP Entry section.
3. In the Interface field, select the interface whose MAC address will be returned in ARP replies.
   Selecting User-defined MAC Address allows you to specify an arbitrary MAC address for the entry.
   Click Apply.
4. (Optional) If you select User-Defined MAC Address, enter a MAC address in the MAC Address text box in the Proxy ARP Entries table.
   Click Apply.
5. Click Save to make your changes permanent.

Note - In VRRP configurations, configuring proxy ARP using static NAT addresses and interface MAC addresses is not supported.

To delete a static ARP entry

1. Click ARP under Configuration > Interface Configuration in the tree view.
2. Click the checkbox in the Delete column next to the table entry to delete.
   Click Apply.
3. Click Save to make your changes permanent.

To view dynamic ARP entries
1. Click ARP under Configuration > Interface Configuration in the tree view.
2. Click the Display or Remove Dynamic ARP Entries link.

**To delete dynamic ARP entries**
1. Click ARP under Configuration > Interface Configuration in the tree view.
2. Click the Display or Remove Dynamic ARP Entries link.
3. Click the check box in the Delete column next to the ARP entry to delete.
   - Click Apply.

**To flush all dynamic ARP entries**
1. Click ARP under Configuration > Interface Configuration in the tree view.
2. Click Flush.
Transparent Mode

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

Note - Transparent mode interoperates with the Check Point firewall. There is no special code or software required for the bridging functionality to be supported by the firewall.

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

The firewall requires one interface in a transparent mode group to have an IP address. From the firewall's perspective, all the interfaces in the group share this address.

By default, transparent mode interfaces forward only IP or ARP packets. Traffic for all other protocols is discarded automatically. You can configure transparent mode to forward traffic for other protocols. See "Forwarding Protocols Other Than IP and ARP" on page 71 for more information.

Limitations

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.
- Transparent mode is not supported with IPv6. You cannot add an interface with an IPv6 address to a transparent mode group, and you cannot enable IPv6 on an interface that is already part of a transparent mode group.
Transparent Mode Processing Details

- Transparent mode is not supported in a cluster environment. You cannot use transparent mode on interfaces that participate in an IPSO cluster.

Note - Transparent mode is supported with VRRP.

Transparent Mode Processing Details

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 time-out 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.
Configuring Transparent Mode in VPN Environments

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 Check Point 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 example, the network administrator of Network A wants to provide Network B with access to certain addresses behind the Check Point 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.
Example of Transparent Mode

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 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.
Example of Transparent Mode

Check Point’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

1. Click Transparent Mode under Configuration > Interface Configuration in the tree view.
2. Enter any positive integer (an integer greater than 0) in the edit box, for example 100 and click Apply.
3. 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.
4. In the Add Interface drop-down box, select an interface to associate with the transparent mode group. In this case, select the logical interface associated with the external IP address 1.5.3.24 and click Apply.
5. In the Add Interface drop-down box, select the interface connected to the internal LAN and click Apply.
   This allows the system to bridge between the internal and external interfaces in the group.
6. Click Transparent Mode in the navigation tree to display the Transparent Mode configuration page.
7. Select Yes in the Enable column associated with XMG 100 and click Apply.
8. 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.
Configuring Transparent Mode

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. If you associate active interfaces with a disabled transparent mode group, you 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, one interface in each group must have an IP address. Check Point recommends that you assign all IP addresses for a transparent mode group to a single interface in the group to avoid confusing the firewall.

Creating and Deleting Transparent Mode Groups

You create a transparent mode group by first creating the group then adding the interfaces to the group. (See “Adding or Removing Interfaces to or from Transparent Mode Groups” on page 69) 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” on page 70)

To create a transparent mode group
1. Click Transparent Mode under Configuration > Interface Configuration in the tree view.
2. Enter any positive integer (an integer greater than 0) in the edit box.
3. Click Apply.
4. Click Save to make your changes permanent.

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, stop and restart the firewall.

To delete a transparent mode group
1. Click Transparent Mode under Configuration > Interface Configuration in the tree view.
2. Click the Delete radio button associated with the group you would like to delete and click Apply.
3. Click Save to make your changes permanent.

Adding or Removing Interfaces to or 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.

When you select interfaces to participate in a transparent mode group, be aware of the following:

- Transparent mode groups are disabled by default. Do not associate an interface that is in use with a disabled transparent mode group. If you do, you will lose connectivity to the interface.
- 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.

To add or remove an interface to/from a transparent mode group

1. Click Transparent Mode under Configuration > Interface Configuration in the tree view.
2. Click the link of the appropriate transparent mode group.
3. To add an interface to the transparent mode group, select it from the Add Interface drop-down box.
4. 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.
5. (Optional) Repeat to add or remove other interfaces to or from the transparent mode group.
6. Click Save to make your changes permanent.
Configuring Transparent Mode

**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 Transparent Mode under Configuration > Interface Configuration in the tree view.
2. Select Yes or No in the Enable column associated with the transparent mode group you want to enable or disable.
3. Click Apply.
4. 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” on page 63. As a VRRP standby, it will drop all packets except those with local destinations.

Check Point recommends that you create the transparent mode group and add all interfaces to it before you create any VRRP circuit that will use the group. Doing this ensures that all the un-numbered interfaces in the transparent mode group are monitored if you use the simplified method to configure monitored-circuit VRRP. See “Configuring Monitored-Circuit VRRP using the Simplified Method” on page 139 for information about configuring VRRP in this way.

To see which transparent mode interfaces are being monitored by VRRP, perform this procedure:

1. Configuration > High Availability > VRRP in the navigation tree.
2. On the VRRP Configuration page, click the VRRP Monitor link.
3. Click the Interface link in the monitor table.
Configuring Transparent Mode

For complete information on configuring VRRP, see “High Availability Solutions” on page 117

To enable or disable VRRP for a transparent mode group
1. Click Transparent Mode under Configuration > Interface Configuration in the tree view.
2. Click the link of the transparent mode group to which you would like to enable VRRP.
3. Select the Yes or No radio button in the VRRP Enabled table.
4. Click Apply.
5. Click Save to make your changes permanent.

Forwarding Protocols Other Than IP and ARP

By default, transparent mode interfaces forward only IP or ARP packets. Traffic for all other protocols is discarded automatically. To configure transparent mode to forward traffic for other protocols, use the Cross Connect Configuration options.

If you enable Cross Connect, transparent mode interfaces forward traffic for all protocols except those you block with filters. If you disable Cross Connect (the default setting), transparent mode interfaces drop traffic for protocols other than IP or ARP unless you create filters to allow specific traffic to be forwarded.

Create Cross Connect filters to configure transparent mode interfaces to forward or discard traffic for specific protocols. For each filter you choose the method of 802 encapsulation and enter the hexadecimal value for the protocol that you want the transparent mode interfaces to forward or drop.

There are two approaches to using this functionality:

- If you want the transparent mode interfaces to forward most traffic types and block traffic for a small number of protocols, you should:
  - Select Yes next to Cross Connect Enabled.
  - Create discard filters for the traffic you want to block.

In this case, IPSO discards packets for the protocols you specify and forwards any other traffic.

If you choose this approach, you might want to create discard filters for IP and ARP packets. IP or ARP packets for VLANs configured on the transparent mode interfaces are always forwarded regardless of whether Cross Connect Enabled is
Monitoring Transparent Mode Groups

set to Yes or No. However, if Cross Connect Enabled is set to Yes, IP or ARP packets for VLANs not configured on the transparent mode interfaces are also forwarded unless you block them with discard filters.

- If you want the transparent mode interfaces to discard most traffic types and forward traffic for a small number of protocols, you should
  - Select No next to Cross Connect Enabled.
  - Create filters for the traffic you want to forward.

In this case, IPSO forwards packets for the protocols you specify and drops any other traffic.

To configure cross connect filters
1. Select the appropriate 802 encapsulation.
2. Specify whether this filter should forward or discard the relevant traffic.
3. Enter the appropriate hexadecimal value for the protocol you want to forward or discard. Use the value of the appropriate Ethernet frame field.
   Do not include “0x” before the hexadecimal value. For example, enter 8000, not 0x8000 for DIX.
   - DIX: Two-byte value of the Type field.
   - LLC: One-byte value of the Destination Service Access Point (DSAP) field.
   - SNAP: Five-byte combined value of the OUID and Type (PID) fields.
4. Click Apply.
5. Click Save to make your changes permanent.

Monitoring Transparent Mode Groups

To monitor transparent mode groups
1. Click Transparent Mode under Monitor in the tree view.
2. Click a transparent mode group under XMODE Group Id.

Transparent Mode and the Check Point Security Gateway

This section explains some details about configuring a firewall to work with transparent mode.
Configuring Antispoofing

The proper configuration for antispoofing depends on how the interfaces in the transparent mode group are configured.

All Interfaces Are Internal

If all the interfaces in the group are internal, you should configure antispoofing normally. You treat the interfaces as being on the same subnet and, any other nested networks must be properly defined so that antispoofing to be aware of them and traffic is not dropped.

One Interface Is External

If one interface is external, do not use antispoofing. If antispoofing is applied, the firewall drops reply packets because they are sourced from the same subnet.

Configuring VRRP

When you use the Check Point 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.
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

Check Point 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 a 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 Network Voyager as unnumbered interfaces and are given logical names in the form tun0c\(n\). 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**

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 Network Voyager or the Check Point VPN shell. The procedure “To create the virtual tunnel interface” describes how to do so using Network Voyager.

**To create the VPN community**

1. Using the Check Point SmartDashboard, create the peer gateway objects.
Creating Virtual Tunnel Interfaces

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.
Creating Virtual Tunnel Interfaces

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**

1. In Network Voyager navigation tree, select Configuration > Interface Configuration > FWVPN tunnel.

2. 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.

3. 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.

4. 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.
Creating Virtual Tunnel Interfaces
Chapter 3

Configuring System Functions

This chapter describes how to configure many basic system functions.

- Configuring Banner and Login Messages  page 81
- Configuring DHCP  page 82
- Configuring the Domain Name Service  page 92
- Configuring Disk Mirroring/RAID  page 93
- Mail Relay  page 95
- System Failure Notification  page 96
- Configuring System Time  page 98
- Configuring Host Addresses  page 102
- Using an Optional Disk (Flash-Based Platforms Only)  page 102
- Configuring System Logging  page 104
- Using a Core Dump Server with Flash-Based Systems  page 114
- Changing the Host Name  page 116
- Managing Configuration Sets  page 117
- Scheduling Jobs  page 119
- Backing Up and Restoring Files  page 121
- Managing Check Point IPSO Images  page 127
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Monitor Reports</td>
<td>133</td>
</tr>
<tr>
<td>Using a Core Dump Server with Flash-Based Systems</td>
<td>114</td>
</tr>
<tr>
<td>Advanced System Tuning</td>
<td>137</td>
</tr>
</tbody>
</table>
Configuring Banner and Login Messages

When a user connects to an IPSO system or logs out, the system displays the message “This system is for authorized use only” by default on the login page. You can change or disable this message on the Banner and MOTD Configuration page. You can also configure an FTP welcome message and a “message of the day” (MOTD) that users see when they log in using the command line.

To configure messages

1. Click Banner and MOTD under Configuration > System Configuration in the tree view.
2. Create or modify the messages as appropriate.
3. Enable or disable the messages as appropriate.
4. Click Apply.
Configuring DHCP

Dynamic Host Configuration Protocol (DHCP) for Check Point IPSO provides complete DHCP client and DHCP server capabilities for your Check Point 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.

The Check Point IPSO implementation of DHCP 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 specify 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.

Configuring DHCP Client Interfaces

To configure the DHCP client interface

1. Click DHCP under Configuration > System Configuration in the tree view.
2. Click the logical interface 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 “Ethernet Interfaces” on page 31.

3. (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.
DHCP Client Configuration

4. Enter a value, in seconds, in the Timeout text box. If you do not enter a value, the configuration defaults to 60 seconds.

5. Enter a value, in seconds, in the Retry text box. If you do not enter a value, the configuration defaults to 300 seconds.

6. Enter a value, in seconds, in the Lease text box for the length of time the IP address will be leased to the interface.

7. 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.

8. Click Apply.

9. Click Save to make your changes permanent.

DHCP Client Configuration

To enable the DHCP client process

1. Click DHCP under Configuration > System Configuration in the tree view.

2. Click Client next to the logical interface link to be configured as a DHCP client in the DHCP Interface Configuration table.

3. In the DHCP Client Configuration table, select Enable.

Note - The Ethernet interface must be enabled before you enable the client. For more information on how to configure Ethernet interfaces see “Ethernet Interfaces” on page 31.

4. Enter a host name in the Hostname text box.

5. Click Apply.

6. Click Save to make your changes permanent.

Configuring the DHCP Server

To configure the DHCP server process

1. Click DHCP under Configuration > System Configuration in the tree view.

2. Click Server in the DHCP Service Selection box.
Configuring the DHCP Server

3. 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 “Ethernet Interfaces” on page 31.

4. Click the Add a new Subnet Entry link.

5. Enter the subnet address of the Ethernet interface you have configured for the DHCP server process in the Subnet text box.

6. Enter the mask length for the subnet in the Mask Length text box.

7. (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.

8. (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.

9. 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.

10. (Optional) Enter the Trivial File Transfer Protocol (TFTP) server clients will use in the TFTP text box.

11. (Optional) Enter the file name where diskless clients will find the boot file in the File Name text box.
DHCP Server Configuration

12. (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.

13. (Optional) Enter the root path where diskless clients mount a network file system (NFS) in the Root Filename text box.

14. Enter the IP address of the default router clients will use in the Router text box.

15. (Optional) Enter the domain name you want clients to use in the Domain text box.

16. (Optional) Enter the time offset for clients in the Time Offset text box.

17. (Optional) Enter the IP address or the name of the swap server diskless clients will use in the Swap Server text box.

18. Enter the Domain Name System (DNS) server clients will use to resolve domain names in the DNS Servers text box.

19. 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.

20. Enter the Simple Mail Transfer Protocol (SMTP) servers available to clients, separated by commas, in the SMTP Servers text box.

21. If you configure NetBIOS, enter the Windows Internet Naming Servers (WINS) available to clients in the WINS text box.

22. If you configure NetBIOS, enter the Datagram Distribution (DD) servers available to clients, separated by commas, in the DD Servers text box.

23. If you configure NetBIOS, enter the node type that the client will configure itself as in the Node Type text box.

24. If you configure NetBIOS, enter the scope for the client in the Scope text box.

25. Click Apply.

26. Click Save to make your changes permanent.

**DHCP Server Configuration**

To enable the DHCP server process

1. Click DHCP under Configuration > System Configuration in the tree view.
Changing DHCP Service

2. Click Server in the DHCP Service Selection box.
3. 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” on page 83, steps 5, 6, and 7. For more information on how to configure Ethernet interfaces, see “Ethernet Interfaces” on page 31.

4. Click Enable in the DHCP Server Process box.
5. Click Apply.
6. Click Save to make your changes permanent.

To disable the DHCP server process
1. Click DHCP under Configuration > System Configuration in the tree view.
2. Click Disable in the DHCP Server Process box.
3. Click Apply.
4. Click Save to make your changes permanent.

Changing DHCP Service

To change the DHCP service
1. Click DHCP under Configuration > System Configuration in the tree view.
2. Click the Change DHCP Service link.
3. Click the service for which you would like to configure your appliance in the DHCP Service Selection box.
4. Click Apply.
5. Click Save to make your changes permanent.

Adding DHCP Address Pools

To add additional IP address ranges to an existing DHCP server configuration
1. Click DHCP under Configuration > System Configuration in the tree view.
2. Click the IP address link for which you would like to add additional address ranges in the DHCP Server Subnet Configuration box.
Enabling or Disabling DHCP Address Pools

3. 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.

4. Click Apply.
5. Click Save to make your changes permanent.

Assigning a Fixed-IP Address to a Client

To assign a fixed-IP address to a client
1. Click DHCP under Configuration > System Configuration in the tree view.
2. Click the Add a new Fixed-IP Entry link in the Fixed-IP Address Client Configuration.
3. (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.
Assigning a Fixed-IP Address to a Client

4. 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.

5. Enter the IP address you want to assign the client in the IP Address text box.

6. (Optional) Enter the Trivial File Transfer Protocol (TFTP) server clients will use in the TFTP 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 a path for clients to get additional configuration options in the Extensions Path text box.

9. (Optional) Enter the root path where diskless clients mount a network file system (NFS) in the Root Filename text box.

10. Enter the IP address of the default router clients will use in the Router text box.

11. (Optional) Enter the domain name you want clients to use in the Domain text box.

12. (Optional) Enter the time offset for clients in the Time Offset text box.

13. (Optional) Enter the IP address or the name of the swap server diskless clients will use in the Swap Server text box.

14. Enter the Domain Name System (DNS) server clients will use to resolve domain names in the DNS Servers text box.

15. 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.

16. Enter the Simple Mail Transfer Protocol (SMTP) servers, separated by commas, available to clients in the SMTP Servers text box.

17. If you configure NetBIOS, enter the Windows Internet Naming Servers (WINS), separated by commas, available to clients in the WINS text box.

18. If you configure NetBIOS, enter the Datagram Distribution (DD) servers, separated by commas, available to clients in the DD Servers text box.

19. If you configure NetBIOS, enter the node type that the client will identify itself as in the Node Type text box.

20. If you configure NetBIOS, enter the scope for the client in the Scope 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.
Creating DHCP Client Templates

21. Click Apply.
22. 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 DHCP under Configuration > System Configuration in the tree view.
2. Click the Template for adding new client entries link.
3. (Optional) Enter the Trivial File Transfer Protocol (TFTP) server clients will use in the TFTP text box.
4. (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.

5. (Optional) Enter the root path where diskless clients mount a network file system (NFS) in the Root Filename text box.
6. (Optional) Enter the file name where diskless clients will find the boot file in the File Name text box.
7. (Optional) Enter the domain name you want clients to use in the Domain text box.
8. (Optional) Enter the time offset for clients in the Time Offset text box.
9. (Optional) Enter the IP address or the name of the swap server diskless clients will use in the Swap Server text box.
10. Enter the Domain Name Servers (DNS) clients will use to resolve domain names in the DNS Servers text box.
11. 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.
12. 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.

13. If you configure NetBIOS, enter the Datagram Distribution (DD) servers, separated by commas, available to clients in the DD Servers text box.

14. If you configure NetBIOS, enter the node type that the client will identify itself as in the Node Type text box.

15. If you configure NetBIOS, enter the scope for the client in the Scope text box.

16. Click Apply.

17. Click Save to make your changes permanent.

Configuring Dynamic Domain Name System Service

DDNS gives you the ability to configure your DHCP server to automatically update DNS servers on your network.

To configure Dynamic Domain Name System (DDNS)
1. Click DHCP under Configuration > System Configuration in the tree view.
2. Click the DDNS Configuration link.
3. Check that enable is selected.
4. Select a style in the Update Style box.
5. Enter a key name in the Key Name text box and click the enable button next to the name.
6. Enter the secret key to be matched by the DNS server in the Key Secret text box.
7. Click Apply.
8. 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” on page 90.

1. Click DHCP under Configuration > System Configuration in the tree view.
2. Click the DDNS Configuration link.
3. Enter the zone identifier in the Zone text box.
4. Check that enable is selected next to the Zone text box.
5. Select a key to associate with the zone in the Key drop-down box.
6. Enter the IP address of the primary DNS server in the Primary text box.
7. (Optional) Enter the IP address of the secondary DNS server in the Secondary text box.
8. Click Apply.
9. Click Save to make your changes permanent.

To add more zones, complete steps 4 through 9 for each new zone.
Configuring the Domain Name Service

IPSO uses the Domain Name Service (DNS) to translate host names into IP addresses. To enable DNS lookups, you must specify the primary DNS server for your system; you can also specify secondary and tertiary DNS servers. When resolving host names, the system consults the primary name server first, followed by the secondary and tertiary name servers if a failure or time-out occurs.

To configure DNS

1. Click DNS under Configuration > System Configuration in the tree view.
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/RAID

The Check Point disk mirroring feature (RAID Level 1) 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.

On some platforms, disk mirroring/RAID is automatic and not configurable using Network Voyager. On other platforms you can enable and disable a mirror set. On all platforms you can monitor the status of a mirror set, synchronization time, and system log entries.

Note - If you need additional help with disk mirroring, refer to Implementing Disk Mirroring or RAID on a Nokia Network Security Appliance at http://downloads.checkpoint.com/dc/download.htm?ID=9869

Note - If you want to physically remove a disk that is part of a mirror set, delete the mirror set (disable disk mirroring) before you do so.

To create a mirror set (enable disk mirroring)
1. Click Disk Mirroring under Configuration > System Configuration in the tree view.
2. 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.
Configuring Disk Mirroring/RAID

3. 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.

To delete a mirror set (disable disk mirroring)

1. Click Disk Mirroring under Configuration > System Configuration in the tree view.
2. Select the Delete check box in the Mirror Sets table.
3. Click Apply.

Note - You can only delete a mirror set that is 100-percent synchronized.
Mail Relay

Mail Relay

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.

IPSO supports the following mail relay features:

- 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

IPSO does not support the following mail relay features:

- 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
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.

To configure failure notification
1. Click System Failure Notification under Configuration > System Configuration in the tree view.
2. Click On next to Enable Failure Notification.
3. Click Apply.
4. Enter the email address of the people you want to notify 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
5. To make your changes permanent, click Save.

Configuring Mail Relay

To configure mail relay for your firewall
1. Click Mail Relay under Configuration > System Configuration in the tree view.
2. Enter either the IP address or host name of the email server that relays outgoing email in the Mail Server text box.
3. 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.
4. Click Save to make your changes permanent.

Sending Mail

To send mail from the firewall
Sending Mail

1. Log in to the firewall as either the admin or monitor user.
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.
Configuring System Time

Synchronized clock times are critical for a variety of purposes, including distributed applications that require time synchronization, 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. For example, in the case of audit logs, the time stamps on different network devices should be accurate to within about a second of each other to correlate events across multiple devices.

You can view the current system time at the top of any Network Voyager page.

You can set the system time using any of the following methods:

- Set the date and time manually.
- Access a time server once.
- Configure Network Time Protocol to access time servers for continuing clock synchronization. For more information, see “Network Time Protocol (NTP)” on page 369.

In addition to setting the system time, you can also configure rules for daylight savings time changes. See “Configuring Daylight Savings Time” on page 99 for more information.

Setting System Time

Set the system time either manually or by using a time server when you initially configure the system. You might need to set it again when you bring the system up after it has been down for a period of time. Use this procedure also to specify the local time zone.

- **Note** - When you reset the system time, the routing table is reset and existing connections might be terminated.

If you have not enabled NTP, you can set the system time once from a time server. For information on configuring NTP to update the time on a regular basis, see “Network Time Protocol (NTP)” on page 369.

**To set system time once**

1. Click Time under Configuration > System Configuration in the tree view.
2. Select the appropriate time zone in the Time Zone list box.
Configuring Daylight Savings Time

By default, the time zone is set to GMT.

3. Either set the time manually or specify a time server:
   1. To set the date and time manually, enter the time and date units to change. You do not need to fill in all fields; blank fields default to their existing values. Specify hours in 24-hour format.
   2. To set the time using a time server, enter the name or IP address of the time server in the NTP Time Server text box.

Note - If NTP is enabled, this option does not appear.

4. Click Apply.
5. Click Save.

Configuring Daylight Savings Time

IPSO allows you to create and configure rules for daylight savings time (DST) changes. You can configure multiple DST rules per time zone.

When you create a DST rule, you must specify whether it is recurring or nonrecurring, according to the following definitions:

- Recurring (always occurs, with no defined stopping point). For example, the United States started using recurring daylight savings rules in 2007.
- Nonrecurring (defined for a specific period of time). For example, the United States previously used daylight savings rules that expired after 2006.

Table 3-1 describes the parameters you supply to create a DST rule. Some of the parameters vary depending on whether the rule is recurring or nonrecurring.

<table>
<thead>
<tr>
<th>Table 3-1 Daylight Savings Time Rule Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Select City</td>
</tr>
<tr>
<td>Start Year</td>
</tr>
<tr>
<td>Start Month</td>
</tr>
</tbody>
</table>
Configuring Daylight Savings Time

Table 3-1  Daylight Savings Time Rule Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Week</td>
<td>Select the occurrence of the day specified by Start Day in the month specified by Start Month. For example, selecting Second for this parameter and selecting Sunday as the starting day specifies that DST will begin on the second Sunday of the specified month. This parameter applies only to recurring rules.</td>
</tr>
<tr>
<td>Start Day</td>
<td>Select the day of week when DST begins. This parameter applies only to recurring rules.</td>
</tr>
<tr>
<td>Start Date</td>
<td>Specify the day of month when DST begins. The range of valid values is 1-31. This parameter applies only to nonrecurring rules.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Specify the time when DST begins in a 24-hour format. You can specify the time using any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• hh</td>
</tr>
<tr>
<td></td>
<td>• hh:mm</td>
</tr>
<tr>
<td></td>
<td>• hh:mm:ss</td>
</tr>
<tr>
<td>End Year</td>
<td>Select the year when the DST rule ends. This parameter applies only to nonrecurring rules.</td>
</tr>
<tr>
<td>End Month</td>
<td>Select the month when DST ends.</td>
</tr>
<tr>
<td>End Week</td>
<td>Select the occurrence of the day specified by End Day in the month specified by End Month. For example, selecting Second for this parameter and selecting Sunday as the ending day specifies that DST will end on the second Sunday of the specified month. This parameter applies only to recurring rules.</td>
</tr>
<tr>
<td>End Day</td>
<td>Select the day of week when DST ends. This parameter applies only to recurring rules.</td>
</tr>
<tr>
<td>End Date</td>
<td>Specify the day of month when DST ends. The range of valid values is 1-31. This parameter applies only to nonrecurring rules.</td>
</tr>
</tbody>
</table>
## Configuring Daylight Savings Time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Time</td>
<td>Specify the time when DST ends in 24-hour format. You can specify the time using any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• hh</td>
</tr>
<tr>
<td></td>
<td>• hh:mm</td>
</tr>
<tr>
<td></td>
<td>• hh:mm:ss</td>
</tr>
<tr>
<td>DST Offset</td>
<td>Specifies the amount by which the time is offset. You can specify the time using any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• hh</td>
</tr>
<tr>
<td></td>
<td>• hh:mm</td>
</tr>
<tr>
<td></td>
<td>• hh:mm:ss</td>
</tr>
</tbody>
</table>
Configuring Host Addresses

Click Host Address under Configuration > System Configuration to perform any of the following tasks:

- View the entries in the hosts table.
- Add an entry to the list of hosts.
- Modify the IP address of a host.
- Delete a host entry.

You should add host addresses for systems that will communicate frequently with the system you are configuring.

To add a static host entry using Voyager fields

1. Click Host Address under Configuration > System Configuration in the tree view.
2. Enter the new host name in the Add new hostname text box.
3. Click Apply.
   
The new host name appears in the list of Current Host Address Assignments.
4. Enter the IP address of the new host in the IP address text box.
5. Click Apply.
6. Click Save to make your changes permanent.

To add a static host entry using the Quick-add method

1. Click Host Address under Configuration > System Configuration in the tree view.
2. Enter host names and addresses using the following format:
   
   hostname  IP-address  <Enter>
   
   You can enter as many pairs as you want.
3. Click Apply.
   
The new host name appears in the list of Current Host Address Assignments.
4. Click Save to make your changes permanent.

To delete a static host

1. Click Host Address under Configuration > System Configuration in the tree view.
2. Select Off next to the host to delete.
3. Click Apply.
4. Click Save to make your changes permanent.
Using an Optional Disk (Flash-Based Platforms Only)

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

- **Log files**—log files that are stored in built-in flash memory are deleted whenever the platform is rebooted. You can configure an optional disk to locally store log files that survive reboot.

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

If the system crashes and stores a kernel core dump on the optional disk, you might want to retrieve the dump to send to Check Point for troubleshooting purposes. See “Using a Core Dump Server with Flash-Based Systems” on page 114 for information about how to do this.

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

When you select a hard disk or card as an optional disk, any existing data on the device is erased. If you remove a PC card that contains log files and want to permanently store the data, insert the card into a PC or other computer and save the data to that system before reinserting the card into a Check Point flash-based platform. The following procedure assumes you have the optional disk already installed. For instructions on installing a flash-memory PC card or a hard disk, see your platform installation guide.

After you install an optional disk and configure it to store files, you must reboot the system to make it available for use.

**To configure an optional disk**

1. Click Configuration > System Configuration > Optional Disk.

   Network Voyager displays information about the optional disks you have installed. If you do not see information about a flash memory card, verify that the card is fully inserted into the slot.

   **Note** - If a flash memory card has insufficient storage capacity, it is displayed as “Too small” and you will not be able to configure it as an optional disk. To ensure sufficient capacity, use only flash-memory cards that are supported for your platform.
Using an Optional Disk (Flash-Based Platforms Only)

2. Select the kind of files you want to store on the optional disk. The options you see depend on your platform.

   **Note** - If an optional disk is an unlabeled hard disk, Network Voyager is unable to detect whether it is a supported disk or not. Network Voyager displays a message to this effect after the list of optional disks. If your hard disk is a supported disk, click the check box that follows the message. You must check this box in addition to selecting the kind of files you want stored. For example, if you want to store log files, you must select both the logs option and the check box.

   Checking the check box causes Network Voyager to label the disk as part of configuring the disk for storing files.

3. Click Apply.

4. Wait until you see a message indicating that you should reboot the system.

   In some cases there might be a long delay before the operation completes and the message appears. You can check on the status of the operation by clicking the Optional Disk link in the navigation tree, which causes the status message to update.

5. When the status message states the operation is complete, click Reboot, Shutdown System.

6. Reboot the system.

   If you selected the kernel dump option, kernel core dumps will be automatically stored on the optional disk if the system crashes.

   **To configure the system to store IPSO log files on the optional disk**

   If you selected the logs option in step 2 in the previous procedure, perform this procedure to configure the system to store IPSO logs on the optional disk.

   1. Click Configuration > System Configuration > System Logging.
   2. Next to Logging to Optional Disk, click On.
   3. Click Apply.
   4. Click Save.

   **Note** - By default on flash-based platforms, the Check Point firewall logs to a remote server. If you install an optional disk and configure it for logging as described in “To configure an optional disk” on page 104 the firewall will automatically log to the optional disk whenever the remote server is unavailable.

   **To remove a PC card optional disk**
Using an Optional Disk (Flash-Based Platforms Only)

If the system is storing logs on the PC card, you should disable local logging before you remove the card by performing steps 1–4. Otherwise, skip to step 5.

1. Click Configuration > System Configuration > System Logging.
2. Next to Logging to Optional Disk, click Off.
3. Click Apply.
4. Click Save.
5. Click Optional Disk under Configuration > System Configuration.
6. Click Optional Disk.
7. Deactivate the card by clicking in the Unselect column.
8. Wait until you see a message indicating that you should reboot the system.
    There is a short delay before the message appears.
9. When the message appears, click the link Reboot, Shutdown System.
10. Reboot the system.
11. Remove the PC card.
Configuring System Logging

System logging is configured differently on flash-based (diskless) and disk-based systems.

Configuring Logging on Disk-Based Systems

This section describes how to configure system logging on disk-based platforms.

Disk-based systems automatically store IPSO log files on the local hard disk. You can also configure system logging to send logging messages to a remote device or to accept unfiltered system log messages from remote devices.

Warning - Do not configure two devices to send system logging messages to each other either directly or indirectly. Doing so creates a forwarding loop, which causes any system log message to be repeated indefinitely on both devices.

Logging to a Remote System

Any log messages sent to remote devices are also stored in the local log directories. You can use this feature, for example, to send log messages to a device that is configured for more secure storage or to reduce the risk of losing log information if you run out of disk space on your IPSO appliance. You might also choose to send all of the logs from multiple computers to one centralized log server, possibly one that is configured for high availability. You can select the severity levels of messages to send to remote devices.

To configure your system to send syslog messages to a remote system, use the following procedure.

To send syslog messages to a remote system

1. Click System Logging under Configuration > System Configuration in the tree view.
2. Enter the IP address of the host machine to which you want to send syslog messages.
3. Click Apply.
4. Click the Added Security Level drop down window and 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. You can choose Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug, or All. If you specify more than one severity level, all messages that are at 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.

5. Click Apply.
   The name of each severity level appears in Log at or above severity field.

6. To disable any of the severity levels, click No next to the name of the severity level you want to delete.

7. Click Apply.

8. Click Save to make your changes permanent.

**Accepting Log Messages**

You can also enable your system to accept unfiltered system log messages from remote devices. If you enable logging from remote systems, network system log packets are tagged with the host name of the sending device and logged as if the messages were generated locally. If logging from remote systems is disabled, network system log packets are ignored.

To set the system to accept unfiltered syslog messages from a remote system, use the following procedure.

**To set the system to accept syslog messages from a remote system**

1. Click System Logging under Configuration > System Configuration in the tree view.

2. Select Yes to accept syslog messages.

3. Click Apply.

4. Click Save to make your changes permanent.
Configuring Logging on Flash-Based Systems

On flash-based (diskless) systems, log files do not persist across system reboots unless they are stored on an appropriate device. You can store log files on remote log servers (primary and secondary). If you want to use remote servers, you must configure them to store the log files.

You can store log files on either or both of the following:

- Remote log servers (primary and secondary)
  If you want to use remote systems, you must configure them to store the log files.

- An optional disk.
  An optional disk can be an internal hard disk (on some systems) or an external flash memory card.

  If you decide to use an optional disk, you must install and configure it before you set up the system logging. (For information about optional disks, see “Using an Optional Disk (Flash-Based Platforms Only)” on page 104.)

**Warning** - When you select a hard disk or PC card as an optional disk, any existing data on the device is erased. If you remove an optional disk that contains log files and want to permanently store the data, insert the device into a PC or other computer and save the data to that system before reinserting the card into a Check Point flash-based appliance.

Log messages are temporarily stored in system memory and are stored to remote log servers and/or an optional disk according to a schedule that you can configure.

Log messages are stored in the following files:

- `/tmp/tmessages` (in memory)—Stores most log messages temporarily.
- `/var/log/messages`—Stores most log messages when an optional disk is installed. When an optional disk is not installed, this directory links to `/tmp/tmessages`.
- `/var/log/wtmp`—Stores messages about shell logins and logouts. When an optional disk is installed, `/var/log/wtmp` is automatically stored on the drive.

**Note** - Messages stored in `http_error_log` or `httpd_access_log` on other platforms are stored in the messages files on flash-based systems.

- `/var/log/wtmp`—Stores messages about shell logins and logouts. When an optional disk is installed, `/var/log/wtmp` is automatically stored on the drive.
Configuring Logging to Remote Log Servers

If you want to use remote systems, you must configure them to store the log files. To configure your flash-based system to send syslog messages to remote log servers, use the following procedure.

To configure a flash-based system to use a remote log server

1. Click System Logging under Configuration > System Configuration in the tree view.
2. Next to Network Logging, click On.
3. Enter the IP address of the primary remote log server. Make sure that the flash-based system has connectivity to the remote server.
4. 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.
5. Set the threshold percentage for saving log messages to the remote server. Flash-based 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.
6. 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.
7. Click Apply.
8. Click Save to make your changes permanent.
Configuring Audit Logs

Configuring Logging to an Optional Disk

If an optional disk is installed and enabled, you can configure the system to save log files on it by selecting the option Logging to Optional Disk. If you enable local logging, log messages are saved in /var/log/message and /var/log/wtmpm on the memory card. The messages are saved to the optional disk according to the settings of the Threshold % and Flush Frequency options.

You can save log files to a remote log server and an optional disk simultaneously.

If an optional disk is full, the system displays a console message to that effect and stops saving log messages to the device. Messages that have been previously saved on the optional disk are not affected. If you have configured the system to send messages to a remote log server, it continues to do so.

Note - If you use SNMP, the system sends SNMP traps when the flash memory file system is 90 percent full 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 \texttt{rm} command to delete files in /var/log/.

Configuring Audit Logs

You enable and configure the audit logs in the same way for both disk-based and flash-based systems.

To make certain log messages more useful, you can configure the system so that messages about system configuration changes are displayed in a textual format instead of the configuration database bindings format. The text format is more informative because the messages are written in “plain English” and include additional information about the configuration changes. Table 3-2 includes a few examples that show log messages in the configuration database style and in the textual format.

Table 3-2 Log Message Formats

<table>
<thead>
<tr>
<th>Configuration Database Format</th>
<th>Textual Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>process:pm:coreaction t</td>
<td>PROCESS_CONFIG: Enabled system failure notification</td>
</tr>
</tbody>
</table>
Configuring Audit Logs

Table 3-2 Log Message Formats

<table>
<thead>
<tr>
<th>Configuration Database Format</th>
<th>Textual Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsrd:instance:default:vrp:nomonitorfw t</td>
<td>VRRP_CONFIG: Disabled VRRP Monitor Firewall State</td>
</tr>
<tr>
<td>mcvr:vr:123</td>
<td>Deleted Monitored-Circuit Virtual Router with vrid 123</td>
</tr>
</tbody>
</table>

(To view system configuration log messages, select the log type LOG_NOTICE or ALL on the System Message Log page.)

If you enable the Voyager Audit Log option, 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, view the System Message Log page. For more information on viewing the system message log, see “Monitoring System Logs” on page 391.

Note - For Network Voyager configuration pages that do not include Apply and Save buttons, such as image.tcl, the log records the relevant action, such as clicking Reboot.

To set the system configuration audit log

1. Click System Logging under Configuration > System Configuration in the tree view.

2. In the System Configuration Audit Log area, select from the following:
   - Logging disabled—The system writes minimal messages to the system log that a configuration change was made, including the name of the host from which the change was made, and the name of the user who made the change.
   - Logging of transient changes—The system writes messages to the system log each time a user applies a configuration change to the running system. Transient changes are those that apply only to the currently running system. Transient changes are equivalent to clicking the Apply button only in Network Voyager.
   - Logging of transient and permanent changes—The system writes messages to the system log each time a user applies a configuration change to the running system or changes the configuration files. Permanent changes are
Configuring Audit Logs

those that 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.

3. Click Apply.

4. If you are using a disk-based system, 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 flash-based systems, you cannot save the messages to another file.

Note - The system configuration audit log setting is not saved in the configuration file. You must reset it after rebooting to enable logging again.

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” on page 507

To enable logging in textual format
1. Click System Logging under Configuration > System Configuration in the tree view.
2. Select the textual format option in the System Configuration Audit Log area.

To set logging of all Network Voyager Apply and Save actions
1. Click System Logging under Configuration > System Configuration in the tree view.
2. In the Voyager Audit Log field, select Enabled or Disabled.
3. Click Apply.
4. Click Save to make your change permanent.

The Voyager Audit Log feature does not record any operations performed using the command-line interface (CLI). To log configuration changes made using either Network Voyager and the CLI, enable the system configuration audit log.

Configure the system configuration audit log to record transient and permanent configuration changes. You can view the syslog messages to determine whether authorized users only are making configuration changes to the system.
Using a Core Dump Server with Flash-Based Systems

On flash-based platforms, application core files are stored in memory in the directory /var/tmp. When the file system is 95% filled, flash-based systems delete older core files to make room for newer ones. Similarly, flash-based platforms store IPSO kernel core dumps in the internal compact flash memory card. If necessary, an older core dump is deleted to make room for a new file.

You can configure flash-based systems to transfer both application and kernel cores to a remote server so that older cores are retained. If you do so, IPSO scans /var/tmp hourly and transfers any application core files it finds to the remote server. This schedule is not configurable. Kernel core dumps are sent to the remote server after the system recovers from the problem that caused the core dump. You can verify that the core file was successfully transferred by checking the log message file for a message similar to the following:

```plaintext
[LOG_NOTICE] xfer_crash: Transferred kernel core file to ftp_server_IP_address
```

This message is not displayed on the console.

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

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

To configure your flash-based system to transfer cores to a remote server, use the following procedure. You must also configure the remote system (FTP or TFTP server) appropriately.

**To configure a flash-based system to transfer core dumps to a remote server**

1. Click Remote Core Dump Server under Configuration > System Configuration in the tree view.
2. Enter the IP address of the remote server to which the core files will be transferred.
3. Select whether to use FTP or TFTP for the transfer protocol.

**Warning** - The TFTP option does not work with TFTP servers running on many Unix-based operating systems. Check Point recommends that you use FTP unless you are sure that your TFTP server accepts writes to files that do not already exist on the server and accepts transfers of files the size of core files.
Using a Core Dump Server with Flash-Based Systems

If you choose FTP, make sure that your server accepts anonymous FTP logins. You cannot use non-anonymous FTP logins to transfer core files.

4. Indicate where the cores should be stored on the remote server by entering the appropriate path and directory.

5. Click Apply.

6. Click Save to make your changes permanent.

**To manually transfer kernel core dumps**

To manually transfer a kernel core dump to a remote FTP server, enter the following command at the IPSO shell prompt:

```
savecore -r ftp://username:password@ftp_server_IP_address/directory/
```

Enter this command twice to transfer two kernel core dumps.
Changing the Host Name

Changing the Host Name

You set the host name during initial configuration. To identify the host name (system name) of your security platform, click Hostname under Configuration > System Configuration in the tree view. The host name is also displayed in each page header.

Note - Host address assignments must match an IP address.

You can change the host name at any time using the following procedure.

To change the host name

1. Click Hostname under Configuration > System Configuration in the tree view.
2. Enter the new host name.
3. Click Apply.
4. Click Save to make your changes permanent.
Managing Configuration Sets

You can save the system state that is currently running to a new configuration database file. You can also create a new configuration database file using factory defaults that is known to work correctly.

To save the active configuration as a new configuration set, use the following procedure. The active configuration might be different from that of the current configuration file if you have applied changes but not saved them.

**To save the current configuration into a new configuration database file**

1. Click Configuration Sets under Configuration > System Configuration in the tree view.
2. Enter the name of the new configuration file in the Save current state to new configuration database field.
3. 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. The new file is saved in `/config/db/`.

To create a new configuration database file that contains only the factory default configuration settings, use the following procedure.

**To create a factory default configuration file**

1. Click Configuration Sets under Configuration > System Configuration in the tree view.
2. Enter a name for the new file in the Create a New Factory Default Configuration field.
3. 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.

**Warning** - If you load this configuration set, all system configurations are deleted from the system. You cannot configure the system through Network Voyager until you configure an IP address through the system console.

To load a different configuration file, use the following procedure.

**To switch a currently active database**
Managing Configuration Sets

1. Click Configuration Sets under Configuration > System Configuration in the tree view.
2. Select from the available configuration database files in the list.
3. Click Apply.
4. To make your changes permanent, click Save.

To delete unwanted configuration database files
1. Click Configuration Sets under Configuration > System Configuration in the tree view.
2. Click the Delete Configuration Databases link.
3. Select Delete for each database file you want to delete.
4. Click Apply.
5. Click Up to return to the Configuration Database Management page.
Scheduling Jobs

You can use Network Voyager to access the crontab file and schedule regular jobs. The cron daemon executes jobs at dates and times you specify through the following procedure.

To schedule jobs
1. Click Job Scheduler under Configuration > System Configuration in the tree view.
2. Enter a name for the job you want the cron daemon to execute in the Job Name text box. Use alphanumeric characters only, and do not include spaces.
3. 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.
4. Select the Timezone under which you want to schedule the job, either Local or Universal, from the drop-down list.
5. Select the frequency (Daily, Weekly, or Monthly) with which you want the job to execute from the Repeat drop-down list.
6. Click Apply.
7. Under Execution Detail, specify the time the job will execute.
8. To receive mail regarding your scheduled jobs, enter your email address in the Email Address text box.

Note - Click Mail Relay to verify that a mail server is configured.

9. Click Apply.
   If your configuration is successful, the job appears in the Scheduled Jobs table. To make your changes permanent, click Save.
10. Click Save to make your changes permanent.

To delete scheduled jobs
1. Click Job Scheduler under Configuration > System Configuration in the tree view.
2. In the Scheduled Jobs table, select Delete next to the name of each job you want to delete.
3. Click Apply.
Scheduling Jobs

4. Click Save to make your changes permanent.
Backing Up and Restoring Files

You can perform manual backups of files or you can configure your system to run regularly scheduled backups, as described in “Creating Backup Files” on page 121 below.

You can also use Network Voyager to manage your backup files, including the following tasks:

- Restore from locally stored files. See “To restore files” on page 125.
- Transfer backup files to, and restore them from, a remote server. See “Transferring Backup Files” on page 123.
- Delete backup files that are stored on the local system. See “To delete local backup files” on page 122.

You can also view a list of backup files that are stored locally by clicking IPSO Configuration > Configuration Summary.

Creating Backup Files

You can create a backup file manually at any time (see “To create a backup file manually” on page 121 below), or configure the system to run scheduled backups automatically (see “To configure scheduled backups” on page 122).

By default, the backup file is saved in /var/backup and contains everything in the following directories:

- configuration (/config)
- cron (/var/cron)
- etc (/var/etc)

Note - Export versions of Check Point IPSO do not include IPSec files.

You can also choose to include the following in your backup file:

- User home directories (stored in /var/emhome)
- Log files (stored in /var/logs)

To create a backup file manually
Creating Backup Files

1. Click Backup and Restore under Configuration > System Configuration in the tree view.
2. Enter a file name for your backup file in the Backup File Name text box. If you do not enter a name, the backup file is not created.
3. Select any additional directories to include in the backup file:
   1. To include the home directories of all active users in the backup file, check the Backup Home Directories check box.
   2. To include log files in the backup file, check the Backup Log Files check box.
   3. To include application package files in the backup file, check the check box for each package to include in the backup file.
      Only installed packages that support backup are listed.
4. Click Apply.
5. Click Save to make your changes permanent.

To delete local backup files
1. Click Backup and Restore under Configuration > System Configuration in the tree view.
2. In the Delete Backup Files section, check the Delete check box next to the name of each backup file to delete.
3. Click Submit.
   The entry for the backup file disappears.

To configure scheduled backups
1. Click Backup and Restore under Configuration > System Configuration in the tree view.
2. In the Scheduled Backup field, click the Frequency drop-down list and select Daily, Weekly, or Monthly to configure how often to perform a regular backup.
   Additional text boxes appear in the Configure Scheduled Backup section.
3. Select times and dates for the scheduled backup from the drop-down lists.
   • For a daily backup, select the hour and minute.
   • For a weekly backup, select the day of the week, hour, and minute.
   • For a monthly backup, select the date of the month, hour, and minute.
Transferring Backup Files

If you select a date for monthly backups that does not occur every month of the year, such as 31, those months are omitted from the backup schedule.

4. Enter a name for your backup file in the Backup File Name text box.
   If you do not enter a name, the backup file is not created.
5. Select any additional directories to include in the backup file:
   1. To include the home directories of all active users in the backup file, check the Backup Home Directories check box.
   2. To include your log files in the backup file, check the Backup Log Files check box.
   3. To include package files in your backup file, select the check box next to the name of each package to include in the backup file.
      Only installed packages that support backup are listed.
6. Click Apply.
7. Click Save to make your changes permanent.

To cancel a regularly scheduled backup
1. Click Backup and Restore under Configuration > System Configuration in the tree view.
2. In the Frequency drop-down list under Scheduled Backup, select None.
3. Click Submit.

Transferring Backup Files

You can transfer backup files to a remote server or download them to the workstation from which you are running Network Voyager. When you transfer backup files to a remote server, they are removed from the system.

Configuring Automatic Transfers

To configure the system to automatically transfer backup files to a remote server, use the following procedure.

To configure automatic transfers of archive files to a remote server
1. Click Backup and Restore under Configuration > System Configuration in the tree view.
Transferring Backup Files

2. Under Automatic Transfer of Archive File, select a file transfer protocol, either TFTP or FTP.
   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.

   **Warning** - 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. Check Point recommends that you use FTP unless you are sure that your TFTP server accepts writes to files that do not already exist on the server.

3. Enter the IP address of the remote server.
4. If you chose FTP as the transfer protocol, indicate where the files should be stored on the remote server by entering the appropriate path and directory.
5. Click Apply.
6. Click Save to make your changes permanent.

**Transferring Backup Files Manually**

To transfer a archive file containing backup files manually to an FTP server using the following procedure.

**To manually transfer archive files to a remote server**

1. Click Backup and Restore under Configuration > System Configuration in the tree view.
2. Under the Manual Transfer of Archive Files section, enter the following
   • IP address of the FTP server.
   • Directory in which to save the backup file.
   • Enter the name of the user account for connecting to the FTP server.
   • Enter the name of the password to use when connecting to the FTP server.
     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.

3. Select the file you want to transfer from either the Manual Backup File or Scheduled Backup File drop-down lists.
Restoring Files from Locally Stored Backup Files

4. Click Save.

Restoring Files from Locally Stored Backup Files

To restore files to the system, you must first create backup files as described in “Creating Backup Files” on page 121.

You can restore either from files stored locally or from files stored on a remote machine.

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

To restore files

1. Verify that the following prerequisites are met:
   - Enough disk space is available on your platform.

   Warning - If you try to restore files and you do not have enough disk space, you risk damaging the operating system.

   - Your system is running the same version of the operating system and the same packages as those of the backup files from which you restore files.

   Warning - Using incompatible versions can result in problems with configuration and data files, which might, or might not, be immediately detectable.

2. Click Backup and Restore under Configuration > System Configuration in the tree view.

3. If the file you are restoring from is stored on the local appliance, go to the Restore from Local section and perform the following steps. Otherwise, proceed to step 4.

   1. Select the name of the backup file from either the Manual Backup File or the Scheduled Backup File drop-down lists, depending on the type of file 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 lists contain lists of all the files in these directories, but some of the files might not be backup files.

2. Proceed to step 5.

4. If the file you want to restore is stored on a remote device, go to the Restore From Remote section of the page. You can use FTP or HTTP to transfer the backup file to the IPSO platform.

To use FTP:

1. Click the FTP button.
2. Enter the following information:
   - IP address of the FTP server.
   - Directory in which to save the backup file.
   - Enter the name of the user account for connecting to the FTP server.
   - Enter the name of the password to use when connecting to the FTP server.
3. Proceed to step 5
4. A list of available files in the directory you specify appears. Select the backup files you want to restore.

To use HTTP:

1. Click the HTTP button.
2. Click the Browse button.
3. Navigate to the location of the backup file.
4. Select the backup file.
5. Proceed to step 5
6. Click Apply.
7. Do not click Save. Ignore any messages indicating that unsaved changes will be lost.
8. Click Reboot and wait for the system to reboot.

Note - You must reboot your system after restoring from backup files.
Managing Check Point IPSO Images

An IPSO image is the operating system kernel and binary files that run the system. You can store multiple versions of the IPSO image on your appliance.

For information about installing images in a cluster environment, see “Upgrading Check Point IPSO Images for a Cluster” on page 130.

For information about downgrading to a previous version of IPSO, see “Downgrading Check Point IPSO Images” on page 131.

Changing Current Image

When the system boots, it reads the kernel file in the directory indicated by the current pointer. To identify the current image, you can either look on the Home page or choose Configuration > System Configuration > Images, click Manage Images and look in the State column. To change the current image, use the following procedure.

To select a new current image

1. Click Manage Images under Configuration > System Configuration > Images in the tree view.
2. Select the radio button for the image you want to select as the new current image.
3. Click Reboot to activate the new image.
   The system will take a few minutes to reboot.

Deleting Images

When there are too many images on your system, the directory gets full and precludes you from logging in. To prevent this problem, delete old images before you install a new image so that you do not have more than three or so images on your system.

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

To delete an Check Point IPSO image
Installing New Images

1. Click Manage Images under Configuration > System Configuration > Images in the tree view.
2. Click Delete IPSO Images.
3. Click the delete button next to the image you want to delete.
4. Click Apply.
5. To make your changes permanent, click Save.

Installing New Images

When you upgrade the image, the system configuration and installed packages are retained.

To upgrade the image, you must first complete an initial installation. For information about how to perform an initial installation and configuration of an image, see the latest version of the IPSO Getting Started Guide and Release Notes at http://supportcontent.checkpoint.com/documentation_download?ID=10292

Upgrade the IPSO image on your platform using Network Voyager using the following procedure.

1. Click Upgrade Images under Configuration > System Configuration > Images in the tree view.
2. Decide whether you want to transfer the image to the Check Point platform by using FTP, entering a complete URL, or navigating to the location where the image is stored.

To use a URL or FTP based transfer:

1. URL or IP address of the FTP, HTTP, or file server on which the Check Point IPSO image is installed.

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, use the standard URL format. For example:

ftp://test.acme.com/tmp/ipso.tgz
Testing a New Image

2. (Optional) If the HTTP site on which the Check Point IPSO image is stored requires authentication, enter the HTTP realm to which authentication is needed.

3. (Optional) If the server on which the Check Point IPSO image is stored requires authentication, enter the user name and password.

To navigate directly to the location where the image is stored:

1. Click Browse.
2. Navigate to the appropriate location.
3. Select the image file.

3. Specify whether to deactivate installed packages (such as VPN-1/FireWall-1 packages) after the system is rebooted with the new image.

4. Click Apply.
   A message appears that tells you that the upgrade process could take a long time if the network is slow.

5. Select Continue.

6. Click Apply again.
   The system downloads the specified image file.

7. To view the status of the download and installation process, click Check Status of Last New Image Installation Operation.

8. The following message at the bottom of the list of messages indicates that the download and installation process is complete:
   
   To install/upgrade your packages run /etc/newpkg after REBOOT

9. If you made configuration changes, click Save.

10. You can either set your new image to be the current image for your platform (see “To select a new current image” on page 127) or test the new image before you set it as the current image (see “To test an image before activating it” on page 130).

Testing a New Image

You can test an IPSO image before you permanently activate it for your platform by performing a test boot. If you perform a test boot of an image, you can choose whether to commit the image used for the test boot or revert to the previous image. If you do not select either option, the system automatically reboots in five minutes using the previous image.
Upgrading Check Point IPSO Images for a Cluster

To test an image before activating it

1. Click Upgrade Images under Configuration > System Configuration > Images in the tree view.

2. Click Manage IPSO images (including REBOOT and Next Boot Image Selection).

3. Select the radio button associated with the image you want to test.

4. Select one of the following options for rebooting the system:
   - To reboot with the 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.

5. 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 performed a test boot and want the system to continue using the new image, you have five minutes after the system restarts to select Commit Testboot. If you do not, the system automatically reboots the previous image in five minutes.

Upgrading Check Point IPSO Images for a Cluster

You can use Cluster Voyager to upgrade the Check Point 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.

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 Check Point 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.

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
- admin password (accounts for any users that have been added are not carried over)
- SNMP user information
- host name
- 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:
Downgrading Check Point IPSO Images

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.
Configuring Monitor Reports

For monitoring purposes, you can configure the system to generate reports on the following types of events:

- Rate Shaping Bandwidth
- Interface Throughput
- Interface Link State
- CPU Utilization
- Memory Utilization

For more information about these reports, see “Generating Monitor Reports” on page 388.

You can configure the options for monitor reports according to your networking and reporting requirements. Table 3-3 shows the parameters that you can configure for monitor reports.

Table 3-3 Monitor Report Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Interval</td>
<td>Specifies, in seconds, how often the data is collected.</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 60 - 2100000.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 60</td>
</tr>
</tbody>
</table>
Configuring Monitor Reports

Table 3-3 Monitor Report Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On/Off</td>
<td>You can enable or disable each data collection event. By default, all events are enabled.</td>
</tr>
<tr>
<td></td>
<td>For the rate-shaping bandwidth report, you can enable packets delayed and bytes delayed separately. Likewise, for the interface throughput report, you can enable one or more of packet throughput, byte throughput, broadcast packets, and multicast packets.</td>
</tr>
<tr>
<td>Data Available for Hours</td>
<td>Specifies how many hours worth of collected data are stored on the system. Data that is older than the specified number of hours is deleted.</td>
</tr>
<tr>
<td></td>
<td>This option controls how much data is available when you use the Detailed Search option on any of the report pages. It does not affect how much data is available when you use the Hourly, Weekly, Daily, or Monthly options on these pages.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 24 - 167 hours</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 24 hours</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> On flash-based systems, Check Point recommends that you set this option to 24 hours (the default value) to avoid exhausting the available storage space.</td>
</tr>
</tbody>
</table>

To configure these parameters, click Monitor Reports under Configuration > System Configuration in the tree view.
Managing Packages

Packages are software bundles that are ready to install on an IPSO system. Each package is installed as a subdirectory of the /opt directory.

You can use Network Voyager to easily install, upgrade, and remove packages.

Installing and Enabling Packages

You can use Network Voyager to enable packages (make them active), to disable and delete packages, and to delete files that you no longer need to maintain on your local system.

To install a package

1. Click Install Packages under Configuration > System Configuration > Packages in the tree view.
2. Click the button for an FTP or HTTP transfer.
3. If you use FTP, enter the following information in the appropriate text boxes. If you use HTTP, proceed to step 4
   • Host name or IP address of the FTP site where the packages are located.
   • FTP directory where the packages reside at the FTP site.
   • (Optional) User account and password to use when connecting to the FTP site. If you leave these fields empty, the anonymous account is used.
4. To use HTTP:
   1. Click the Browse button.
   2. Navigate to the location of the package file.
   3. Select the package file.
5. Click Apply.

A list of files ending with extensions .tgz, .Z, and .gz in the specified FTP directory appears in the Site Listing field.
6. Select a package to download from the Site Listing field.
7. Click Apply.

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.
Installing and Enabling Packages

The selected package is downloaded to the local Check Point IPSO system. After the download is complete, the package appears in the Unpack New Packages field.

8. Select the package in the Unpack New Packages field, then click Apply.

The package is unpacked into the local file system.

9. Click the Click Here to Install/Upgrade [File Name] link.

10. (Optional) Click Yes next to Display all packages, then click Apply to display all of your installed packages.

11. (Optional) Click Yes next to Install, then click Apply to perform a first-time installation.

12. (Optional) Click Yes next to Upgrade.

13. (Optional) Click the button of the package from which you want to upgrade under Choose one of the following packages to upgrade from.

14. Click Apply.

15. Click Save to make your changes permanent.

To enable or disable a package

1. Click Manage Packages under Configuration > System Configuration > Packages in the tree view.

2. Click On or Off next to the package you want to enable or disable.

3. Click Apply.

4. Click Save.

To delete a package

1. Disable the package you intend to delete.

2. Click Manage Packages under Configuration > System Configuration > Packages in the tree view.

3. Click the Delete Packages link.

4. Click Delete next to the package you want to delete.

5. Click Apply.

6. 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.

Controlling SecureXL

If the Check Point Security Gateway is installed on the system, you enable or disable some SecureXL features in IPSO. These features are listed in the SecureXL TCP box, which appears on the Voyager Advanced System Tuning page.

Sequence Validation

For enhanced security, IPSO supports the SecureXL sequence validation (TCP state detection version 2) functionality. This feature allows the firewall to stop exploits that make use of out-of-sequence TCP packets.

To use Sequence Validation, you should enable it in both SmartDashboard and in IPSO. (This is true for standalone systems and high-availability configurations.) This feature is disabled by default.

If you want to enable sequence validation, follow these steps:

1. On the Advanced System Tuning page in Network Voyager, click the button to enable sequence validation.
2. Enable sequence validation in SmartDashboard.
3. Push the new policy to the IPSO platform.

Delayed Notification and Auto-Expiry

Delayed Notification and Auto-Expiry improve performance by reducing the amount of required communication between IPSO and the firewall and reducing the amount of synchronization between the members of IP clusters or VRRP groups, thereby reducing overhead processing.

On stand-alone systems, delayed notification is enabled by default and requires no configuration in SmartDashboard. Delayed notification is enabled by default in high-availability configurations (IP clusters or VRRP groups), but you must also enable delayed synchronization (per service) in SmartDashboard using the Advanced TCP Service Properties dialog box for the appropriate service—for example, HTTP.
Delayed synchronization is automatically disabled for any connections matching a rule that uses any of the following Check Point features:

- Logging
- Accounting
- Worm catcher

In high-availability configurations, you can configure delayed synchronization so that connections that expire before a time you set are not synchronized. For example, if you configure HTTP traffic to be synchronized after 10 seconds, HTTP connections that expire before this time are not synchronized to the other systems. (Should a failover occur, unsynchronized connections do not survive.)

Delayed notification and synchronization are particularly beneficial when a system processes many short-lived connections.

Auto-Expiry is enabled by default. This option improves performance by allowing IPSO to terminate certain connections. IPSO informs the firewall that it has terminated these connections.

**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 4
High Availability Solutions

This chapter describes several solutions that you can use to create a highly available and redundant configuration to ensure that your network traffic continues to flow in the event that one of your firewall platforms fails.

Check Point provides the following high availability solutions:

- IP clustering
- External load balancer support
- HA Voyager
- VRRP

For information about IP clustering, see the *Clustering Configuration Guide for Check Point IPSO 6.2*

The remaining high availability solutions are described in this chapter.

In This Chapter

- Using an External Load Balancer  page 141
- HA Voyager  page 143
- VRRP Overview  page 154
- How VRRP Works  page 155
- Configuring Network Switches  page 158
- Before You Configure VRRP  page 159
- Configuring VRRP  page 160
Configuring the Check Point Security Gateway for VRRP page 177
Monitoring VRRP page 181
Troubleshooting VRRP page 183
Using an External Load Balancer

You can use an external load balancer to balance traffic to multiple IPSO firewalls without using IP clustering or VRRP. By configuring the firewalls to synchronize traffic with each other you can provide high availability as well. Using an external load balancer also has the advantage of not requiring you to use virtual IP addresses on the IPSO firewalls. You enable this feature on the Configuration -> High Availability -> External Load Balancer Support page.

If you use an external load balancer, be aware that this product must be capable of detecting a firewall failure and adjusting its balancing decisions. You should also be aware that some firewall functionality is not supported with this high availability approach—see “Unsupported Firewall Features” on page 142 for more information.

Configuring the Firewall for a Load Balancer

Here are some details about how to use Check Point’s SmartDashboard to configure the firewall to work with a load balancer:

- Create a gateway cluster.
- Do not use ClusterXL.
- Use the following settings on the 3rd Party Configuration tab:
  - Enable High Availability.
  - Use Check Point VRRP or Other OPSEC as the 3rd Party Solution.
  - Enable state synchronization.
  - Leave the remaining options disabled.
- Use the Edit Topology dialog box to perform the following:
  - Define the internal and external interfaces as private.
  - Define a synchronization interface that is separate from the internal and external interfaces.

Note - Be sure to connect the synchronization interfaces.

- Do not define any other interfaces.
Unsupported Firewall Features

The following firewall features are not supported or are partially supported if you use an external load balancer:

- ConnectControl is not supported.
- NAT is partially supported (asymmetric connections are not supported).
- VPNs are partially supported (asymmetric connections are not supported).
- Using a Virtual IP address on a cluster interface is not supported.
HA Voyager

IPSO 6.1 introduces a new approach that you can use to create and manage VRRP configurations. The main VRRP configuration page now includes a link for creating an HA configuration group. Using this option allows you to configure and manage all the members in a VRRP group in a centralized way by using HA Voyager on one system. (When you use HA Voyager to configure VRRP, you create a simplified monitored-circuit configuration.)

When you create an HA configuration group, Voyager displays a new tab (labeled HA Voyager) in the navigation tree. Clicking this tab displays many of the same links that appear under the System tab in the navigation tree. When you access a configuration page by using the HA Voyager navigation tree, any changes you make are implemented on all the members of the group. This simplifies your work and helps you keep the configuration of the group members synchronized.

To easily configure and manage a VRRP group using HA Voyager, follow this basic approach:

1. If necessary, configure the firewall to allow you to use HA Voyager. See “Configuring the Firewall for HA Voyager” for more information.

2. Create an HA configuration on one of your Check Point platforms.

3. Use HA Voyager to add members to the HA configuration.

4. Use HA Voyager to configure simplified monitored-circuit VRRP on all the members of the HA configuration group.

5. When making configuration changes to group members, use HA Voyager whenever possible so that the changes are implemented on all the members.

Note - When you add a member to the group, HA Voyager is enabled on the member.

Note - You can use HA Voyager on any member of the group. Regardless of which member you log into, your changes will be implemented on all the other members when you click Apply and saved on all the members when you click Save.

“HA Voyager Configuration Example” on page 149 presents a step-by-step example of how to use HA Voyager to set up an HA configuration group and configure VRRP for the group.
Configuring the Firewall for HA Voyager

Before you can use HA Voyager on a platform on which a Check Point firewall is running, you must do the following:

1. Using Check Point’s SmartDashboard, create a rule with the IPSO_Clustering_Mgmt_Protocol service enabled.
2. Push the policy with this rule to the platform on which you will enable HA Voyager.

If you do not configure the firewall in this way, it prevents you from using HA Voyager.

Creating an HA Configuration

To create an HA configuration, perform these steps:

1. In the navigation tree, click System > Configuration > High Availability > VRRP.
2. On the VRRP Configuration page, click the HA VRRP Configuration link.
3. Fill out the following fields:
   - HA Group Secret: Enter a secret that will be used to encrypt messages between the members of the VRRP group.
   - Select Local Address: Select an IP address of the interface that will be used for HA configuration messages.
     Check Point recommends that you use an IP address of an internal interface.

   **Note** - This address does not have to have an associated VRRP backup (virtual) address. That is, this does not have to be an address of an interface that will forward production traffic. This address will be used only for HA configuration messages between group members.

4. Click Apply.

Voyager displays a the HA Voyager tab in the navigation tree. Click this tab to access links for adding HA group members and configuring all the members in the group simultaneously.
Adding and Configuring HA Members

To add members to the HA configuration group, click HA Voyager > High Availability > Members in the navigation tree. IPSO displays the HA Configuration page, which includes fields for entering information about new members.

You can add a new member by entering the required information on this page and clicking Apply. If you do so, the settings for all the features listed on the HA Configuration Cloning page are copied to the new member. To verify or configure which settings will be cloned or disable cloning, scroll to the bottom of the HA Configuration page and click HA Configuration Cloning before you enter the required information for the new member. See “Using Configuration Cloning” for more information about this option.

Using Configuration Cloning

You might want to configure certain settings of your group members identically. For example, you probably want each member to have the same static routes and settings for DNS, time, and Voyager web access. HA Voyager makes it easy for you to configure the members in this way by providing the Configuration Cloning option.

To use cloning, follow these steps:

1. Create an HA configuration on platform A.
2. Using HA Voyager on platform A, scroll to the bottom of the HA Configuration page and click HA Configuration Cloning.
   
   Voyager displays the HA Configuration Cloning page, which includes a list of features whose configuration can be cloned.
3. Verify that cloning is enabled (this is the default setting).
4. If desired, deselect those features that you do not want to clone. Otherwise, leave all the features selected (the default setting).
5. Click Apply.

When you add members to the HA configuration group, the appropriate configuration settings are implemented (cloned) on the new members.
Adding and Configuring HA Members

If a group member reboots when cloning is enabled, it clones settings from the first group member it connects to after the reboot. Because all members should have the same settings for cloned features, it should not matter which member the rebooted member clones its settings from.

**Note** - If a group member fails while you are using HA Voyager and you attempt to display a new page immediately afterward, there is a short delay before the page is displayed.

**Adding an HA Member**

After you verify that cloning is configured appropriately, you are ready to add new members to the HA configuration group.

1. Click HA Voyager > High Availability > Members in the navigation tree.
2. Fill out the following fields:
   - **Member Address**: Enter an IP address that HA Voyager will use on this system.
     Remember that this address is used for HA configuration messages between members. For simplicity, Check Point recommends that this address be in the same LAN as the address you entered for the first member and that you use an internal interface.
   - **Admin Password**: Enter the admin password for the system you are adding to the group.
   - **HA Secret**: Enter the secret that you entered for the first member.
3. Click Add New Member.
   The member is added to the group and HA Voyager is enabled on the member.
4. Click Save to save your changes.

**Configuring an HA Member**

Remember that any changes you make using HA Voyager are implemented on all the HA configuration group members. Once you create an HA configuration group, you should use HA Voyager as much as possible to make any configuration changes so that the appropriate settings remain identical on all the members.
Configuring VRRP with HA Voyager

If you make configuration changes on an HA group member using “normal” Voyager (use the System tab in the navigation tree), those changes are implemented only on the member you are logged into. If you do this for a feature that is selected for cloning, the setting you make using normal Voyager will be changed if the member reboots. Here is an example of this scenario.

1. You create an HA configuration group on platform A with configuration cloning enabled and all the cloneable features selected. (This is the default setting.)
2. You use HA Voyager to set the session timeout to 120 minutes on platform A.
3. You add member B to the HA configuration group.
   The session timeout is set to 120 minutes on platform B because Voyager Web Access settings are cloneable by default.
4. You use normal Voyager to change the session timeout is set to 60 minutes on platform B.
   Platform A is unaffected by this change because you used normal Voyager on platform B.
5. You reboot platform B.
   After the reboot, the session timeout is set to 120 minutes on platform B because it cloned the setting from platform A after it restarted.

**Configuring VRRP with HA Voyager**

You can use HA Voyager to easily configure VRRP on all the members of an HA configuration group. This is the simplest way to configure VRRP, and it also makes it easy for you to ensure that the global VRRP options are set identically on all the members.

When you use HA Voyager to configure VRRP, you create a simplified monitored-circuit configuration, and all the requirements of simplified monitored-circuit apply. For example, before you create a VRRP backup (virtual) address you must make sure that each member has an address with the same network address as the backup address. For example, the following is a valid combination:

- Member A address: 10.1.1.1
- Member B address: 10.1.1.2
- VRRP backup address: 10.1.1.3
Rebooting an HA Configuration Group

For complete information on configuring simplified monitored-circuit VRRP, see “Understanding Monitored-Circuit VRRP” on page 163 and “Configuring Monitored-Circuit VRRP using the Simplified Method” on page 170.

To configure VRRP using HA Voyager, perform the following steps:

1. On any member of the HA configuration group, click HA Voyager > High Availability > VRRP in the navigation tree.
   Voyager displays the VRRP (HA) Configuration page.
2. Configure the global settings appropriately.
3. Enter a valid identifier for the VRRP virtual router you will create.
4. Select which HA configuration members will participate in VRRP and assign each one a unique VRRP priority value.
5. Click Apply.
   Voyager displays a link for the virtual router identifier (VRID) and lists the IP addresses of the participating members.
6. Click the VRID link.
7. Configure VRRP as you normally would when using the simplified monitored-circuit method.
8. Click Apply.
9. Click Save.

Rebooting an HA Configuration Group

You can reboot the members of an HA configuration group in a staggered manner so that only one member is out of service at a time. For example, if you reboot a two-member group, the member you are logged into waits until the other member has successfully rebooted before rebooting itself. If the other member does not successfully reboot, the member you are logged into does not reboot itself. This type of reboot is a traffic safe reboot. To perform one, follow these steps:

1. Click HA Voyager > Configuration > System Configuration > Reboot or Shut Down System.
2. Click the Traffic Safe Reboot link.
3. Check the Continue checkbox.
4. Click Apply.
You can also reboot all the HA members simultaneously. To do so, follow these steps:

1. Click HA Voyager > Configuration > System Configuration > Reboot or Shut Down System.
2. Click Reboot.

**HA Voyager Configuration Example**

This section presents an example of creating and configuring an HA configuration group and configuring VRRP for the group. Figure 4-1 shows the configuration that you would create by following the example procedures.
To create an HA configuration group
1. Log into firewall A.
2. In the navigation tree, click System > Configuration > High Availability > VRRP.
3. On the VRRP Configuration page, click the HA VRRP Configuration link.
4. Enter a secret that will be used to encrypt messages between the members of the group.
5. Select an IP address to use for HA configuration messages between members.
HA Voyager Configuration Example

In this example you would select 172.16.0.1.

6. Click Apply.

Voyager displays a message indicating that the apply was successful and the HA Voyager tab appears in the navigation tree.

To configure cloning

1. In the HA Voyager tab of the navigation tree, click Configuration > High Availability > Members.
2. Click the HA Configuration Cloning link.
3. In this example, assume that you want all the cloneable features to be configured identically on both members of the group except for job scheduling because you do not want the scheduled jobs to execute at the same time on both members.
   - Uncheck Job Scheduler, but leave everything else on the page checked.
4. Click Apply.
5. Click Save.

Before you add a member to the group

Before you add firewall B to the HA configuration group, make sure that the settings for all the selected cloneable features are as you want them on firewall A. Remember that firewall B will get the settings for all the cloneable features except for job scheduling from firewall A.

Note - Use HA Voyager to confirm or configure any settings for cloneable features on firewall A.

To add firewall B to the group

1. In the HA Voyager tab of the navigation tree, click Configuration > High Availability > Members.
   - HA Voyager displays the HA Configuration page.
2. In the Member Address field, enter an IP address to use for HA configuration messages between members.
   - In this example you would enter 172.16.0.2.
3. Enter the administrative password for firewall B in the Admin Password field.
4. Enter the HA secret that you used when you created the group.
HA Voyager Configuration Example

5. Click Add New Member.
   Firewall B appears in the list of group members.

6. Click Apply.

7. Click Save.

To create virtual routers for the group

1. In the HA Voyager tab of the navigation tree, click Configuration > High Availability > VRRP.
   HA Voyager displays the VRRP (HA) Configuration page.

2. Under Create New Monitored-Circuit Virtual Router, enter a virtual router ID (VRID) for the virtual router on the internal side.
   In this example, you would enter 100.

3. Check the boxes after both group members so that they both run VRRP.

4. Assign each member a unique VRRP priority value.
   In this example, you might assign firewall A a priority of 100 and firewall B a priority of 90.

5. Click Apply.
   Voyager displays a link for VRID 100.

6. Under Create New Monitored-Circuit Virtual Router, enter a VRID for the virtual router on the external side.
   In this example, you would enter 200.

7. Check the boxes after both group members so that they both run VRRP.

8. Assign each member a unique VRRP priority value.
   In this example, you might assign firewall A a priority of 100 and firewall B a priority of 90.

9. Click Apply.
   Voyager displays a link for VRID 200.

10. Configure the VRRP Global Settings.
    See “Choosing Global Settings” on page 161 for more information.

11. Click Apply.

12. Click Save.
To configure the virtual routers

You can now configure the virtual routers for the HA configuration group using the simplified method of monitored-circuit VRRP.

1. On the VRRP (HA) Configuration page, click the link for VRID 100 in the table of VRIDs.
   
   HA Voyager displays the configuration page for virtual router 100.

2. Under Backup Addresses, enter 10.0.0.99.

3. Configure the remaining settings for virtual router 100 as you normally would.
   
   See “Selecting Node Parameters” on page 164 for information about how to configure the remaining settings.

4. Click Apply.

5. Click Save.

6. In the HA Voyager tab of the navigation tree, click Configuration > High Availability > VRRP.
   
   HA Voyager displays the VRRP (HA) Configuration page.

7. Click the link for VRID 200 in the table of VRIDs.
   
   HA Voyager displays the configuration page for virtual router 200.


9. Configure the remaining settings for virtual router 200 as you normally would.

10. Click Apply.

11. Click Save.

12. If you want to verify that VRRP is active and configured correctly, click the VRRP Monitor link.
VRRP Overview

VRRP Overview

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 Check Point implementation of VRRP includes all of the features described in RFC 3768, plus the additional feature of monitored circuit, described below.

Check Point supports VRRP for IPv6. For more information about the Check Point implementation and how to configure VRRP for IPv6 interfaces, see “Configuring VRRP for IPv6” on page 227.

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.

Check Point offers several approaches to using VRRP:

- Monitored-Circuit VRRP simplified method: Check Point recommends that you use this simplified version of monitored-circuit VRRP, which is a Check Point enhancement to VRRP.

- 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.

- VRRPv2: Use this method only if you do not have an extra IP address to use for monitored-circuit VRRP.
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.

Check Point 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 4-2 shows a simple VRRP configuration with a master (Platform A) and one backup (Platform B).

Figure 4-2 Simple VRRP Configuration
How VRRP Works

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 4-3.

**Figure 4-3**  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 4-4. This is known as an active-active configuration.
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.
Configuring Network Switches

Use the information in this section as a guide when connecting your Check Point platforms to network switches.

Use Port Fast with Spanning Tree Protocol

If you use the spanning tree protocol on Cisco switches in a network connected to Check Point systems running VRRP, also enable the Port Fast feature, which causes interfaces to be set to the spanning-tree forwarding state without waiting for the standard forward-time delay. If you use switches from another vendor, use the equivalent feature provided by that vendor.

Using the spanning tree protocol without Port Fast or a similar feature can prevent VRRP failovers from occurring properly.

Do Not Cascade Switches

Do not connect interfaces participating in the same VRRP virtual router to separate cascaded switches. For example, avoid the following configuration:

- Master node: Interface of virtual router 1 connected to switch A.
- Backup node: Interface of virtual router 1 connected to switch B.
- Switch A and switch B connected by an uplink connection.

Using this configuration can prevent VRRP failovers from occurring properly.
Before You Configure VRRP

Complete the following steps on your Check Point platforms before you configure VRRP:

1. 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.

2. 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 VRRP

Configuring VRRP

When you begin to configure VRRP, you must decide which VRRP method to use and how to configure the global settings that apply regardless of which method you choose.
Choosing Global Settings

The global settings for VRRP are described in Table 4-1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Connections to VRRP IPs</td>
<td>The VRRP protocol specifies that IP packets destined to an adopted VRRP IP address should not be accepted or responded to. You can use this option to override this behavior and allow the system to accept and respond to IP packets destined to an adopted VRRP IP address. You can use this option to enhance interaction with network management tools, and you must enable it when deploying a highly available application whose service is tied to a VRRP IP address. Note that VRRP IP addresses accept connections regardless of how this option is configured if the following Check Point firewall option is enabled: Cluster Properties &gt; 3rd Party Configurations &gt; Forward Cluster's incoming traffic to Cluster Member's IP address. If you disable the Check Point firewall option, then the Voyager option determines whether VRRP IP addresses accept connections. <strong>Options:</strong> Disabled / Enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Options:</strong> Disabled / Enabled.</td>
</tr>
<tr>
<td></td>
<td>• Disabled specifies compliance with the VRRP protocol specification not to accept or respond to IP packets destined to an adopted VRRP IP address.</td>
</tr>
</tbody>
</table>
Choosing a VRRP Method

You can configure VRRP using one of three methods:

Table 4-1  Global VRRP Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Firewall State</td>
<td>This option allows VRRP to monitor Firewall State. Check Point recommends that you do not disable the Monitor Firewall State option when running a firewall on a security platform. If you change the setting for Monitor Firewall State from enabled (the default) to disabled, VRRP negotiation for master state might start before the firewall is completely started. This can result in both VRRP nodes assuming the master state while the firewall processes are starting. Options: Disabled / Enabled. Default: Enabled.</td>
</tr>
</tbody>
</table>
| Coldstart Delay          | You can use this option to specify a number of seconds that the system should wait after starting before joining a VRRP group. You might want to configure a delay to allow routing adjacencies to form or for applications to synchronize before a system becomes the VRRP master. You can use this option with or without firewall monitoring. If you also enable firewall monitoring, the system begins to monitor the firewall after the coldstart delay period has elapsed. You might choose to use a cold start delay by itself because the following problems can occur if you enable firewall monitoring:  
  • If all the VRRP interfaces in a VRRP group fail (for example, because a switch fails), all the nodes become backup systems. None of the nodes is able to become the master, so no traffic is forwarded.  
  • If you change the time on any of the nodes, a VRRP transition (failover) occurs.  
  • Under certain circumstances, installing a firewall policy causes a VRRP transition to occur. This can happen if it takes a long time to install the policy.  
Firewall monitoring is enabled by default and cold start delay is disabled by default. To enable cold start delay, assign a value in the range 1–3600. |
Choosing a VRRP Method

- **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 “Understanding Monitored-Circuit VRRP”.

- **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 “Understanding Monitored-Circuit VRRP”.

- **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”.

**Understanding Monitored-Circuit VRRP**

The Check Point 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 platform failing). IPSO does this by releasing priority over all of the interfaces in the virtual router to allow the backup to take over entirely.

*Note* - You can choose to implement the industry standard VRRPv2 on your Check Point appliance instead of monitored-circuit VRRP. For information on implementing VRRPv2, see “Configuring VRRPv2” on page 175.

To understand the advantage of monitored-circuit VRRP, consider the configuration pictured in Figure 4-3. 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.
Selecting Node Parameters

To release the priority, IPSO subtracts the priority delta, a Check Point-specific parameter that you configure when you set up the VRID, from the priority to calculate an effective priority. If you configure 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.

See “Configuring Monitored-Circuit VRRP using the Simplified Method” and “Configuring Monitored-Circuit VRRP using the Full Method” for configuration details.

Selecting Node Parameters

Regardless of which method you use, you need to choose the values you want for the configuration parameters described in Table 4-2. You must configure these parameters on each node.

Table 4-2  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>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. Check Point recommends you use a standard priority delta, such as 10, to simplify your configuration. For more information, see “Priority Delta”.</td>
</tr>
</tbody>
</table>
Selecting Node Parameters

Table 4-2  VRRP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Interval</td>
<td>Range is 1 to 255; default setting is 1 second.</td>
</tr>
<tr>
<td></td>
<td>Set the same value for all nodes in the VRID.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Hello Interval”</td>
</tr>
<tr>
<td>Authentication</td>
<td>Choose whether you want to implement no authentication or simple password.</td>
</tr>
<tr>
<td></td>
<td>You must select the same authentication method for all nodes in the VRID.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Authentication”.</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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Backup Address”</td>
</tr>
<tr>
<td>VMAC mode</td>
<td>Choose the method by which the VMAC address is set.</td>
</tr>
<tr>
<td></td>
<td>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.

**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 Check Point’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.
Selecting Node Parameters

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 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

\[ \text{Master\_Down\_Interval} = (3 \times \text{Hello\_interval}) + \text{Skew\_time} \]

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 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.
Selecting Node Parameters

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 Check Point'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.

**Note** - If there is no interface configured on the subnet of the backup address, the system does not always display an error message. Verify that the backup address subnet is configured on your system.
Selecting Node Parameters

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.

If you change the VMAC mode on a virtual router operating as master, it broadcasts a gratuitous ARP so that adjacent layer 2 devices will update their ARP caches with the new mapping.

If you change the mode on a backup router, it does not broadcast a gratuitous ARP. If it later becomes the master, it broadcasts a gratuitous ARP at that time.

- **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.
Configuring Monitored-Circuit VRRP

- **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.

**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**—Check Point recommends you use this method. The simplified method automatically includes all the VRRP-configured interfaces on the platform in the virtual router you create. You do not have to separately specify settings for each interface. For more information, see “Configuring Monitored-Circuit VRRP using the Simplified Method”.
Configuring 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 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, priority delta, hello interval, and backup address. You do this for each appliance in each VRRP group. 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 VRRP under Configuration > High Availability in the tree view.
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.
Configuring Monitored-Circuit VRRP

7. Additional fields are displayed showing the configuration parameters. Enter values into these fields. For more information see “Selecting Node 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 the Check Point Security Gateway, 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. Click VRRP under Configuration > High Availability in the tree view.

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. Click VRRP under Configuration > High Availability in the tree view.

2. In the appropriate text box, you can change the priority, priority delta, hello interval, authentication method, password for simple authentication, and backup address for an existing virtual router.

   For information on these parameters, see “Selecting Node 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.

Note - You cannot move a 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 disconnecting an interface, delete the VRID on the interface and re-create it using the new IP address, then configure it as it was configured before.

In addition to the configuration parameters used with the simplified configuration method (see Table 4-2 on page 164), Table 4-3 shows the additional parameters you can set when using the full configuration method.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preempt mode</td>
<td>You can exercise control over the number of VRRP transitions (changes of master) by using the Preempt mode option:</td>
</tr>
<tr>
<td></td>
<td>• Enabled (the default setting): If the original master fails, a backup system becomes the acting master (a failover occurs). When the original master returns to service, it becomes the master again (a failback occurs).</td>
</tr>
<tr>
<td></td>
<td>• Disabled: If the original master fails, a backup system becomes the acting master. When the original master returns to service, it does not becomes the master again (a failback does not occur). A system with Preempt mode disabled allows any other system—even one with a lower priority—to be VRRP master. Configuring this setting on a master is useful when you want to prevent the VRRP transition that would occur when a failed master recovers and would normally reacquire forwarding responsibility from the VRRP backup.</td>
</tr>
</tbody>
</table>
You can use Preempt mode and Auto-deactivation to prevent a failed master from causing an extra VRRP transition when it recovers but still ensure high availability by using the following configuration:

- Disable preempt mode on the configured master only.
- Enable Auto-deactivation and configure the Priority and Priority Delta values to be equal on the configured backup only.

With this configuration, a recovered configured master (acting backup) does not take over if the acting master (configured backup) is functioning properly. However, if the acting master fails, the recovered configured master becomes the master again even though it has Preempt Mode disabled.

### To add a virtual router

1. Click VRRP under Configuration > High Availability in the tree view.
2. Click VRRP Legacy Configuration.
3. In the row for the interface you want to configure, select the Monitored Circuit radio button.
4. Click Apply.
   
   The Create Virtual Router text box appears.
5. Enter the value you want to use to identify the virtual router and click Apply.
   Additional fields appear.
6. 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 4-2. 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 4-3.

7. Click Apply.

8. 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. Click VRRP under Configuration > High Availability in the tree view.
   2. Click VRRP Legacy Configuration.
   3. 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.
   4. Click Apply.
   5. Click Save to make your changes permanent.

   **Configuring Monitored-Circuit VRRP using the Quick-Add Method**

   If you use the full monitored circuit mode of VRRP configuration, you can use the
   Quick-add box to configure VRRP interfaces without entering text in Voyager fields.

   **To use the Quick-add box**
   1. Click VRRP under Configuration > High Availability in the tree view.
   2. Click VRRP Legacy Configuration.
   3. Enter information into the Quick Add box using the following format:

      `interface-name mc virtual-router-id priority
      backup-address monitor-interface-name priority-delta
      <Enter>`

      You can add multiple lines to configure as many interfaces as you want.
4. Click Apply when you are done.

**Configuring VRRPv2**

Use VRRPv2 rather than Check Point’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. Click VRRP under Configuration > High Availability in the tree view.
2. Click VRRP Legacy Configuration.
3. In the row for the interface you want to configure, select the VRRPv2 radio button in the Mode column.
4. Click Submit.
   
   Text boxes for Own VRID and Backup Router with VRID appear.
5. 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.
6. Click Apply.
   
   Additional fields appear.
7. 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.
8. Click Apply.
9. 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 the Check Point Security Gateway for VRRP

The guidelines in this section list some considerations for configuring the Check Point Security Gateway 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.

When you use the Check Point cpconfig program, follow these guidelines:

- Install the Check Point Security Gateway on each node. Do not install the Check Point Security Gateway and Security Management server together on the same node.
- After you choose to install the Check Point Security Gateway, 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, make sure that it is enabled 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 (backup) address of the interface that faces the external network.
- Add a gateway object for each Check Point appliance to the gateway cluster object.
- In the General Properties dialog box for the gateway cluster object, do not check ClusterXL.
Configuring the Check Point Security Gateway for VRRP

- 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 Check Point 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 Check Point Encrypt Card in one appliance and the older Check Point 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 the Check Point Security Gateway, 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.
Configuring VRRP Rules for the Check Point Security Gateway

To enable sequence validation in the Check Point management application and IPSO

1. Click Advanced System Tuning under Configuration > System Configuration in the tree view.

   **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 the Check Point Security Gateway

This section provides information about configuring firewall rules to work with VRRP.

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>Firewalls</td>
<td>mcast-224.0.0.18</td>
<td>vrrp</td>
<td>Accept</td>
</tr>
<tr>
<td>fwcluster-object</td>
<td>mcast-224.0.0.18</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.

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
Configuring VRRP Rules for the Check Point Security Gateway

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>
Monitoring VRRP

You can use the following CLI commands to view and monitor VRRP information:

<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 VRRP Monitor on the VRRP Configuration page.

VRRP monitoring information 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.

**Note** - 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.
Monitoring the Firewall State

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.
- **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.

Note - If the advertisement is from the address owner (priority=255) that packet is accepted, even with the configuration mismatch.

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. Click VRRP under Configuration > High Availability in the tree view.
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 Check Point Customer Support, go to http://support.checkpoint.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 Check Point Encrypt Card in one appliance and the older Check Point 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.
Firewall Policies

- 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.

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.
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.
Chapter 5
Configuring SNMP

This chapter describes the Check Point IPSO implementation of Simple Network Management Protocol (SNMP) and how to configure it on your system.

In This Chapter

- SNMP Overview  page 188
- SNMP Proxy Support for Check Point MIB  page 193
- Enabling SNMP and Selecting the Version  page 194
- Configuring the System for SNMP  page 196
- Interpreting Error Messages  page 203
- Configuring SNMPv3  page 206
SNMP Overview

The Simple Network Management Protocol (SNMP) is the Internet standard protocol used to exchange management information between network devices. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

IPSO implements UCD-SNMP 4.0.1 as the base version of SNMP. Changes have been made to the base version to address security and other fixes. For more information on Net-SNMP, go to http://www.net-snmp.org.

**Warning** - If you use SNMP, Check Point strongly recommends that you change the community strings for security purposes. If you do not use SNMP, you should disable the community strings.

SNMP, as implemented on Check Point platforms, supports the following:

- GetRequest, GetNextRequest, GetBulkRequest, and a select number of traps. The Check Point implementation also supports SetRequest for three attributes only: sysContact, sysLocation, and sysName. You must configure a read-write community string to enable set operations.

- SNMP v1, v2, and v3. For more information about SNMP v3, see “Managing SNMP Users”.

**Note** - The Check Point 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>
</tbody>
</table>
### SNMP Overview

<table>
<thead>
<tr>
<th>MIB</th>
<th>Source</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Types MIB</td>
<td>proprietary</td>
<td>Contains OID values for the different types of circuit cards used in Check Point 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>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>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The isdnMibCallInformation trap is not supported by IPSO.</td>
</tr>
<tr>
<td>VRRP MIB</td>
<td>RFC 2787</td>
<td>Provides dynamic failover statistics.</td>
</tr>
<tr>
<td>RIP MIB</td>
<td>RFC 1724</td>
<td>Describes RIP version 2 protocol.</td>
</tr>
<tr>
<td>SNMP Framework MIB</td>
<td>RFC 2571</td>
<td>Outlines SNMP management architecture.</td>
</tr>
<tr>
<td>SNMP MPD MIB</td>
<td>RFC 2572</td>
<td>Provides message processing and dispatching.</td>
</tr>
<tr>
<td>SNMP User-based SM MIB</td>
<td>RFC 2574</td>
<td>Provides management information definitions for SNMP User-based Security Model</td>
</tr>
<tr>
<td>SNMPv2 MIB</td>
<td>RFC 1907</td>
<td>Defines SNMPv2 entities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The warmStart trap is not supported.</td>
</tr>
<tr>
<td>SNMPv2 SMI</td>
<td>RFC 2578</td>
<td></td>
</tr>
<tr>
<td>SNMPv2 TC</td>
<td>RFC 854</td>
<td>Defines textual conventions for various values reported in OIDs and Traps.</td>
</tr>
</tbody>
</table>
### SNMP Overview

<table>
<thead>
<tr>
<th>MIB</th>
<th>Source</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial-Control MIB</td>
<td>RFC 2128</td>
<td>Describes peer information for demand access and other kinds of interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> IPSO does not support the dialCtlPeerCallInformation and dialCtlPeerCallSetup traps.</td>
</tr>
<tr>
<td>Entity MIB</td>
<td>RFC 2737</td>
<td>Represents the multiple logical entities that a single SNMP agent supports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPSO does not support the entConfigChange trap.</td>
</tr>
<tr>
<td>Tunnel-MIB</td>
<td>RFC 2667</td>
<td>Provides statistics about IP tunnels.</td>
</tr>
<tr>
<td>UDP-MIB</td>
<td>RFC 2013</td>
<td>Provides statistics about UDP implementations.</td>
</tr>
<tr>
<td>Frame Relay DTE MIB</td>
<td>RFC 2115</td>
<td>Keeps statistics and errors in one or more circuits of a device implementing Frame Relay.</td>
</tr>
<tr>
<td>Token Ring MIB</td>
<td>RFC 1748</td>
<td>Statistics and version information on any firewalls currently installed.</td>
</tr>
<tr>
<td>Check Point MIB</td>
<td>proprietary</td>
<td>Statistics and version information on any firewalls currently installed.</td>
</tr>
<tr>
<td>1213 MIB</td>
<td>RFC 1213</td>
<td>Contains the original definition of MIB-II. Check Point provides this MIB with the system to ensure backwards compatibility with SNMP v1.</td>
</tr>
<tr>
<td>IPSO-LBCluster-MIB</td>
<td>proprietary</td>
<td>Provides information about IPSO load-balancing systems.</td>
</tr>
<tr>
<td>HWM MIB</td>
<td>proprietary</td>
<td>Contains hardware management information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> IPSO does not send the traps that this MIB supports when the Check Point platform is used as an IP security device.</td>
</tr>
<tr>
<td>Nokia Common MIB</td>
<td>proprietary</td>
<td></td>
</tr>
<tr>
<td>OID Registration MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia Common NE Role MIB</td>
<td>proprietary</td>
<td></td>
</tr>
<tr>
<td>Nokia Enhanced SNMP Solution Suite Alarm IRP MIB</td>
<td>proprietary</td>
<td><strong>Note:</strong> IPSO does not send traps that this MIB supports when the Check Point platform is used as an IP security device.</td>
</tr>
</tbody>
</table>
SNMP Overview

<table>
<thead>
<tr>
<th>MIB</th>
<th>Source</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nokia Enhanced SNMP Solution Suite Common</td>
<td>proprietary</td>
<td>Note: IPSO does not send traps that this MIB supports when the Check Point platform is used as an IP security device.</td>
</tr>
<tr>
<td>Definition MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia Enhanced SNMP Solution Suite PM</td>
<td>proprietary</td>
<td>Note: IPSO does not send traps that this MIB supports when the Check Point platform is used as an IP security device.</td>
</tr>
<tr>
<td>Common Definition MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia Enhanced SNMP Solution Suite PM IRP</td>
<td>proprietary</td>
<td></td>
</tr>
<tr>
<td>MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia NE3S Registration MIB</td>
<td>proprietary</td>
<td></td>
</tr>
<tr>
<td>Nokia Link Aggregation MIB</td>
<td>proprietary</td>
<td>Contains the traps required for managing link aggregation.</td>
</tr>
<tr>
<td>Nokia NTP MIB</td>
<td>proprietary</td>
<td></td>
</tr>
<tr>
<td>SNMPv2-CONF</td>
<td>proprietary</td>
<td>IPSO does not support this MIB but it is included for those customers who need it to enable their management tools. This MIB resides in the /etc/snmp/mibs/unsupported directory.</td>
</tr>
</tbody>
</table>

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 Check Point IPSO enables an SNMP manager to monitor the device and to modify the sysName, sysContact and sysLocation objects only.

Note - If you select the Disable checkbox all community strings are disabled and SNMPv1 and v2 do not function. This has the same effect as selecting only SNMPv3 in the previous step.

Use Network Voyager to perform the following tasks:
- Define and change one read-only community string,
SNMP Overview

- Define and change one read-write community string.
- Enable and disable the SNMP daemon.
- Create SNMP users.
- Modify SNMP user accounts.
- 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

SNMP Proxy Support for Check Point MIB

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 Check Point 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 Check Point 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 returns valid values to only one request.

Because IPSO uses a proxy to support the Check Point MIB, reference the Check Point documentation for any limitations of the CP-SNMPd.
Enabling SNMP and Selecting the Version

The SNMP daemon is enabled by default. If you choose to use SNMP, configure it according to your security requirements. At minimum, you must change the default community string to something other than public. You should also select SNMPv3, rather than the default v1/v2/v3, if your management station supports it.

**Warning** - If you do not plan to use SNMP to manage the network, disable it. Enabling SNMP opens potential attack vectors for surveillance activity by enabling an attacker to learn about the configuration of the device and the network.

You can choose to use all versions of SNMP (v1, v2, and v3) on your system or to allow SNMPv3 access only. If your management station supports v3, select to use only v3 on your IPSO system. SNMPv3 limits community access; only requests from users with enabled SNMPv3 access are allowed and all other requests are rejected.

**To enable or disable SNMP**

1. Choose SNMP under Configuration in the tree view.
2. Select Yes or No for Enable SNMP Daemon.
3. If you are enabling SNMP, click Apply.

   The SNMP configuration options appear.

**Warning** - To run the Check Point and SNMP daemons simultaneously, you must start the Check Point SNMP daemon after you start the Check Point Security Gateway services. If you start the Check Point SNMP daemon before you start Security Gateway services, the IPSO daemon does not start.

4. From the SNMP version drop-down list, select the version of SNMP to run:
   - **SNMPv1/v2/v3**
     Select this option if your management station does not support SNMPv3.
   - **SNMPv3**
     Select this option if your management station supports v3. SNMPv3 provides a higher level of security than v1 or v2.
Enabling SNMP and Selecting the Version

5. If you selected v1/v2/v3, enter a new read-only community string under Community Strings. This is a basic security precaution that you should always take.

   **Note** - If you select the Disable checkbox all community strings are disabled and SNMPv1 and v2 do not function. This has the same effect as selecting only SNMPv3 in the previous step.

6. (Optional). Set a read-write community string.

   **Warning** - Set a read-write community string only if you have reason to enable set operations, only if you enabled SNMPv3 (not v1/v2/v3), and if your network is secure.

7. Click Apply.
8. Click Save to make your changes permanent.
Configuring the System for SNMP

When you enable SNMP for your system, you can configure the following:

- Specify an agent address. See “Setting an Agent Address” on page 196
- Configure traps. See “Configuring Traps” on page 196.

Setting an Agent Address

An agent address is a specific IP address at which the SNMP agent listens and responds to requests. The default behavior is for the SNMP agent to listen to and respond to requests on all interfaces. If you specify one or more agent addresses, the system SNMP agent listens and responds only on those interfaces.

You can use the agent address as another way to limit SNMP access. For example, you can limit SNMP access to one secure internal network that uses a particular interface by configuring that interface as the only agent address.

To set an SNMP agent address

1. Choose SNMP under Configuration in the tree view.
2. Enter the valid IP address of a configured interface in the Agent New Address field.
   You can use the IP address of any existing and valid interface.
3. Click Apply.
   The IP address and a corresponding Delete check box appear.
4. Click Save to make your change permanent.

Note - If no agent addresses are specified, the SNMP protocol responds to requests from all interfaces.

Configuring Traps

Managed devices use trap messages to report events to the network management station (NMS). When certain types of events occur, the platform sends a trap to the management station.

Traps are defined in text files located in the /etc/snmp/mibs directory:

- System traps are defined in the Nokia-IPSO-System-MIB.
Configuring Traps

- The ifLinkUpDown trap is defined in the IF-MIB.
- Clustering traps are defined in the Nokia-IPSO-LBCluster-MIB.
- Disk mirror traps are defined in the Nokia-IPSO-System-MIB.

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 5-1 lists the types of SNMPv1 and SNMPv2 traps which IPSO supports.

**Note** - The Check Point 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>lamemberActive</td>
<td>Supplies notification when a port is added to a link aggregation group.</td>
</tr>
<tr>
<td>lamemberInactive</td>
<td>Supplies notification when a port is removed from a link aggregation group.</td>
</tr>
</tbody>
</table>
Configuring Traps

Table 5-1  Types of SNMP Traps

<table>
<thead>
<tr>
<th>Type of Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 an VRRP hello message is not properly authenticated.</td>
</tr>
<tr>
<td>systemTrapConfigurationChange</td>
<td>Supplies notification when a change to the system configuration is applied.</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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Note: The systemTrapDiskFailure applies only to Check Point platforms that support disk mirroring.</td>
</tr>
<tr>
<td>systemTrapDiskMirrorSetCreate</td>
<td>Supplies notification when a system disk mirror set is created.</td>
</tr>
</tbody>
</table>
Configuring Traps

### Table 5-1 Types of SNMP Traps

<table>
<thead>
<tr>
<th>Type of Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>systemTrapMirrorSetDelete</td>
<td>Supplies notification when a system disk mirror set is deleted.</td>
</tr>
<tr>
<td>systemTrapDiskMirrorSyncSuccess</td>
<td>Supplies notification when a system disk mirror set is successfully synced.</td>
</tr>
<tr>
<td>systemTrapDiskMirrorSyncFailure</td>
<td>Supplies notification when a system disk mirror set fails during syncing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The disk mirror traps are supported only on systems where disk mirroring is supported.</td>
</tr>
<tr>
<td>clusterMemberReject</td>
<td>Supplies notification when a member request to join a cluster is rejected.</td>
</tr>
<tr>
<td>clusterMemberJoin</td>
<td>Supplies notification when a member node joins the cluster.</td>
</tr>
<tr>
<td>clusterMemberLeft</td>
<td>Supplies notification when a member node leaves the cluster.</td>
</tr>
<tr>
<td>clusterNewMaster</td>
<td>Supplies notification when a cluster is formed and a new master is elected.</td>
</tr>
<tr>
<td>clusterProtocolInterfaceChange</td>
<td>Supplies notification when a failover occurs from the primary cluster network to the secondary cluster network.</td>
</tr>
<tr>
<td>systemPowerSupplyFailure</td>
<td>Supplies notification when a power supply for the system fails.</td>
</tr>
<tr>
<td></td>
<td>This trap includes the power supply index and is supported only on platforms with two power supplies installed and running.</td>
</tr>
<tr>
<td>systemFanFailure</td>
<td>Supplies notification when a CPU or chassis fan fails. This trap includes the fan index.</td>
</tr>
</tbody>
</table>
Configuring Traps

Table 5-1 Types of SNMP Traps

<table>
<thead>
<tr>
<th>Type of Trap</th>
<th>Description</th>
</tr>
</thead>
</table>
| SystemOverTemperature        | Supplies notification when a power supply failure occurs because of high temperature.  
|                              | This trap is followed by a power supply failure trap that specifies the power supply index that failed. The power supply failure trap is supported only on platforms with two power supplies installed and running. |
| systemSnmpProcessShutdown    | Supplies notification when the status of the SNMP daemon is changed, either turned off or turned on. |

To configure traps, specify the following information:

- The location of the trap receiver (management station). See “Configuring Trap Receivers” on page 200.
- Which types of traps to enable. See “Enabling or Disabling Trap Types” on page 201.
- An agent address to be included in each trap message sent to the management station to identify which network device generated the trap. See “Setting the Trap PDU Agent Address” on page 201.
- Location and contact information provided to the management system about where your device is located and who to contact about it. See “Configuring Location and Contact Information” on page 202.

**Configuring Trap Receivers**

You must specify the management station that accepts traps from your appliance, and the community string used on your management station (receiver) to control access.

**To configure trap receivers**

1. Choose SNMP under Configuration in the tree view.
2. Enter the IP address (or the hostname if DNS is set) of a receiver in the Add New Trap Receiver text field.
3. Enter the community string for the specified receiver in the Community String for new Trap Receiver field.
4. Select the Trap SNMP Version for the trap receiver in the drop-down menu.
The options are v1 or v2, and the default is v1. This is the version of SNMP used by your management station.

5. Click Submit.

**Enabling or Disabling Trap Types**

When you enable types of traps, the system sends a trap message when that type of event occurs. For example, if you enable authorization traps, the system sends a trap message to the management station when it receives a packet with an incorrect community string.

**To enable or disable traps**

1. Choose SNMP under Configuration in the tree view.
2. To enable any type of trap, click On next to the name of the trap and click Apply.
3. To disable any type of trap, click Off next to the name of the trap and click Apply.
4. To make your changes permanent, click Save.

**Setting the Trap PDU Agent Address**

The trap PDU address is included in the protocol data unit (PDU) of each trap message sent to the management station that uses it to identify which network device generated the trap.

This address must belong to a configured interface.

If you do not configure an agent address for traps, the system identifies the trap agent address as 0.0.0.0 in SNMP traps (in accordance with RFC 2089). (For releases of Check Point IPSO previous to 3.7, the default was to use the IP address of the first valid interface.)

**To set the trap PDU agent address**

1. Choose SNMP under Configuration in the tree view.
2. To specify the IP address to be used for sent trap PDU, enter the IP address in the Trap PDU Agent Address field.
3. Click Apply.
4. Click Save to make your changes permanent.
Configuring Location and Contact Information

The settings for location and contact information provide information to the management system about where your device is located and who to contact about it.

Set the location and contact strings when you perform the initial configuration for SNMP on your system.

To configure location and contact information
1. Choose SNMP under Configuration in the tree view.
2. In the SNMP Location String text field, enter the actual location of the device. Click Apply.
3. In the SNMP Contact String text field, enter the name of department or person who has administrative responsibility for the device.
4. Click Apply.
5. Click Save to make your changes permanent.
Interpreting Error Messages

This section lists and explains certain common error status values that can appear in SNMP messages. Within the 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>
<th>Error status code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>noError</td>
<td>10</td>
<td>wrongValue</td>
</tr>
<tr>
<td>1</td>
<td>tooBig</td>
<td>11</td>
<td>noCreation</td>
</tr>
<tr>
<td>2</td>
<td>NoSuchName</td>
<td>12</td>
<td>inconsistentValue</td>
</tr>
<tr>
<td>3</td>
<td>BadValue</td>
<td>13</td>
<td>resourceUnavailable</td>
</tr>
<tr>
<td>4</td>
<td>ReadOnly</td>
<td>14</td>
<td>commitFailed</td>
</tr>
<tr>
<td>5</td>
<td>genError</td>
<td>15</td>
<td>undoFailed</td>
</tr>
<tr>
<td>6</td>
<td>noAccess</td>
<td>16</td>
<td>authorizationError</td>
</tr>
<tr>
<td>7</td>
<td>wrongType</td>
<td>17</td>
<td>notWritable</td>
</tr>
<tr>
<td>8</td>
<td>wrongLength</td>
<td>18</td>
<td>inconsistentName</td>
</tr>
<tr>
<td>9</td>
<td>wrongEncoding</td>
<td></td>
<td></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.
Interpreting Error Messages

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-binding</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>
Interpreting Error Messages

*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 SNMPv3

IPSO supports the user-based security model (USM) component of SNMPv3 to provide message-level security. With USM (described in RFC 3414), access to the SNMP service is controlled on the basis of user identities. Each user has a name, an authentication pass phrase (used for identifying the user), and an optional privacy pass phrase (used for cryptographically protecting against disclosure of SNMP message payloads).

The system uses the MD5 hashing algorithm to provide authentication and integrity protection and DES to provide encryption (privacy). Check Point 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 IPSO system responds accordingly.

Note - Check Point systems do not protect traps with authentication or encryption.

Request Messages

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u name</td>
<td>Specifies the user name.</td>
</tr>
<tr>
<td>-a MD5</td>
<td>Use MD5 hashing for authentication.</td>
</tr>
<tr>
<td>-x DES</td>
<td>Use DES for encryption.</td>
</tr>
<tr>
<td>-A password</td>
<td>Specifies the user’s password/passphrase. Use for authentication. The password/passphrase must have at least 8 characters.</td>
</tr>
</tbody>
</table>

Table 5-2 Security Related Options Used in Request Messages
Managing SNMP Users

For example, to send an snmpwalk request from your manager with full protection, you would enter the following command:

```
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.

### Managing SNMP Users

SNMP users are maintained separately from system users. You can create SNMP user accounts with the same names as existing user accounts or different. You can create SNMP user accounts that have no corresponding system account. When you delete a system user account, you must separately delete the SNMP user account.

To view existing SNMP users, click SNMP under Configuration > System Configuration in the tree view and click Manage SNMP Users. Alternatively, you can click the Manage SNMP User Access link located on the Configuration > Security and Access > Users page.

The admin user or a user with privileges for the SNMP feature can modify the security level, authentication pass phrase, and privacy pass phrase for existing SNMP users, and create or delete SNMP users. Pass phrases differ from passwords only in length—pass phrases are usually much longer than passwords. Their greater length makes pass phrases more secure.

The IPSO implementation of SNMP supports DES and MD5 authentication to automatically generate USM keys.

---

**Table 5-2  Security Related Options Used in Request Messages**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-X password</code></td>
<td>Specifies the security level:</td>
</tr>
<tr>
<td></td>
<td>• authNoPriv: use authentication only</td>
</tr>
<tr>
<td></td>
<td>• authPriv: use authentication and encryption is enabled</td>
</tr>
<tr>
<td>`-l [authNoPriv</td>
<td>authPriv</td>
</tr>
</tbody>
</table>

For more information about USM, see RFC 3414.
Managing SNMP Users

SNMP must be enabled on the system before you can set an SNMP user authentication or privacy pass phrase.

**Note** - If you change the security level from either authPriv or authPrivReq to authNoPriv, the privacy pass phrase is automatically deleted. If you change it back to authNoPriv, you must supply a privacy pass phrase.

**To add an SNMP user**
1. Click SNMP under Configuration in the tree view.
2. Click Manage USM Users.
3. Enter the following information for the new user:
   - User Name—The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user's name for system access, though the SNMP user account is handled as a separate entity.
   - Security Level. Select from the following:
     - Authentication + Privacy—The user has authentication and privacy pass phrases and can connect with or without privacy encryption.
     - Authentication, no privacy—The user has only an authentication pass phrase and can connect only without privacy encryption.
     - Authentication and privacy required—The user must connect using both authentication and encryption pass phrases.
   - Authentication Pass Phrase—Used to identify the user. Enter a password for the user that is between 8 and 128 characters in length.
   - Privacy Pass Phrase—Used to cryptographically protect against disclosure of SNMP message payloads. Enter a pass phrase that is between 8 and 128 characters in length.
4. Click Apply.
   An entry for the new user appears in the SNMP USM Users table.
5. Click Save to make your changes permanent.

**To delete a USM user**
1. Click SNMP under Configuration in the tree view.
2. Click Manage USM Users at the bottom of the page.
   The Manage SNMP Users page appears.
Managing SNMP Users

3. Select the appropriate Delete check box.
4. Click Apply.
5. Click Save to make your changes permanent.
Managing SNMP Users
Chapter 6
Configuring IPv6

This chapter describes the IPv6 features supported by Check Point IPSO and how to configure them on your system.

- IPv6 Overview  page 212
- Interfaces  page 214
- IPv6 and IPv4 Compatibility  page 217
- Routing Configuration  page 221
- Router Discovery  page 225
- VRRP for IPv6  page 227
- Traffic Management  page 237
- Security and Access Configuration  page 238
IPv6 Overview

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)
- IPv6 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 Overview

- 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

To configure IPv6 logical interfaces
1. Click IPv6 Interfaces under Configuration > System Configuration > IPv6 Configuration in the tree view.
2. Click the logical interface link to configure in the Logical column. Example: eth-s1p1c0
3. 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.
4. Click Apply.
5. Click Save to make your changes permanent.
6. Click Up at the top of the page to take you back to the IPv6 Logical Interfaces page.
7. To enable the IPv6 address, click On in the IPv6 Active field.
8. Click Apply.
9. Click Save to make your change permanent.

To delete an IPv6 address
1. Click IPv6 Interfaces under Configuration > System Configuration > IPv6 Configuration in the tree view.
2. Click the logical interface link to configure in the Logical column for which you want to delete an IPv6 address. Example: eth-s1p1c0
3. Check the delete box next to the IPv6 address you want to delete.
4. Click Apply.
5. Click Save to make your changes permanent.

To disable IPv6 on an interface
1. Click IPv6 Interfaces under Configuration > System Configuration > IPv6 Configuration in the tree view.
Interfaces

2. 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.

3. Click Apply.

   The list of addresses in the IPv6 address field for the specified logical interface disappear.

4. Click Save to make your changes permanent.

**To configure IPv6 Neighbor Discovery**

1. Click IPv6 Neighbor Discovery under Configuration > System Configuration > IPv6 Configuration in the tree view.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. Click Apply.

8. Click Save to make your changes permanent.
9. To flush current dynamic Neighbor Discovery entries, click Flush in the Dynamic Neighbor Discovery Entries field.

10. 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.

**To configure IPv6 in IPv4 tunnels**

1. Click IPv6 in IPv4 Tunnels under Configuration > System Configuration > IPv6 Configuration in the tree view.
2. Enter the IPv4 address of the local tunnel endpoint in the Local IPv4 Address text box.
3. Enter the IPv4 address of the remote tunnel endpoint in the Remote IPv4 Address text box.
4. (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.
5. (Optional) Enter the remote IPv6 link-local address of the remote tunnel endpoint in the Remote IPv6 Link Local text box.
6. (Optional) Enter a value in the Time to Live text box for the Time to Live (TTL) packets sent on the tunnel.
7. Click Apply.
8. Click Save to make your changes permanent.

**Note** - The local address must be the address of another interface configured for the router.

Configuring IPv6 to IPv4

This feature allows you to connect an IPv6 domain through IPv4 clouds without configuring a tunnel.

**To configure IPv6 to IPv4**

1. Click IPv6 to IPv4 under Configuration > System Configuration > IPv6 Configuration in the tree view.
Configuring IPv6 over IPv4

2. In the Enable IPv6 to IPv4 field, click Yes.
3. 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.
4. 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.

5. (Optional) Enter a value for the Time to Live (TTL) packets sent.
6. Click Apply.
7. 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.

To configure IPv6 over IPv4
1. Click IPv6 over IPv4 Tunnels under Configuration > System Configuration > IPv6 Configuration in the tree view.
2. In the Enable IPv6 over IPv4 field, click Yes.
3. 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.
4. 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.

5. (Optional) Enter a value in the for the Time to Live (TTL) packets sent.
6. Click Apply.
7. 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.

To configure IPv4 in IPv6 tunnels
1. Click IPv6 in IPv4 Tunnels under Configuration > System Configuration > IPv6 Configuration in the tree view.
2. Enter the IPv6 address of the local tunnel endpoint in the Local IPv6 Address text box.
3. Enter the IPv6 address of the remote tunnel endpoint in the Remote IPv6 Address text box.
4. (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.
5. Click Apply.
6. Click Save to make your changes permanent.

Configuring an IPv6 Default or Static Route

To configure an IPv6 default or static route
2. To enable a default route:
   1. Select On in the Default field.
   2. Click Apply.
3. To create a new static route:
   1. Enter the IPv6 address prefix in the New Static Route text box.
   2. Enter the mask length (number of bits) in the Mask Length text box.
   3. Click Apply.
4. Select the type of next hop the route will take from the Next Hop Type drop-down list—Normal, Reject, or Black Hole.
Configuring an IPv6 Default or Static Route

5. Select the interface that the 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.
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 Routing Configuration under Configuration > System Configuration > IPv6 Configuration in the tree view. For more information, see “OSPF” on page 239.

Configuring OSPFv3 with VRRPv3

To use OSPFv3 with VRRPv3, enable the Virtual Address option on the OSPFv3 configuration page. If the configured interface is part of the VRRP master virtual router, OSPFv3 runs on the interface. When you enable this option, OSPFv3 uses VRRPv3’s virtual link-local address for the interface as the source of its control packets. This cannot be the automatically configured link-local address—that is, you must change the link-local address for the interface to something other than the default. You must configure the same link-local address on all the routers in the VRRP group.

VRRP installs the link-local address only on the master, so OSPFv3 runs only on that router. If a failover occurs, VRRPv3 installs the link-local address on the new master and OSPFv3 starts running on that system. Because OSPFv3 runs on one router at a time, there is no synchronization of OSPFv3 state between the VRRP group members.

Note - When configuring VRRPv3 to work with OSPFv3, you must also configure VRRPv3 to accept connections to virtual IPv6 addresses by enabling the Accept Mode option.

Configuring RIPng

1. Click RIPng under Configuration > System Configuration > IPv6 Configuration > Routing Configuration in the tree view.
2. To enable RIPng, click On next to the logical interface on which you want to run RIP, and then click Apply.
3. 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.
4. Click Apply.
Creating IPv6 Aggregate Routes

5. Click Save to make your changes permanent.

Creating IPv6 Aggregate Routes

1. Click IPv6 route Aggregation under Configuration > System Configuration > IPv6 Configuration > Routing Configuration in the tree view.
2. Enter the IPv6 prefix for the new aggregate route in the Prefix for New Aggregate text box.
3. Enter the mask length (number of bits) in the Mask Length text box.
4. Click Apply.
5. Scroll through the New Contributing Protocol List click the protocol you want to use for the new aggregate route.
6. Click Apply.
7. Click Save to make your changes permanent.
8. Click On in the Contribute All Routes from <Protocol> field.
9. (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.
10. Click Apply, and click Save to make your changes permanent.

Creating Redistributed Routes

Redistributing Static Routes into RIPng

1. Click IPv6 Route Redistribution under Configuration > System Configuration > IPv6 Configuration > Routing Configuration in the tree view.
2. Click Static Routes.
3. To redistribute all currently valid static routes into RIPng, click the On button in the Redistribute All Statics in the RIPng field.
4. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.
5. Click Apply.
6. Click Save to make your changes permanent.
7. 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.
Creating Redistributed Routes

8. Enter a value in the Metric text box for the metric cost that the created RIPng route(s) will have.
9. Click Apply.
10. Click Save to make your changes permanent.

**Redistributing Aggregate Routes in RIPng**

1. Click IPv6 Route Aggregation under Configuration > System Configuration > IPv6 Configuration > Routing Configuration in the tree view.
2. To redistribute all currently valid aggregate routes into RIPng, click On in the Redistribute all Aggregates into RIPng field.
3. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.
4. Click Apply.
5. Click Save to make your changes permanent.
6. 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.
7. Enter a value in the Metric text box for the metric cost that the created RIPng route will have.
8. Click Apply.
9. Click Save to make your changes permanent.

**Redistributing Interface Routes into RIPng**

1. Click IPv6 Route Redistribution under Configuration > System Configuration > IPv6 Configuration > Routing Configuration in the tree view.
2. Click Interface Routes.
3. To redistribute all currently active interface routes into RIPng, click On in the Export all Interfaces into RIPng field.
4. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.
5. Click Apply.
6. Click Save to make your changes permanent.
7. To redistribute a specific interface route or routes into RIPng, click On next to the IPv6 interface for the route to redistribute into RIPng.
Creating Redistributed Routes

8. Enter a value in the Metric text box for the metric cost that the created RIPng routes will have.

9. Click Apply.

10. 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. Check Point implements only the ICMPv6 router discovery server portion, which means that the Check Point 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” on page 227.

1. Click ICMPv6 Router Discovery under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.
2. To enable ICMPv6 router discovery, click On next to the interface on which you want to run the protocol.
3. Click Apply.
4. (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.
5. (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.
6. (Optional) To enable the MTU options field in the router advertisement packet, click Yes in the Send MTU Option field.
7. (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.
8. (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.

9. (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.

10. (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.

11. (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.

12. (Optional) Enter a value in the Cur Hop Limit text box for the router advertisement packets hop limit field.

13. (Optional) To specify that the IPv6 prefix can be used for on-link determination, click Yes in the Onlink Flag field.

14. (Optional) To specify that the IPv6 prefix can be used for autonomous address configuration, click Yes in the Autonomous Flag field.

15. (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.

16. (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.

17. Click Apply.

18. Click Save to make your changes permanent.
VRRP for IPv6

Configuring VRRP for IPv6

Beginning with IPSO 3.8.1, VRRP configuration was supported for IPv6 interfaces. Check Point 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 general information about VRRP, see “VRRP Overview” on page 127.

For more information about how to configure the Check Point Security Gateway for VRRP for IPv6 see, “Configuring Check Point NGX for VRRP” on page 144

Note - The Check Point Security Gateway does not support user, session, or client authentication for IPv6 interfaces.

Also, Check Point Security Gateway 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 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” on page 225

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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.
Creating a Virtual Router to Back Up Another VRRP Router Addresses Using VRRPv3

2. Click VRRPv3 button next to the interface for which to enable VRRP.

3. Click Apply.

4. 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.

5. 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.

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 (1 second).

7. Click Apply.

8. To make your changes permanent, click Save.

   Note - When configuring VRRPv3 to work with OSPFv3, you must also configure VRRPv3 to accept connections to virtual IPv6 addresses by enabling the Accept Mode option.

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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.

2. Click VRRPv3 button next to the interface for which to enable VRRP.

3. Click Apply.

4. 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.

5. (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.

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 (1 second).

7. (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.

8. (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.

   **Note** - When configuring VRRPv3 to work with OSPFv3, you must enable the Accept Mode option.

9. Enter an IPv6 address for this virtual router in the Backup Address text box. 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 had more than one IP address, repeat step 10.

11. 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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.

2. Click Enabled in the Monitor Firewall State field.

3. To disable this option, if you have enabled it, click Disabled. The default is Enabled.

4. 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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.
Setting a Virtual MAC Address for a Virtual Router

2. You can set the VMAC option for an interface on which you enable VRRP or Monitored Circuit

   1. 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.

   2. 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.

3. 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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.
2. 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.
3. 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.
4. To add an IP address, select an address from the Address drop-down list. Click Apply.
5. To add a backup IP address, enter the IP address in the Backup Address text box. Click Apply.
6. 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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.
2. Locate the virtual router to remove.
Creating a Virtual Router in Monitored Circuit Mode for IPv6

1. To locate a virtual router used to back up the local interface IP addresses, find the correct virtual ID in the Own VRID field.

2. 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.

3. Click off next to the entry for the VRID of the virtual router you want to remove.

4. Click Apply.
   All the information about that specific virtual router disappears from the Network Voyager configuration page.

5. 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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.

2. To enable Monitored Circuit, click the Monitored Circuit button next to the interface for which to enable Monitored Circuit, and then click Apply.

3. 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.

4. (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 (1 second).
5. (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.

6. (Optional) Click Enabled next to Accept Mode if you want 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.

7. 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.

8. (Optional) If the router you are backing up has more than one IP address, repeat step 10.

9. (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.

10. (Optional) To configure a virtual MAC (VMAC) address for the virtual router, see “Setting a Virtual MAC Address for a Virtual Router.”

11. 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 VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.
2. Click the Monitor Interface drop-down list for the specific virtual router entry and select the interface you want to monitor.
3. 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.

4. Click Apply.
5. Repeat steps 4 and 5 for each interface you want to monitor.
6. 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
7. Click Save to make your changes permanent.

Changing the List of Addresses in a Monitored Circuit Virtual Router for IPv6

1. Click VRRP for IPv6 under Configuration > System Configuration > IPv6 Configuration > Router Services in the tree view.
Changing the List of Addresses in a Monitored Circuit Virtual Router for IPv6

2. 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.

3. To remove an IP address from the list, click Off next to the address you want to delete. Click Apply.

4. 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.

5. To make your changes permanent, click Save.
Traffic Management

**Traffic Management**

Configuring traffic management features for IPv6 is essentially the same as for IPv4. See Chapter 9, “Configuring Traffic Management” for more information.
Security and Access Configuration

Security and Access Configuration

To enable FTP, TFTP, or Telnet access

2. Select Yes next to the types of access you want to allow for IPv6—FTP, Telnet, and TFTP.
3. Click Apply.
4. Click Save to make your changes permanent.
Chapter 7
Managing Security and Access

This chapter describes how to manage passwords, user accounts, and groups, how to assign privileges using role-based administration, and how to configure network access, services, and Network Voyager session management. It also describes how to configure AAA for a new service, encryption acceleration, and virtual tunnel interfaces (VTI) which support Check Point route-based VPN.

**Note** - When users log in to Network Voyager, the navigation tree displayed depends on the role or roles assigned to their user account. If the roles do not provide access to a feature, they will not see a link to the feature in the tree. If they have read-only access to a feature, they will see a link and be able to access the page, but all the controls will be disabled.

In This Chapter

- Password and Account Management  page 241
- Changing Passwords  page 252
- Managing User Accounts  page 253
- Managing Groups  page 260
- Role-Based Administration  page 262
- Configuring Network Access and Services  page 266
- Configuring Network Voyager Access  page 269
- Secure Shell (SSH)  page 274
Password and Account Management

One of the important elements of securing your Check Point network security platform is setting user passwords and creating an effective password policy. When considering password creation and password policy, keep in mind that having users create strong, unique passwords that use a variety of character types and creating a password policy that requires users to change their passwords often are key factors to your overall network security.

The following sections provide information on how to configure your platform using Network Voyager to:

- Enforce creation of strong passwords
- Force users to change passwords at regular intervals
- Track and prevent reuse of old passwords
- Lock out users after failed login attempts
- Lock out accounts that have been inactive for a period of time

The features included in password and account management provide a global and comprehensive way to manage passwords. We recommend that you use the functions in password and account management to set and manage your user passwords and password policies.

The password policies you set with password and account management are sharable across a cluster.

None of the password and account management features apply to nonlocal users, whose login information and passwords are managed by authentication servers such as RADIUS servers. Nor do they apply to non-password authentication, such as the public key authentication supported by SSH.

You can also manage user passwords through the change password and user management features. For more information see “Changing Passwords” on page 252 and “Managing User Accounts” on page 253 respectively.

Configuring Password Strength

Part of an effective security policy is to make sure that users create strong, unique passwords. As an administrator, you can configure a policy that requires that users who log in to the platform create passwords that:

- Are a certain length. The default minimum length is six characters.
Configuring Password Strength

- Use more than one character type. The default is three character types.
- Are not palindromes. Palindromes are words that can be read the same forward and backward such as racecar or the phrase straw warts.

The following section describes how to configure a policy for strong passwords. This policy applies to both regular user passwords and SNMPv3 USM user pass phrases. It does not affect passwords that have already been set.

Table 7-1 lists the password strength options that you can configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Minimum password length | Specifies the minimum number of characters a password must have.  
  **Note** - The minimum pass phrase length for SNMPv3 USM users is always eight characters. If you set this option to less than eight characters, SNMP users still will be unable to create pass phrases of less than eight characters.  
  **Default:** 6  
  **Range:** 6-128 |
Configuring Password Strength

Table 7-1  Password Strength Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password complexity</td>
<td>Password characters are divided into four types: upper case alphabetic (A-Z), lower case alphabetic (a-z), digits (0-9), and other (everything else such as !, #, &amp;). The options for password complexity are:</td>
</tr>
<tr>
<td></td>
<td>• Don’t check—disables complexity checking.</td>
</tr>
<tr>
<td></td>
<td>• Require two character types—requires that passwords are composed of a minimum of two character types, for example, abcABC.</td>
</tr>
<tr>
<td></td>
<td>• Require three character types—requires that passwords are composed of a minimum of three character types, for example, ab1ABC. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• Require four character types—requires that passwords are composed of a minimum of four character types, for example, ab1AB#.</td>
</tr>
<tr>
<td>Default:</td>
<td>Require three characters types</td>
</tr>
<tr>
<td>Check for palindromes</td>
<td>Checks for passwords that are read the same left to right or right to left, such as racecar or the phrase straw warts. The palindrome check is not case-sensitive: racecaR is considered a palindrome.</td>
</tr>
<tr>
<td>Default:</td>
<td>On.</td>
</tr>
</tbody>
</table>

To configure the minimum password length
1. Click Security and Access under Configuration in the tree view.
2. Click Password and Account Management.
3. Enter a number in the Minimum password length text box.
4. Click Apply.
5. Click Save to make your changes permanent.

To configure the number of character types required in a password
1. Click Security and Access under Configuration in the tree view.
2. Click Password and Account Management.
3. Click the radio button corresponding to the number of character types you wish to enforce in passwords.
4. Click Apply.
5. Click Save to make your changes permanent.

**To configure palindrome check**
1. Click Security and Access under Configuration in the tree view.
2. Click Password and Account Management.
3. Click the on radio button for Check for a passwords that are palindromes.
4. Click Apply.
5. Click Save to make your changes permanent.

---

**Configuring Password History Check**

The password history feature checks for the reuse of passwords and forces users to use a new password every time they change their password. The number of previous passwords this feature checks against is defined by the history length.

The password history feature works in concert with the forced password change feature that requires users to use new passwords at defined intervals. Password history check is enabled by default.

The password history check applies to user passwords set by the administrator as well as passwords set by the user. The history check does not apply to SNMPv3 USM user pass phrases.

**Note** - The password history check does not apply to cluster administrator (cadmin) users. These users sometimes need to recreate cluster configurations and might want to reuse the original cluster administrator password when they do so.

The following are considerations you might want to be aware of when you use this feature:

- The password history file for a user is updated only when the user successfully changes password. This means that if you change the history length—for example, change the length from ten to five—the number of passwords stored in the password history file does not immediately change. The next time the user attempts to change password, the new password is checked against all the
Configuring Mandatory Password Change

passwords in the file, which might be more than five. After the password change succeeds, the password file is updated to store only the five most recent passwords.

- A password is entered into a user password history file only if the password history feature is enabled when the user creates the password.
- This feature always checks the new password against the immediately previous password, regardless of whether the previous password is in the password history file or not. For example, when a user changes password for the first time after the password history check is enabled, the previous password is still checked against even though it is not in the history file.

Table 7-2 lists the password history options that you can configure.

### Table 7-2 Password History Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for reuse of passwords</td>
<td>Enables password history checking.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> on.</td>
</tr>
<tr>
<td>History length</td>
<td>Specifies how many passwords are kept and checked against.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 10</td>
</tr>
</tbody>
</table>

**To configure password history check**

1. Click Security and Access under Configuration in the tree view.
2. Click Password and Account Management.
3. Click the on radio button for Check for reuse of passwords (default is on).
4. Enter a number in the history length text box from 1-1000 (default is 10).
5. Click Apply.
6. Click Save to make your changes permanent.

**Configuring Mandatory Password Change**

Forcing users to change their passwords at regular intervals or to change to their administrator-assigned password to their own unique password is another important element in a strong security policy. Using Network Voyager, you can:
Configuring Mandatory Password Change

- Set user passwords to expire after a certain number of days. When a password expires, the user is forced to change the password the next time the user logs in. This feature works in conjunction with the password history check to force users to use new passwords at regular intervals.

- Force users to change their password when they next log in after an administrator has given them a new password.

- Force new users to change their password from their initial administrator-provided password when they log in for the first time.

You have the option of locking out users if they do not change expired passwords within a certain number of days after password expiration. Once a user is locked out, you can unlock the user account from the User Management page (Configuration > Security and Access > Users).

You can also force an individual user to change password the next time the user logs in, independent of any policy you have set up. To do so, use the Force Password Change option on the User Management page. Be aware that users who have access to the User Management page can override a forced password change.

Although the mandatory password change settings can be shared across a cluster, changes to the local user passwords are not propagated over a cluster. In addition, the cadmin user cannot be forced to change their password. This eliminates the risk of having different cadmin passwords on different cluster nodes, which would complicate cluster management. For more information on cadmin configuration see “Creating Cluster Administrator Users”.

This feature does not apply to SNMPv3 USM user pass phrases.

Note - Password history checking and session management must be enabled for mandatory password change to work. See “Configuring Password History Check” and “Network Voyager Session Management” respectively for more information on configuring these features.

Table 7-3 lists the mandatory password change options that you can configure.
Configuring Mandatory Password Change

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password expiration lifetime</td>
<td>Specifies the length of time in days since the last password change before a user is required to change the password again. Once the specified time has passed, the password expires and the user is required to change it the next time the user logs in. The value “never” disables the feature.  &lt;br&gt;<strong>Default:</strong> never &lt;br&gt;<strong>Range:</strong> 1-1827 days or never</td>
</tr>
<tr>
<td>Warn users before password expiration</td>
<td>Specifies the number of days before a password expires that a user starts receiving a password expiration warning message. &lt;br&gt;The warning message appears in the lower right hand corner of the Network Voyager window and in the command line right after the user logs in. &lt;br&gt;<strong>Default:</strong> 7 &lt;br&gt;<strong>Range:</strong> 1-366 days or never</td>
</tr>
</tbody>
</table>
Configuring Mandatory Password Change

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock out users after password expiration</td>
<td>Locks out a user in the specified number of days after password expiration if the user has not changed the password. To allow users an unlimited amount of time in which to change an expired password, enter “never”.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> never</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 1-1827 days or never</td>
</tr>
<tr>
<td>Force users to change passwords at first login after</td>
<td>Forces the user to change password at login after certain events. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Don’t force password change</strong>—disables this feature, but does not disable password expiration lifetime.</td>
</tr>
<tr>
<td></td>
<td>• <strong>User’s password is changed from User Management</strong>—forces a user to change a password after it has been set by the administrator in User Management. This applies both to existing users whose password is being changed by the administrator and to new users whose password is being set for the first time. This does not apply to passwords that have been changed by the user using the Change Current User’s Password page or because of forced change at login.</td>
</tr>
<tr>
<td></td>
<td>• <strong>First password change</strong>—forces a new user to change password the first time the user logs in after the user account has been created and the initial password set.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Don’t force password change</td>
</tr>
</tbody>
</table>

To configure password expiration

1. Click Security and Access under Configuration in the tree view.
2. Click Password and Account Management.
3. In the Mandatory Password Change section, enter the number of days before a password expires in the Password expiration lifetime text box.
Denying Account Access After Failed Login Attempts

4. In the Warn users before password expiration text box, enter how many days before a password expires that a warning message should start displaying.

5. In the Lock out users after password expiration text box, enter how many days after a password expires that a user who has not changed the expired password should be locked out.

6. Click Apply.

7. Click Save to make your changes permanent.

**To configure mandatory user password change**

1. Click Security and Access under Configuration in the tree view.

2. Click Password and Account Management.

3. In the Mandatory Password Change section, click the radio button under Force users to change passwords at first login after that corresponds to your security needs. The selection Don’t force change disables the feature.

4. Click Apply.

5. Click Save to make your changes permanent.

---

**Denying Account Access After Failed Login Attempts**

You can lock out a user for a length of time after a number of failed login attempts. Both the length of time the user is locked out and the number of failed login attempts that trigger a lockout are configurable.

An account that is locked out because of failed login attempts can be unlocked in two ways:

- The user issues no login attempts during the lockout period and then logs in successfully on the first attempt after the lockout period expires.

  If the user issues a login attempt during the lockout period, the lockout period is restarted, whether or not the attempt would have been successful. If, after the lockout period expires, the user’s first attempt to log in is unsuccessful, the user will be locked out again for the full period.

- The administrator manually unlocks the account.

  When a user is locked out, a control appears in the user account information on the User Management page that allows you to manually unlock the account. The reason for the lockout is also given.
Denying Account Access After Failed Login Attempts

When enabling this function, be aware that it leaves the system vulnerable to a denial of service attack. An attacker could lock out an account by issuing the requisite number of failed login attempts and then repeatedly issue login attempts during the lockout period to extend the lockout indefinitely.

**Warning** - If you enable this feature, be careful not to lock out administrator accounts by providing incorrect login information.

Table 7-4 lists the failed login attempts options that you can configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access after failed login attempts</td>
<td>Locks out a user after a configurable number of failed logins.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: off</td>
</tr>
<tr>
<td>Maximum number of failed attempts allowed</td>
<td>Sets the number of failed logins a user can have before being locked out.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 10</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 2-1000</td>
</tr>
<tr>
<td>Allow access again after time</td>
<td>Sets the length of time a user is locked out after failed login attempts. Once this time expires, the user is able to log in again.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 1200 seconds (20 minutes)</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 60-604800 seconds</td>
</tr>
</tbody>
</table>

**To enable deny access after failed login attempts**

1. Click Security and Access under Configuration in the tree view.
2. Click Password and Account Management.
3. In the Deny Access After Failed Login Attempts section, click the on radio button.
4. Enter a number of failed attempts you will allow in the Maximum number of failed attempts allowed text box.
5. Enter the number of seconds the user should be locked out after failed attempts in the Allow access again after time text box.
6. Click Apply.
7. Click Save to make your changes permanent.

### Denying Access to Unused Accounts

You can deny access to accounts that have been inactive for a specified length of time. An account is considered inactive if there has been no logins to the account.

When a user is locked out, a control appears in the user account information on the User Management page that allows you to manually unlock the account. The reason for the lockout is also given.

**Note** - Account lockout for inactivity does not apply to the admin user nor to users logging in on the serial console.

Table 7-5 lists the unused accounts options that you can configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access to unused accounts</td>
<td>Locks out users after they have not logged in for a configurable amount of time.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> off</td>
</tr>
<tr>
<td>Days of non-use before lock-out</td>
<td>Specifies the number of days an account can be inactive (that is, no logins) before the user is locked out.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 365 days</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 30-1827 days</td>
</tr>
</tbody>
</table>
Changing Passwords

Changing Passwords

You can change your own password. Any user with privileges to the Users feature can change the passwords of any user, including the admin and monitor users, without providing the current password.

| Warning | Because a user with read/write permission to the Users feature can change the password of any user, including the admin user, you should be cautious in assigning this permission. |

To change the current user’s password
1. Click Change Password under Configuration in the tree view.
2. Enter your old password in the Old Password text box.
3. Enter your new password and enter it again in the Confirm New Password text box.
4. Click Apply.
5. Click Save to make your changes permanent.

To change another user’s password
1. Log in as a user who has read/write permissions for the Users feature.

| Note | Admin users or any user with the User feature assigned to them can change a user’s password without providing the existing password. |

2. Click Manage User under Configuration > Security and Access > Users in the tree view.
3. In the table for the user whose password you want to change, enter the new password in the New Password and in the Confirm New Password text boxes.
4. If you want to force the user to change password again when the user next logs in, click the yes option for Force Password Change.

| Note | If you have a password management policy in effect that forces a user to change password after you have changed it, the Force Password Change attribute will automatically be set to yes after you click Apply. You do not need to set this option manually. |

5. Click Apply.
6. Click Save to make your changes permanent.
Managing User Accounts

You can use Network Voyager to add users to your IPSO system, and to edit the user ID, group ID, home directory, and default shell for a user. You can also enter a new password for a user and force a user to change their password the next time they log in. For information about how to give privileges to users, see “Role-Based Administration” on page 262.

To view a list of all users, choose Configuration > Security and Access > Users in the tree view. You can also view the user name that you used to log in by clicking Home under Configuration in the tree view.

The following users are created by default and cannot be deleted.

- **admin**—Has full read/write capabilities to all features accessible through Network Voyager and the CLI. This user has a User ID of 0, and thus has all of the privileges of a root user.
- **monitor**—Has read-only capabilities for all features in Network Voyager and the CLI, and can change its own password. You must establish a password for monitor before the account can be used.
- **cadmin**—Has full read/write capabilities to all features on every node of the cluster. This user only appears if clustering is configured on your system.

When you add a new user, the user is given read-only privileges to the Network Voyager home page and CLI prompt but they cannot access other Network Voyager pages or execute commands from the CLI prompt.

**Note** - You can assign administrative privileges or any read/write roles without assigning a user ID of 0. If you assign a user ID of 0 to a user account, the user is equivalent to the Admin user and the roles assigned to that account cannot be modified.

After you create a new user, go to Role-Based Administration > Assign Role to Users to grant the user additional access privileges. For more information, see “Role-Based Administration” on page 262.
Managing User Accounts

Table 7-6 describes the attributes associated with each user account.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| Default Shell                 | Use this field to configure IPSO to time out (end) a shell or CLI session after a specified period of inactivity (a period in which there is no user entry and no active foreground process). When you configure this setting, it does not affect any current shell or CLI session. You can enter:<br>
   • \textit{Hh} to specify the time in hours<br>
   • \textit{M[m]} to specify the time in minutes<br>
   • \textit{HhMm} to specify the time in hours and minutes.<br><br>Default: 0 (no timeout) |
| Name                          | Name used to identify the user. The valid characters are alphanumeric characters, dash (-), and underscore (_).<br><br>Range: 1-32 characters |
| User ID                       | Unique ID number for the user account. The system will not allow you to create a user with a duplicate User ID.<br><br>Range: 0-65535; 0-102 and 65534 are reserved for system use. For example, the admin user is UID 0, the monitor user is UID 102, and the cluster administrator (cadmin) is UID 101. |
| Group ID                      | Primary group for the user. The user can be assigned to other groups as reflected on the Groups page. Files and directories owned by the user are assigned the permissions of that user's primary group.<br><br>Range: 0-65535. Check Point recommends that you reserve 0 to 100 for system use, although this is not enforced. Numbers 0 and 10 are reserved for the predefined Wheel and Other groups respectively. GIDs 65533 & 65534 are also reserved. |
| Home directory                | This is the full UNIX path name of a directory where the user will log in. The home directory for all users must be in /var/emhome/. |
| Shell                         | All users except the admin user are assigned by default to the CLI shell (/etc/cli.sh). |
Managing User Accounts

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Password Change</td>
<td>Forces the user to set a new password the next time the user logs in.</td>
</tr>
<tr>
<td></td>
<td>The initial setting of this attribute reflects the global password management policy regarding forced password changes. If no global password policy is in place or if the conditions of the password policy that force a password change have not been met, this attribute is set to no. If a policy is in place and the conditions that force a password change are met, this attribute is set to yes. You can override the initial setting by manually setting the attribute. When this attribute is set to yes, either by the administrator or by a password policy, the Reason field gives the reason. The attribute is automatically reset to no when the user changes the password the next time the user logs in. <strong>Note</strong> - If a mandatory password change is in effect for users when their passwords are set or changed by the administrator, the system automatically sets this option to yes after you successfully change a user password.</td>
</tr>
<tr>
<td>Locked Out; Unlock</td>
<td>Unlocks the user account. This check box appears only if the user is locked out—for example, for too many failed login attempts. The reason field gives the reason the user is locked out. If the user is locked out because of password expiration and you unlock the account, the user is given the currently configured amount of time to change the expired password. If the user does not change the password before this time expires, the user is locked out again.</td>
</tr>
<tr>
<td>New password</td>
<td>Use this field to enter a new password if you are changing it. <strong>Range</strong>: 6-128 characters. All printable characters are allowed. <strong>Note</strong> - If you use an asterisk (*) in a password, users with that password are unable to log in.</td>
</tr>
<tr>
<td>New password (verify)</td>
<td>Re-enter the new password if you are changing it.</td>
</tr>
</tbody>
</table>
Adding and Deleting Users

In addition to regular users who have access to various features of Network Voyager and the CLI, you can create SNMP users. SNMP users are visible only in the Manage SNMP Users page of Network Voyager, they are not displayed on the system User Management pages. For more information on SNMP users, see “Managing SNMP Users” on page 165.

**Note** - When you add a user with cluster permissions, the user is not automatically created on the other nodes of the cluster. To add this user to other nodes of the cluster, you must log in to each node as a system admin user (cluster admin users do not have RBA access).

**To add a user**

1. Click Users under Configuration > Security and Access Configuration in the tree view.
2. In the Add New User section, enter the name of the user (1–31 characters), a unique user ID, and the home directory for the new user. The home directory must be `/var/emhome/username`.

**Note** - You must complete all fields (Username, UID, and Home Directory). If you do not complete these fields, an error message appears that says “not all fields are complete”.

3. Click Apply.
   An entry for the new user appears on the page.
4. Enter a password in the New password text box and enter it again in the New password (verify) text box.
5. (Optional) Modify the primary Group ID and Shell.
6. (Optional) If you want to force the new user to change password again when the user next logs in, click the yes option for Force Password Change.

**Note** - If you have a password management policy in effect that forces all new users to change their passwords the first time they log on, the Force Password Change attribute automatically sets to yes after you click Apply on this page.

7. Click Apply.
8. Click Save to make your changes permanent.

**To remove a user**

Note - When you add a user with cluster permissions, the user is not automatically created on the other nodes of the cluster. To add this user to other nodes of the cluster, you must log in to each node as a system admin user (cluster admin users do not have RBA access).
Managing and Using S/Key

1. Click Users under Configuration > Security and Access Configuration in the tree view.
2. Select the Off option next the user name.
3. Click Apply.
4. Click Save to make your changes permanent.

**Note** - When you remove a user, that user can no longer log in although the user’s home directory remains on the system. To remove the user’s directory, use the Unix shell. Also, since the user accounts for SNMP are maintained separately, you may need to delete the SNMP account for the user, if there is one. For more information, see “Managing SNMP Users” on page 165.

### Managing and Using S/Key

S/Key is a one-time password system that you can enable to protect the password of admin or monitor accounts when users connect through Telnet or FTP. You must first enable S/Key and then enter an S/Key secret password. After you configure the S/Key for a user, a sequence number and a seed appear before each Telnet or FTP password prompt. Enter these two items as arguments to the S/Key program running on a secure machine. After you enter these arguments and your S/Key secret key, the key program produces a password that you use to log in only once.

**To configure S/Key**

1. Click Users under Configuration > Security and Access Configuration in the tree view.
2. Enable the Admin S/Key or Monitor S/Key by selecting either the Allowed or Required radio buttons.
   - Disabled—S/Key passwords are turned off and cannot be used.
   - Allowed—the user can use either a standard text password or an S/Key one-time password.
   - Required—only S/Key one-time passwords are allowed for connecting through Telnet or FTP.
3. Click Apply.

4. Enter the current standard password in the Current Standard password text box.
Managing and Using S/Key

5. Choose 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.

6. Enter the S/Key secret password again in the S/Key Secret Password (verify) text box.

7. 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**

You must have 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.

*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.

**To use the S/Key**

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.
Managing and Using S/Key

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.

Disabling S/Key

To disable S/Key
1. Click Users under Configuration > Security and Access Configuration in the tree view.
2. Click Disabled in the S/Key Password field.
3. Click Apply.
   The sequence number and seed disappear.
4. Click Save to make your changes permanent.
Managing Groups

You can define and configure groups with IPSO as you can with similar UNIX-based systems. This capability is retained under IPSO for advanced applications and for retaining compatibility with UNIX.

To view a list of all existing groups, click Manage Groups under Configuration > Security and Access > Groups in the tree view.

Two groups are created by default and cannot be deleted:

- **Other group**—All users are assigned by default to the Other group. If you edit a user’s primary group ID to be something other than the default, you can use the Edit Group page to add the user to the Other group. All of the users in the Users group might not appear in the list of current members, because the list does not show users who are added to the group by default, only users who are explicitly added.

- **Wheel group**—Controls which users have root access to the system. Users must be members of the wheel group to use the su command to log in as root.

Use groups for the following purposes:

- Specify UNIX file permissions. By default all users are assigned to the Other group.
- Use the Wheel group to control which users have root access to the system.
- Control who can log in through SSH.

For most other functions that are generally associated with groups, use the role-based administration feature, described in “Role-Based Administration” on page 262.

To add or edit a group

1. Click Groups under Configuration > Security and Access Configuration in the tree view.

2. Under Add Group Name, enter the name (eight or fewer characters) of the new group and a group ID number.

   The group ID must be unique. Suggested values are between 101 and 65000. Range: 0-65535. Check Point recommends that you reserve 0 to 100 for system use, although this is not enforced. Numbers 0 and 10 are reserved for the predefined Wheel and Other groups respectively. GIDs 65533 & 65534 are also reserved.

3. Click Apply.
Managing Groups

The new group information appears on the page.

4. To add a new member to a group, enter the user name in the Add new member text box and click Apply.

5. To delete a member from the group, select the user name from the Delete member text box and click Apply.

6. Click Save to make your changes permanent.
Role-Based Administration

When you add a new user, the user is given read-only privileges to the Network Voyager home page and CLI prompt but cannot access other Network Voyager pages or execute commands from the CLI prompt. You must assign roles to the user to provide additional access privileges.

Role-based administration (RBA) allows IPSO administrators to create and use separate roles. With RBA, an administrator can allow users to access specific features by including the features in a role and assigning the role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to still other features. This feature also provides improved auditing capabilities.

To assign a set of access permissions to a user, create a role that specifies levels of access to features you want to include, then assign this role to the relevant user. You can also specify which access mechanisms (Network Voyager or the CLI) are available to the user when you assign a role to the user.

If your system is part of a cluster, you can create and assign roles that provide access to the entire cluster for the associated features. See “Creating Cluster Administrator Users” for detailed information about this type of user.

Managing Roles

To view a list of existing roles on your system, click Manage Roles under Configuration > Security and Access >Role Based Administration in the tree view.

The following roles are predefined on the system:

- **adminRole**—Gives the user read/write access to every feature on the system.
- **monitorRole**—Gives the user read-only access to every feature on the system.
- **clusterAdminRole**—Gives the user read/write access to every feature on every node in the cluster except for role-based administration. To configure role-based administration, you must log in to each node of the cluster as an admin rather than a cluster admin.
Managing Roles

When you create a new role, you can select only system access features or cluster access features, not a combination of both. Likewise, a single user can only be assigned system roles or cluster roles, you cannot assign an system role and a cluster role to the same user.

**Note** - When you assign a role containing access to a feature to a user, the user gets access to the configuration pages for that feature but not to the monitor pages for that feature. To provide access to the monitor pages, you must include the monitor privilege for that feature in the role definition.

**To add or edit a role**

1. Select one of the following:
   - To add a role, click Add Role under Configuration > Security and Access > Role Based Administration in the tree view.
   - To edit a role, click Manage Roles under Configuration > Security and Access > Role Based Administration in the tree view, then click the name of the role.

**Warning** - Because a user with read/write permission to the Users feature can change the password of any user, including the admin user, you should be cautious in assigning roles that contain this permission.

2. If applicable, select a role type from the Role Type drop-down list.
   
   You might see only one selection, System, meaning that this role will apply to this machine only. The Cluster selection appears only if clustering is enabled. A user account be assigned only roles containing system access features or cluster access features, not a combination of both.

3. If you are adding a role, enter a name in the Role Name text box. The role name can be any combination of letters and numbers, but it must start with a letter.
   
   You cannot edit the name of an existing role.

4. Add features by moving them to the RW (Read/Write) or RO (Read Only) columns, depending on the permission level you want to give to this role.

   Remove the features by moving them back to the Available column. Press Shift-Click to select a range of features, or Ctrl-click to select multiple features one at a time.

**Note** - If you assign the Clustering feature to a user with the role type System, that user can configure clustering on individual nodes but cannot use Cluster Voyager or the CCLI.
Assigning Roles and Access Mechanisms to Users

5. Click Apply.
6. Click Save to make your changes permanent.

To delete a role
1. Click Manage Roles under Configuration > Security and Access > Role Based Administration in the tree view.
2. Check the Delete check box for the role.
3. Click Apply.
4. Click Save to make your changes permanent.

Note - You cannot delete the adminRole, clusterAdminRole, or monitorRole default roles.

Assigning Roles and Access Mechanisms to Users

To give a user permissions for various features, assign the role or roles that contain the feature permissions to the user. You can also specify whether a user can use Network Voyager and the CLI by assigning access mechanisms to the user from the Assign Roles to User page.

When you create a role, you associate a role type. The role types are:

- **System**—A system role assigned to a user provides the user with access to the associated features on this machine only.
- **Cluster**—A cluster role assigned to a user provides the user with access to the associated features on every node in the cluster.

To assign roles and access mechanisms to users
1. Click Assign Role to Users under Configuration > Security and Access > Role Based Administration in the tree view.
2. Click the name of the user to which you want to assign roles.
   The Assign Roles to User page appears.
3. Assign roles to or remove them for the user by selecting them and clicking Assign or Remove.
Creating Cluster Administrator Users

Use Shift-Click to select a range of roles, or Ctrl-click to select multiple roles at a time.

**Note** - You cannot change the roles assigned to the Admin, Cluster Admin, or Monitor users.

4. If you assign a cluster role to a user, you must also assign them the domain value that matches the appropriate cluster ID.
5. Click Apply.
6. Click Save to make your changes permanent.

**Creating Cluster Administrator Users**

You can create users and make them cluster administrators by assigning them a cluster role. Be aware of the following constraints:

- You must log in as a system user to use role-based administration—this feature is not accessible if you log in as a user with a cluster role. (This is also true if you log in as cadmin.)
- If you do not assign the default cluster administrator role (clusterAdminRole) to the users you create, be sure to assign them a role of type Cluster. The implications of this choice are explained below.
  - Users with the role clusterAdminRole automatically log into Cluster Voyager or the CCLI and have full access to all clustering features.
  - Users with the role type Cluster automatically log into Cluster Voyager or the CCLI and have access to the features that you assign to the role.
- To allow a user to administer a cluster, you must assign them the domain value that matches the appropriate cluster ID.
- If you want to log into a node as a cluster administrator, you must create the user on that node. That is, if you create a cluster administrator user on node A but not on node B, you cannot log into node B as this user. However, any changes that you make to node A using Cluster Voyager or the CCLI are also implemented on node B. (You can log into all nodes as cadmin because this user is created automatically on each node.)

**Note** - If you assign the Clustering feature to a user with the role type System, that user can configure clustering on individual nodes but cannot use Cluster Voyager or the CCLI.
### Configuring Network Access and Services

Table 7-7 lists the options that you can configure for network access.

#### Table 7-7  
Network Access Configuration Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Access</td>
<td>Enable or disable FTP access to this appliance. You can use FTP access to obtain configuration files from the appliance. FTP access is disabled by default. You should only enable it when it is specifically required due to the security vulnerabilities inherent in FTP. If you enable FTP access, you usually should require S/Key passwords for the admin and monitor users as described in “Managing and Using S/Key” on page 257.</td>
</tr>
<tr>
<td>FTP Port Number</td>
<td>Specifies the port number on which the FTPD server listens. Normally, this value should be left at 21, the default value.</td>
</tr>
<tr>
<td>TFTP Access</td>
<td>Enable or disable TFTP access to this appliance.</td>
</tr>
<tr>
<td>Telnet Access</td>
<td>Enable or disable Telnet access to this appliance. Telnet access is disabled by default. Once you have enabled SSH and have tested your SSH access, you should disable Telnet access to avoid security vulnerabilities. If you enable Telnet access, you usually should require S/Key passwords for the admin and monitor users as described in “Managing and Using S/Key” on page 257.</td>
</tr>
<tr>
<td>Admin Network Login</td>
<td>Allow or prevent admin login for Telnet access to this appliance. Note that this does not affect admin connections through Network Voyager or FTP.</td>
</tr>
<tr>
<td>COM2 Login</td>
<td>Allow or prevent login on the serial port ttyd1 com2.</td>
</tr>
<tr>
<td>COM3 Login</td>
<td>Allow or prevent login on the serial port ttyd2 com3.</td>
</tr>
<tr>
<td>Allow USB Modem Login</td>
<td>Allow or prevent login through a modem attached to the USB port.</td>
</tr>
</tbody>
</table>
Configuring Network Access and Services

Table 7-8 describes the USB modem configuration parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Sets modem parameters to comply with standards of the specified country.</td>
</tr>
<tr>
<td># of Rings to Answer</td>
<td>Specifies the number of times the incoming call should ring before the modem answers the call.</td>
</tr>
<tr>
<td>Enable Dialback</td>
<td>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.</td>
</tr>
<tr>
<td>Dialback Number</td>
<td>If you enable modem dialback, enter a value in the Dialback Number field. You can enter commas to cause the dialing to pause briefly. To increase the length of the pause, enter multiple adjacent commas, as in 650,,555,,1212.</td>
</tr>
</tbody>
</table>

Table 7-9 lists the services you can enable on the appliance or for the cluster.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo</td>
<td>The echo service sends back to the originating source any data it receives.</td>
</tr>
<tr>
<td>Discard</td>
<td>The discard service throws away any data it receives.</td>
</tr>
<tr>
<td>Chargen</td>
<td>The chargen service sends data without regard to the input. The data sent is a repeating sequence of printable characters.</td>
</tr>
<tr>
<td>Daytime</td>
<td>The daytime service sends the current date and time as a character string without regard to the input.</td>
</tr>
<tr>
<td>Time</td>
<td>The time service sends back to the originating source the time, in seconds, since midnight January 1, 1900. This value is sent as a binary number, not a human-readable string.</td>
</tr>
</tbody>
</table>

To enable network access options and services

1. Click Network Access and Services under Configuration > Security and Access in the tree view.
2. Select the Yes radio button for the access options and services you want to enable.
3. If you are enabling a USB modem, configure it as described in Table 7-8 on page 267.
4. Click Apply.
5. Click Save to make your changes permanent.
Configuring Network Voyager Access

When you set up your system for the first time, perform the following tasks:

- Configure basic Network Voyager options.
- Change your SSL/TLS certificate from the default certificate.

Configuring Basic Network Voyager Options

You can configure the following options for Network Voyager access:

- Allow Network Voyager access (enabled by default)
- Enable session management (enabled by default)
- Specify a Network Voyager SSL/TLS port number
- Require encryption

**Note** - Changes to some of these settings might make Network Voyager unusable. You can use the CLI `set voyager` commands to regain access.

To configure Web access for Network Voyager

1. Click Voyager Web Options under Configuration > Security and Access > Voyager in the tree view.
2. Select Yes for the Allow Voyager Web Access field. This option is selected by default.
3. To enable cookie-based session management, select Yes for the Enable Session Management field.
4. Enter the time interval for which a Network Voyager user is allowed to be logged in without activity in the Session Timeout in Minutes text box. The default value is 20 minutes. If the user closes the browser without logging out, the exclusive configuration lock remains in effect until the session time-out interval expires.
5. Enter the number of the port to use for SSL/TLS-secure connections in the port number text box.

**Warning** - If you uncheck the check box, you must use the CLI to access your IP security platform.
Generating and Installing SSL/TLS Certificates

The default is port 443.

Using the default port allows users to connect to Network Voyager without specifying a port number in the URL. If you change the port number, users must specify a port number in the URL: for example, https://hostname:<portnumber>/.

6. Select the appropriate encryption level for your security needs from the Require Encryption drop-down list; for example, 40-bit key or stronger.

Note - The encryption level you enter is the minimum level of encryption you require. You might obtain stronger encryption by default if your Web browser supports it.

7. Click Submit.

Generating and Installing SSL/TLS Certificates

IPSO uses the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol to secure connections over the Internet from the Network Voyager client to the IPSO system. SSL/TLS, the industry standard for secure Web connections, gives you a secure way to connect to Network Voyager. Creating a unique private key for your security platform and keeping it secret is critical to preventing a variety of attacks that could compromise the security platform security.

When you set up your system for the first time, change your SSL/TLS certificate from the default certificate. IPSO includes a default sample certificate and private key in the /var/etc/voyager_ssl_server.crt and /var/etc/voyager_ssl_server.key files respectively.

The certificate and private key are for testing purposes only and do not provide a secure SSL/TLS connection. You must generate a certificate, and the private key associated with the certificate, to create a secure connection by using SSL/TLS.

Note - For security purposes, generate the certificate and private key over a trusted connection.

Generating an SSL/TLS Certificate and Keys

To generate a certificate and its associated private key

2. Choose the Private Key Size that is appropriate for your security needs.
   The larger the bit size, the more secure the private key. The default and recommended choice is 1024 bits.

3. (Optional) Enter a passphrase in the Enter Passphrase and the Re-enter Passphrase fields.
   The passphrase must be at least four characters long. If you use a passphrase, you must enter the phrase later when you install your new key.

4. In the Distinguished Information section, enter identifying information for your system:
   1. In the Country Name field, enter the two-letter code of the country in which you are located.
   2. In the State or Province Name field, enter the name of your state or province.
   3. (Optional) In the Locality (Town) Name field, enter the name of your locality or town.
   4. In the Organization Name field, enter the name of your company or organization. If you are requesting a certificate from a certificate authority, the certificate authority may require the official, legal name of your organization.
   5. (Optional) In the Organizational Unit Name field, enter the name of your department or unit within your company or organization.
   6. In the Common Name (FQDN) field, enter the common name that identifies exactly where the certificate will go. The common name is most commonly the fully qualified domain name (FQDN) for your platform: for example, www.ship.wwidgets.com. If you are generating a certificate signing request for a CA, that CA might impose a different standard.
   7. (Optional) In the Email Address field, enter the email address to use to contact the person responsible for this system or for its certificate.

5. Select one of the following:
   • Certificate Signing Request (CSR)
     Select this option if you are requesting a certificate from a certification authority. The request will be signed with a SHA-1 hash.
   • Self-Signed X.509 Certificate
Generating and Installing SSL/TLS Certificates

Select this option to create a certificate that you can use immediately, but that will not be validated by a certification authority. The certificate will be signed with a SHA-1 hash.

6. Click Submit.

7. 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.
   1. 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-----.
   2. Store the new private key that your certification authority securely sends. Install the private key and the certificate. (See Installing a Certificate later in this section.)

8. If you generated a *self-signed certificate*, a screen appears that contains a certificate (New X.509 Certificate) and its associated private key.
   You must perform a cut-and-paste operation to move the certificate and the private key to the Voyager SSL Certificate page, as described in the following procedure.

*Installing the SSL/TLS Certificate*

To install the certificate and its associated private key

2. Open the files that contain your certificate and private key.
3. Perform a cut-and-paste operation on your certificate to move it to the New server certificate field in the Install Certificate for SSL page.
   Be sure to include the lines -----BEGIN CERTIFICATE ----- and -----END CERTIFICATE -----.
4. Perform a cut-and-paste operation on your private key to move it to the Associated private key field in the Install Certificate for SSL page.
   Be sure to include the lines -----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----.
5. If you entered a passphrase when you generated the certificate and private key, you must enter the passphrase in the Passphrase field.
6. Click Submit.
Troubleshooting SSL/TLS Configuration

You might have trouble accessing Network Voyager if SSL/TLS is not configured correctly. If you have trouble accessing Network Voyager, try the following remedies.

- Check that you are using the correct URL. When you enable SSL/TLS, you must use `https` rather than `http` when you connect through your Web browser, unless the Redirect HTTP Requests to HTTPS option is enabled.

- 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. You can view the certificate and private key in the `/var/etc/voyager_ssl_server.crt` and `/var/etc/voyager_ssl_server.key` files respectively.

- 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 can help you troubleshoot further and might contain important information for Customer Support should you contact them.
Secure Shell (SSH)

Secure Shell (SSH)

IPSO uses the Secure Shell (SSH) program to provide secure connections for the CLI. SSH 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. SSH provides a connection similar to Telnet or rlogin, except that the traffic is encrypted and both ends are authenticated.

The Check Point 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.

Properly used, SSH 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)

You should use SSH, instead of utilities such as Telnet or rlogin that are not secure, to connect to the system. You can also tunnel HTTP over SSH to use Network Voyager to securely manage your platform.

To use SSH, you must obtain an SSH client for the other end of the connection. SSH clients are available for a number of platforms. Some are free while others are commercial. An SSH client is already installed on your platform; however, you probably want a client to connect from another host, such as your desktop computer, and you must install a client there as well.

Initial SSH Configuration

When you first activate your system, SSH is already enabled and host keys for your platform are generated and installed. SSH automatically authenticates users who log in with the standard password mode of login.
Initial SSH Configuration

You do not need to do any other configuration unless you want users to be able to use public-key authentication as well. To permit public-key authentication, you must first authorize the users’ client identity keys for this system, as described in “Configuring Secure Shell Authorized Keys” on page 278.

To configure SSH

1. Click SSH Configuration under Configuration > Security and Access > Secure Shell (SSH) in the tree view.
2. Select 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.

3. Click Apply.
4. Select whether the admin user can log in with SSH.
   - **Yes**—the admin user can log in using SSH and can use the password mode of authentication to do so. This is the default setting.
   - **No**—the admin user cannot log in.
   - **Without Password**—the admin user can log in, but must use public-key authentication to do so.

5. Click Apply.

   **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 Check Point does not recommend using it.

6. Click Apply.
7. (Optional) In the Configure Server Protocol Details field, click the version of SSH to be used. The default is both 1 and 2.
8. (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.
9. Click Apply.
10. (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.
11. Click Apply.
Configuring Advanced Options for SSH

12. (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.

13. Click Apply.

14. Click Save to make your changes permanent.

Note - When you generate new keys, you might need to change the configurations of each client, or the clients might return errors. For more information, see your SSH client documentation.

Configuring Advanced Options for SSH

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 configure advanced options

1. Click SSH Server Advanced Options under Configuration > Security and Access > Secure Shell (SSH) in the tree view.

2. 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.

3. Click Apply.

4. (Optional) In the Configure Server Access Control table, enter the group and user names in the appropriate text boxes.

You can use wild card characters when you specify multiple group or user names separated by spaces.

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 “Managing User Accounts” on page 253 and “Managing Groups” on page 260.

5. Click Apply.

6. Click the option to use in the Permit Admin User to Log In field.
Configuring Advanced Options for SSH

The default is Yes, which allows the admin user to log in using SSH.

7. Click Apply

8. 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 Check Point does not recommend using it.

9. Click Apply

10. (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.

11. Click Apply

12. (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 the this field, the setting reverts to the default setting.

13. Click Apply.

14. (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>Allow remote connections to forward ports</td>
<td>No</td>
</tr>
<tr>
<td>Ignore user’s own known_hosts file</td>
<td>No</td>
</tr>
<tr>
<td>Ignore .rhosts and .shosts files</td>
<td>Yes</td>
</tr>
<tr>
<td>Time (seconds) before regenerating server key</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Login grace time (sec)</td>
<td>600 seconds</td>
</tr>
<tr>
<td>Max unauthenticated connections</td>
<td>10</td>
</tr>
</tbody>
</table>
Configuring Secure Shell Authorized Keys

15. Click Apply.
16. (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.
17. Click Apply.
18. Click Save to make your changes permanent.

**Configuring Secure Shell Authorized Keys**

Secure Shell (SSH) authorized keys allows you to 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 SSH Authorized Keys under Configuration > Security and Access > Secure Shell (SSH) in the tree view.

   **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.

2. Select the user name from the Username drop-down list.
3. Complete the following, depending on the authorized key you are adding.

   - To add 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.
   - To add 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.
Changing Secure Shell Key Pairs

- To add 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.

4. Click Apply.
5. 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 SSH Key Pairs under Configuration > Security and Access > Secure Shell (SSH) in the tree view.
2. (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.
3. Click Apply.
4. (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.
5. Click Apply.
6. (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.
7. Click Apply.
8. Click Save to make your changes permanent.

Note - The most secure value is 1024 bits. Values over 1024 bits cause problems for some clients, including those based on RSAREF.

3. Click Apply.
4. (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.
5. Click Apply.
6. (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.
7. Click Apply.
8. 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 SSH Key Pairs under Configuration > Security and Access > Secure Shell (SSH) in the tree view.
2. Click the View/Create Identity Keys for User ‘user name’ link for the appropriate user.
3. To create an RSA or DSA identity, select the key length in the appropriate section:
   • 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.
   • 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.
   • 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.
4. Enter the passphrase in the Enter password field, and then again to verify it.
5. Click Apply.
6. 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. Depending on what type of terminal you are using complete the following.
   • From a UNIX terminal—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
```
Tunneling HTTP Over SSH

- **From a Windows terminal**—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.
  4. 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.
  5. Click OK twice to return to the connection dialog box.
  6. Press OK to connect to the remote host.

**Note** - 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.
Network Voyager Session Management

IPSO session management lets administrators prevent multiple users from making simultaneous configuration changes, whether they are using Network Voyager or the CLI. When you log in, you can 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 period of inactivity that you can specify, or the user can manually log out at any time.

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.

For information about configuration locks and instructions about how to override a configuration lock, see “Obtaining a Configuration Lock” on page 25.

Enabling or Disabling Session Management

Note - Your browser must be configured to accept cookies to enable session management.

To enable or disable session management
2. Select Yes for Enable Cookie-Based Session Management to enable session management; select No to disable session management.
3. Click Apply.

A new login window opens. See “Obtaining a Configuration Lock” on page 25.
4. Close your browser and make a new connection to the system.

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, the configuration lock remains in effect until the interval expires.

To set the session timeout interval
Configuring Session Timeouts

1. Click Voyager Web Options under Configuration > Security and Access > Voyager in the tree view.
2. In the Session Timeout text box, enter the time in seconds. The default is 20 minutes.
3. Click Submit.
Authentication, Authorization, and Accounting (AAA)

The AAA component of the system manages user access to the appliance. Generally, AAA includes Authentication (identifying a user), Authorization (determining what a user is permitted to do), and Accounting (tracking some aspects of a user's activity).

Check Point IPSO implements Pluggable Authentication Modules (PAM), an industry-standard framework for authenticating and authorizing users. Using PAM, authentication, account management, and session management algorithms are contained in shared modules that you configure on your appliance.

Note - Generally, AAA uses the terms authentication, authorization, and accounting while PAM uses related, but not quite identical, terms authentication, account management, and session management. In particular, note that “accounting” is not the same as “account management.”

Warning - If you configure a system so that users can be authenticated only by a PAM-based method (you disable local authentication), you cannot log in using a console connection.

Configuring AAA Service Modules

To configure a new AAA service on your appliance, you configure a service module that is then shared by applications which need to invoke authentication, account management, or session management algorithms.

When you create or modify a service module profile, you specify the service profile it will use. Each service profile is composed of the authentication profiles, account management profiles, and session profiles that it uses. For each type of profile (authentication, account management, and session), you can specify multiple service profiles using stacking.

Names of service modules and profiles can be composed of alphanumeric and underscore (_) characters.

Note - Check Point strongly recommends that you adopt a naming convention.

The following service modules are included by default and cannot be deleted:
Configuring AAA Service Modules

- httpd
- login
- other
- snmpd
- sshd

However, you can modify any of these service modules by modifying the service profiles it uses, or by modifying the authentication, account management, or session profiles that are likewise used by a service profile.

You cannot delete services or profiles if they are referenced by other definitions. For example, if the service `my_service` uses the profile `my_profile`, you cannot delete `my_profile` until you delete `my_service`. You can delete both a service and any or all of its profiles at the same time.

To configure a service module

1. Click AAA under Configuration > Security and Access in the tree view.
2. You can use an existing session profile, modify an existing session profile, or create a new one. The session profile contains information about how to assign IP addresses to sessions.
   1. If you are creating a new session profile, scroll down to the Session Profile table and enter a name profile in the New Sess. Profile text box. The name must not match the name of any existing session profiles.
   2. Select the profile type from the drop-down list for the new session profile, or for an existing session profile.
      Select from the following types:
      - PERMIT—Does nothing, always returns success. (pam_permit.so.1.0 module)
      - UNIX—Logs a message to indicate that a session has started or stopped. Checks whether the password is still valid. (pam_unix_sess.so.1.0 module)
3. Select a value from the Control drop-down list. For information on control types, see Table 7-10 on page 288.
4. Click Apply.

Note - These modules reside in the `/usr/lib` directory.
Configuring AAA Service Modules

3. You can use or modify existing account management or authentication profiles or create new ones:
   1. Scroll to the Account Management Profile Configuration section or the Authentication Profile Section.
   2. Modify the existing profile by using the associated drop-down lists, or, if you are creating a new profile, enter a name in the New Profile text box that does not match any existing profile names.
   3. Select the profile type from the drop-down list.
      • For Account Management profiles, the choices are PERMIT and UNIX, described in step 2, above.
      • For Authentication profiles, the choices are described in Table 7-11 on page 288.
   4. Select control type from the drop-down list. For information on the control types, see Table 7-10 on page 288.
   5. Click Apply.

4. You can use or modify an existing service profile or define a new one. Service profiles describe the characteristics of the PAM service module, by referencing specific Authentication, Accounting and Session profiles.
   1. Scroll to the Service Profile Configuration Section.
   2. If you are creating a new service profile, enter a name in the Service Profile text box that does not match any existing service profile names. If you are modifying an existing service profile, enter the name of the profile you want to modify.
   3. Enter names of existing authorization, account, and session profiles which you want this service profile to use. Leave any of these text boxes blank if the service requirements do not include them. You can include multiple services of any type (authentication, account management, or session).

Note - Profiles are invoked in the order that they appear in the relevant list (top to bottom). When you add profiles, they are added to the end of the list. To change the order, delete the profiles that are out of order and add them back in the desired order.

4. Click Apply.

5. Modify an existing service module:
   1. Enter the name of the service profile that you want the service module to reference in the Profile text box.
2. Click Apply.
6. Click Save to make your changes permanent.

Note - If multiple authentication servers are configured for the same user, the roles for the user should be identical on all the servers. If the roles are different, the role assigned in the last server (the one lowest in the list) will be used.

To delete a service module or service profile
1. Click the Delete check box for the module or profile you want to delete.
2. Click Apply.
3. Click Save to make your changes permanent.

Note - You cannot delete a profile that is used by a service module or another profile. You also cannot delete any of the default service modules or profiles.

To remove a profile from a service profile
To remove a profile (authentication, accounting, or session) from a service profile, perform this procedure:
1. Select the authentication, accounting, or session profile in the appropriate service profile.
2. Click the Delete check box for the service profile.
3. Click Apply.
4. Click Save to make your changes permanent.

Note - The authentication and accounting profiles that begin with “tally” and “nonuse” are used by certain Password and Account Management features and are required for the features to work.

Table 7-10 describes the profile control types used to determine how the results of multiple authentication, accounting, or session algorithms are handled and when multiple items are defined in the auth. profile, acct. profile or session profile lists for a given Service Profile, a feature known as stacking. (You specify lists of
Configuring AAA Service Modules

algorithms by defining multiple entries under the Auth. Profile, Acct. Profile, and Session Profile columns of a Service Profile). Values other than required are effective only when the service requires more than one profile.

Table 7-10  Profile Control Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>The result is retained and the next algorithm is invoked. If the algorithm is at the end of the list, 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>A result of failure is reported immediately and no further algorithms are invoked. If the algorithm is at the end of the list, the result is reported immediately.</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. If the algorithm is at the end of the list, the result is reported immediately.</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. If the algorithm is at the end of the list, a result of success is reported.</td>
</tr>
<tr>
<td>nokia-server-auth-sufficient</td>
<td>Used in Auth. Profiles only. It is the same as sufficient, except that a result of 'authentication error' for this algorithm is reported immediately and no further algorithms are invoked.</td>
</tr>
</tbody>
</table>

This type is intended for use with algorithms that access remote servers and where the modules have different result codes for 'authentication error' and 'server not reachable'.

Table 7-11 describes the authentication algorithms that are available in the drop-down list when you create a new authentication profile.

Table 7-11  Authentication Profile Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMIT</td>
<td>Does not do any authentication. Is considered to succeed when invoked.</td>
</tr>
<tr>
<td></td>
<td>Module: pam_permit.so.1.0</td>
</tr>
<tr>
<td>DENY</td>
<td>When invoked, always fails (acts as if a wrong password were entered).</td>
</tr>
</tbody>
</table>
Configuring AAA Service Modules

### Table 7-11  Authentication Profile Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>A client/server authentication system which offloads authentication processing and some other management functions from the IPSO system to a RADIUS server. Defined in RFC2865. Requires additional configuration, as described in “Configuring RADIUS” on page 290.*</td>
</tr>
<tr>
<td></td>
<td>Module: pam_radius_auth.so.1</td>
</tr>
<tr>
<td>ROOTOK</td>
<td>Performs one task: if the user ID is 0, it returns success. It can be used to allow password-free access to some services for root. Caution: This module can bypass password checking, which in some cases might be undesirable.</td>
</tr>
<tr>
<td></td>
<td>Module: pam_rootok_auth.so.1.0</td>
</tr>
<tr>
<td>TACPLUS</td>
<td>A client/server authentication system, which offloads authentication processing and some other management functions from the IPSO system to a RADIUS server. Requires additional configuration, as described in “Configuring TACACS+” on page 294.</td>
</tr>
<tr>
<td></td>
<td>Module: pam_tacplus_auth.so.1.0</td>
</tr>
<tr>
<td>TALLY</td>
<td>Maintains a count of attempted accesses and resets count on success.</td>
</tr>
<tr>
<td></td>
<td>Module: pam_tally_auth.so.1.0</td>
</tr>
<tr>
<td>UNIX</td>
<td>Uses the local password database to authenticate the user. When the user enters user name and password, this module is called to authenticate the user.</td>
</tr>
<tr>
<td></td>
<td>Module: pam_unix_auth.so.1.0</td>
</tr>
</tbody>
</table>

Note - Modules are located in the /usr/lib directory.
Configuring RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client/server 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. A host contacts a RADIUS server, which determines who has access to that service. IPSO will accept users configured on a RADIUS server even if there is no corresponding local account on the Check Point system (assuming that you configure the RADIUS server and IPSO appropriately). See “Configuring Nonlocal RADIUS Users” on page 292 for more information.

You can configure RADIUS as an AAA module so that your appliance functions as a RADIUS client. Check Point systems do not include RADIUS server functionality.

You can configure your appliance to contact more than one RADIUS server. If the first server in the list is unreachable, the next RADIUS server in the priority ranking is contacted to provide the functionality. You can remove a server at any time by checking the Delete check box next to the row for the server you want to remove.

In the following procedure, these names are used for purposes of example:

- Auth Profile is called RADIUS_httpd_authprofile.
- Service profile is called RADIUS_prof_httpd.
- Username is cpadmin.

To configure RADIUS client on your appliance

1. Click AAA under Configuration > Security and Access in the tree view.
2. Create an authorization profile called RADIUS_httpd_authprofile:
   1. Scroll to the Auth. Profile section.
   2. Enter RADIUS_httpd_authprofile in the New Auth. Profile text box.
   3. Click the Type drop-down list and select RADIUS.
   4. Select a control type from the drop-down list. For descriptions of profile control types, see Table 7-10 on page 288.
   5. Click Apply and click Save to make your changes permanent.

   The name of the RADIUS authentication profile appears in the Auth. Profile table. A link labeled Servers also appears in the same row.

3. Specify the RADIUS servers this client will use:
   1. Scroll to the Service Profile section and click the Servers link for the profile you just created.
Configuring RADIUS

The AAA RADIUS Authorization Servers Configuration page appears.

2. Enter values in the following fields:

- **Priority**—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. You can configure multiple servers for a profile, and the priority value determines which server to try first. A smaller number indicates a higher priority.

- **Host address**—Enter the IP address of your RADIUS server. RADIUS supports only IPv4 addresses.

- **Port number**—Enter the port number of the UDP port to contact on the server host. The default is 1812, which is specified by the RADIUS standard. The range is 1 to 65535.

- **Secret**—Enter the shared secret used to authenticate the authorization profile between the RADIUS server and the local client. Enter a text string without a backslash. You must also configure this same value on your RADIUS server. 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.

- **Timeout** (optional)—Enter the number of seconds the system waits for a response after contacting the server. The default value is 3. Depending on your client configuration, if the client does not receive a response, it retries the same server or attempts to contact another server.

- **Max Tries** (optional)—Enter the maximum number attempts to contact the server. The default is 3. If all the attempts do not make a reliable connection within the timeout period, the client stops trying to contact the RADIUS server.

**Warning** - 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.

**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.

3. Click Apply.

4. Click Save to make your changes permanent.
Configuring RADIUS

5. To configure additional RADIUS authentication profiles, repeat this procedure 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.

4. Create a service profile:
   1. Scroll to the Service Profile section.
   2. Enter the following values in the appropriate text boxes:
      - **Service profile**—Enter RADIUS_prof_httpd. This is the name of the authorization profile you created in step 2.
      - **Acct. Profile**—Enter base_httpd_acctprofile.
      - **Session Profile**—Enter base_httpd_sessprofile.
   3. Click Apply, then click Save to make your changes permanent.

5. Associate the service module httpd with the RADIUS_prof_httpd profile.

6. Click Users under Configuration > Security and Access, and create a user called cpadmin with UID=0 and home directory of /var/emhome/cpadmin. This user is shown for purposes of example; you can also use any other locally-configured user.

7. Configure the cpadmin user and password on your RADIUS server.

8. Test Network Voyager access by using the RADIUS login ID cpadmin.

**Configuring Nonlocal RADIUS Users**

To allow access by nonlocal users (users defined on a RADIUS server but not defined on the Check Point system), you must configure the RADIUS server and Check Point system appropriately.

- **Note** - If you configure a RADIUS user with a blank password (on your RADIUS+ server), IPSO will not grant access to that user.

**To configure a RADIUS server for nonlocal IPSO users**

1. Copy the file nokiaipso.dct (for Steel-Belted RADIUS servers) or dictionary.nokia (for freeRADIUS servers) to your RADIUS server.
   These files are in /etc on the Check Point system.
2. Define the user roles by adding the following Check Point vendor-specific attribute (VSA) for the appropriate users in your RADIUS user configuration file:

   Nokia-IPSO-User-Role =
   "role1[domain1;domain2;....],role2[domain1:....]

   For example:

   Nokia-IPSO-User-Role = "foorole, barrole"
   Nokia-IPSO-User-Role = "foorole:foodomain, barrole"
   Nokia-IPSO-User-Role = "foorole:foodomain;bardomain,
   barrole:foodomain;bardomain"

   Note - Make sure the role names match existing roles in the IPSO system.

   If a nonlocal user is a cluster administrator, you must also specify the cluster ID, as in

   Nokia-IPSO-User-Role = "clusterAdminRole:100"

   in which 100 is the cluster ID.

3. Specify whether the Check Point users should have superuser access to the IPSO shell by adding the following VSA:

   Nokia-IPSO-SuperUser-Access = <0|1>

   in which

   • 0 provides nonsuperuser access
   • 1 provides superuser access

   To configure a Check Point system for nonlocal users

   1. On your Check Point system, create the roles that are to be assigned to the nonlocal users.

   2. Create an authentication profile of type RADIUS and set the control level to sufficient.

   3. Add the new authentication profile to each appropriate service profile.

   4. Make the RADIUS authentication profile the first authentication mechanism for each appropriate service by deleting the other authentication profiles for each service and then adding them back again.
Configuring TACACS+

The other profiles are then added after the RADIUS authentication profile. See step 4 on page 286 for information about adding an authentication profile to a service. See “To remove a profile from a service profile” on page 287 for more information about deleting an authentication profile from a service.

5. For critical users, you should configure the Check Point system to allow access even if the RADIUS server is unavailable:
   1. Create local accounts for these users.
   2. If necessary, add a local authentication profile after the RADIUS profile for all the service profiles.

To log in as a superuser

If the Check Point Superuser VSA is set to 1 for a nonlocal user, they can log into the IPSO shell with superuser privileges if they perform the following procedure:

1. Log into the system using command line.
   The default shell is the IPSO CLI.
2. Enter
   shell
   to access the IPSO shell.
3. Enter
   sudo /usr/bin/su -
   The user now has superuser privileges.

Configuring TACACS+

The TACACS+ (Terminal Access Controller Access Control System) authentication protocol allows a remote server to authenticate users on behalf of the IPSO system. IPSO will accept users configured on a TACACS+ server even if there is no corresponding local account on the Check Point system (assuming that you configure the TACACS+ server and IPSO appropriately). See “Configuring Nonlocal TACACS+ Users” on page 296 for more information. All information sent to the TACACS+ server is encrypted.

IPSO supports TACACS+ for authentication only, and not for accounting. Challenge-response authentication, such as S/Key, over TACACS+ is not supported.
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. If the server fails or is unreachable, the password is not recognized and the user is not allowed access.

**To configure TACACS+ servers for a single authentication profile**

1. Click AAA under Configuration > Security and Access in the tree view.
2. Create a TACACS+ authorization profile:
   1. Scroll to the Auth. Profile Section.
   2. Enter a name in the New Profile text box which does not match any existing profile names.
   3. From the profile type drop-down list, select TACPLUS. See Table 7-11 on page 288 for descriptions of the profile types.
   4. Select a control type from the drop-down list. For descriptions of control types, see Table 7-10 on page 288.
   5. Click Apply, and then click Save to make your changes permanent.

The name of the TACACS+ authentication profile appears in the Auth. Profile table. A link labeled Servers also appears in the new row.

3. Configure one or more TACACS+ servers for the authentication profile you created:
   1. In the Auth. Profile table, click the Servers link in the row for the TACACS+ authorization profile you configured in step 2.

   The AAA TACACS+ Authorization Servers Configuration page appears.

   2. Enter values in the following text boxes:
      - **Priority**—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. You can configure multiple servers for a profile, and the priority value determines which server to try first. A smaller number indicates a higher priority.
      - **Host address**—Enter the IP address of the TACACS+ Server. TACACS+ supports only IPv4 addresses.
      - **Port number**—Enter the port number of the TCP port to contact on the server host. The default is 49, as specified by the TACACS+ standard. The range is 1 to 65535.
Configuring TACACS+

- **Secret**—Enter the shared secret used to authenticate the authorization profile between the TACACS+ server and the local client. You must also configure this same value on your TACACS+ server. Enter a text string without a backslash.

- **Timeout** (optional)—Enter the number of seconds to wait for a response after contacting the server. Depending on your client configuration, if the client does not receive a response, it retries the same server or attempts to contact another. The default is 3.

3. Click Apply, and then click Save to make your changes permanent.

4. Repeat step 2 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.

5. Repeat step 3 of this procedure to configure additional AAA TACACS+ authentication servers for existing TACACS authentication profiles.

6. Associate the service module `httpd` with the name of the TACACS+ authorization profile that you created in step 2.

**Configuring Nonlocal TACACS+ Users**

To allow access by nonlocal users (users defined on a TACACS+ server but not defined on the Check Point system), you must configure the TACACS+ server and Check Point system appropriately.

**Note** - If you configure a TACACS+ user with a blank password (on your TACACS+ server), IPSO will not grant access to that user.

To **configure a TACACS+ server for nonlocal IPSO users**

1. Define the following IPSO-specific service in your TACACS+ server:

   ```
   service = nokia-ipso {
     Nokia-IPSO-User-Role = "role_name_on_IPSO"
     Nokia-IPSO-SuperUser-Access = <0|1>
   }
   ```

   **Note** - Make sure the role name matches an existing role in the IPSO system.
Configuring TACACS+

In

Nokia-IPSO-SuperUser-Access = <0|1>
• 0 provides nonsuperuser access
• 1 provides superuser access

2. Configure the appropriate user accounts in the TACACS+ server. The following is an example:

```
#key = password
group = ipso-admin {
service = nokia-ipso {
Nokia-IPSO-User-Role = "adminRole"
Nokia-IPSO-SuperUser-Access = 1
}
}

#IPSO admin users
user = admin {
member = ipso-admin
login = cleartext changeme
}
user = Landon {
member = ipso-admin
login = cleartext changeme
}
Cluster administrator role for cluster ID 100

group = cluster-admin {
service = nokia-ipso {
Nokia-IPSO-User-Role = "clusterAdminRole:100"
Nokia-IPSO-SuperUser-Access = 1
```
Configuring TACACS+

{ }

# Cluster administrator users
user = cadmin {
    member = cluster-admin
    login = cleartext changeme
}

user = Mia{
    member = cluster-admin
    login = cleartext changeme
}

If a nonlocal user is a cluster administrator, you must also specify the cluster ID, as in

Nokia-IPSO-User-Role = "clusterAdminRole:100"

in which 100 is the cluster ID.

To configure a Check Point system for nonlocal users

1. On your Check Point system, create the roles that are to be assigned to the nonlocal users.

2. Create an authentication profile of type TACACS+ and set the control level to sufficient.

3. Add the new authentication profile to each appropriate service profile.

4. Make the TACACS+ authentication profile the first authentication mechanism for each appropriate service by deleting the other authentication profiles for each service and then adding them back again.

   The other profiles are then added after the TACACS+ authentication profile. See step 4 on page 286 for information about adding an authentication profile to a service. See “To remove a profile from a service profile” on page 287 for more information about deleting an authentication profile from a service.

5. For critical users, you should configure the Check Point system to allow access even if the TACACS+ server is unavailable:
Configuring TACACS+

1. Create local accounts for these users.
2. If necessary, add a local authentication profile after the TACACS+ profile for all the service profiles.

To log in as a superuser

If TACACS+ allows a nonlocal user superuser access, the user must also perform the following procedure to obtain superuser privileges in the IPSO shell:

1. Log into the system using command line.
   The default shell is the IPSO CLI.
2. Enter
   
   shell

   to access the IPSO shell.
3. Enter
   
   sudo /usr/bin/su -

   The user now has superuser privileges.
Encryption Acceleration

The Check Point encryption accelerator cards provide high-speed cryptographic processing that enhance the performance of virtual private network (VPN) tunnels. By taking over cryptographic processing, the cards allows the appliance CPU to perform other tasks.

These cards include the Check Point Encryption Accelerator Card and the Check Point 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 Accelerator Cards

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. Click IPSec under Security and Access in the tree view.
2. Scroll down the page and click IPSec Advanced Configuration.
3. At Hardware Device Configuration, click On.
4. Click Apply to enable the card.

Monitoring Cryptographic Acceleration

You can also monitor encryption accelerator card interfaces with Network Voyager.

To monitor the encryption accelerator cards, click Cryptographic Accelerator Statistics under Monitor > Hardware Monitoring in the tree view.
Chapter 8
Configuring Routing

This chapter describes the IPSO routing subsystem, how to configure the various routing protocols that are supported, route aggregation, and route redistribution.

Routing Overview ........................................... page 302
OSPF ......................................................... page 306
RIP ........................................................ page 321
PIM ......................................................... page 327
Static Multicast Routes ........................................... page 347
IGRP ......................................................... page 348
DVMRP .................................................... page 355
IGMP ......................................................... page 358
Static Routes ................................................. page 363
Route Aggregation ............................................ page 368
Route Rank .................................................. page 371
BGP ......................................................... page 374
Route Redistribution ........................................... page 418
Inbound Route Filters ........................................ page 426
Routing Overview

The Check Point routing subsystem, Ipsilon Scalable 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. IPSRD provides routing protocols, allows routes to be converted or redistributed between routing protocols, and, when there are multiple protocols with a route to a given destination, allows you to specify a ranking of protocols. Based on the ranking, a single route is installed in the forwarding table for each destination.

You can monitor routing by following links from Network Voyager.

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” on page 363. For more information on aggregate routes, see “Route Aggregation” on page 368.

NAT

Network Address Translation (NAT) is an IETF standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

- **Interface**—Specifies whether NAT is enabled on the specified interface. User can select only one internal and only one external interface.
  - **Options:** On/Off.
  - **Default:** Off.
Routing Protocols

- **External translated address**—External translated address to be configured by the user. The address configured will be the translation for all the internal addresses.
  - **Range:** Dotted-quad ([0-255],[0-255],[0-255],[0-255]).
  - **Default:** None.

**RIP**

RIP is a commonly used IGP. RIP version 1 is described in RFC 1058, and RIP version 2 is described in RFC 1723. IPSRD supports these version, as well as RIPng, which supports IPv6 interfaces.

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.

**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 is described in RFC 2328. 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. Instead, BGP uses TCP as its underlying transport mechanism and sends update only when necessary.

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.

**Route Maps**

Route maps are used to control which routes are accepted and announced by dynamic routing protocols. Use route maps to configure inbound route filters, outbound route filters and to redistribute routes from one protocol to another.

You can define route maps only using the CLI, this feature is not available in Network Voyager. For information on route map commands, see the CLI Reference Guide.

Route maps support both IPv4 and IPv6 protocols, including RIP, BGP, RIPng, OSPFv2, and OSPFv3. BGP-4++ policy can only be specified using route maps. For the other protocols, you can use either route maps or the Route Redistribution and
Inbound Route Filters features that you configure using Network Voyager. Route map for import policy corresponds to Inbound Route Filters; route map for export policy corresponds to Route Redistribution.

**Note** - Route maps offer more configuration options than the Network Voyager configuration for route redistribution and inbound route filters. They are not functionally equivalent.

Protocols can use route maps for redistribution and Network Voyager settings for inbound route filtering and vice versa. However, if one or more route maps are assigned to a protocol (for import or export) any corresponding Network Voyager configuration (for route redistribution or inbound route filters) is ignored.
OSPF

OSPF

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.

You can run OSPF over a route-based VPN by enabling OSPF on a virtual tunnel interface (VTI). You must use an unnumbered interface for the VTI.

Types of Areas

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, of the following types:

• Normal Area—Allows all LSAs to pass through. The backbone is always a normal area.

• Stub Area—Stub areas do not allow Type 5 LSAs to be propagated into or throughout the area and instead depends on default routing to external destinations. You can configure an area as a stub to reduce the number of entries in the routing table (routes external to the OSPF domain are not added to the routing table).

• NSSA (Not So Stubby Area)—Allows the import of external routes in a limited fashion using Type-7 LSAs. NSSA border routers translate selected Type 7 LSAs into Type 5 LSAs which can then be flooded to all Type-5 capable areas. Configure an area as an NSSA if you want to reduce the size of the routing table, but still want to allow routes that are redistributed to OSPF.
Area Border Routers

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. Check Point 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 2328 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 Check Point 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). These are the routes calculated from Type 5 LSAs.
High Availability Support for OSPF

- **NSSA ASE Router**—Have destinations external to AS. These are the routes calculated from Type 7 LSAs.

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 Support for OSPF**

**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.

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 “Choosing Global Settings” on page 131.

**Note** - You must use monitored-circuit VRRP, not VRRP v2, when configuring virtual IP support for OSPF or any other dynamic routing protocol.

IPSO also supports OSPF over VPN tunnels that terminate at a VRRP group. Only active-passive VRRP configurations are supported. Active-active configurations are not supported.

**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.

**Note** - IPSO does not support OSPFv3 in an IP cluster.
Check Point strongly recommends that you not configure OSPF or any other routing protocol on the primary or secondary cluster protocol interfaces of an IP cluster.

**Configuring OSPF**

To configure OSPF on your system, you must complete the following:

1. **Specify a Router ID.**

   The Router ID 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.

   Check Point 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.

2. **Define the OSPF areas, and global settings on each platform, as described in “Configuring OSPF Areas and Global Settings.”**

3. **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 > Routing Configuration > OSPFv3.
Configuring OSPF

**Configuring OSPF Areas and Global Settings**

Table 8-1 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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add New Address Range | You can configure any area with any number of address ranges. Use these ranges to reduce the number of routing entries that a given area emits into the backbone and thus all areas. If a given prefix aggregates a number of more specific prefixes within an area, you can configure an address that becomes the only prefix advertised into the backbone. You must be careful when configuring an address range that covers parts of a prefix not contained within the area. By definition, an address range consists of a prefix and a mask length.  

**Note:** You can prevent a specific prefix from being advertised into the backbone, by selecting On in the Restrict field next to the entry for that prefix. |
| Add New Stub Network | OSPF can advertise reachability to prefixes that are not running OSPF using a stub network. The advertised prefix appears as an OSPF internal route and can be filtered at area borders with the OSPF area ranges. The prefix must be directly reachable on the router where the stub network is configured; that is, one of the router's interface addresses must fall within the prefix to be included in the router-LSA. You configure stub hosts by specifying a mask length of 32.  
This feature also supports advertising a prefix and mask that can be activated by the local address of a point-to-point interface. To advertise reachability to such an address, enter an IP address for the prefix and a cost with a value other than zero. |
| Area Type           | Choose Normal, Stub, or NSSA. For descriptions of area types, see “Types of Areas” on page 306.                                              |
Configuring OSPF

Table 8-2 describes the configuration parameters for stub areas. These fields appear if you define the area as a stub area.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost for Default Route</td>
<td>Enter a cost for the default route to the stub area. Range: 1-16777215. There is no default.</td>
</tr>
<tr>
<td>Import Summary Routes</td>
<td>Specifies if summary routes (summary link advertisements) are imported into the stub area or NSSA. 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. Default: On.</td>
</tr>
</tbody>
</table>

Table 8-3 describes the configuration parameters for NSSA areas. These fields appear if you define the area as an NSSA (Not So Stubby Area). For more information on NSSA, see RFC 3101.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translator Role</td>
<td>Specifies whether this NSSA border router will unconditionally translate Type-7 LSAs into Type-5 LSAs. When role is Always, Type-7 LSAs are translated into Type-5 LSAs regardless of the translator state of other NSSA border routers. When role is Candidate, this router participates in the translator election to determine if it will perform the translations duties. If this NSSA router is not a border router, then this option has no effect. Default: Candidate.</td>
</tr>
<tr>
<td>Translator Stability Interval</td>
<td>Specifies how long in seconds this elected Type-7 translator will continue to perform its translator duties once it has determined that its translator status has been assumed by another NSSA border router. This field appears only if an area is defined as an NSSA with translator role as Candidate. Default: 40 seconds.</td>
</tr>
<tr>
<td>Import Summary Routes</td>
<td>Specifies if summary routes (summary link advertisements) are imported into the stub area or NSSA. 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. Default: On.</td>
</tr>
</tbody>
</table>
To configure OSPF, use the following procedure.

**To configure OSPF**

1. Complete “Ethernet Interfaces” for the interface and assign an IP address to the interface.
2. Click OSPF under Configuration > Routing Configuration in the tree view.

---

**Table 8-3  NSSA (Not So Stubby Area) Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost for Default Route</td>
<td>Enter a cost associated with the default route to the NSSA.</td>
</tr>
<tr>
<td>Default Route Type</td>
<td>Specifies the route type associated with the Type-7 default route for an NSSA when routes from other protocols are redistributed into OSPF as ASEs. If a redistributed route already has a route type, this type is maintained. If summary routes are imported into an NSSA, only then a Type-7 default route is generated (otherwise a Type-3 default route is generated). This field appears only if an area is defined as an NSSA into which summary routes are imported. The route type can be either 1 or 2. A type 1 route is internal and its metric can be used directly by OSPF for comparison. A type 2 route is external and its metric cannot be used for comparison directly. Default: 1</td>
</tr>
<tr>
<td>Redistribution</td>
<td>Specifies if both Type-5 and Type-7 LSAs or only Type-7 LSAs will be originated by this router. This option will have effect only if this router is an NSSA border router and this router is an AS border router. Default: On</td>
</tr>
<tr>
<td>Type 7 Address Ranges</td>
<td>An NSSA border router that performs translation duties translates Type-7 LSAs to Type-5 LSAs. An NSSA border router can be configured with Type-7 address ranges. Use these ranges to reduce the number of Type-5 LSAs. Many separate Type-7 networks may fall into a single Type-7 address range. These Type-7 networks are aggregated and a single Type-5 LSA is advertised. By definition, a Type-7 address range consists of a prefix and a mask length. Note: To prevent a specific prefix from being advertised, select On in the Restrict field next to the entry for that prefix.</td>
</tr>
</tbody>
</table>
Configuring OSPF

3. Enter the router ID in the Router ID text box.

4. If you want to define additional OSPF areas besides the backbone area:
   1. Enter each name in the Add New OSPF Area text field and click Apply.
   2. Select an Area Type—Normal, Stub, or NSSA. For more information, see “Types of Areas” on page 306.
   3. If you select a stub or NSSA area type, configure the additional parameters that appear, as described in Table 8-2 and Table 8-3.

5. (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.

   Note - To prevent a specific prefix from being advertised into the backbone, click the On button in the Restrict field next to the entry for that prefix.

6. Configure virtual links for any area that does not connect directly to the backbone area, as described in “Configuring Virtual Links” on page 313.

7. Configure the OSPF interfaces, as described in “To configure an OSPF interface” on page 318.

Configuring Virtual Links

You must configure a virtual link for any area that does not connect directly to the backbone area. 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.

To configure a virtual link

1. Create an area that does not connect directly to the backbone area and configure an interface to be in that area.

2. In the Add a New Virtual Link text field, enter the router ID of the remote endpoint of the virtual link.

3. Select the transit area from the drop-down box. This is the area that connects both to the backbone and to the discontiguous area.

   Additional fields appear.

4. Configure the following parameters for the virtual link:
Configuring OSPF

- **Hello interval**—Length of time, in seconds, between hello packets that the router sends on the interface. For a given link, this field must be the same on all routers or adjacencies do not form. Default: 30.

- **Dead interval**—Number of seconds after the router stops receiving hello packets that it declares the neighbor is down. Typically, the value of this field should be four times that of 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 zero.
  
  Range: 1-65535. Default: 120.

- **Retransmit interval**—Specifies the number of seconds between LSA retransmissions for adjacencies belonging to 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 unnecessary retransmissions.
  
  Range: 1-65535 in number of seconds. Default: 5.

- **Auth Type**—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: None / Simple / MD5. Default: None.

5. If you selected MD5 for the auth type, you must also configure the following parameters:

- **Add MD5 Key**—If the Auth type selected is MD5, the Key ID and MD5 Secret fields appear. Specify the Key ID and its corresponding MD5 secret to configure a new MD5 key. If you configure multiple Key IDs, the Key ID with the highest value is used to authenticate outgoing packets. All keys can be used to authenticate incoming packets.

- **Key ID**—The Key ID is included in the outgoing OSPF packets to enable the receivers to use the appropriate MD5 secret to authenticate the packet.
  
  Range: 0-255. Default: None

- **MD5 Secret**—The MD5 secret is included in encrypted form in outgoing packets to authenticate the packet. Range: 1-16 alphanumeric characters. Default: None

6. Click Apply.

7. To make your changes permanent, click Save.

8. Repeat this procedure on both the ABR for the discontiguous area and an ABR that connects to the backbone area.
Configuring OSPF

**Configuring Global Settings**

Table 8-4 shows the global settings that you can specify for OSPF. Configure these settings by clicking OSPF under Configuration > Routing Configuration in the tree view and scrolling down to these fields.

<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>
<tr>
<td>Default ASE Route Type</td>
<td>Specifies a route type for routes redistributed into OSPF as ASEs, unless these routes already have a type assigned.</td>
</tr>
<tr>
<td></td>
<td>There are two types:</td>
</tr>
<tr>
<td></td>
<td>• Type 1 external: Used for routes imported into OSPF which are from IGP's 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Graceful Restart Helper</td>
<td>When a router running OSPF restarts, all the routing peers detect that the session failed and recovered. This transition results in a routing flap and causes routes to be recomputed, updates to be generated, and unnecessary churn to the forwarding tables. Enabling this option minimizes the negative effects caused by peer routers restarting by causing the Check Point system to maintain the forwarding state advertised by peer routers even when they restart.</td>
</tr>
</tbody>
</table>
## Configuring OSPF Interfaces

Table 8-5 lists the parameters for interfaces that you use when configuring OSPF on your platform.

<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.</td>
</tr>
<tr>
<td>Hello interval</td>
<td>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.</td>
</tr>
<tr>
<td>Dead interval</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 310.

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.

Range: 1-65535 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.
Configuring OSPF

Table 8-5 Configuration Parameters for OSPF Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retransmit interval</td>
<td>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 1-65535 in seconds. Default is 5.</td>
</tr>
<tr>
<td>OSPF cost</td>
<td>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.</td>
</tr>
<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>
</tbody>
</table>
Configuring OSPF

Table 8-5 Configuration Parameters for OSPF Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 138. 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. |

To configure an OSPF interface

1. Assign the appropriate interface 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.
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 “Ethernet Interfaces.”
2. Initiate a Network Voyager session to Nokia Platform C.
3. Click OSPF under Configuration > Routing Configuration in the tree view.
4. Click the backbone area in the drop-down list for e1; then click Apply.
5. In the Add New OSPF Area text box, enter 1; then click Apply.
6. In the Add new address range: prefix text box for the backbone area, enter 192.168.24.0.
7. In the Mask Length text box, enter 24; then click Apply.
8. Click 1 area in the drop-down list for e2; then click Apply.
9. Click Save.
10. Initiate a Network Voyager session to Nokia Platform D.
11. Click Config on the home page.
12. Click the OSPF link in the Routing Configuration section.
13. In the Add New OSPF Area text box, enter 1; then click Apply.
14. Click 1 area in the drop-down list for e3, then click Apply.
15. Click Save.
RIP

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
RIP 1

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 Check Point 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, Check Point 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” on page 323.

*Note* - Check Point 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.
Configuring RIP

Using Network Voyager, you can configure the following options:

Table 8-6 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, Check Point 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 “Ethernet Interfaces” for the interface.
2. Click RIP under Configuration > Routing Configuration in the tree view.
3. Click on for each interface to configure; then click Apply.
4. Click either 1 or 2 in the Version field to select RIP 1 or RIP 2, respectively, for each interface; then click Apply.

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

5. (Optional) Enter a new cost in the Metric text box for each interface; then click Apply.

6. (Optional) To configure the interface to not accept updates, click on the on radio button in the Accept updates field; then click Apply.

7. (Optional) If you want to configure the interface to not send updates, click on in the Send updates field; then click Apply.

8. (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. Check Point recommends that you not operate RIP 1 and RIP 2 together.

9. (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.

10. (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 Check Point platforms. Click Apply.

11. 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.

12. 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 RIP under Configuration > Routing Configuration in the tree view.
2. To modify the update interval, enter the new update interval in the Update Interval text box; then click Apply.
3. To modify the expire interval enter the new expire interval in the Expire Interval text box; then click Apply.
4. 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 RIP under Configuration > Routing Configuration in the tree view.
2. To enable auto-summarization, click on in the Auto-Summarization field; then click Apply.
3. To disable auto-summarization click off in the Auto-Summarization field; then click Apply.
4. 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 “Ethernet Interfaces.”
2. Click RIP under Configuration > Routing Configuration in the tree view.
3. Click on for the eth-s2p1c0 interface; then click Apply.
4. (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, Check Point recommends RIP 2 over RIP 1.

1. First configure the interface as in “Ethernet Interfaces.”
2. Click RIP under Configuration > Routing Configuration in the tree view.
3. Click on for the eth-s2p1c0 interface; then click Apply.
4. Click on in the Version 2 field for the eth-s2p1c0 interface; then click Apply.
5. (Optional) Enter a new cost in the Metric text box for the eth-s2p1c0 interface; then click Apply.
6. (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) 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.


You can run PIM over a route-based VPN by enabling PIM on a virtual tunnel interface (VTI). You must use an unnumbered interface for the VTI.
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.”

You can run PIM over a route-based VPN that is terminated by a VRRP group. If you do so, VRRP uses the IP address of the proxy interface of the (unnumbered) VTI as the virtual IP address.

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, Check Point supports PIM, both Dense-Mode and Sparse-Mode, in a cluster. Check Point also supports IGMP in a cluster.

Note - Check Point 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 Check Point 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 Check Point 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.

**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 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.

**Note** - For both PIM-SM and PIM-DM, the Check Point 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-SIM is implemented. If the Check Point appliance is the designated router, it does not generated such a join message, but it propagates these join messages when sent by another router.

### Configuring Check Point VPN-1 Pro/Express

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.

2. Click the 3rd Party Configuration tab and configure as follows only when PIM-SM or PIM-DM is enabled with IP Clustering:
   1. For the availability mode of the gateway cluster object, select load sharing.
   2. In the third-party drop-down list, select Nokia IP clustering.
   3. 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.

**Note** - All available check boxes should be checked if you are not enabling PIM-SM or PIM-DM in an IP cluster.

4. 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 PIM under Configuration > Routing Configuration in the tree view.

2. Enable or disable state refresh, as appropriate. See “PIM Dense Mode State Refresh” on page 332 for more information.

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.
Disabling PIM

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 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.

**PIM Dense Mode State Refresh**

PIM dense mode builds multicast distribution trees that operate on a flood and prune principle. Multicast packets from a source are flooded throughout a PIM dense mode network. PIM routers that receive multicast packets and have no directly connected multicast group members or PIM neighbors send a prune message back up the source-based distribution tree toward the source of the packets. As a result, subsequent multicast packets are not flooded to pruned branches of the distribution tree. However, the pruned state in PIM dense mode times out approximately every three minutes and the entire PIM dense mode network is reflooded with multicast packets and prune messages. This reflooding of unwanted traffic throughout the PIM dense mode network consumes network bandwidth unnecessarily.

Use the PIM Dense Mode State Refresh feature to keep the pruned state in PIM dense mode from timing out by periodically forwarding a control message down the distribution tree. The control message refreshes the prune state on the outgoing interfaces of each router in the tree. This saves network bandwidth by greatly reducing the reflooding of unwanted multicast traffic to pruned branches of the PIM dense mode network.

Note - You must enable state refresh on all the PIM routers in the distribution tree to take advantage of this feature.

**Disabling PIM**

You can disable PIM on one or more interfaces you configured on each Check Point platform.

1. Click PIM under Configuration > Routing Configuration in the tree view.
Setting Advanced Options for Dense-Mode PIM (Optional)

2. 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.

3. Click Apply; then click Save to make your change permanent.

Setting Advanced Options for Dense-Mode PIM (Optional)

1. Click PIM under Configuration > Routing Configuration in the tree view.

2. 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.

3. Click Apply, and then click Save to make your changes permanent.

4. (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.

5. (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).

6. Click Apply, and then click Save to make your changes permanent.

7. 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.

   Note - The number of interfaces on which you can run PIM is unlimited.

   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. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. Click Apply.
Configuring Sparse-Mode PIM

16. To make your changes permanent, click Save.

**Configuring Sparse-Mode PIM**

1. Click PIM under Configuration > Routing Configuration in the tree view.
2. In the PIM Instance Mode field, click On for sparse.
3. Click Apply.
4. 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.

5. Click Apply.
6. (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.

7. Click Apply.
8. (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.

9. (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
Sparse-Mode PIM for NAT

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 the CLI:

```
show pim neighbor <ip_address>
```

For neighbors that advertise a DR election priority value, the following message appears in the summary:

- **DRPriorityCapable Yes.**

10. Click Apply.

11. To make your changes permanent, click Save.

**Sparse-Mode PIM for NAT**

PIM Sparse mode can be used with Network Address Translation (NAT). If NAT is used, follow these guidelines:

1. The NAT Rendezvous Point and the multicast sources must be on the same side of the gateway.
2. Static routes is the unicast protocol in the external network towards the receiver.
3. OSPF is the unicast protocol in the internal network towards the NAT Rendezvous Point.
4. Only one firewall is used between two domains.
5. Only one internal and one external interface is configured for PIM.

**To configure Sparse-Mode PIM for NAT:**

1. Click NAT under Configuration > Routing Configuration in the tree view.
2. In the Interfaces section, click external on one interface and internal on a different interface.

- **Note** - The routing protocol on the external interface must be a Static Route; the routing protocol on the internal interface must be an OSPF.

3. In the External Translated Address field, enter the Hide behind IP Address configured during FW NAT configuration ("Translation Method" set to "Hide").
4. Click Apply.
Configuring High-Availability Mode

5. Click PIM under Configuration > Routing Configuration in the tree view.
6. In the PIM Instance Mode field, click On for sparse.
7. Select the "NAT mode" check-box.
8. Click Apply.
9. In the Interfaces section, click On for each interface on which NAT was configured as external or internal during NAT configuration.
10. Click Apply.
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.

Enable high-availability mode only if all of the following conditions are true:

- Sparse-mode PIM is being used. (HA mode does not apply to dense-mode PIM.
- Two or more routers are being used to backup each other in a high-availability situation.
- VRRP virtual address option is not enabled on the PIM interfaces.
- IP clustering is not enabled.

When this option is enabled, all PIM interfaces are brought up only if each such interface is up and has a valid address assigned to it. If any of these interfaces subsequently fails or all the addresses of an interface are deleted then each interface is brought down (with respect to PIM) and kept in that state till each interface is available again.

**Note** - This option overrides the interface-specific virtual address option, so enabling both options results in PIM ignoring the VRRP state on one or more interfaces.
Configuring High-Availability Mode

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.”

1. Click PIM under Configuration > Routing Configuration in the tree view.
2. In the PIM Instance Mode field, click On for sparse.
3. Click Apply.
4. In the HA Mode field, click On to enable the high-availability mode.
5. Click Apply.
6. In the Interfaces section, click On for each interface to run PIM.

Note - The number of interfaces on which you can run PIM is unlimited.

7. Click Apply.
8. (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.

9. (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 the CLI:
show pim neighbor <ip_address>
For neighbors that advertise a DR election priority value, the following message appears in the summary:
DRPriorityCapable Yes.
Configuring this Router as a Candidate Bootstrap and Candidate Rendezvous Point

10. Click Apply.
11. To make your changes permanent, click Save.

**Configuring this Router as a Candidate Bootstrap and Candidate Rendezvous Point**

1. Click PIM under Configuration > Routing Configuration in the tree view.
2. In the PIM Instance Mode field, click On button for sparse.
3. Click Apply.
4. 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.

5. Click Apply.

6. In the Sparse Mode Rendezvous Point (RP) Configuration section, to enable this router as a candidate bootstrap router:
   1. Click On in the Bootstrap Router field.
   2. (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.
   3. (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.

7. In the Sparse Mode Rendezvous Point (RP) Configuration section, to enable this router as a Candidate Rendezvous Point:
   1. Click On in the Candidate RP Router field.
2. (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.

3. (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.

8. (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).

9. Click Apply.

10. To make your changes permanent, click Save.

**Configuring a PIM-SM Static Rendezvous Point**

1. Click PIM under Configuration > Routing Configuration in the tree view.
2. In the PIM Instance Mode field, click On for sparse.
3. Click Apply.
4. 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.

5. Click Apply.
Setting Advanced Options for Sparse-Mode PIM (Optional)

6. 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.

7. Enter the IP address of the router to configure as the static rendezvous point in the RP Address text box. Click Apply.

8. (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).

9. Click Save to make your changes permanent.

**Setting Advanced Options for Sparse-Mode PIM (Optional)**

1. Click PIM under Configuration > Routing Configuration in the tree view.

2. In the PIM Instance Mode field, click On for sparse.

3. Click Apply.

4. 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.

5. Click Apply.

6. 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.
7. 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.

8. 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.

9. 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.

10. 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 Check Point appliance being accepted by a Cisco router that is the elected rendezvous point (RP), configure this option. A Check Point appliance that is the elected RP accepts register messages that calculate the checksum with or without the multicast payload, that is, it accepts all register messages. Enable this option only if all of the following conditions are true:
- A Cisco router is the RP.
- The Cisco is running an older version (~11.0) of IOS.
- The Check Point system is the DR for locally-connected sources of multicast traffic.
Debugging PIM

The checksum of PIM register messages (data packets tunneled by the DR of the multicast source to the RP) is calculated without including the multicast payload. However, early releases of Cisco’s sparse-mode implementation calculated this checksum by including the multicast payload also. This option is therefore included as a workaround.

If a Check Point system is the RP, it will accept both types of checksums.

22. Click Apply.

23. To make your changes permanent, click Save.

Debugging PIM

The following CLI 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 interfaces</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 CLI 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>
</tbody>
</table>
To log information about errors and events.

1. Click Routing Options under Configuration > Routing Configuration in the tree view.

2. 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.

3. 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.
Debugging PIM

- **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.
Static Multicast Routes

PIM expects packets to arrive on the reverse-path forwarding (RPF) interface, that is, the interface used to reach the source of the multicast data. PIM also checks the RPF to learn which interface it should use to send join/prune messages. By default, PIM identifies the RPF interface by checking the unicast routing table, but you can use static multicast routes to provide an alternative route table to use for the RPF check. If both a static multicast route and a unicast route are available for a specific destination, PIM uses the static multicast route.

Static multicast routes allow PIM to be independent of unicast routing and let you deploy topologies in which multicast and unicast traffic flow over different paths. For instance, if you want to balance your traffic load by separating the path used by HTTP traffic from the path used by streaming stock quotes, you could configure a static multicast route to the source network that specifies a next hop gateway address that is different from the next hop address (for the same source) in the unicast routing table.

To configure static multicast routes using Network Voyager, click Configuration > Routing > Static Multicast Routes in the navigation tree.

Note - PIM is the only protocol that uses static multicast routes.
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:

- Configured autonomous system number
- Current edition number of the routing table
- Checksum of the update message
- Count of the number of routes included
- List of route entries

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
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
IGRP

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 Check Point 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.
Generation of Exterior Routes

- **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

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

1. Complete “Ethernet Interfaces” for the interface.
2. Click IGRP under Configuration > Routing Configuration in the tree view.
3. Enter the AS number in the Autonomous System Number text box.
4. Click on for each interface to configure; then click Apply.
5. (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.
6. (Optional) Enter a new bandwidth metric in the Bandwidth text box for each interface (for example, 1000 for 10Mbps Ethernet); then clickApply.
   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.
7. (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.
8. (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.

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.)
Configuring IGRP

9. (Optional) In the Protocol section, click No in the Holddown field; then click Apply.
   This action disables the global route holddown parameter.

10. (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.

11. (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.

12. (Optional) In the Protocol section, enter the new invalid interval metric in the Invalid interval text box; then click Apply.

13. (Optional) In the Protocol section, enter the new hold interval metric in the Hold interval text box; then click Apply.

14. (Optional) In the Protocol section, enter the new flush interval metric in the Flush interval text box; then click Apply.

15. (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.

16. 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.

To enable IGRP on an interface:
1. Configure the interfaces as in “Ethernet Interfaces.”
2. Click IGRP under Configuration > Routing Configuration in the tree view.
3. Enter the AS number in the Autonomous System Number text box.
4. (Required) Enter a delay metric in the Delay text box for each interface; then click Apply.
5. (Required) Enter a bandwidth metric in the Bandwidth text box for each interface; then click Apply.
Configuring IGRP

6. (Required) Enter a reliability metric in the Reliability text box for each interface; then click Apply.

7. (Required) Enter the load metric in the load text box for each interface; then click Apply.
   The load metric is a fraction of 255.

8. (Required) Enter the MTU metric in the metric text box for each interface; then click Apply.
   A larger MTU reduces the IGRP cost.

9. Click on for eth-s1p1c0; then click Apply.
DVMRP

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.

The IPSO implementation of DVMRP supports the following features.

- DVMRP v.3
- Prune and graft messages
- Generation ID
- Capability flags
- Interface metric and threshold configuration
- Interface administrative scoping on the 239.X.X.X addresses
• Interfaces with secondary addresses
• Monitoring template
• Tracks the number of subordinate routers per route.

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 “Ethernet Interfaces” for the interface.
2. Click DVMRP under Configuration > Routing Configuration in the tree view.
3. For each interface you want to configure for DVMRP, Click on for the interface; then click Apply.
4. (Optional) Enter a new minimum IP time to live (TTL) threshold in the Threshold text box for each interface; then click Apply.
5. (Optional) Enter a new cost metric for sending multicast packets in the Metric text box for each interface; then click Apply.
6. To make your changes permanent, click Save.

Configuring DVMRP Timers

You can configure values for DVMRP timers. Check Point 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 DVMRP under Configuration > Routing Configuration in the tree view.
2. Click the Advanced DVMRP options link.
   This action takes you to Advanced Options for DVMRP page.
3. (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
Configuring DVMRP Timers

4. (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.

5. (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.

6. (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.

7. (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.

8. (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.

9. Click Apply, and then click Save to make your changes permanent.
IGMP

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.

The IPSO implementation of IGMP supports the following features.

- IGMPv3 source filtering
- Complete IGMPv2 functionality
- Multicast traceroute
- Complete configurability of protocol timers
Configuring IGMP

- Administratively-blocked groups
- Support for interfaces with secondary addresses
- Monitoring template

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.

Check Point 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 see “PIM” on page 327.

Configuring IGMP

1. Complete “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” on page 327 or “DVMRP” on page 355.
3. Click IGMP under Configuration > Routing Configuration in the tree view.
4. Complete the following steps for each interface on which you enabled a multicast routing protocol.
5. Click the button for the appropriate version. See “IGMP Version 3” on page 360 for information about this version of the protocol.
6. Click Apply.

Note - IGMP version 2 is compatible with IGMP version 1, and version 3 is compatible with versions 2 and 1. Check Point recommends that you use version 1 only on networks that include multicast routers that are not upgraded to IGMP versions 2 or 3.
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.

**IGMP Version 3**

IPSO provides IGMP version 3 source filtering to support source-specific multicast (SSM), which enables the IPSO system to request traffic from specific sources via PIM join/prune messages without requiring the presence of a rendezvous point (RP). This enables the IPSO system to forward traffic from only those sources from which receivers requested traffic. IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic.

With IGMP version 3, receivers (hosts) identify their membership to a multicast group in the following two modes:
Configuring IGMP

- Include mode: Receivers announce membership to a group and provide a list of IP addresses (the include list) from which they want to receive traffic.
- Exclude mode: Receivers announce membership to a host group and provide a list of IP addresses (the exclude list) from which they do not want to receive traffic. To receive traffic from all sources, a host sends an empty exclude list.

The multicast group address range 232/8 (232.0.0.0 to 232.255.255.255) is reserved for use by SSM protocols and applications. The DRs of senders do not send register packets to any RPs in the SSM group range.

When SSM is enabled, all other multicast groups are treated as in normal sparse-mode.

**Configuring Local and Static Groups**

You can facilitate multicast routing by creating IGMP local and static groups. You create these groups on a per-interface basis, and for each group you specify an address for a multicast group. IPSO then acts as a receiver for that multicast group and builds a routing tree to the source regardless of whether there are any hosts on the downstream LAN that want to receive traffic for that group. When hosts later join the multicast group, they start receiving traffic sooner because the routing tree is already built.

This feature is useful in any situation in which multicast receivers might not be permanently attached to the downstream LAN. For example, if you have laptop users who regularly detach from the LAN and reattach when they return to work and who also want to receive multicast traffic from a known source when their laptop is connected to the LAN, you can create a local or static group using the multicast address of the known source. IPSO then maintains the reverse path forwarding tree without waiting for requests from the laptops.

The differences between local and static groups are explained below.

- When you create a local group:
  - IGMP sends a membership report out of the appropriate interface.
  - If the system is running a parent multicast routing protocol, IGMP informs the parent protocol about the simulated local receiver.
- When you create a static group:
  - IGMP does not send a membership report for the group. You might want to use static groups if you do not want other devices to receive IGMP membership reports from your IPSO system.
Configuring IGMP

- If the system is running a parent multicast routing protocol, IGMP informs the parent protocol about the simulated local receiver.

Note - IGMP local and static groups are supported in IP clusters.
Static Routes

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 parameters:

- 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.

**To configure a default or static route**

1. Click Static Routes under Configuration > Routing Configuration in the tree view.

2. To enable a default route,
   1. Click On in the Default field
   2. Click Apply.

3. To configure a new static route:
   1. Enter the network prefix in the New Static Route text box.
   2. Enter the mask length (number of bits) in the Mask Length text box.

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.
Static Routes

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.
8. Click Apply.
9. To make your changes permanent, click Save.

**To setting the rank for static routes**
1. Click Static Routes under Configuration > Routing Configuration in the tree view.
2. Click Advanced Options.
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.

**To add and configure many static routes at the same time**
1. Click Static Routes under Configuration > Routing Configuration in the tree view.
2. 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” on page 363.
3. 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

4. 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.

5. Click Apply.

The newly configured additional static routes appear in the Static Route field at the top of the Static Routes page.

Note - The text box displays any entries that contain errors. Error messages appear at the top of the page.

6. 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.

To create a static default route
1. Use Network Voyager to connect to Nokia Platform A.
2. Click Static Routes under Configuration > Routing Configuration in the tree view.
3. Click on in the Default field; then click Apply.
4. 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.

To create a static route (non-default)
1. Click Static Routes under Configuration > Routing Configuration in the tree view.
2. In the New Static Route text box enter: 192.168.24.0.
3. In the Mask Length text box enter 24.
4. In the Gateway text box enter 192.168.26.70.
5. Click Apply.

If you have configured OSPF or RIP on your remote office network, you now have connectivity to the Internet.

To disable a static route
Backup Static Routes

1. Click Static Routes under Configuration > Routing Configuration in the tree view.
2. Click off for the route you want to disable
3. Click Apply.

Backup Static Routes

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 cannot use them for any static route.

To create a backup static route
1. Click Static Routes under Configuration > Routing Configuration in the tree view.

   **Note** - This example assumes that a static route has already been configured and the task is to add backup gateways.

2. Enter the IP address of the gateway in the Additional gateway text box.
3. 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 2 and 3.
4. To make your changes permanent, click Save.
Route Aggregation

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.

To create aggregate routes

1. Click Route Aggregation under Configuration > Routing Configuration in the tree view.

2. Enter the prefix for the new contributing route in the Prefix for new aggregate text box.

3. 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.

4. Scroll through the New Contributing Protocol list and click the protocol to use for the new aggregate route; then click Apply.

5. Click on in the Contribute All Routes from <protocol> field.
Route Aggregation Example

6. (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.

7. To make your changes permanent, click Save.

To remove aggregate routes

1. Click Route Aggregation under Configuration > Routing Configuration in the tree view.

2. Click off for the aggregate route disable; then click Apply.

3. 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 Route Aggregation under Configuration > Routing Configuration in the tree view.
Route Aggregation Example

3. Enter 192.168.24.0 in the Prefix for New Aggregate text box and enter 24 in the Mask Length edit box; then click Apply.

4. Click OSPF2 in the New Contributing Protocol drop-down list; then click Apply.

5. Click on in the Contribute all matching routes from OSPF2 field; then click Apply.

6. Click direct in the New Contributing Protocol drop-down list; then click Apply.

7. Click on in the Contribute All Matching Routes from direct field; then click Apply.

8. Click Top.

9. Click the Route Redistribution link in the Routing Configuration section.

10. Click the Aggregates Routes link in the Redistribute to RIP section.

11. 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

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>
<tr>
<td>RIP routes</td>
<td>100</td>
</tr>
<tr>
<td>Aggregate routes</td>
<td>130</td>
</tr>
</tbody>
</table>
To set route rank

1. Click routing options under Configuration > Routing Configuration in the tree view.
2. 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.
3. 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:
Routing Protocol Rank 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 Routing Options under Configuration > Routing Configuration in the tree view.
2. Enter 10 in the OSPF edit box.
3. 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.
BGP

Border Gateway Protocol (BGP) is an inter-AS protocol, meaning that it can be deployed within and between autonomous systems (AS). 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 BGP version 4 and 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.

You can run BGP over a route-based VPN by enabling BGP on a virtual tunnel interface (VTI). You must use an unnumbered interface for the VTI.

**Support for BGP-4++**

IPSO implements BGP-4++ to support multiprotocol extensions and exchange IPv6 prefixes as described in RFCs 2545, 2858, and 3392.

You must use an IPv4 address for the router ID (BGP identifier). After the BGP session is up, prefixes can be advertised and withdrawn by sending normal UPDATE messages that include either or both of the new multiprotocol attributes MP_REACH_NLRI (used to advertise reachability of routes) and MP_UNREACH_NLRI (used to withdraw routes).

The new attributes are backward compatible. If two routers have a BGP session and only one supports the multiprotocol attributes, they can still exchange unicast IPv4 routes even though they cannot exchange IPv6 routes.

On each peer you configure the type of routes (capability) that should be exchanged between peers. Choose from the following selections:

- IPv4 unicast (the default)
BGP Sessions (Internal and External)

- IPv6 unicast
- IPv4 unicast and IPv6 unicast

For peering to be established, the routers must share a capability.

If your system is exchanging IPv4 routes over IPv6 or vice versa, use route map commands to set nexthop to match the family of the routes being exchanged. If they do not match, the routes will not be active.

**Note** - Do not use the route redistribution and inbound filter pages of Network Voyager to configure routing policies for BGP-4++. Instead use the route map commands in the CLI.

**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.
BGP Sessions (Internal and External)

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.

**Preventing Private AS Numbers from Propagating**

An ISP can assign private AS numbers (64512 to 65535) to a customer in order to conserve globally unique AS numbers. When an ISP does so, a BGP update from a customer network to the ISP has the private AS number in its AS_PATH attribute. When the ISP propagates its network information to other ISPs, the private AS number would normally be included. To avoid this, you can configure IPSO to remove the private AS number from BGP update messages to external peers.

To configure IPSO to remove private AS numbers from BGP updates, enable the Remove Private AS option on the configuration page for an external peer.

If you enable this option, private AS numbers are removed from BGP updates according to the following rules:

- If the AS_PATH includes both public and private AS numbers, the private AS numbers are not removed.
- If the AS_PATH contains the AS number of the destination peer, private AS numbers are not removed.
- If the AS_PATH includes confederations and all the AS numbers in the AS_PATH are private, all the private AS numbers are removed.

**BGP Route Refresh**

IPSO supports the ability to dynamically request BGP route updates from peers and to respond to requests for BGP route updates. For example, if you change the inbound routing policy, you can request that a peer readvertise its previously advertised routes so that the routes can be checked against the new policy. This feature is often referred to as a soft reset because it provides the ability to refresh routes received from a peer without tearing down the established session.

To configure BGP route updates, click the appropriate buttons in the Route Refresh section of the configuration page for a peer.

These options work only with peers that support the same capabilities. IPSO systems can also peer with systems that do not support these options.
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>
</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.

**Note** - 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.
Redistributing Routes to BGP

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 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 (0xFFFFFF01)</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>
</tbody>
</table>
Route Reflection

<table>
<thead>
<tr>
<th>Community attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO_ADVERTISE (0xFFFFFFFF02)</td>
<td>Not advertised to other BGP peers.</td>
</tr>
<tr>
<td>NO_EXPORT_SUBCONFED(0xFFFFFFFF03)</td>
<td>Not advertised to external BGP peers. This includes peers in other members’ autonomous systems inside a BGP confederation.</td>
</tr>
</tbody>
</table>

For further details, refer to the communities documents, RFCs 1997 and 1998.

**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 cannot 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** - Check Point 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.
EBGP Multihop Support

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.

**Warning** - 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.
TCP MD5 Authentication

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.

Note - TCP MD5 authentication is not available for BGP session over IPv6.

BGP Support for Virtual IP for VRRP

The Check Point IPSO implementation of BGP 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 “VRRP Overview” on page 127.

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.
BGP Support for Virtual IP for VRRP

**Note** - BGP support for advertising the virtual IP address of the VRRP virtual router is only available for IPv4 BGP sessions, not for IPv6. In a VRRPv2 pair, if you select the Virtual Address option on the Advanced BGP page, it affect only IPv4 BGP peers. In a VRRPv3 pair, this option is not available for IPv6 BGP peers.

Perform the following procedure to configure a peer autonomous system, corresponding local address, and to enable support for virtual IP for VRRP.

1. Click BGPs under Configuration > Routing Configuration in the tree view.
2. Enter a value between 1 and 65535 in the Peer Autonomous System Number edit box.
3. 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” on page 382.
4. Click Apply.
5. Click the Advanced BGP Options link on the BGP page.
6. For the specific external or routing group, enter a local virtual IP address in the Local address text box.

**Note** - To make VRRP support function properly, you must enter a virtual IP address that is owned by the local system.

7. Click On in the Virtual Address field to enable virtual IP for VRRP support.
8. Click Apply.
9. Click Save to make your changes permanent.
BGP Support for IP Clustering

Check Point IPSO supports BGP in IP clusters. If a failover occurs, BGP stops running on the previous master and establishes its peering relationship on the new master. You must configure a cluster IP address as a local address when you run BGP in clustered mode.

**Note** - Check Point recommends that you configure BGP in an IP cluster so that peer traffic does not run on the cluster protocol interfaces.

**Note** - BGP support for IP clustering is only available for IPv4 BGP sessions, not for IPv6. On an IP cluster, you are not allowed to configure IPv6 peer.

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**

- 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.
BGP Memory Requirements

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:

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 6.05MB, which means that BGP requires 6.05MB 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 -auxw | grep ipsrd
```

The fourth column labeled, %MEM, displays the percentage of memory that IPSRD occupies.
BGP Neighbors Example

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.

To configure IBGP on Nokia Platform A
1. Configure the interface as in “Ethernet Interfaces” on page 31.
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” on page 309 or “To configure a default or static route” on page 363.
3. Click BGP under Configuration > Routing Configuration in the tree view.
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 100 in the AS number text box.
6. Enter 100 in the Peer autonomous system number text box.
7. Click Internal in the Peer group type drop-down list; then click Apply.
8. Enter 10.50.10.2 in the Add remote peer IP address edit box; then click Apply.
9. Configure an inbound route filter for AS 100 according to “BGP Route Inbound Policy Example” on page 428.

To configure IBGP on Nokia Platform B
BGP Neighbors Example

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” on page 309 or “To configure a default or static route” on page 363
3. Click BGP under Configuration > Routing Configuration in the tree view.
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 100 in the AS number edit box.
6. Enter 100 in the Peer autonomous system number text box.
7. Enter 10.50.10.1 in the Add remote peer IP address text box; then click Apply.
8. Enter 170.20.1.1 in the Add remote peer IP address text box; then click Apply.
9. Configure an inbound route filter for AS100 according to “BGP Route Inbound Policy Example.”

To configure 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” on page 309 or “To configure a default or static route.”
3. Click BGP under Configuration > Routing Configuration in the tree view.
4. 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.
5. Enter 100 in the AS number text box.
6. Enter 100 in the Peer autonomous system number text box.
7. Click Internal in the Peer group type drop-down list; then click Apply.
8. Enter 170.20.1.2 in the Add remote peer IP address text box; then click Apply.
9. Configure an inbound route policy for AS100 according in “BGP Route Inbound Policy Example.”

To configure Nokia Platform C as an IBGP peer to Nokia Platform A
10. Click BGP under Configuration > Routing Configuration in the tree view.
11. Enter 10.50.10.1 in the Add remote peer IP address text box.
12. Click Apply.

**To configure 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.
4. Click Apply.

**To configure EBGP on Nokia Platform A**
1. Configure the interface on Nokia Platform A as in “Ethernet Interfaces.”
2. Click BGP under Configuration > Routing Configuration in the tree view.
3. Enter 200 in the Peer autonomous system number text box.
4. Click External in the Peer group type drop-down list; then click Apply.
5. Enter 129.10.21.2 in the Add Remote Peer IP Address text box; then click Apply.
6. Configure route redistribution policy according to “Redistributing Routes to BGP” on page 419.
7. Configure an inbound route filter according to “BGP Route Inbound Policy Example.”

**To configure EBGP on Nokia Platform C**
1. Click BGP under Configuration > Routing Configuration in the tree view of Platform C.
2. Enter 300 in the AS number text box.
3. Click External in the Peer group type drop-down list; then click Apply.
4. Enter 172.17.10.2 in the Add remote peer IP address text box; then click Apply.
5. Configure route redistribution policy according to “Redistributing Routes to BGP” on page 380.
6. Configure an inbound route filter according to “BGP Route Inbound Policy Example” on page 428 to allow Nokia Platform C to accept routes from its EBGP peer.

**To configure EBGP on Nokia Platform D**
1. Configure the interface as in “Ethernet Interfaces.”
2. Click BGP under Configuration > Routing Configuration in the tree view.
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 200 in the AS Number text box.
5. Enter 100 in the Peer Autonomous System Number text box
6. Click External in the Peer group type drop-down window; then click Apply.
7. Enter 129.10.21.1 in the Add remote peer IP address text box; then click
   Apply.
8. Configure route inbound policy according to “BGP Route Inbound Policy
    Example.”
9. Configure route redistribution policy according to “Redistributing Routes to
    BGP” on page 380.
10. Configure an inbound route filter according to “BGP Route Inbound Policy
    Example.”

To configuring EBGP on Nokia Platform E
1. Configure the interface as in “Ethernet Interfaces.”
2. Click BGP under Configuration > Routing Configuration in the tree view.
3. Enter 300 in the AS number edit box.
4. Enter 100 in the Peer autonomous system number text box.
5. Click External in the Peer group type drop-down list; then click Apply.
6. Enter 172.17.10.1 in the Add remote peer IP address edit box; then click
   Apply.
7. Configure route inbound policy according the “BGP Route Inbound Policy
   Example” on page 428.
8. Configure route redistribution policy according to “Redistributing Routes to
   BGP” on page 380.
9. Configure an inbound route filter according to “BGP Route Inbound Policy
   Example” on page 428.
Path Filtering Based on Communities Example

**Verification**

To verify that you configured BGP neighbors correctly, run the following command:

```
show bgp neighbor
```

For more information about this command, see “Viewing Routing Protocol Information.”

**Path Filtering Based on Communities Example**

![Note]

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 “To configure route inbound policy on Check Point 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 “To configure route inbound policy on Check Point 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.

- To configure Default MED for Nokia Platform D
- To configure MED Values for all peers of AS200
- To configure MED Values for each external BGP peer for Nokia Platform D
- To configure MED Values and a route redistribution policy on Nokia Platform D

**To configure Default MED for Nokia Platform D**

1. Click BGP under Configuration > Routing Configuration in the tree view.
2. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”
3. Click the Advanced BGP Options link on the main BGP page. This action takes you to the Advanced Options for BGP page.
4. In the Miscellaneous settings field, enter a MED value in the Default MED edit box; then click Apply.
5. 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.

**To configure MED Values for all peers of AS200**

1. Click BGP under Configuration > Routing Configuration in the tree view.
BGP Multi Exit Discriminator Example

2. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”

3. Click Advanced BGP Options link on the main BGP page. This action takes you to the Advanced Options for BGP page.

4. 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.

**To configure MED Values for each external BGP peer for Nokia Platform D**

1. Click BGP under Configuration > Routing Configuration in the tree view.

2. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”

3. Click the link for the peer IP address for Nokia Platform A under AS100.

4. Enter 100 in the MED sent out text box.

5. Click on in the Accept MED from external peer field; then click Apply.

6. Click the link for the peer IP address for Nokia Platform B under AS100.

7. Enter 200 in the MED sent out text box.

8. Click on in the Accept MED from external peer field; then click Apply.

9. Click the link for the peer IP address for Nokia Platform C under AS200.

10. Enter 50 in the MED sent out text box.

11. Click on in the Accept MED from external peer field; then click Apply.

12. 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.

**To configure MED Values and a route redistribution policy on Nokia Platform D**

1. Click BGP under Configuration > Routing Configuration in the tree view.
BGP Multi Exit Discriminator Example

2. Configure EBGP peers in AS100 and AS200 according to the “BGP Neighbors Example.”
3. Click the Route Redistribution link the Routing Configuration section.
4. Click the BGP link in the Redistribute to BGP section.
5. Enter 100 in MED edit box next to the Enable redistribute bgp routes to AS100 field.
6. Enter necessary information for route redistribution according to the “BGP Multi Exit Discriminator Example”; then click Apply.
7. 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:

- show route
- show bgp neighbor <peerid> advertised
- show route bgp metrics

For more information on these commands, see “Viewing 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 “Ethernet Interfaces.”
2. Click IGBP under Configuration > Routing Configuration in the tree view.
3. Enter 100 in the AS number text box; then click Apply.

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.

To set 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 Based on Autonomous System Number.
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.
Changing the Local Preference Value Example

7. Click Accept in the All Routes from BGP AS 100 field; then click Apply.

To configure the static routes required for an IBGP session
1. Click Static Routes under Configuration > Routing Configuration in the tree view.
2. Enter 10.10.10.0 in the New static route text box.
3. Enter 24 in the Mask length text box.
4. Enter 20.10.10.2 in the Gateway text box; then click Apply.

To configure the static routes required for Nokia Platform B
1. Configure the interface as in “Ethernet Interfaces.”
2. Click BGP under Configuration > Routing Configuration in the tree view.
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.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click Advanced BGP Options.
   3. Enter 65525 in the Confederation text box.
   4. Enter 65528 in the Routing domain identifier text box; then click Apply.
2. Create confederation group 65524.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
BGP Confederation Example

2. Click Advanced BGP Options.
3. Enter 65524 in the Peer Autonomous System Number text box.
4. Click Confederation in the Peer Group Type drop-down list; then click Apply.
   Define properties for the above group.
5. Click On in the All field.
6. Click On in the All Interfaces field; then click Apply.
7. Enter 192.168.40.1 in the Add a new peer text box; then click Apply.

3. Create confederation group 65528.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Enter 65528 in the Peer Autonomous System Number text box.
   3. Click Confederation in the Peer Group Type drop-down list; then click Apply.
   Define properties for the above group.
4. Click on in the all field.
5. Click on in the All Interface field; then click Apply.
6. 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.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click the Based on ASPath Regular Expressions link.
   3. Enter 1 in the Import ID text box and enter .* in the ASPATH Regular Expression text box; then click Apply.
4. Click On in the Import All Routes From AS Path field; then click Apply.

5. Define route redistribution.
   1. Click Route Redistribution under Configuration > Routing Configuration in the tree view.
   2. Click the BGP link in the Redistribute to BGP section.
   3. Click 65528 in the Redistribute to Peer AS drop-down list.
   4. Click 65524 in the From AS drop-down list; then click Apply.
5. Click On in the Enable Redistribution of Routes From AS 65524 into AS 65528 field; then click Apply.
BGP Confederation Example

6. Click On in the all BGP AS 65524 routes into AS 65528; then click Apply.
7. Click Save.

Configuring Platform B

1. Set up the confederation and the routing domain identifier.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click Advanced BGP Options.
   3. Enter 65525 in the Confederation text box.
   4. Enter 65527 in the Routing domain identifier text box; then click Apply.
2. Create confederation group 65524.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click the Advanced BGP Options link.
   3. Enter 65524 in the Peer Autonomous System Number text box.
   4. Click Confederation in the Peer Group Type drop-down list; then click Apply.
   
   Define properties for the above group.
   5. Click On in the All field.
   6. Click On in the All Interfaces field; then click Apply.
   7. Enter 192.168.30.1 in the Add a new peer text box; then click Apply.
3. Create confederation group 65527.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Enter 65528 in the Peer Autonomous System Number text box.
   3. Click Confederation in the Peer Group Type drop-down list; then click Apply.
   Define properties for the above group.
   4. Click On in the All field.
   5. Click On in the All Interface field; then click Apply.
   6. 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.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click the Based on ASPath Regular Expressions link.
3. Enter 1 in the Import ID text box and enter .* in the ASPATH Regular Expression text box; then click Apply.

4. Click On in the Import All Routes from AS path field; then click Apply.

5. Define route redistribution.

   1. Click Route Redistribution under Configuration > Routing Configuration in the tree view.
   2. Click the BGP link in the Redistribute to BGP section.
   3. Click 65528 in the Redistribute to Peer AS drop-down list.
   4. Click 65524 in the From AS drop-down list; then click Apply.
   5. Click On in the Enable Redistribution of Routes From AS 65524 Into AS 65527 field; then click Apply.
   6. Click On in the All BGP AS 65524 Routes Into AS 65528 field; then click Apply.
   7. 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.

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.
Route Reflector Example

**Configuring Platform B as Route Reflector**

1. Assign an AS number for this router.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Enter 65526 in the AS number text box; then click Apply.

2. Create an external peer group.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click Advanced BGP Options.
   3. Enter 65525 in the Peer Autonomous System Number text box.
   4. Click External in the Peer Group Type drop-down list; then click Apply.

3. Enter the peer information.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click Advanced BGP Options.
   3. 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.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click Advanced BGP Options.
   3. Enter 65526 in the Peer auto autonomous system number text box.
   4. Select Internal in the Peer group type drop-down list; then click Apply.

5. Configure parameters for the group.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click Advanced BGP Options.
   3. Click On in the All field.
      
      This option covers all IGP and static routes.

   4. Click On in the All Interfaces field; then click Apply.

6. Enter the peer information.
   1. Click BGP under Configuration > Routing Configuration in the tree view.
   2. Click the Advanced BGP Options link.
   3. Enter 192.168.20.2 in the Add remote peer ip address text box under the AS65526 routing group.
Route Reflector Example

4. Select Reflector Client from the Peer type drop-down list; then click Apply.
5. Click BGP under Configuration > Routing Configuration in the tree view.
6. Click the Advanced BGP Options link.
7. Enter 192.168.30.2 in the Add remote peer ip address text box under the AS65526 routing group.
8. Select Reflector Client from the Peer type drop-down list; then click Apply.

Configuring Platform C as IBGP Peer of Platform B
1. Click BGP under Configuration > Routing Configuration in the tree view on Platform C.
2. 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.
3. Enter 65526 in the AS Number text box.
4. Enter 65526 in the Peer Autonomous System Number text box.
5. Click Internal in the Peer group type drop-down list; then click Apply.
6. Enter 192.168.20.1 in the Add remote peer IP address text box; then click Apply.
7. Click Save to make your changes permanent.

Configuring Platform D as IBGP Peer of Platform B
1. Click BGP under Configuration > Routing Configuration in the tree view on Platform D.
2. 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.
3. Enter 65526 in the AS Number text box.
4. Enter 65526 in the Peer Autonomous System Number text box.
5. Click Internal in the Peer Group Type drop-down list; then click Apply.
6. Enter 192.168.30.1 in the Add remote peer IP address text box; then click Apply.
7. Click Save to make your changes permanent.
Route Reflector Example

**Configuring BGP Route Inbound Policy on Platform B**

1. Click Inbound Route Filters under Configuration > Routing in the tree view.
2. Click the Based on Autonomous System Number link.
3. Enter 512 in the Import ID text box and enter 65526 in the AS edit box; then click Apply.
4. Click Accept in the All BGP Routes From AS 65526 field; then click Apply.
5. Enter 513 in the Import ID edit box and enter 65525 in the AS edit box; then click Apply.
6. Click Accept in the All BGP Routes From AS 65525 field; then click Apply.
7. 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 Route Redistribution under Configuration > Routing in the tree view.
2. Click the BGP Routes Based on AS link in the Redistribute to BGP section.
3. Select 65526 in the Redistribute to Peer AS drop-down list and select 65525 in the From AS drop-down list.
4. Click On in the Enable Redistribute BGP Routes From AS 65525 Into AS 65526 field; then click Apply.
5. Click Accept in the All BGP ASPATH 65525 Routes Into AS 65526 field; then click Apply.
6. Select 65525 in the Redistribute to Peer AS drop-down list and select 65526 in the From AS drop-down list.
7. Click On in the Enable Redistribute BGP Routes From AS 65526 Into AS 65525 field; then click Apply.
8. Click Accept in the All BGP ASPATH 65526 Routes Into AS 65525 field; then click Apply.
9. 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.
EBGP Load Balancing Example: Scenario #1

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 “Ethernet Interfaces.”
2. Click Interface Configuration under Configuration in the tree view.
3. Click the Logical Address Loopback link.
4. Enter 1.2.3.4 in the New IP Address text box; then click Apply.
EBGP Load Balancing Example: Scenario #1

Configuring a Loopback Address on Platform B
1. Configure the interface as in “Ethernet Interfaces.”
2. Click Interface Configuration under Configuration in the tree view.
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 Static Routes under Configuration > Routing in the tree view.
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 Static Routes under Configuration > Routing in the tree view.
2. Enter 1.2.3.4 in the New static route text box to reach the loopback address of Platform A.
3. Enter 32 in the Mask length text box; then click Apply.
4. Enter 129.10.2.1 in the Additional Gateway edit box; then click Apply.
5. 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 “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.
EBGP Load Balancing Example: Scenario #2

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 “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 “Ethernet Interfaces.”
2. Click Interfaces under Configuration > Interface Configuration in the tree view.
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 “Ethernet Interfaces.”
2. Click Interfaces under Configuration > Interface Configuration in the tree view.
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 OSPF under Configuration > Routing in the tree view.
EBGP Load Balancing Example: Scenario #2

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 OSPF under Configuration > Routing in the tree view.
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 “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, 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. Click Apply.

**Configuring an EBGP Peer on Platform B**

1. Configure an EBGP peer on Nokia Platform B as in “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.
Adjusting BGP Timers Example

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:
```
show bgp neighbor
show route bgp
```

For more information on these commands, see “Viewing 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

TCP MD5 Authentication Example

1. Configure the interface as in “Ethernet Interfaces.”
2. Click BGP under Configuration > Routing in the tree view.
   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 “Ethernet Interfaces.”
2. Click BGP under Configuration > Routing in the tree view.
   The following three steps enable BGP function on Nokia Platform B.
BGP Route Dampening Example

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 BGP under Configuration > Routing in the tree view.
2. Click the Advanced BGP Options link.
3. 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>
</tbody>
</table>

Chapter 8  Configuring Routing  413
4. 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:

```
show route bgp suppressed
```

For more information on this command, see “Viewing 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 Check Point 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default value</th>
<th>Units of measurement</th>
</tr>
</thead>
<tbody>
<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>
BGP-4++ Example

• 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.

BGP-4++ Example

This example describes how to configure a BGP4 session over IPv6 transport. In this example, a connection is established between 2 routers (Router 1 and Router 2) in different autonomous systems over an IPv6 network to exchange both IPv4 and IPv6 routes.

The following procedure describes the process, which consists of configuring the connection on each router, and then advertising the routes to Router 2.

To configure a BGP4 session over IPv6 transport

1. Determine whether Router 1 and Router 2 are directly connected.
   1. If Router 1 and Router 2 are directly connected, use IPv6 addresses of the interface through which they are connected.
      
      If they are directly connected, you can use their link-local addresses for BGP peering. To do this, on BGP configuration page, specify the link-local address in the Add Remote Peer's Address (IPv6) text box, and then select the name of the interface by which this router is connected to the BGP peer in Outgoing Interface drop-down list.

   2. If Router 1 and Router 2 are not directly connected, then verify that both routers have an IPv6 route to the IPv6 address that is used by the other router for BGP peering. You can verify this by going to the IPv6 Route Monitor page or using the show IPv6 route command.

2. Log in to Router 1 using Network Voyager and configure the connection as follows.
   1. Click BGP under Configuration > Routing in the tree view.
   2. Enter AS number of the other router.
BGP-4++ Example

3. In the Peer Group Type drop-down list, select External.
4. Click Apply.
5. Under AS2 External Group, in the Add Remote Peer Address (IPv6) text box, enter the IPv6 address of Router 2.
6. Click Apply.
7. Under Peer, click on the IP address link for Router 2.
   The BGP Peer <ipv6_addr> in AS2 page appears.
8. Under Multicast Capabilities, select On for IPv6 Unicast. IPv4 unicast capability is already selected by default—retain this setting.
9. Click Apply.
10. If Router 1 and Router 2 are not directly connected, select On for EBGP Multihop.
11. Click Apply.
12. To make your changes permanent, click Save.
13. Repeat these steps on Router 2.

3. On Router 1, create a route map named `advertise_to_as2` to advertise the routes from Router 1 to Router 2.

   **Note** - For information on creating and using route maps, see the CLI Reference Guide for Check Point IPSO.

4. On Router 1, use this route map by executing the following CLI command to send both IPv4 and IPv6 unicast routes to AS 2.

   ```
   set bgp external remote-as 2 export-routemap advertise_to_as2 preference 1 family inet-and-inet6
   ```

   **Note** - The actual routes sent will be based on the match conditions of the route map.

5. On Router 2, configure a routemap called `accept_from_as2` to accept incoming IPv4 and IPv6 routes advertised by router 1. (BGP by default does not accept incoming routes.)
6. On Router 2, execute the following CLI command to use this route map to accept the incoming routes.
BGP-4++ Example

```plaintext
set bgp external remote-as 1 import-routemap accept_from_as2
preference 1 family inet-and-inet6
```
Route Redistribution

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, such as the default route, or aggregates into a protocol.

Note - Route metrics are not translated between different routing protocols.

Note - You can also use route maps to redistribute routes from one protocol to another. You can define route maps only using CLI commands. For information on route maps, see “Route Maps” on page 304 and the CLI Reference Guide.

When you leak routes between protocols, you specify routes that are to be injected and routes that are to be excluded. In the case where the prefix is redistributed, you can specify the metric to advertise. The 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.

In some cases you can create RIP and OSPF route tags. You can do so by using the following Voyager pages:

- Redistribute from OSPF External to RIP
- Redistribute from BGP (AS NUMBER) to RIP
- Redistribute from ASPATH to RIP
- Redistribute from BGP (AS NUMBER) to OSPF
- Redistribute from ASPATH to OSPF

Note - Check Point systems also forward OSPF and RIP route tags that they receive from other routers.

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:
Redistributing Routes to BGP

- **Normal**—Matches any route that is equal to or more specific than the given prefix. This is the default modifier.
- **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.

The `redistribute_list` specifies the source of a set of routes based on parameters such as 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.

**Redistributing Routes to 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.
BGP Route Redistribution Example

Route redistribution allows you to redistribute routes from one autonomous system into another autonomous system.

To configure BGP route redistribution on Nokia Platform D
1. Click Route Redistribution under Configuration > Routing in the tree view.
2. Click BGP Routes Based on AS 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.

To redistribute 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.

To redistribute 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 Routes to RIP and IGRP

Redistributing Routes 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 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.
To redistribute routes 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. Check Point does not currently support the notion of trusted hosts for authentication of RIP routes.

2. Click Route Redistribution under Configuration > Routing in the tree view.
3. Click the RIP link under the Redistribute to OSPF External section.
4. 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.

5. 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:

   1. 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.
2. 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.
3. Click Apply.

The filter is fully configured.

To redistribute routes from the Nokia OSPF network to the Corporate RIP Network.
1. Use the Network Voyager connection to Nokia Platform A you previously created.
2. Click Route Redistribution under Configuration > Routing in the tree view.
3. Click the OSPF link in the Redistribute to RIP section.
4. 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.
5. 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.
6. 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.
1. 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.
2. 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.
3. Finally, click Restrict in the Action field. This specifies that we want to discard the routes that match this prefix.
4. Click Apply.

The filter is fully configured.

Redistributing OSPF to BGP Example

In the following example, Nokia Platform A is running OSPF and BGP and its local AS is 4.
Redistributing Routes with OSPF

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.

To redistribute OSPF to BGP through Nokia Platform A
1. Click Route Redistribution under Configuration > Routing in the tree view.
2. Click the OSPF link in the Redistribute to BGP section.
3. To redistribute OSPF routes into peer AS 100, select 100 from the Redistribute to Peer AS drop-down list, then click Apply.
4. (Optional) Enter the MED in the MED text box; then click Apply.
5. (Optional) Enter the local preference in the LocalPref text box, then click Apply.
6. 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.

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:
Redistributing Routes with OSPF

- Type 1
- Type 2

See the OSPF protocol configuration for a detailed explanation of the two types.
Inbound Route Filters

Inbound route filters allow a network administrator to restrict or constrain the set of routes accepted by a given routing protocol. The filters let an operator 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.

You can specify two possible actions for each prefix—accept the address into the routing protocol (with a specified rank) or exclude the prefix.

You can specify the type of prefix matching done for filter entries in the following ways:

• Routes that exactly match the given prefix; that is, have the same network portion and prefix length.
• 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.
• 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.
• 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.

To configure IGP inbound filters
1. Click Inbound Route Filters under Configuration > Routing in the tree view.
2. Click Filter Inbound RIP Routes.

Note - All other IGPs are configured in exactly the same way.
3. 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.

4. 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.

5. 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.

6. Click On or Off to enable or disable filtering of this route.

7. From the Match Type field drop-down list, select Normal, Exact, Refines, or Range.

8. In the Action field, click Accept or Restrict to determine what to do with the routes that match the given filter.

9. In the Rank field, enter the appropriate value, and then click Apply.

10. If this completes your actions for this route filtering option, click Save.

11. If this does not complete your actions for this route filtering option, begin again at step 3.
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.

To configure route inbound policy on Check Point Platform D based on an autonomous system number

1. Click Inbound Route Filters under Configuration > Routing in the tree view.
2. Click the Based on Autonomous System Number link.
3. 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.
4. Enter 100 in the AS text box; then click Apply.
   This is the AS number from which routes are to be filtered.
5. (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
BGP Route Inbound Policy Example

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.

To configure route inbound policy on Check Point Platform D based on ASPATH regular expressions

1. Click Inbound Route Filters under Configuration > Routing in the tree view.

2. Click the Based on ASPATH Regular Expressions link.

3. 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.

4. 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.

5. 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.
6. 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.

7. 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.

8. Select Refines in the Match type drop-down list.
   This specifies routes that are strictly more specific than 10.0.0.0/8.

9. Finally, click Restrict in the Action field.
   This specifies to discard the routes that match this prefix.

10. 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 ASPATH regular expressions, neighbors (AS numbers), or community IDs.

To filter BGP updates based on ASPATH regular expressions, see “To configure route inbound policy on Check Point Platform D based on ASPATH regular expressions” on page 429 The following examples, however, give a more detailed description of how to create ASPATH regular expressions.

**ASPATH Regular Expressions**

1. To accept routes that transit through AS 3662, enter the following ASPATH regular expression in the ASPATH Regular Expression text box:
   
   (.* 3662 .*)

   Select Any from the Origin drop-down list; then click Apply.

2. To accept routes whose last autonomous system is 3662, enter this ASPATH regular expression in the ASPATH Regular Expression text box:
   
   (.* 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 ASPATH regular expression in the ASPATH Regular Expression text box:
BGP AS Path Filtering Example

2041 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 ASPATH regular expression in the ASPATH Regular Expression text box:

   (1239 .* 7018 .* ) | (1239 .* 3561 .* )

   Select Any from the Origin drop-down window.

5. Apply.

6. Click Save to make your changes permanent.
Chapter 9
Configuring Traffic Management

This chapter describes the traffic management functionality in IPSO. IPSO provides traffic management through implementations of Differentiated Services (DiffServ) and policy based routing. IPSO also allows you to collect Netflow records so that you can analyses and understand network traffic patterns.

In This Chapter

- Traffic Management with Differentiated Services  page 434
- Configuring Policy Based Routing  page 457
- Configuring Netflow Services  page 463
Traffic Management with Differentiated Services

You can use the traffic management features in IPSO to provide different levels of service—or quality of service (QoS)—to different types of network traffic. Broadly speaking, you might want to employ traffic management to accomplish goals such as:

- prioritizing mission-critical applications
- maximizing your existing network infrastructure (and avoiding the expense and effort of upgrades)
- improving the performance of applications that are particularly sensitive to latency
- responding to unexpected traffic patterns in your network

With the DiffServ implementation in IPSO, you can configure systems to classify, shape, and prioritize packet streams in conformance with RFCs 2597 and 2598 of the IETF DiffServ Working Group. There are three main components in the DiffServ implementation:

- Access control lists (ACLs) classify traffic (separate it into discrete streams). IPSO supports ACLs for IPv4 and IPv6 traffic.
- Aggregation classes (AGCs) are used to police and shape traffic (drop or buffer traffic to conform it to throughput goals).
- Queue classes implement an output scheduling discipline to prioritize traffic and manage congestion.

You can configure ACLs and AGCs to process all incoming or outgoing traffic from one or more interfaces.

Performance Considerations

When you enable DiffServ QoS on any IPSO system there is some level of performance degradation for the affected traffic. If you use QoS only to classify packets the degradation is relatively small, but it can be significant if you also have the system prioritize traffic. You should employ this functionality only in circumstances in which the overall benefit outweighs the costs. For example, you might want to prioritize mission-critical traffic (such as VOIP traffic) that traverses a low bandwidth link, such as a T1 WAN connection. In this circumstance, the performance cost might be insignificant given the limitations of the narrow pipe. If
you have a high bandwidth connection such as a Gigabit Ethernet link, the performance cost imposed by QoS is probably much more significant and is likely to be prohibitive.

Your throughput will be affected by variables specific to your configuration, including packet sizes and traffic mix, so you should determine how QoS functions in your environment before deploying it in a production network.

**Note** - DiffServ traffic management is integrated with Check Point's SecureXL acceleration functionality. This allows you to manage the quality of service for traffic accelerated by SecureXL.

### Configuring Access Control Lists

To set up an ACL, you must select the interface(s) with which you want to associate the ACL. To select an interface, see “To apply or remove an ACL to or from an interface” on page 436 When associating an interface with an ACL, note the following restrictions:

- You can select a link aggregation interface or a link redundancy interface for an ACL, but you cannot assign these interfaces to a queue class. This means that traffic transiting these interfaces can be marked for QoS (so that other systems can provide QoS for this traffic), but IPSO systems cannot provide QoS on these interfaces.

- You cannot associate an Accelerated Data Path (ADP) interface with an ACL.

**Warning** - Lengthy ACLs can degrade performance because all traffic first must be compared to the ACL. Use ACLs with caution.

**To create, delete, or disable an ACL**

1. Click Access List under Configuration > Traffic Management in the tree view.
2. To create an ACL, enter a name for the ACL in the Create a New Access List edit box and click Apply.
   
   The Access Control List name and check boxes for deleting and disabling the ACL appear.

3. To delete or disable an ACL, click the appropriate check box and click Apply.
   
   The Access Control List name disappears from the Access List Configuration page.

4. Click Save to make your changes permanent.
Configuring Access Control Lists

To apply or remove an ACL to or from an interface

1. Depending on whether you are using IPv4 or IPv6, click the following link.
   1. For IPv4 ACLs, click Access List under Configuration > Traffic Management in the tree view.
   2. For IPv6 ACLs, click IPv6 Access List under Configuration > IPv6 Configuration > Traffic Management in the tree view.

2. Click the link for the appropriate ACL in the ACL Name field.
   The page for that ACL appears.

3. To apply an interface to the ACL:
   1. Select the appropriate interface from the Add Interfaces drop-down window.
   2. Select either Input or Output from the Direction drop-down window.

   You can apply the same direction to an interface for both an IPv4 and an IPv6 ACL. However, you cannot apply the same direction to an interface for more than one IPv4 ACL, or to more than one IPv6 ACL. Selecting the "input" direction for a ACL with a rule whose action is set to "prioritize" is equivalent to setting the action to "skip."

   Note - Only the default rule appears in the Access Control List until you create your own rule.

3. Click Apply.

   The new interface appears in the Selected Interfaces section.

4. To remove an ACL from an interface:
   1. Select Delete for the appropriate interface in the Selected Interfaces table
   2. Click Apply.

   The interface disappears from the Selected Interfaces section.

5. To make your changes permanent, click Save.
Configuring ACL Rules

An ACL is a container for a set of rules that separate traffic into packet streams. 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.

Rule Actions

You can associate the following actions with a rule:

- **Accept**—forward the traffic.
- **Bypass-FW**—forward ICMP traffic without sending it to the firewall. Traffic other than ICMP is not affected by this action.
- **Drop**—drop the traffic without any notification.
- **Reject**—drop the traffic and send an ICMP error message to the source.
- **Skip**—skip this rule and proceed to the next rule.
- **Shape**—coerce this traffic’s throughput according to the parameters specified by an aggregation class by buffering traffic that exceeds the parameters.
- **Prioritize**—give this traffic stream preferential scheduling on output. If you also configure an aggregation class for this rule, traffic that exceeds the parameters configured in the aggregation class is dropped.
- **PBR**—direct the traffic to a policy based routing table. See “Configuring Policy Based Routing” on page 457 for more information.

You can configure an access list to control the traffic from one or more interfaces and each access list can be associated with incoming or outgoing traffic from each interface. However, the prioritize action is only executed on outgoing traffic.

Note - IPSO versions previous to 6.1 supported rate shaping as an action for ACL rules. Shaping is no longer supported.

Traffic Properties used for Matching

Rules can be set up to match any of the following properties. All of these properties are used to match traffic:

- IP source address
Configuring ACL Rules

- 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

Masks can be applied to most of these properties to allow wildarding. The source and destination port properties can be edited only when the IP protocol is UDP, TCP, or the keyword "any."

When a packet matches a rule, the rule is executed immediately and no further rule scanning is done, so rule ordering is very important. You can change the order in which rules are applied by using the Change Rule Position option. If the packet matches no user-defined rule, then the action specified by the final default rule will be taken.

**Netflow Metering**

To enhance your understanding of network traffic patterns and performance, you can configure IPSO to capture and export information about network "flows," which are unidirectional streams of packets that share a given set of characteristics. You can define a flow by creating an ACL rule—traffic that matches the rule is part of the same flow. To use a rule for this purpose, you must enable the Netflow Metering option. See “Configuring Netflow Services” on page 463 for more information about using the Netflow feature.

**Marking and Queuing Traffic**

Enter values in these fields to mark traffic:

- DSfield: enter a DiffServ codepoint (DSCP) value
- QueueSpec: enter a queue specifier of your choice

These fields are available only when the Action field is set to "prioritize." The packets that match a rule whose action is set to "prioritize" are marked with the corresponding DSCP value and sent to the queue specified in the QueueSpec field. Traffic that is marked with a DSCP should receive the assigned level of service by all DiffServ-enabled routers in the network.

IPSO can apply a DSCP on egress or ingress:
For packets that are not destined for an IPSec tunnel, IPSO applies the appropriate DSCP when the packet exits the system.

If a queued packet is destined for an IPSec tunnel, IPSO applies the appropriate DSCP before the packet is encrypted. When it encrypts the packet, the firewall then copies the DSCP value to the header of the encrypted packet. The DSCP value is therefore visible to routers, which allows the packet to receive prioritized service as it transits the tunnel. Because DSCP values must be applied to packets before they are encrypted and packets are encrypted before egress, IPSO applies the DSCP marking to these packets on ingress.

IPSO supports expedited forwarding (EF) and assured forwarding (AF) per hop behaviors. You enable assured forwarding by assigning DSCP values that specify an AF class and drop precedence.

When you use assured forwarding, you assign types of traffic to four AF classes, class 1 through 4. The classes are in descending order, meaning that class 4 has the highest priority and traffic assigned to this class is serviced before traffic assigned to the other classes. In addition to the four classes, assured forwarding provides three drop precedences—low, medium, and high—within each class. You can use these drop precedence levels to fine tune how an interface responds to congestion.

Table 9-1 lists all the supported queues, and Table 9-2 lists the DSCP values to use to assign assured forwarding classes and drop precedences.

Note - You must use hexadecimal notation to specify DSCP values. Table 9-2 also shows the equivalent AF notation for your convenience.
Configuring ACL Rules

You should assign DSCP 0xc0 to internetwork control traffic, such as routing messages. Locally originated internetwork control traffic is automatically assigned to the appropriate queue. Traffic assigned to queues 7 (internetwork control) and 6 (expedited forwarding) is always prioritized over AF traffic.

<table>
<thead>
<tr>
<th>Queue Name</th>
<th>Queue Priority</th>
<th>DSCP</th>
<th>QueueSpecifier</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>AF Class 4</td>
<td>2</td>
<td>See Table 9-2</td>
<td>Configurable. Default is 5.</td>
</tr>
<tr>
<td>AF Class 3</td>
<td>3</td>
<td>See Table 9-2</td>
<td>Configurable. Default is 4.</td>
</tr>
<tr>
<td>AF Class 2</td>
<td>4</td>
<td>See Table 9-2</td>
<td>Configurable. Default is 3.</td>
</tr>
<tr>
<td>AF Class 1</td>
<td>5</td>
<td>See Table 9-2</td>
<td>Configurable. Default is 2.</td>
</tr>
<tr>
<td>Best Effort</td>
<td>7</td>
<td>no value</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drop Precendence</th>
<th>AF Class 1</th>
<th>AF Class 2</th>
<th>AF Class 3</th>
<th>AF Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>0x28 (AF11)</td>
<td>0x48 (AF21)</td>
<td>0x68 (AF31)</td>
<td>0x88 (AF41)</td>
</tr>
<tr>
<td>Medium</td>
<td>0x30 (AF12)</td>
<td>0x50 (AF22)</td>
<td>0x70 (AF32)</td>
<td>0x90 (AF42)</td>
</tr>
<tr>
<td>High</td>
<td>0x38 (AF13)</td>
<td>0x58 (AF23)</td>
<td>0x78 (AF33)</td>
<td>0x98 (AF43)</td>
</tr>
</tbody>
</table>

You should assign DSCP 0xc0 to internetwork control traffic, such as routing messages. Locally originated internetwork control traffic is automatically assigned to the appropriate queue. Traffic assigned to queues 7 (internetwork control) and 6 (expedited forwarding) is always prioritized over AF traffic.

To add a new rule to an ACL

1. Depending on whether you are using IPv4 or IPv6, click the following link.
Configuring ACL Rules

1. For IPv4 ACLs, click Access List under Configuration > Traffic Management in the tree view.

2. For IPv6 ACLs, click IPv6 Access List under Configuration > IPv6 Configuration > Traffic Management in the tree view.

2. Click the link for the appropriate Access Control List in the ACL Name field. The page for that ACL appears.

3. Click the Add New Rule Before check box.

4. Click Apply.

This rule appears above the default rule.

As 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.

5. To make your changes permanent, click Save.

Modifying a Rule

Rules provide filtering criteria for an access list. You can add a new rule, modify a rule, change the order in which rules are applied, or delete an existing rule.

To modify a rule, navigate to the page for the ACL that contains the rule, as described in “To add a new rule to an ACL” on page 440.
Configuring ACL Rules

Table 9-3 describes the attributes of an ACL rule that you can modify. To delete a rule, select the delete check box for that rule and click Apply.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>A rule action can be one of the following six actions:</td>
</tr>
<tr>
<td></td>
<td>- Accept—Forward this traffic stream.</td>
</tr>
<tr>
<td></td>
<td>- Bypass-FW—Forward ICMP traffic without sending it to the firewall.</td>
</tr>
<tr>
<td></td>
<td>- Drop—Silently drop all traffic belonging to this stream.</td>
</tr>
<tr>
<td></td>
<td>- Reject—Drop all traffic in this stream and attempt to deliver an ICMP error to the source.</td>
</tr>
<tr>
<td></td>
<td>- Skip—Skip this rule proceed to next.</td>
</tr>
<tr>
<td></td>
<td>- Shape—Coerce the throughput of this traffic according to a set of parameters given by an aggregation class.</td>
</tr>
<tr>
<td></td>
<td>- Prioritize—Give this traffic stream preferential scheduling on output.</td>
</tr>
<tr>
<td><strong>Aggregation Class</strong></td>
<td>This link takes you to the Traffic Condition Configuration page, where you can view and modify existing rate shaping aggregation class configurations on the system. It also allows you to add new aggregation classes or to delete existing aggregation classes from the system.</td>
</tr>
<tr>
<td><strong>Source IP Address</strong></td>
<td>Specifies the source IP address to be used for matching this rule.</td>
</tr>
<tr>
<td><strong>Source Mask Length</strong></td>
<td>Specifies the source filter mask length to be used for matching this rule.</td>
</tr>
<tr>
<td><strong>Destination IP Address</strong></td>
<td>Specifies the destination IP address to be used for matching this rule.</td>
</tr>
<tr>
<td><strong>Destination Mask Length</strong></td>
<td>Specifies the destination filter mask length to be used for matching this rule.</td>
</tr>
<tr>
<td><strong>Source Port Range</strong></td>
<td>Specifies the source port range to be used for matching this rule. You can specify the Source Port Range only if the selected protocol is either “any,” 6, TCP, 17, or UDP.</td>
</tr>
</tbody>
</table>
### Table 9-3  ACL Rule Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Port Range</td>
<td>Specifies the destination port range to be used for matching this rule. You can specify the Destination Port Range only if the selected protocol is either &quot;any,&quot; 6, TCP, 17, or UDP.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the IP protocol to be used for matching this rule. Range: 0-255 or any Default: Any</td>
</tr>
<tr>
<td>TCP-Establishment flag</td>
<td>When it is selected, traffic matches this rule when it is part of the initial TCP handshake. This option applies only to IPv4 ACLs. You can specify the TCP Establishment flag only if the selected protocol is TCP, 6, or &quot;any.&quot;</td>
</tr>
<tr>
<td>Type of Service (TOS) for IPv4</td>
<td>Specifies the type of service to be used for matching this rule. Range: any or 0x0-0xff Default: Any</td>
</tr>
<tr>
<td>Traffic Class for IPv6</td>
<td>Default: Any</td>
</tr>
<tr>
<td>DSfield</td>
<td>Specifies the DiffServ codepoint with which to mark traffic which matches this rule. 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. The DSfield and QueueSpec field can be configured only when the rule’s action is set to &quot;prioritize.&quot;</td>
</tr>
</tbody>
</table>
Configuring Aggregation Classes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Queue Specifier (QueueSpec)</td>
<td>Specifies the logical queue specifier value to be used by the output scheduler for traffic matching this rule.</td>
</tr>
<tr>
<td></td>
<td>Range: None or 0-7</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td></td>
<td>The DSfield and QueueSpec field can be configured only when the rule's action is set to &quot;prioritize.&quot;</td>
</tr>
<tr>
<td></td>
<td>When the DSfield is set to one of the predefined codepoints, for example, Internetwork Control, EF, or best effort, then the QueueSpec field is not used.</td>
</tr>
<tr>
<td>Aggregation Class</td>
<td>See “To associate an aggregation class with a rule” on page 446.</td>
</tr>
<tr>
<td>Netflow Metering</td>
<td>Specifies whether this rule should be used to define a network flow. See “Configuring Netflow Services” on page 463 for more information.</td>
</tr>
<tr>
<td>Change Rule Position</td>
<td>Use this option to change the order in which rules are applied to traffic. Each rule must be assigned a position, and you cannot assign the same position to more than one rule.</td>
</tr>
</tbody>
</table>

**Configuring Aggregation Classes**

Use aggregation classes to set and enforce throughput goals for packet streams. Traffic that meets these goals is conformant and is marked with the Differentiated Services Codepoint (DSCP) set by the appropriate ACL rule. When such traffic is processed by the output queue scheduler, it receives favorable priority treatment. Traffic that does not meet these goals is nonconformant and is policed (dropped).

**Note** - You can use aggregation classes to group traffic that has been classified by different ACL rules.

You should configure aggregation classes so that the aggregate of the internetwork control (IC) and expedited forwarding (EF) streams consumes no more than 50 percent of the output link bandwidth. This prevents lower-priority traffic from being starved. The other policers should also be configured to prevent the lower-priority queues from being starved. See RFC 2598 for more information.
Configuring Aggregation Classes

Classified traffic can be policed or shaped to a mean rate. This is implemented using a token bucket algorithm, which means that you can configure a burst size 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 dropping packets (policing) or delaying them by forcing them to wait for more tokens to arrive in the bucket (shaping). When more bursts arrive than can be accommodated by the shaping queue, that traffic is dropped. Both outgoing and incoming traffic streams can be poiced or shaped.

You can configure an aggregation class with two parameters:

- **Mean Rate**—The rate, in kilobits per second (kbps), to which the traffic rate should be coerced when measured over a long interval.
- **Burst Size**—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 burst size you configured for the AGC. When the burst reaches the configured burst size, traffic is nonconformant, but the AGC increases the rate at which traffic is transmitted based on the configured mean rate. Traffic that arrives consistently at a rate less than or equal to the configured mean rate will always be marked conformant and will not be dropped or delayed in the policer or shaper stages.

**To create an Aggregation Class**

1. Depending on whether you are using IPv4 or IPv6, click the following link.
   - For IPv4 ACLs, click Aggregation Class under Configuration > Traffic Management in the tree view.
   - For IPv6 ACLs, click IPv6 Aggregation Class under Configuration > IPv6 Configuration > Traffic Management in the tree view.

2. Enter the following in the Create a New Aggregation Class section:
   - A name for the aggregation class in the Name edit box.
   - Bandwidth in the Mean Rate (kbps) edit box.
   - Burst size in the Burst Size (bytes) edit box.

3. Click Apply.

   The aggregation class you have just created appears in the Existing Aggregation Classes table.
4. Click Save to make your changes permanent.

To delete an aggregation class, select the Delete check box next to the aggregation class that you want to delete and click Apply. This aggregation class disappears from the Existing Aggregation Classes section.

**To associate an aggregation class with a rule**

1. Depending on whether you are using IPv4 or IPv6, click the following link.
   1. For IPv4 ACLs, click Access List under Configuration > Traffic Management in the tree view.
   2. For IPv6 ACLs, click IPv6 Access List under Configuration > IPv6 Configuration > Traffic Management in the tree view.

2. Click the link for the appropriate Access Control List in the ACL Name field.
   The page for that Access Control List appears.

3. Select Shape or Prioritize from the Action drop-down window.

4. Click Apply.
   A drop-down list appears in the Aggregation Class field.

5. Select an existing aggregation class from the Aggregation Class drop-down list.

   **Note** - If there is no aggregation class listed, you need to create an aggregation class. Go to “To create an Aggregation Class” on page 445.

6. Click Apply.

7. Click Save to make your changes permanent.

**Configuring Queue Classes**

Traffic classified by an ACL rule can be given preferential treatment in conformance with RFCs 2597 and 2598. Traffic that conforms to the policing rate set by an aggregation class is marked with the Differentiated Services Codepoint (DSCP) set by the appropriate ACL rule. When such traffic is processed by the output queue scheduler, it receives favorable treatment. Higher-priority traffic must be policed to prevent starvation of lower-priority service traffic.
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.

**Note** - Prioritization is only relevant for outgoing traffic. Incoming traffic is never prioritized.

There are a maximum of 8 priority-level queues for a queue class. You can configure the size (in packets) of each queue level as well as the queue specifier. The queue specifier is assigned by an ACL rule 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. You can assign the remaining queues any name and specifier you want. Table 9-4 lists the predefined queues:

<table>
<thead>
<tr>
<th>Name of Queue Level</th>
<th>Priority</th>
<th>DSCP</th>
<th>Queue Specifier</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>

Internetwork control traffic, such as routing messages and keepalives, should be configured to use the internetwork control 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.

**Throughput and Latency**

A queue class can be configured to maximize device throughput or to minimize prioritized traffic latency.

- If you configure a queue class to minimize latency, IPSO uses a smaller threshold value for the number of packets that can be given to an interface for outbound transmission by any queue. After that number of packets is transmitted, IPSO checks to see if any higher priority traffic is waiting to be serviced. This option is more costly for forwarding performance but allows the least amount of head-of-line blocking for high priority traffic.
Configuring Queue Classes

- If you configure a queue class to maximize throughput, IPSO uses a greater threshold value for the number of packets that can be given to an interface for outbound transmission by any queue. This allows more packets to be transmitted in a schedule round but increases the possibility that higher priority traffic must wait for service.

**Congestion Management**

You can exercise control over how the available bandwidth is divided up among traffic classes by using the following scheduling disciplines:

- Strict Priority
- Weighted round robin (WRR)
- Cascade

If you use strict priority scheduling, higher priority queues are emptied before IPSO services lower priority queues. This can cause lower priority queues to be starved.

If you enable WRR, you assign weight values of 0-8 to individual queues. These values tell IPSO how much processing resources to allocate to each queue relative to the other queues being processed by that interface. For example, traffic assigned to a queue with a weight of 2 will receive twice as much processing resources as traffic assigned to a queue with a weight of 1. Traffic assigned to a queue with a weight of 3 will receive 50 percent more processing resources as traffic assigned to a queue with a weight of 2. Queues with greater weight values can send more bytes/packets per scheduling round.

Cascade scheduling is similar to WRR but imposes the following constraints:

- Queue 7 (priority 0) and queue 6 (priority 1) must be assigned the weight Strict Priority.
- You must configure the remaining queues so that their weights are in descending order. You can configure adjacent queues to have identical weights, but the weight assigned to a given queue cannot be greater than that assigned to a queue with a greater queue specifier.

**Congestion Avoidance (Drop Management)**

When the amount of outgoing traffic exceeds the transmission capabilities of the interface it is attempting to transit, the interface is congested and packets are dropped. If you enable WRR or Cascade scheduling, you can configure IPSO to respond to congestion in a way that makes the most sense in your network environment.
Configuring Queue Classes

IPSO has two methods of deciding which packets to drop when egressing traffic congests an interface. Each method applies to a specific queue—that is, to a given class of traffic. The methods are explained below:

- Tail drop: Tail drop simply discards any packets that arrive for a queue after the queue is full. By using tail drop you can possibly reduce the number of dropped packets, especially if you configure large queues. On the other hand, using large queues can incur increased delays (because more packets wait for the queue to be serviced).

  Using tail drop can also lead to inefficient use of link bandwidth because of global synchronization. This happens when the sliding window size for multiple TCP connections decreases simultaneously, with the result that all the senders send fewer packets per interval. If this happens repeatedly, the average utilization of the link decreases.

- Weighted random early detection (WRED): When you enable WRED, IPSO monitors queues and drops packets according to a configurable scheme.

  WRED is based on the random early detection (RED) method, which drops packets before queues are filled based on configurable threshold values. This reduces or eliminates the potential for global synchronization because different senders do not see packets dropped simultaneously.

  WRED adds a weighting scheme that allows you to prioritize some traffic so that fewer of its packets are dropped. The weighting is based on the IP precedence value for a packet, which is controlled by the first three bits of the type of service field in the IP header. A greater IP precedence value results in a smaller probability of packets being dropped. (See RFC 791 for more information about IP precedence.) WRED configuration values are explained below.

  - Minimum threshold: If the average queue length is less than or equal to this value, no packets are dropped.
  
  - Maximum threshold: If the average queue length is greater than or equal to this value, all arriving packets are dropped.

  If the average queue length is between the minimum and maximum values, IPSO attempts to avoid congestion by dropping packets based on the drop rates:

  - Drop rate 1: This drop rate is for low precedence traffic. If the value is 1024 (the default), IPSO drops one packet after servicing approximately 1024 packets.
Configuring Queue Classes

- Drop rate 2: This drop rate is for medium precedence traffic. If the value is 512 (the default), IPSO drops one packet after servicing approximately 512 packets.

- Drop rate 3: This drop rate is for high precedence traffic. If the value is 256 (the default), IPSO drops one packet after servicing approximately 256 packets.

You can configure how adaptive WRED is to traffic bursts by setting the Constant value between 1 and 16. Choosing a higher value creates a slower moving average, which has the benefit of reducing the variation in queue length (and therefore reducing packet drops caused by traffic bursts) but causes the system to react slower to congestion. Choosing a lower value allows the system to react faster to congestion but might result in packet drops caused by overreactions to temporary bursts in traffic.

To create or delete a queue class
1. Depending on whether you are using IPv4 or IPv6, click the following link.
   - For IPv4 ACLs, click Queue Class under Configuration > Traffic Management in the tree view.
   - For IPv6 ACLs, click IPv6 Queue Class under Configuration > IPv6 Configuration > Traffic Management in the tree view.
2. To create a new queue class, enter its name in the Create a New Queue Class edit box and click Apply.
   The new queue class appears in the Existing Queue Classes field.
3. To delete an existing queue class, select the Delete check box in the Existing Queue Classes table for the Queue class you want to delete and click Apply.
   The queue class disappears from the Existing Queue Classes field.
4. Click Save to make your change permanent.

To set or modify queue class configuration values
1. Depending on whether you are using IPv4 or IPv6, click the following link.
   - For IPv4 ACLs, click Queue Class under Configuration > Traffic Management in the tree view.
   - For IPv6 ACLs, click IPv6 Queue Class under Configuration > IPv6 Configuration > Traffic Management in the tree view.
2. In the Existing Queue Class table, click the name of queue class you want to configure.
Configuring Queue Classes

The configuration page for that queue class appears, listing the queues in the queue class. Each queue class can have up to eight queues. Three queues are reserved for Internetwork Control, Expedited Forwarding, and Best Effort traffic.

3. For each queue you want to configure, enter the following:
   1. **Logical Name**—This name appears on the queue monitoring page. Choose a name (with no spaces) that will allow you to identify the queue’s purpose.
   2. **Queue Specifier**—An integer used to address each queue you configure within a queue class.
   3. **Max Queue Length**—Value for the maximum number of packets that can be queued before packets are dropped. Enter a value of zero (0) to disable a queue. Neither the Internetwork Control nor the Best Effort queue can be disabled.

4. Configure any other options, as appropriate.

5. Click Apply

6. Click Save to make your changes permanent.

To associate a queue class with an interface

Note - You can select a link aggregation interface or a link redundancy interface for an ACL, but you cannot assign these interfaces to a queue class. This means that traffic transiting these interfaces can be marked for QoS (so that other systems can provide QoS for this traffic), but IPSO systems cannot provide QoS on these interfaces.

1. Depending on whether you are using IPv4 or IPv6, click the following link.
   1. For IPv4 ACLs, click Queue Class under Configuration > Traffic Management in the tree view.
   2. For IPv6 ACLs, click IPv6 Queue Class under Configuration > IPv6 Configuration > Traffic Management in the tree view.

2. In the List of Available Physical Interfaces table, click the name physical interface with which you wish to associate a queue class.

The physical interface page for the interface you selected appears.

3. To enable QoS queuing, select either Max Throughput or Min QoS Latency from the Queue Mode drop-down list.

4. Click Apply.

A drop-down list appears in the Queue Class field.
5. Select the queue class you want to associate with the interface from the Queue Class drop-down list.
   If you do not select a queue class, the default class is used. The default queue class has two queues, Internetwork Control and Best Effort.

6. Click Apply.

7. Click Save to make your changes 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 Access List under Configuration > Traffic Management in the tree view.

2. To create the Access Control List, enter its name in the Create a New Access List edit box.

3. Click Apply.

4. Click the Add Rule Before check box next to the last rule.

5. Click Apply.

6. Enter tcp in the Protocol edit box and enter 20 in both the Source or Destination Port Range edit box.

7. Click Apply.

8. Select Shape from the Action drop-down window.

9. 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 Mean rate (Kbps) edit box.

5. Enter 5000 in the Burst size (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.
Example: Expedited Forwarding

1. Click Configuration Sets under Configuration > System Management in the tree view.
2. Enter pre-QoS in the Save Current State to New Configuration Database edit box.
3. Click Apply, and then click Save to make your change permanent.

2. Create an Aggregation Class
   1. Click Aggregation Class under Configuration > Traffic Management in the tree view.
   2. Enter wan_1_ef in the Name edit box in the Create a New Aggregation Class section.
   3. Enter 100 in the Mean Rate (Kbps) edit box.
   4. Enter 5000 in the Burstsize (bytes) edit box.
   5. Click Apply, and then click Save to make your Changes permanent.

3. Create a Queue Class
   1. Click Queue Class link under Configuration > Traffic Management in the tree view.
   2. Enter wan_1_ef in the Create a New Queue Class edit box.
   3. Click on the link to wan_1_ef in the Existing Queue Classes section to view existing queue class values.

Note - The queue specifier associated with expedited forwarding queue is 6.

4. Associate the wan_1_ef queue class with the appropriate interface.
   1. Click Interfaces under Configuration > Interface Configuration in the tree view.
   2. Click on ser-s3p1 in the Physical column.
   3. In the Queue Configuration field, select Max Throughput from the Queue Mode drop-down window.
   4. Click Apply.
   5. In the Queue Configuration field, select wan_1_ef from the Queue Class drop-down window.
   6. Click Apply.
Example: Expedited Forwarding

7. Click Save to make your changes permanent.
5. Create a new Access Control List rule to classify, condition, and prioritize telnet traffic.
   1. Click Access List under Configuration > Traffic Management in the tree view.
   2. Enter \texttt{wan\_1\_telnet} in the Create a New Access List edit box.
   3. Click Apply.
   4. Select ser-s3p1 from the Add Interfaces drop-down window.
   5. Select Output from Direction drop-down window.
   6. Click Apply.
   7. In the Existing Rules for \texttt{wan\_1\_telnet} section, click on the Add New Rule Before check box.
   8. Click Apply.
   9. Select prioritize from the Action drop-down window, and then click Apply.
   10. Select \texttt{wan\_1\_ef} from the Aggregation Class drop-down window, and then click Apply.
   11. 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.

\begin{itemize}
   \item \textbf{Note} - The telnet port number is 23.
   \item 12. Enter \texttt{tcp} in the Protocol edit box; enter 0xB8 in the DSfield edit box; and enter 6 in the QueueSpec edit box.
   \item \textbf{Note} - 0xB8 is the IETF differentiated-services codepoint (in hexadecimal) for expedited forwarding traffic.
   \item 13. Click Apply, and then click Save to make your changes permanent.
\end{itemize}

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.
Example: Expedited Forwarding

1. Click Interfaces under Configuration > Interface Configuration in the tree view.
2. Click on the link for ser-s3p1 in the Physical column.
3. Click on the Interface Statistics link.
4. 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.
   1. Click Interfaces under Configuration > Interface Configuration in the tree view.
   2. Click on the link for ser-s3p1 in the Physical column.
   3. Click on the Interface Statistics link.
   4. 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.
Configuring Policy Based Routing

You can exert detailed control over traffic forwarding by using policy based routing (PBR). When you use PBR, you create routing tables of static routes and direct traffic to the appropriate tables by using an access control list (ACL). Using an ACL in this way lets you direct traffic flow by filtering on one or more of the following:

- Source address
- Source mask length
- Destination address
- Destination mask length
- Source port
- Destination port
- Protocol type

**Note** - Policy based routing does not work if a VPN is enabled on the system.

Combining PBR with Other Routing

You can use policy based routing in combination with routing protocols or static routes configured in the normal way. To set this up, make sure that the action of the last rule in your ACL is Accept. This causes all packets that are not forwarded using a PBR table to be forwarded according to the standard routing configuration.

If you employ a routing protocol that uses multicast addresses to form adjacencies (OSPF or RIP, for example), configure a rule in the ACL with the following settings:

- Action: Accept
- Src IP Addr: 0.0.0.0
- Dest IP Addr 224.0.0.0
- Dest Mask Len: 4

This rule should be next to last in the ACL.

You cannot use PBR to route locally destined packets, locally originated packets, multicast packets, or broadcast packets. You can configure an ACL rule to match this traffic, but the traffic will not be forwarded by a PBR table.
Creating a PBR Table

To configure a policy based routing table, follow this procedure:


2. Enter a unique name for the policy based routing table in the text box and click Apply.

   Additional fields appear. (See Table 9-5 for more information on the parameters.)

3. Configure the table as appropriate.

4. Click Apply.

5. Click Save to make your changes permanent.

Table 9-5 Policy Based Routing Configuration Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On/Off</td>
<td>Clicking On enables the policy based static route. Clicking Off disables the static route.</td>
</tr>
<tr>
<td>Next hop type (Default Gateway)</td>
<td>Specifies the next hop type for the static route. The following are the types:</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>• Multipath</td>
</tr>
<tr>
<td></td>
<td>The default is Normal.</td>
</tr>
</tbody>
</table>
Creating a PBR Table

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next hop select</td>
<td>This option is available only if the next hop type is Multipath. The options are:</td>
</tr>
<tr>
<td></td>
<td>• None: Traffic is dropped. Use this option to prevent this route from being used.</td>
</tr>
<tr>
<td></td>
<td>• scrdsthash: The system chooses the outgoing interface based on a hash of the source and destination addresses.</td>
</tr>
<tr>
<td></td>
<td>• srchash: The system chooses the outgoing interface based on a hash of the source address.</td>
</tr>
<tr>
<td></td>
<td>• dsthash: The system chooses the outgoing interface based on a hash of the destination address.</td>
</tr>
<tr>
<td></td>
<td>• roundrobin: The system chooses the outgoing interface based on a round robin method.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a unique description about the PBR static route.</td>
</tr>
</tbody>
</table>
Creating a PBR Table

Table 9-5  Policy Based Routing Configuration Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next hop type (New route)</td>
<td>Specifies the next hop type for the static route. The following are the types:</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>• Reject</td>
</tr>
<tr>
<td></td>
<td>• Blackhole</td>
</tr>
<tr>
<td></td>
<td>• Multipath</td>
</tr>
<tr>
<td>Gateway type</td>
<td>Specifies the type of additional gateways that will be used for equal-cost path splitting to the PBR static route. The following are the options:</td>
</tr>
<tr>
<td></td>
<td>• Gateway Address: Specifies the IP address of the gateway to which packets for this PBR static route are sent. The address must be the address of a router that is directly connected to the system you are configuring. Range: Dotted-quad (0-255.0-255.0-255.0-255.) No default.</td>
</tr>
<tr>
<td></td>
<td>• Gateway Logical: Specifies an unnumbered interface as the next hop gateway.</td>
</tr>
</tbody>
</table>
Deleting a PBR Table

2. Click the link of the policy based routing table to be changed.
3. Delete all configured routes by selecting Off in the Gateway column.
4. Click the Delete check box.
5. Click Apply.
6. Click Save to make your changes permanent.

Configuring an Access Control List for PBR

When you define an ACL, make it as restrictive (specific) as possible. For example, if you use PBR to route HTTP traffic only, define the ACL with the port number for HTTP and protocol value for TCP. (See “Configuring Access Control Lists” on page 435 for more information about creating ACLs.)

To create an ACL for use with policy based routing, follow this procedure:
1. In Network Voyager, navigate to the access control list page: Configuration > Traffic Management > Access List.
2. Enter a unique name in the Create a new Access List text box.

### Table 9-5 Policy Based Routing Configuration Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New route</td>
<td>Specifies the network address of a new static route. The static route cannot have host bits set, that is, there should be no bits in the address set beyond the specified mask length. Range: Dotted-quad (0-255. 0-255. 0-255. 0-255.)</td>
</tr>
<tr>
<td>Mask length</td>
<td>Defines the mask length for the new static route. Range: 0-32.</td>
</tr>
</tbody>
</table>
Using PBR with VRRP and IP Clustering

3. Click Apply.
4. Click the link in the ACL Name column.
5. Select the interface from the Add Interface drop-down list.
6. Select the direction from the Direction drop-down list.
7. Check the Add Rule Before check box and click Apply.
8. In the Action column, select PBR and click Apply.
9. In the Policy Based Routing Table column, select the name of the appropriate policy based routing table.
10. Complete the configuration of the rule so that it matches the appropriate traffic.
11. Click Apply.
12. If you use a routing protocol that uses multicast addresses to form adjacencies, create a rule as described in “Combining PBR with Other Routing” on page 457.
13. Set the action of the last rule appropriately:
   - If you use ACLs only for PBR, you probably want the action of the last rule to be Accept (so that the system forwards non-matching traffic).
   - If you use ACLs for PBR and also to filter other traffic (that is, use ACLs for their traditional purpose), you might want the action of the last rule to be Drop.
14. Click Save to make your changes permanent.

Using PBR with VRRP and IP Clustering

If you use PBR in combination with VRRP or IP clustering, follow these guidelines:

- To use PBR in a VRRP configuration, you must configure PBR and the ACL on the master and backup nodes.
- With IP clustering, you can use Cluster Voyager to configure PBR (so that you configure it only once), but you must configure an ACL on the individual nodes.
- If you use PBR with IP clustering in forwarding mode, apply the PBR ACL on the cluster protocol network interfaces.
Configuring Netflow Services

You can use the Netflow support in IPSO to collect information about network traffic patterns and volume. To provide this information, IPSO tracks network “flows.” A flow is a unidirectional stream of packets that share a given set of characteristics. Click Configuration > Traffic Management > Netflow to access the Netflow Configuration page.

IPSO exports information about flows in flow records. To gather and analyze flow records, you must export them to a Netflow collector. Check Point has tested the following collectors:

- Scrutinizer (Plixer International): supports Versions 5 and 9
- NetFlow Analyzer (AdventNet, Inc): supports Versions 5 and 9

You must enter the IP address and application port number for your collector in the Collector IP and Collector Port fields.

You can specify the source (local) IP address to be used in export flow records. If you do not do so, the address is chosen based on the route to the collector’s address.

Defining Flows

You control how IPSO defines flows by using metering modes:

- Flows mode: If you use this mode, a flow is any sequence of packets that share
  - Source and destination IP addresses
  - Source and destination port numbers
  - IP protocol

  When you use flows mode, IPSO exports each flow in an individual flow record. This mode requires that a firewall is running and SecureXL is enabled.

  **Note** - When you enable flows mode, IPSO automatically reduces the concurrent connection capacity by 25 percent. If you later disable flows mode, IPSO automatically increases the connection capacity to the previous value. When you enable or disable this mode, you should make the same adjustment in Check Point’s SmartDashboard application.

- ACL mode: If you use this mode, you define flows by configuring ACL rules. Traffic that matches a rule is a flow. (You must also enable the Netflow Metering option for any rule that you want to use for this purpose.). When you use ACL mode, all the traffic that matches a rule is exported in one flow record.
Flow Records

For example, if you configure a rule that selects traffic between specific networks, all the matching traffic between those networks is exported in a single flow.

You can use both modes simultaneously. In this case, traffic that matches an ACL rule is reflected in a Flows mode flow and also in an ACL mode flow.

Flow Records

You configure IPSO to export flow records using the formats specified by Cisco for NetFlow Versions 5 and 9. (Version 9 is specified in RFC 3954.) Regardless of which export format you choose, IPSO exports values for the following fields:

- source IP address
- source subnet mask (used only when record is generated by an ACL flow)
- destination IP address
- destination subnet mask (used only when record is generated by an ACL flow)
- source port
- destination port
- input physical interface index (defined by SNMP)
- output physical interface index (defined by SNMP)
- packet count for this flow
- byte count for this flow
- start of flow timestamp (FIRST_SWITCHED)
- end of flow timestamp (LAST_SWITCHED)
- IP protocol number

Specifying When to Export Flow Records

IPSO exports a record for a flow when it detects the end of the flow. You can also control how IPSO exports flow records by configuring the following options:

- Active Timeout: Specifies the number of seconds after which IPSO should export a record for a flow when the flow is still active.
- Inactive Timeout: Specifies the number of seconds to wait while a flow is inactive (no traffic) but has not been terminated. If the specified number of seconds elapses, IPSO exports a record for the flow.
Chapter 10
Configuring Router Services

This chapter describes how to enable your system to forward broadcast traffic by enabling the IP Broadcast Helper, forward BOOTP/DHCP traffic by enabling BOOTP relay, how to enable router discovery, and how to configure for Network Time Protocol (NTP).

A Check Point appliance, like any routing device, does not forward broadcast traffic outside its broadcast domain as per ethernet standards. To have your appliance forward broadcast traffic, you must enable the IP Broadcast Helper, as described in “IP Broadcast Helper” on page 471. To forward BOOTP/DHCP traffic, you must enable Bootp/DHCP Relay, as described in “BOOTP/DHCP Relay” on page 468. Both of these services listen for broadcasts on the configured interface and change them into a unicast transmission to the configured destination host.

In This Chapter

- BOOTP/DHCP Relay  page 468
- IP Broadcast Helper  page 471
- Router Discovery  page 473
- Network Time Protocol (NTP)  page 477
BOOTP/DHCP Relay

BOOTP/DHCP 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/DHCP Relay offers the following advantages over standard BOOTP/DHCP:

- You can provide redundancy by configuring an interface on the Check Point system to relay client configuration requests to multiple servers. With this setup, configuration requests are relayed to all the listed servers simultaneously.
- You can provide load balancing by configuring multiple interfaces on the Check Point system to relay client configuration requests to different servers.
- It allows you to centrally manage client configuration across multiple LANs. This is particularly useful in large enterprise environments.

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.

Configuring BOOTP/DHCP Relay

You can use Network Voyager to enable BOOTP/DHCP Relay on each interface. If the interface is enabled for relay, you can set up a number of servers to which to forward BOOTP/DHCP requests. Enter a new IP address in the New Server text box for each server. To delete a server, turn it off.
Configuring BOOTP/DHCP Relay

Table 10-1 describes the parameters that you can configure for BOOTP/DHCP relay

Table 10-1  BOOTP/DHCP configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary IP</td>
<td>If you enter an IP address in the Primary IP text box, all BOOTP/DHCP requests received on the interface are stamped with this gateway address. This can be useful on interfaces with multiple IP addresses (aliases).</td>
</tr>
<tr>
<td>Wait Time</td>
<td>Specifies the minimum number of seconds to wait for a local configuration server to answer the boot request before forwarding the request through the interface. This delay provides an opportunity for a local configuration server to reply before attempting to relay to a remote server. Set the wait time to a sufficient length to allow the local configuration server to respond before the request is forwarded. If no local server is present, set the time to zero (0).</td>
</tr>
<tr>
<td>New Server</td>
<td>Enables forwarding of BOOTP/DHCP requests to a configuration server. You can configure relay to multiple configuration servers independently on each interface. Configuring different servers on different interfaces provides load balancing, while configuring multiple servers on a single interface provides redundancy. The Server IP Address cannot be an address belonging to the local machine.</td>
</tr>
</tbody>
</table>

To enable BOOTP/DHCP relay on an Interface

1. Click BOOTP/DHCP Relay under Configuration > Router Services in the tree view.
2. Select On for the interface on which you want to enable BOOTP/DHCP.
3. Click Apply.
   Additional fields appear.
4. (Optional) Enter values for one or more of the following parameters, described in Table 10-1, above.
   - **Primary IP**—Enter the IP address to use as the BOOTP/DHCP router address.
   - **Wait Time**—Enter the minimum client-elapsed time (in seconds) before forwarding a BOOTP/DHCP request.
   - **New Server**—Enter the IP address of the BOOTP/DHCP configuration server to which to relay BOOTP/DHCP requests.
5. Click Apply.
6. Repeat to relay BOOTP/DHCP requests to more than one server.
7. Click Save to make your changes permanent.

To disable BOOTP/DHCP relay on an interface
1. Click BOOTP/DHCP Relay under Configuration > Router Services in the tree view.
2. Select Off for the interface on which you want to disable BOOTP/DHCP.
3. Click Apply to disable the interface.
   When you click off, then apply, the BOOTP/DHCP relay parameters (primary IP, wait time, and new server) disappear, however the parameters are still stored in the system. If you select On, then Apply, these parameters reappear.
4. Click Save to make your changes permanent.
IP Broadcast Helper

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. IP Broadcast Helper allows the relaying of broadcast UDP packets on a LAN as unicasts to one or more remote servers. This is useful when you relocate servers or hosts from their original common segment and still want the service to be available.

Note - For further information, see RFC1542 section 4.

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 client sends a broadcast BOOTP packet to the router, which sends a modified packet to the server. The router modifies the packet by inserting its IP address in the giaddr field of the BOOTP packet (this field is used by the server to identify the network where the packet originated).

Table 10-2 describes the parameters that you can configure for IP broadcast helper.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Nonlocal</td>
<td>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. Selecting Disabled requires that packets be generated by a source directly on the receiving interface to be eligible for relay. Enabled allows forwarding of packets even if the source is not directly on the receiving interface. The default is Disabled, which requires that packets be generated by a source directly on the receiving interface to be eligible for relay.</td>
</tr>
<tr>
<td>IP Helper Interface On/Off</td>
<td>Specifies whether IP helper service is running on the interface. After you select On and click the Apply button, configuration options for IP broadcast helper for the interface appear.</td>
</tr>
</tbody>
</table>
To configure the relaying of broadcast UDP packets on your system, use the following procedure.

**To configure IP broadcast helper**

1. Click IP Broadcast Helper under Configuration > Router Services in the tree view.
2. Click On for each interface to support IP Helper services.
3. Click Apply.
   
   The New UDP Port field appears under that interface.
4. To add a new UDP Port to the helper services:
   
   1. Enter the new UDP port number in the New UDP Port text box.
   2. Click Apply.
   
   The UDP port appears in the table for that interface with On and Off radio buttons. To delete forwarding for a UDP service select Off and then click Apply.
5. To add a new server to a UDP port:
   
   1. Enter the new server’s IP address in the New Address for UDP Port X text box.
   2. Click Apply.
   
   The server IP address appears under the UDP port. To delete forwarding for a server select Off and then click Apply.
6. Verify that each interface, UDP port, or server is enabled (On) or disabled (Off) for IP helper support according to your requirements.
7. Click Save to make your changes permanent.
Router Discovery

The ICMP Router Discovery protocol is an IETF standard protocol that allows hosts running an ICMP router discovery client to learn dynamically about the presence of a viable default router on a LAN. 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.

Note - Only the server portion of the Router Discovery Protocol is supported.

IPSO implements only the ICMP router discovery server portion, which means that a Check Point router can advertise itself as a candidate default router, but it will not adopt a default router using the router discovery protocol.

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.

Router Discovery Overview

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.

**Note** - Router discovery is not supported when clustering is enabled.

## Configuring Router Discovery

Table 10-2 describes the parameters that you can configure for router discovery.

### Table 10-3  Router discover configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Discovery Interface On/Off</td>
<td>Specifies whether ICMP router discovery is running on the interface. When you select On and click Apply, configuration options for the interface appear.</td>
</tr>
<tr>
<td>Min. Advertise Interval</td>
<td>Specifies the minimum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMP Router Advertisements on the interface.</td>
</tr>
<tr>
<td></td>
<td>Range: Between 3 seconds and the value of Maximum Advertisement Interval.</td>
</tr>
<tr>
<td></td>
<td>Default: 0.75 times the value in the Maximum advertisement interval field.</td>
</tr>
<tr>
<td>Max. Advertise Interval</td>
<td>Specifies the maximum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMP Router advertisements on the interface.</td>
</tr>
<tr>
<td></td>
<td>Range: 4-1800</td>
</tr>
<tr>
<td></td>
<td>Default: 600</td>
</tr>
<tr>
<td>Advertisement Lifetime</td>
<td>Specifies the time (in seconds) to be placed in the Lifetime field of Router Advertisement packets sent from the interface.</td>
</tr>
<tr>
<td></td>
<td>Range: Between the value in the Maximum advertisement interval field and 9000 seconds.</td>
</tr>
<tr>
<td></td>
<td>Default: 3 times the values in the Maximum advertisement interval field.</td>
</tr>
</tbody>
</table>
Configuring Router Discovery

Table 10-3  Router discover configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertise Address</td>
<td>For each IP address associated with the interface, specifies whether the address should be advertised in the Router Advertisement packets. This option applies to each address on the interface and not to the interface itself. Default: Yes</td>
</tr>
<tr>
<td>Preference</td>
<td>Specifies the preferability of the address as a default router address, relative to other router addresses on the same subnet. The minimum value (0x80000000) is specified by the &quot;Ineligible&quot; button and indicates that the address is not to be used as a default router. 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.</td>
</tr>
</tbody>
</table>

To configure the router discovery services on your system, use the following procedure.

To enable router discovery services
1. Click Router Discovery under Configuration > Router Services in the tree view.
2. Select On for each interface to support router discovery service.
3. Click Apply.
   Additional fields appear.
4. (Optional) Enter values for the following parameters, described in Table 10-3.
   - Minimum Advertisement Interval
   - Maximum Advertisement Interval
   - Advertisement Lifetime
5. (Optional) For each IP address on the interface, you can specify the following parameters, described in Table 10-3.
   - Advertise Address
   - Preference
Configuring Router Discovery

6. Click Apply.
7. Click Save to make your changes permanent.

To disable router discovery services
1. Click Router Discovery under Configuration > Router Services in the tree view.
2. Click Off for each interface to disable support for router discovery service.
3. Click Apply.
4. Click Save to make your changes permanent.
Network Time Protocol (NTP)

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, Check Point 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

You can enable or disable NTP on your system; when NTP is active the local clock is synchronized as configured and hosts will be able to set their time through this machine.

To set the time manually, see “Setting System Time” on page 88.

To configure NTP

1. Click NTP under Configuration > Router Services in the tree view.
2. Click Yes in the Enable NTP field.
3. Click Apply.
Configuring NTP

The NTP configuration page appears.

4. Enter the new server IP address in the Add New Server Address edit box.

5. Click Apply.
   
The IP address for the new NTP server appears in the NTP Servers field. By default, this new server is enabled.

6. Enable Prefer Yes if you want his server to be preferred over any other servers you configure.

7. Enable Autokey if you want to use autokey authentication to ensure that your IPSO system updates its time from a trusted source. See “Configuring Autokey Authentication” for more information.

8. If you will use autokey authentication, enter the client password you use to create the group (client) key file.

9. To add another new server, repeat step 4 and click Apply.

10. (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. Check Point recommends that you keep these defaults.

11. 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.

12. 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.

13. (Optional) Enable the NTP reference clock by clicking Yes in the NTP Master field.

   Note - Only enable the NTP reference clock if you cannot reach an NTP server.

14. Click Apply.

478
Configuring NTP

The Stratum and Clock source fields appear. By default, the Stratum value is 1, and the Clock source is set to Local Clock. Check Point recommends that you keep these defaults.

15. Click Save to make your changes permanent.

Configuring Autokey Authentication

You can use autokey authentication to ensure that your IPSO system updates its time from a trusted source. To do so, you must

1. Configure your NTP server appropriately. See http://support.ntp.org/bin/view/Support/ConfiguringAutokey for information about how to configure your server.

2. Create keys on the server.

3. Install the group (client) key on the IPSO system.

To create keys

Perform the following steps on your NTP server:

1. Enter the following command to create the server parameter file:
   ntp-keygen -T -I -p serverpassword

2. Enter the following command to extract the group (client) key:
   ntp-keygen -e -q serverpassword -p clientpassword
   The system displays a key that begins with a key file name such as ntpkey_1FFkey_servername.1234567891 (in which the server name and numeric characters will vary).

3. Enter the command
   ntp-keygen -e -q serverpassword -p clientpassword > keyfilename
   using the key file name generated in step 2.
   The system creates a group client key file with the supplied name.

4. Copy the key file created in step 3 to your IPSO system.

To install the client key

Perform the following steps on your IPSO system:

1. On the NTP Configuration page, click the Install Autokey client certificate link.
   The system displays the Install Autokey Certificate page.

2. On the Install Autokey Certificate page, perform the following steps:
Configuring NTP

1. Paste the contents of the group (client) key file into the Group/Client Key File box.
2. Enter the name of the group key file into the Group Key File Name field.
3. Enter the fully qualified domain name of the NTP server into the Server Name field.
4. Click Apply.
5. Click Save.
Chapter 11

Using Voyager Tools

This chapter describes how to use the features that you access by clicking Tools on the Network Voyager navigation tree. You can use these tools to migrate configuration from one Check Point platform to another, gather a variety of information for troubleshooting purposes, and tune the firewall kernel.

In This Chapter

Migrating a System Configuration  page 482
Using the Enhanced Configuration Summary Tool  page 488
Tuning the Check Point Firewall Kernel  page 491
Migrating a System Configuration

There are times when you probably want to copy much of the configuration information from one Check Point network security platform to another. For example, when you replace a Check Point network security platform with another platform, you might want to migrate much of the configuration from the system being replaced to the new system. This chapter describes how to do this using Network Voyager and the Configuration Migration feature. You can access the Voyager pages for this feature by clicking Tools > Configuration Migration at the bottom of the Voyager navigation tree.

When using the Migrate Configuration feature, keep the following terms in mind:

- **Source platform**: This is the platform from which you will acquire the configuration information. If you are replacing a platform, you probably want to use the platform being replaced as the source.
- **Target platform**: This is the platform on which you will apply the migrated configuration. If you are replacing a platform, the target is the new (replacement) platform.

**Note** - You perform almost all the operations discussed in this chapter using Voyager on the target platform. The only operations you might need to perform on the source are creating a configuration file or database file and enabling network access to the source.

It’s important to understand that the Migrate Configuration feature is designed to copy configuration from one platform to another, not to make configuration changes on the target. If you want to make configuration changes on the target platform—for example, if you want to assign new IP addresses that are not assigned to the source platform—do so after you complete the migration. Think of it as a two or three step process:

1. Migrate the configuration from the source to the target.
2. Make any required changes on the target.
3. If desired, export the configuration from the target to another system.

Migrate Configuration allows you to map interface configuration across the platforms. For example, you can map interface A on the source to interface B on the target so that interface B is configured identically to A.

You can also choose whether to migrate configuration information for specific features. For example, if you use Protocol-Independent Multicast (PIM) on the source but don’t want to use it on the target, you can choose not to migrate it. You might also choose not to migrate PIM if you do intend to use it on the target but...
Acquiring Configuration Information

want to configure it from scratch. Choosing to not migrate a feature means only that the configuration information for that feature is not migrated. The feature itself is still available on the target. In this example, PIM is still be available on the target after the migration but it is not enabled or configured.

Acquiring Configuration Information

You can acquire configuration information from a Check Point platform running any version of IPSO between IPSO 3.7 and IPSO 4.2 (inclusive). You acquire configuration information by copying an IPSO configuration file or backup file from the source to the target. See “Managing Configuration Sets” on page 101 for information about creating configuration files. See “Creating Backup Files” on page 103 for information on creating these files.

You can move these files directly from the source to the target (using Voyager or another method) or move them to a workstation. Depending on how you want to move the file to the target, use the following options on the Acquire Configuration page:

- Remote Device: Use this option to transfer a file directly from the source to the target.
  - You must have network access to the source.
  - If you specify a file (configuration file or backup file), you must specify the complete path.
  - If you do not specify a file, IPSO automatically copies the current configuration database file from the source.
- Upload: Use this option if you have moved the IPSO configuration file or backup file from the source to your workstation (the computer that is running Network Voyager).
- Local File: Use this option if you have moved the IPSO configuration file or backup file from the source to the target using FTP or a similar method. If you use this option, you must save the configuration file or backup file in one of several specified directories. To see which directories you can use, expand the directory tree in the Select File to Acquire box.
  Select the appropriate configuration or backup file by clicking on it. Voyager then displays the selected file in bold.

Regardless of which method you choose, click Apply once you have selected the appropriate file. If IPSO recognizes that the file is a valid configuration file or backup file (and transfers it to the target, if necessary), you see a message indicating that the process succeeded and telling you to access the Migrate
Migrating Configuration Information

Configuration page. If either of the following is true, IPSO also displays information about the model number of the source platform and the IPSO version used to make the configuration or backup file:

- You acquired a backup file (using any option).
- You used SCP as the protocol when using the Remote Device option to acquire a configuration file.

Migrating Configuration Information

Access the Migrate Configuration page by clicking the appropriate link under Migration in the Voyager navigation tree.

If there are any unsaved configuration changes (changes to the current configuration on the target platform), Voyager displays a message telling you to click Save. After you do so, you can continue with the migration.

Voyager displays the IPSO version of the source configuration at the top of the page to help you verify that you acquired appropriate configuration information.

IPSO needs to know the model number of the source platform. If IPSO was able to determine the number because of the method you used to acquire the configuration or backup file, the number is displayed near the top of the page. Otherwise there is a menu from which you must choose the model of the source platform.

Mapping Interfaces and Completing the Process

You use the Migrate Configuration page primarily to map interfaces from the source to the target. Voyager provides information to help you choose which interfaces on the target are the best matches for the interfaces on the source. The table on the left lists all the physical interfaces on the source platform and also identifies all the attributes associated with each interface. For example, you can see whether routing protocols, VRRP, SNMP, and so on are configured for an interface. This table also lists the configured speeds for the source interfaces. The table on the right lists the physical interfaces on the target platform and their available speeds.

In addition to the physical interfaces on the source platform, the table on the left lists all the logical interfaces that have IP addresses assigned. When you map a physical interface, IPSO migrates all the logical configuration for that interface to the physical interface on the target. You cannot map logical interfaces individually. If there is a logical interface without an associated IP address on the source platform (for example, if there is a VLAN interface without an address), the logical interface does not appear in the table and is not migrated to the target.
You must map each source interface or explicitly choose to not migrate it by making selections in the Interface on Target Platform column. If you click Next or Finish without making a selection for every source physical interface, Voyager displays a message telling you that you must choose an entry for every interface and does not display the next page.

**Warning** - If an interface on the target is configured *before* you perform the migration, that configuration information is deleted when the new configuration is applied even if you do not choose a mapping for it. For example, if a target interface has an IP address before the migration and you do not select it during the mapping process, the IP address is deleted when the new configuration is applied.

You cannot map multiple source interfaces to one interface on the target platform. If you attempt to do so, Voyager displays a message telling you that this is invalid.

**Note** - You should not map ADP interfaces to non-ADP interfaces or non-ADP interfaces to ADP interfaces.

The actual steps you take to complete the migration vary depending on whether there are any link aggregation group (LAG) or link redundancy group (LRG) interfaces on the source platform. (See “Link Aggregation” on page 35 and “Link Redundancy” on page 41 for information about these types of interfaces.)

**If there are no LAG or LRG interfaces**

1. For each interface, choose a mapping or explicitly choose to not migrate it.
2. Choose to migrate all features (accept the default setting) or prohibit selected features from being migrated.
   
   Remember that choosing to not migrate a feature means only that the configuration information for that feature is not migrated. The feature itself is still available on the target. See “Migrating Features” on page 486 for important information about this step.
3. Reboot or test boot the target platform.
   
   (See “Testing a New Image” on page 110 for information about test booting.)

**If there are LAG or LRG interfaces on the source**

If there are LAG or LRG interfaces on the source, the process is similar except that the LAG and LRG interfaces are presented on separate pages:

1. Map or explicitly choose to not migrate each non-LAG/non-LRG interface.
2. Map or explicitly choose to not migrate each LAG interface (if any).
Migrating Configuration Information

3. Map or explicitly choose to not migrate each LRG interface (if any).
   • If an LAG interface is part of an LRG interface, you can choose whether to migrate it as part of the LRG or whether to remove it from the LRG during the migration. (If you chose to not migrate this LAG interface in step 2, it is still listed in the table of LRG interfaces but you cannot migrate it as part of the LRG.)

4. Choose to migrate all features (accept the default setting) or prohibit selected features from being migrated.

   See “Migrating Features” on page 486 for important information about this step.

   Note - Whenever the Finish button is available, you can click it to skip the process of selecting features to migrate. In this case, all the IPSO features on the source are migrated (the default setting). Clicking Finish always displays a page that allows you to complete the migration by rebooting or test booting the target platform.

Migrating Features

If you include Users as one of the features that will be migrated (the default setting), the admin password of the source platform becomes the admin password of the target platform after you reboot it. If you want to prevent this, remove Users from the list of features that will be migrated before you finish the migration. In this case, the original admin password of the target platform is retained after you reboot the target.

Configuration information for certain features cannot be migrated because it is not stored in IPSO configuration files. Examples include:

• IP clustering
• HA Voyager
• packages
• optional disks
• PPPoE
• ISDN
• IPv6 host address (if the source configuration is from an IPSO version previous to 6.1)

If configuration information for a feature cannot be migrated, the feature is not included in the list.
Exporting Configuration Information

You can back up the migrated configuration to another system by using the Export Configuration page. This page requires you to choose a transfer protocol (SCP or FTP) and specify the system and directory where the exported files will be stored. After the process is complete, a number of files are saved in the specified location:

- the source configuration file
- initial.new_pre_upgrade
- initial.new_post_upgrade
- convert_cfg.status
- other files used in the migration process
Using the Enhanced Configuration Summary Tool

The Enhanced Configuration Summary Tool (ECST) allows you to capture your current IPSO configuration, log files, core dumps and other information in a single file that can be sent to Check Point customer support for analysis. Typically, you would run ECST if you have opened a case with Check Point support and you have been asked to provide an ECST file.

When you run ECST, you can include any or all of the following information in the output file:

- **Offline Network Voyager pages**—captured Network Voyager pages that show your current configuration and that can be viewed offline by Check Point customer support.

  You must supply your user name and password for ECST to capture the Network Voyager pages. To ensure that all the configuration information is captured, you should have at least read-only access to all IPSO features.

  When you include offline Network Voyager pages, ECST saves your current configuration before it captures the pages.

- **Firewall information**—firewall status, objects, tables, and diagnostics, as captured from utilities such as cpinfo, cpstat, and fw tab.

- **IPSO information**—captured output from the utilities listed below.

  - date
  - uname -a
  - ifconfig -v -a
  - ps -auxw
  - df -k
  - pstat -ks
  - netstat
  - arp -a
  - vmstat -mis
  - dbget -rv dynamic
  - ipsct1 -a
  - ntpdc -pn
  - ls -l

- **IPSO log files**—copies of the syslog log files, httpd access logs, httpd error logs, cron logs, and other logs.

- **IPSRD/Core dumps**—copies of the configuration files in /config, user directories in /var/emhome, IPSRD and core dumps, and firewall logs.
Running ECST Using Network Voyager

All ECST output files are stored in /opt/ecst_output on the appliance. Because the ECST output files can be quite large if you include the Network Voyager offline pages, Check Point recommends that you do not keep more than three output files on your appliance at a time.

You can run ECST from Network Voyager or the IPSO shell, as described in the next two sections.

Running ECST Using Network Voyager

The following two procedures describe how to use Network Voyager to run ECST.

To collect all information
1. Select Tools > ECST Configuration from the Network Voyager navigation tree.
2. Check the Select All box.
3. Enter your user name and password.
4. Check the Generate Configuration Summary box.
5. Click Apply.

The ECST tool will begin to run, collecting the required information. To monitor the collection process, click the ECST Configuration link on the Network Voyager navigation tree again. This causes the page to automatically refresh every few seconds, allowing ECST to post updated status information.

When ECST finishes, it updates the Notice message with:

   ECST execution completed successfully
   Output file is CST-host-date-time.tgz

6. Download the ECST output file by clicking on the link in the Download table.

To collect selected information
1. Select Tools > ECST Configuration from the Network Voyager navigation tree.
2. If the Select All box is already checked, uncheck it and click Apply.
3. Click the check boxes for the information you want to collect.
4. If you selected Offline Voyager, enter your user name and password.
5. Check the Generate Configuration Summary box.
6. Click Apply.
Running ECST from the IPSO Shell

The ECST tool will begin to run, collecting the required information. To monitor the collection process, click the ECST Configuration link on the Network Voyager navigation tree again.

When ECST finishes, it updates the Notice message with:

- ECST execution completed successfully
- Output file is CST-host-date-time.tgz

7. Download the ECST output file by clicking on the link in the Download table.

Running ECST from the IPSO Shell

You can also run ECST from the IPSO shell, using the command:

# ecst [ -cfhilv ]

If you include no options with the command, ECST collects information based on the configuration in its current configuration file. The contents of its configuration file are determined by the Service Summary selections in Network Voyager. If no configuration file exists, ECST collects all information.

If you specify options, ECST ignores the content of its configuration file and collects just the information specified by the options. The options are described in Table 11-1.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>Specifies that the core dump files, configuration files, and user home directories should be collected.</td>
</tr>
<tr>
<td>-f</td>
<td>Specifies that firewall information should be collected.</td>
</tr>
<tr>
<td>-h</td>
<td>Displays help for the ecst command.</td>
</tr>
<tr>
<td>-i</td>
<td>Specifies that the output of various utilities should be captured (same content as the legacy ipsoinfo utility)</td>
</tr>
<tr>
<td>-l</td>
<td>Specifies that the log files should be collected.</td>
</tr>
<tr>
<td>-v</td>
<td>Specifies that Network Voyager pages should be captured for offline viewing.</td>
</tr>
</tbody>
</table>

The files produced by ECST are in /opt/ecst_output directory.
Tuning the Check Point Firewall Kernel

You can use Voyager to modify Check Point firewall kernel variables by using the Firewall Kernel Tuning Configuration page. This page provides the same functionality as the modzap shell command.

**Warning** - Use this feature only in consultation with a customer service representative. Do not modify firewall kernel variables unless instructed to do so by a service representative.

When you install IPSO or run Voyager for the first time on a new platform, the Firewall Kernel Tuning Configuration page does not appear. If a customer service representative instructs you to use this page, you must first display it by performing these steps:

1. Establish a command line connection to the platform (using a network connection or a console connection).
2. At the IPSO shell prompt, enter
   ```shell
dbset advanced:loader t
   
   Run Voyager (or exit Voyager and run it again if Voyager was open when you entered the previous command).
3. Click Configuration > Tools > Firewall Kernel Tuning in the navigation tree.

To use this page, enter the firewall kernel variables as instructed by your customer service representative and then click Apply. Clicking Apply applies the firewall kernel variables and also saves the Voyager configuration so that the Firewall Kernel Tuning Configuration page will appear again if you reboot the platform.

If you do not want Voyager to display the Firewall Kernel Tuning Configuration page, perform these steps:

1. Establish a command line connection to the platform (using a network connection or a console connection).
2. At the IPSO shell prompt, enter
   ```shell
dbset advanced:loader
   
   Run Voyager (or exit Voyager and run it again if Voyager was open when you entered the previous command).

When you run Voyager after entering this command, the Firewall Kernel Tuning Configuration page does not appear, but your settings for firewall kernel variables are preserved. If you also want to undo all the settings you implemented, delete the
Tuning the Check Point Firewall Kernel

file /image/current/loader.conf and reboot the platform. After the reboot, any variables you configured by using the Firewall Kernel Tuning Configuration page have their previous values.
Chapter 12
Monitoring System Configuration and Hardware

This chapter provides information on monitoring your system. You can use Network Voyager to monitor many aspects of your IP security platform in order to better maintain performance and security. You can, for example, monitor state information for each interface, view the contents of IP routing tables, and generate reports on events such as throughput, bandwidth utilization, and link states over specific periods of time.

In This Chapter

- Viewing Performance Information  page 494
- Viewing System Utilization Statistics  page 498
- Generating Monitor Reports  page 502
- Monitoring System Health  page 505
- Monitoring System Logs  page 507
- Viewing Cluster Status and Members  page 509
- Viewing Routing Protocol Information  page 510
- Hardware Monitoring  page 512
- Preventing Full Log Buffers and Related Console Messages  page 514
IPSO provides a detailed view of your system’s performance by allowing you to monitor a variety of historical information presented in graphical format. You can configure the graphs to show a wide range of time periods.

Use the information provided by this feature to tune your system for optimum performance, troubleshoot difficult performance issues, or simply confirm that traffic patterns are as expected. For example, you can compare how much of your traffic has been accelerated by SecureXL versus the amount that has been sent to the firewall for processing and see how much traffic has been forwarded by Check Point Accelerated Data Path (ADP) interfaces versus non-ADP interfaces.

To view performance information, click Monitor > Performance Monitoring on the Voyager navigation tree. The views are organized into configurable dashboards.

**Connection Dashboard**

- **Connection Life histogram**: Displays the number of connections within a configurable time and their lifetimes in IPSO. The lifetime of a connection is the amount of time it occupies IPSO memory. This histogram is helpful in understanding variations in connection table size.

- **Transaction Size histogram**: Displays the transaction sizes associated with different connections within a configurable time. The transaction size is the number of bytes exchanged in the context of a connection from the start to the end of the connection.

- **Templates vs Non-Templates**: Displays the percentage of connections created by templates within a configurable time. You can use this information to help you define a firewall policy so that more connections are created by templates (and are therefore accelerated).

- **Transactions vs Connections**: Displays the rates of connection and transaction creation within a configurable time. For TCP, connection creation is defined as the arrival of a SYN packet, and transaction creation is defined as the completion of 3-way handshake. For non-TCP connections, connection and transaction creation occurs at the same rate.

When multiple Firewall instances are enabled, the Transactions Vs. Connections graph represents the total number of transactions and Connections across all the Firewall instances enabled for the selected time interval.
Connection Map Dashboard

- Accelerated Connections Map: Displays the total number of connections within a configurable time and the number that were accelerated. The difference between the total number of connections and the number of accelerated connections gives the number of connections for which every packet was inspected by the firewall. Accelerated connections are further classified as connections accelerated by ADP and connections accelerated by IPSO.

- VPN Connections Map: Displays the total number of connections within a configurable time and the number that required VPN services. This information is helpful in understanding the percentage of traffic that is encrypted by a VPN.

- NAT Connections Map: Displays the total number of connections within a configurable time and the number that required NAT services. This information is helpful in understanding the percentage of traffic that requires NAT services.

- TCP Connections Map: Displays the total number of connections within a configurable time and the number of TCP connections. The difference between total connections and TCP connections gives the number of non-TCP connections, such as UDP, ICMP, etc.

- Any or all of the Firewall instances that are active in the selected time interval can be selected. Individual line graphs are displayed for each Firewall instance selected. By default the graph displays one line which is the consolidated sum of all connections across all Firewall instances.

Traffic Dashboard

- IPSO Packet Size Map: Displays the distribution of packet sizes forwarded by IPSO within a configurable time. This information is helpful in understanding which packet sizes are dominant.

- ADP Packet Size Map: This graph is present only on platforms on which an ADP module is detected. It displays the distribution of packet sizes that were forwarded by ADP interfaces. This information is helpful in understanding which packet sizes are dominant in traffic transiting ADP interfaces.
Forwarding Dashboard

- Accelerated Traffic Map: Displays the total number of packets that were forwarded by IPSO and the number of packets that were accelerated by IPSO within a configurable time. The difference between the total number of packets and the number of accelerated packets is the number of packets that were forwarded to the firewall.
- VPN Traffic Map: Displays the total number of packets that were forwarded by IPSO and the number of packets that required VPN services within a configurable time. This information is helpful in understanding the percentage of traffic that requires VPN services.
- NAT Traffic Map: Displays the total number of packets that were forwarded by IPSO and the number of packets that required NAT services within a configurable time. This information is helpful in understanding the percentage of traffic that requires NAT services.

Interface Dashboard

- Packet Throughput: Displays the rates of incoming and outgoing packets on a given interface within a configurable time.
- Byte Throughput: Displays the rates of incoming and outgoing bytes on a given interface within a configurable time. This information is helpful in determining if a link is reaching its capacity.
- Multicast Throughput: Displays the rates of incoming and outgoing multicast packets on a given interface within a configurable time. This information is helpful in determining if a link is reaching its capacity.
- Broadcast Throughput: Displays the rates of incoming and outgoing broadcast packets on a given interface within a configurable time. This information is helpful in determining if a link is reaching its capacity.

System Dashboard

- CPU Utilization: Displays the CPU utilization for all the CPU cores within a configurable time.
- Memory Utilization: Displays the memory utilization in IPSO within a configurable time.
**ADP Dashboard**

This dashboard displays the number of packets that were forwarded by IPSO and number of packets that were forwarded by the ADP subsystem within a configurable time. You can also see the average and maximum number of buffers utilized at the interface layer in incoming and outgoing directions within a configurable time. This information is helpful in understanding the value provided by ADP modules.

**Custom Dashboard**

Use this dashboard to create custom profiles that include your choice of performance graphs. After you have created profiles, click the Custom Dashboard link again to select a profile to display.
Viewing System Utilization Statistics

Use the system utilization statistics to monitor and tune the allocation of system resources. For example, if the percentage shown under file system capacity becomes a high percentage, you should take action, such as deleting old IPSO images and packages or move your log files to a remote system.

To view statistical information on system utilization, click either CPU-Memory Live Utilization, Disk and Swap Space Utilization, or Process Utilization under Monitor > System Utilization in the tree view.

CPU-Memory Live Utilization

The CPU-Memory Live Utilization page shows system resources usage, including CPU and memory usage. This page retrieves the updated CPU and memory usage every 20 seconds.

The CPU Utilization table summarizes CPU usage.

The System Load table summarizes the load averages, which are the number of processes in the system run queue averaged over the last 1, 5, and 15 minutes, respectively. Load averages that are high, such as over 2 in all three fields, indicate that the system is under continuous heavy load.

The Memory Utilization table summarizes memory usage in KBs. Free memory (memory that is available to the operating system) is defined as free pages + cache pages. The remainder is active memory (memory the operating system is currently using). The free memory might differ (will mostly be lower) as compared to output of a vmstat command.

Disk and Swap Space

The Disk and Swap Space Utilization page shows system resources use, including disk and swap space use. This page retrieves the updated disk and swap space use every 20 seconds.

For each file system, you can monitor the number of kilobytes used and available, the percentage of disk space being used, the number of inodes used and free, and the location where it is mounted. The inode is the internal identifier for a file and a limited number are available in a partition. A system can run out of inodes before running out of disk space.
Monitoring Process Utilization

For swap space, you can monitor the name of the device, total number of swap data blocks on the device, the number of used and free swap data blocks on the device, and the type of device.

**Note** - You should monitor the /config, /var, and /opt partitions, since these store the configuration files and logs and optional user software. Unlike read-only partitions, these can grow dynamically.

Monitoring Process Utilization

The Process Utilization page shows the status of processes. You must monitor and control processes to manage CPU and memory resources.

This page retrieves the updated process status every 30 seconds. When you access this page, a table displays the following fields for each process:

- **USER**—User who initiated or executed the process.
- **PID**—Identifier used by the kernel to uniquely identify the process.
- **%CPU**—Percentage of CPU used by the process while active. This is a decaying average taken over a time period of up to the previous minute. Because the time base over which CPU utilization of the process is computed varies (processes might be very young), the sum of all CPU fields can exceed 100%.
- **%MEM**—Percentage of real memory used by the process while active.
- **VSZ**—Virtual size of the process in KBs (also called vsize).
- **RSS**—Real memory (resident set) size of the process in KBs.
- **WCHAN**—Wait channel (as a symbolic name). This is the event on which a process waits.
- **STAT**—Symbolic process state given as a sequence of letters. For example, R indicates a runnable process (R) that is a session leader (s). For more information, see the process status man page (man ps).
- **STARTED**—Time the command started.
- **TIME**—Accumulated CPU time: user plus system (alias cputime).
- **COMMAND**—Command and arguments.
When you are troubleshooting any system, it is helpful to have an understanding of the daemons, or system processes, that are operating in the background.

The process monitor (PM) monitors critical IPSO processes. The PM is responsible for:

• Starting and stopping the processes under its control
• Automatically restarting the processes if they terminate abnormally

The 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>
<tr>
<td>ntpd</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>monitor</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. Responds to queries via SNMP.</td>
</tr>
</tbody>
</table>
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 of the PM is not user configurable.
Generating Monitor Reports

You can generate reports of data collection events. To generate a report, click the link for the appropriate report under Monitor > Reports in the tree view.

For information on configuring monitor reports, see “Configuring Monitor Reports” on page 112. The administrator can configure how often the data is collected, whether each data collection event is enabled or disabled, and how many hours worth of collected data are stored on the system.

<table>
<thead>
<tr>
<th>Table 12-1</th>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Rate-Shaping Bandwidth | Shows specific bandwidth utilization. You can use traffic shaping to implement a specific policy that controls the way data is queued for transmission. For information on creating aggregate classes and configuring traffic rules, see Chapter 9, “Configuring Traffic Management”
Inclusion of number of packets delayed and bytes delayed is configurable by the administrator. By default, both are included. |
| Interface Throughput | Shows historical throughput for each interface. You can often use this information to optimize network performance or troubleshoot issues network traffic congestion.
Inclusion of packet throughput, byte throughput, broadcast packets, and multicast packets for each interface is configurable by the administrator. By default, all are included. |
| Network Throughput | Similar to the interface throughput report, except that the query is based on the network address rather than interface name. |
| Interface Link State | Shows information about the link state of each interface. The first signs of problems with interfaces is frequently seen in link errors. You can use this report to determine if an interface is experiencing problems or has been incorrectly configured. |
Generating Monitor Reports

To display reports

1. Click the name of the report under Monitor > Reports in the tree view.
2. Under Select Report Type, select one of the following:
   - **Hourly**—Hourly report with a 1-hour display up to a maximum of 7 interval day data.
   - **Daily**—Daily report with 1-day display interval up to a maximum of 35 day data.
   - **Weekly**—Weekly report with 7-day display interval up to a maximum of 52 weeks.
   - **Monthly**—Monthly report with 1-month display interval up to a maximum of 60 months.
   - **Detailed Search**—Select a specific time period. These reports have a default data interval of one minute. The number of hours worth of data stored for detailed searches is configured by the administrator. For more information, see “Configuring Monitor Reports” on page 112.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Utilization</td>
<td>Shows historical CPU utilization data, including percentages of CPU time for each of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>User%</strong>—Percentage of CPU time spent in User-level instructions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Nice%</strong>—Percentage of CPU time spent in &quot;Nice&quot; processes.</td>
</tr>
<tr>
<td></td>
<td>- <strong>System%</strong>—Percentage of CPU time spent in System level instructions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Interrupt%</strong>—Percentage of CPU time spent in servicing interrupts.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Idle%</strong>—Percentage time CPU was idle.</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>Shows historical memory utilization, including:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Active Real Memory</strong>—Kilobytes of real memory being used in a given time interval.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Free Real Memory</strong>—Kilobytes of real memory free in a given time interval.</td>
</tr>
</tbody>
</table>
Generating Monitor Reports

3. For the Rate-Shaping Bandwidth report, select an aggregation class for which you want to display a report or select 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. For more information, see chapter 9, “Configuring Traffic Management” on page 433

4. For the Interface Throughput, Network Throughput, or Interface Link State reports, select All Logical or a specific interface name from the Select Interface drop-down list.

5. Under Select Format, choose Graphical View or Delimited Text.
   - If you select Delimited Text, select Semi-Colon(;), Comma(,), or Tab from the Delimiter drop-down list.
   - The Graphical View option displays pie and graph charts, as well as in table format. The Delimited Text option displays the report in a new page from which you can download the information.

6. Click Apply.
Monitoring System Health

The system health links allow you to display statistics to help you monitor the status of your IP security platform. To view this information, click the appropriate link under Monitor > System Health in the tree view.

- **System Statistics**—Summarizes configuration information, including the following:
  - Active Routes—The number of active routes configured.
  - Packets Forwarded—The number of packets forwarded.
  - VRRP Masters—The number of VRRP masters configured.
  - Real Memory Used—The percentage of the real memory being used.
  - Disk Capacity—The percentage of the disk space being used.

- **Interface Traffic Statistics**—For each physical and logical interface, shows the current state, input and output bytes, input and output errors. For logical interfaces, also shows the type of device accessed through the logical interface (for example, Ethernet, Gigabit Ethernet). This page includes a link to the Link Aggregation Statistics page, which displays information about link aggregation groups and the individual interfaces in the groups. It also shows counters for the following interface ingress errors:
  - RxError: Counts the number of packets received in which I_RX_ER was asserted by the PHY.
  - RxNoBuffer: Counts the number of times that frames were received when there were no available buffers in host memory to store those frames (receive descriptor head and tail pointers were equal). The packets are still received if there is space in the FIFO.
  - CarrierExtnError: Counts the number of packets received in which the carrier extension error was signaled across the internal PHY interface. The PHY propagates carrier extension errors to the MAC when an error is detected during the carrier extended time of a packet reception.
  - LengthError: Counts receive length error events. A length error occurs if an incoming packet passes the filter criteria but is undersized or oversized.
  - AlignmentError: Counts the number of receive packets with alignment errors (the packet is not an integer number of bytes in length).
  - CRCError: Counts the number of receive packets with CRC errors.
  - DropError: Counts the number of missed packets. Packets are missed when the receive FIFO has insufficient space to store the incoming packet.
For more information on these interface errors, see http://www.intel.com/design/network/manuals/8254x_GBe_SDM.htm.

- **Interface Queue Statistics**—Shows the current information for interface queues, including the following:
  - Logical Name—The configured name of the queue.
  - Maximum Packets—Configured maximum number of packets which can be buffered by this queue.
  - Packets Passed—Number of packets sent from this queue to the physical interface.
  - Bytes Passed—Number of bytes sent from this queue to the physical interface.
  - Packets Dropped—Number of packets dropped at this queue due to lack of buffer space.
  - Bytes Dropped—Number of bytes dropped at this queue due to lack of buffer space.

- **SecureXL Connection Statistics** — shows SecureXL connections. This page retrieves the updated system statistics information every 15 seconds. The table summarizes connections information, such as existing, added and deleted connections handled by IPSO's SecureXL and ADP, if present in the system.
  - Existing: The number of active connection.
  - Added: The number of connection created in the last interval.
  - Deleted: The number of connection torn down in the last interval.

- **Live SecureXL FW Connection Statistics** — shows a separate graph for each firewall instance. Each graph plots number of connections created, deleted, current number of active connections, connections created from templates, NAT and TCP connections. The graph refreshes every 20 seconds.
Monitoring System Logs

The system logs links allow you to display updated system logs. To view system logs, click the appropriate link under Monitor > System Logs in the tree view. To refresh the information in a log, reload the Web page.

System logs include the following:

- **System Message Log**—You can view the message log file in its entirety or select search criteria to view specific system log activity. Search criteria include:
  - Types of log activity—Select one or more from All, Emergency, Alerts, Critical, Errors, Warnings, Notifications, Informational or Debug Messages.
  - Month
  - Particular date. You must also select a month to activate this option.
  - Keyword. To make the keyword search case-sensitive, select the Case Sensitive check box.
  - You can include certain zipped files in your search by clicking the appropriate check box in the Include Zipped Files in Search section.

  **Note** - The system log also displays messages generated by the system configuration audit log. For information configuring the audit log, see “To set the system configuration audit log” on page 98.

- **Web Server Access Log**—Shows information about accesses to the Network Voyager interface using HTTP or HTTPS. Messages include IP Address from which the local host did an http access to the system, user, date, time, and HTTP access command.

- **Web Server Error Log**—Shows error messages from the HTTPD Error Log File, including date and time the error occurred, transaction (type of log message), location, and contents of log message.

- **User Login/Logout Activity**—Shows login and logout activity for users. By default, activity for all user is displayed. You can view activity for a particular user by selecting the user name from the drop-down list.

- **Management Activity Log**—Shows user login activity as well as details about changes made to the IPSO configuration. The log includes a time stamp, the hostname or IP address from which the user logged in, and the config entry, which displays the entry changed in the configuration database.

For more information, see “To set the system configuration audit log” on page 98.
Monitoring System Logs

**Note** - You do not need to configure the Web Server Access log or the Web Server Error log.
Viewing Cluster Status and Members

To view information about cluster status and members, click Clustering Monitor under Monitor in the tree view.

This page summarizes 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.

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.
Viewing Routing Protocol Information

To view statistical information for routing protocols, click the appropriate link under Monitor > Routing Protocols. You can select from the following links:

- OSPF Monitor
- BGP Monitor
- RIP Monitor
- IGRP Monitor
- VRRP Monitor
- PIM Monitor
- DVMRP Monitor
- IGMP Monitor

To monitor routing protocol information for IPv6, you can select from the following links under Monitor > IPv6 Monitor:

- OSPFv3 Monitor
- RIPng Monitor
- IPv6 VRRP Monitor
- IPv6 Router Discovery Monitor
- IPv6 Route Monitor
- IPv6 Forwarding Table

Displaying the Kernel Forwarding Table

To view the IP forwarding table that the kernel is using to make its forwarding decisions, click Forwarding Table under Monitor > Routing Protocols in the tree view.

For IPv6, click IPv6 Forwarding Table under Monitor > IPv6 Monitor.

Displaying Route Settings

To view the route settings for your system, click Route under Monitor > Routing Protocols in the tree view.

For IPv6, click IPv6 Route Monitor under Monitor > IPv6 Monitor.
Displaying Interface Settings

To view the interface settings for your system, click Route under Monitor > Routing Protocols in the tree view.
Hardware Monitoring

You can use Network Voyager to monitor the following hardware elements.

- **Watchdog timer**—Monitors the kernel to detect system hangs. If it detects a hang, it reboots the system. You can view the following information about the watchdog timer:
  - Current state of the watchdog timer.
  - Mode—i.e. reset mode indicates that the watchdog timer detects a hardware problem or when the timer expires, it will reset the system.
  - Tickles—Number of times the system *tickled* the watchdog timer. Tickled means the kernel contacted the timer to indicate the kernel is operating normally.
  - Last Reboot—Whether the last system reboot was done manually either using the shutdown command or by power-cycling.

- **Fan sensors**—Shows the fan ID number, location, status, current value, normal value, and fan limit.

- **Power supply**

- **Temperature sensors**

- **Voltage sensors**

- **Slots**—Status of each device slot that is in use.

- **Cryptographic Accelerator**—Statistics of cryptographic accelerator if one is installed on your IP security platform. These include the following statistics:
  - Packet statistics—Packets Received: number of packets passed to the driver for processing. Packets Dropped: number of packets that could not be processed by the device. Packets Processed: number of packets successfully processed by the device
  - Byte statistics—Bytes Received: number of data bytes received by the driver for processing. Bytes Dropped: number of data bytes that could not be processed by the device. Bytes Processed: number of data bytes successfully processed by the device. **Note:** Byte statistics may overflow quickly on a heavily utilized encrypted channel.
  - Error statistics—Received Digest: number of times an invalid digest was encountered when a received message was processed. Random Number: number of times a random number could not be generated. Buffer Alignment: number of buffers passed to the device that were incorrectly aligned. Device: number of times that a device was not available to process
Hardware Monitoring

a data message. Memory: number of times that memory could not be allocated to process a data message. Context: number of times that an invalid context was specified to process a data message. Packet Header: number of times that an mbuf did not have a valid header.
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**

  Proceed as follows:

  1. To confirm that you have sufficient resources to increase the buffer size, issue the following command:
     
     ```
     fw ctl get int fw_log_bufsize
     ```
     
     If the value returned is less than 2097152 (2Mb) then you must increase it

  2. Run the command
     
     ```
     dbset advanced:loader t
     ```

  3. Connect to Network Voyager and log in

  4. Goto the **Tools > Firewall Kernel Tuning** page.

  5. In the group labeled **Add New Firewall Variable:**
     
     - Set **Name** to `fw_log_bufsize`
     - Set **Type** to `Integer`
Preventing Full Log Buffers and Related Console Messages

- Set Value to 2097152
6. Click Apply
   A message appears saying you must reboot.
7. Reboot the system.
Preventing Full Log Buffers and Related Console Messages
Index

A

ABR (area border router) 307
Accept Connections to VRRP IPs option 161
Accept mode 228
access control lists
adding rule to 440
configuring 435
configuring rules 437
for policy based routing 461
modifying rules 441
rule attributes 442
VRRP 184
access mechanisms
assigning to users 264
described 252
active route 371
admin network login 266
admin role 262
admin user
described 253
initial configuration 13
SSH login permission 275
Advanced system tuning
router alert IP option 137
SecureXL 137
agent address 196
aggregate routes
configuring 368
described 368
IPv6 222
weight 371
Aggregation class
configuring 444
aggregation class 442
Aggregation classes 434
aggregation classes
associating with rules 446
Apply button 16
area border routers 307
areas
OSPF, defined 306
ARP
ARP Mirroring for HA, global 60
ARP Mirroring for HA, interface specific 26
changing global parameters 60
deleting dynamic table entries 62
flushing dynamic entries 62
table entries 60
viewing dynamic entries 61
AS numbers, private 376
AS_PATH path attribute 377
ASE routes 307
ASPATH regular expressions 430
Asset Management page 19
ATOMIC_AGREGATE path attribute 378
attacks
person-in-the-middle 274
audit log
configuring 111
message formats 111
authentication
VRRP 165, 166
authorized keys, SSH 278
auto-deactivation 173
auto-negotiation
enabling 26
autonomous system (AS)
BGP 379
described 302
backups
cancelling scheduled 123
scheduling 122
bandwidth utilization 502
Banner message 81
Bellman Ford algorithm 303
Bellman-Ford algorithm 348
BGP capability 374
communities 380
community example 406
congestion example 399
confederations 382
described 374
external session (EBGP) 375
importing 379
interactions with IGPs 378
internal session (IBGP) 375
LocalPref 371
MED 378
memory requirements 387
multi-exit discriminator (MED) 375
multihop connections 384
neighbors example 389
overview 304
path attributes 377
redistributing routes 419
redistributing routes to 380
route dampening 384
route flapping 384
route reflection 381
route reflector example 402
route refresh 376
VRRP with clusters 387
with VRRP 385
BIOS 19
black hole static routes 363
BOOPT relay
about 468
enabling on interfaces 468
Bootp relay
disabling 470
Bootp Relay (BooP)
enabling 469
B
Back button 16
backup address, VRRP 165, 167
backup files
default contents 121
manually creating 121
restoring from local 125
transferring 123
backup state, VRRP 181
bootstrap protocol 468
broadcast traffic forwarding 467

c

cadmin user 253
Certificate Signing Request 271
chargen service 267
chassis fan
failure trap 199
Check Point MIB 190, 193
Check Point Security Gateway configuring for VRRP 177
clearing
disk cache 17
memory cache 17
CLI
described 11
inactivity timeout 254
CLI Reference Guide
accessing 17
cluster
admin role 262
cluster roles 264
clustering
transparent mode 64
clusters
roles 262
traps 199
viewing members 509
viewing status of 509
with BGP 387
with OSPF 308
cold start trap 197
COM2 login 266
COM3 login 266
communities, BGP 380
community strings 194
confederations, BGP 382
configuration
change log 507
saving 117
configuration file
creating 117
configuration locks
described 14
log in with 14

overriding 15
configuration summary tool 488
shell commands 490
configuring
Ethernet interfaces 25
IP addresses 22
mail relay 96
network devices 22
NTP 477
OSPF 309
S/key 257
Secure Shell (SSH) 275, 278, 279
SSH 274
cookies
session management 269
core files
on flash-based systems 114
CPRID process 500
CPU
fan failure trap 199
CPU information
viewing 19
CPU memory
historical utilization 503
live utilization 498
CPU utilization
report 503
CPU utilization report
configuring 133
cron jobs
ensuring correct time 98
cron jobs, scheduled times 477
crontab
scheduling jobs 119
cross-site request forgery
protection 16
cryptographic accelerator
monitoring 512

d

dashboards, performance monitoring 494
data transmission, queuing 502
date setting 98
daylight savings time rules 99
daylight service 267
DDNS 90
default route
configuring 363
deleting
IP address, VRRP considerations 170
dense mode
described 327
in clusters 328
DES authentication 207
DHCP 468
address ranges 86
configuring 82
configuring client interfaces 82
configuring server 85
enabling client process 83
firewall rules 82
server process 83
dial-control MIB 190
Differentiated services (DiffServ) 434
disabling
router discovery 476
static route 366
discard service 267
disk cache, clearing 17
disk information, viewing 19
disk mirroring 93
disk mirrors
traps 197
disk space
traps 198
disk utilization 498
displaying
routing protocol information 510
DNS
described 92
DNS spoofing 274
domain name service 92
DSA
generating host keys 276
user identities 280
DSField 438, 443
duplex mode
ethernet interface 25
duplicate IP addresses error message 169
DVMRP
configuring 356
described 355
overview 304
DVMRP tunnels 56
timers 356
Dynamic Host Configuration Protocol (DHCP) enabling 469

DVRMP 356
Dynamic Host Configuration Protocol (DHCP) enabling 469

E
EBGP connections 383
Echo service 267
Effective priority, VRRP 164
enabling Bootp Relay (Bootp) 469
DVRMP 469
encryption for network voyager 269
enabled encryption accelerator cards 300
encryption level, specifying 270
enhanced configuration summary tool 488
shell commands 490
tenant MIB 190
error messages duplicate IP addresses 169
EtherLike MIB 189
Ethernet interfaces bonding 38
configuring 25
expedited forwarding example 453
extended mode, VMAC 169
exterior routes, IGRP 351
External load balancer 141

F
firewall state, monitoring for VRRP 182
FireWall-1 12
flow 463
forward button 16
forwarding broadcast traffic 467
forwarding table viewing 510
frame relay DTE MIB 190
FreeBSD 12
FTP configuring for 257
enabling access 266
port number 266
full log buffers, preventing 514
FWD process 500
FWVPN 74

G
Generic Routing Encapsulation (GRE) 48
GetBulkRequest 205
GetNextRequest 205
GetRequest error messages 204
Gigabit Ethernet interfaces configuring 41
graceful restart helper, OSPF 315
GRE tunnels 48
groups adding 260
described 260
editing 260
group ID 260
ID 254
other group 260
SSH privileges 276
viewing list of 260
wheel 260

H
HA Voyager 143
configuration example 149
configuring VRRP 147
HA configuration 144
HA members 145
Hardware management MIB 190
monitoring 512
viewing summary information 19
hello interval VRRP 165, 166
help opening a second help window 18
High availability disk mirroring 93
GRE tunnels 52
HA Voyager 143
link redundancy 30
home directory, user 254
host address 102
host keys generating DSA 276
generating RSA 275
host resources MIB 189
hostname changing 116
how to change passwords 252
clear memory cache 17
enable SSH 275
open Network Voyager 13
HTTP tunneling over SSH 280
HTTP daemon error message log 273
HTTPD error log file 507
process 500

I
IANAifType MIB 189
ICMP router discovery protocol 473
ICMPv6 router discovery 225
IF MIB 189
ifLinkUpDown trap 197
ifm process 500
IFWD process 500
IGMP described 358
IGP 321

IGRP

configuring 352
overview 303, 348
redistributing routes to 421
interface throughput report 502
images
changing current 127
deleting 127
downgrading 131
installing 128
managing 127
testing 129
upgrading for cluster 130
inactivity timeout, shell 254
inetd process 500
initialize state, VRRP 181
inodes 498
interarea routes 307
interface
queue statistics 506
interface link state report 502
interface link state report configuring 133
interface mode, VMAC 169
interface throughput report configuring 133
interfaces
enabling Ethernet 25
logical 22
loopback 46
setting duplex mode 25
types of 22
viewing settings 511
interfaces, ethernet
adding an identifying string 26, 41
setting interface speed 25
loopback adding an IP address 46
tunnel 46
changing IP address 46
interfaces 46
sending mail 96
master state, VRRP 181
 maximum segment size 28
IP forwarding MIB 189
IP MIB 189
IP source routing 274
IP spoofing 274
IP2250 and IP2255 jumbo frames 41
Ipsilon Routing Daemon (IPSRD) description 302
overview 12
IPSO
managing images managing 127
overview 12
registration MIB 188
system MIB 188
IPSRD 302
described 12
ipsrd process 500
IPSRD, see also Ipsilon routing Daemon
IPv6
aggregate routes 222
configuring logical interfaces 214
default routes 219
in IPv4 tunnels 217
OSPFv3 221
overview 212
RIPv 221
security and access 238
through IPv4 without tunnel 217
VRRP 227
ISDN MIB 189
J

jobs, scheduling 119
jumbo frames 41

L

LACP 36
trap 197
link down trap 197
link recognition delay 26
link redundancy configuring 39
described 38
link speed
setting interface 25
link state advertisements 306
link trap parameter 25
link up trap 197
Load balancer, external 141
LOCAL_PREF path attribute 377
LocalPref parameter 371
log buffers
preventing full 514
logging
configuring on disk-based systems 107
configuring on flash-based systems 109
logging off 14
logical queue specifier 444
login
viewing user activity 507
Login messages 81
logs
files on diskless system 109
system message 507
web server access 507
loopback
adding an IP address 46
classless static routing 46
tunnel 46
LSA
overview 306

M

MAC address
VRRP 168
mail relay
configuring 96
description 95
features 95
sending mail 96
master state, VRRP 181
maximum segment size 28
MD5 authentication 207
MED 378
memory viewing 19
memory cache, clearing 17
memory utilization report configuring 133
message log 507
Messages
  banner 81
  login 81
  MOTD 81
MIBs
  list of 188
  mirror set 93
modem
dialback 267
modem configuration parameters 267
modzap functionality 491
Monitor Firewall State option 162
monitor interface parameter 173
monitor reports 502
  configuring 133
monitord process 500
monitored-circuit VRRP
  configuring 169
monitoring
  fan sensors 512
  hardware 512
  monitor role 262
  monitor user 253
  power supply 512
  routing protocols 510
  slots 512
  system logs 507
  system resources 498
  voltage sensors 512
  watchdog timer 512
monitoring cryptographic accelerator 512
MOTD (message of the day) 81
MSS 28
MTU
ssetting for GigE
Interfaces 41
MULTI_EXIT_DISC path attribute 377
multicast routers 358
multicast routing protocol 304
multicast static routes 347
multicast tunnels
  changing endpoint address 50
  configuring addresses 356
multi-exit discriminator
  (MED) 378
  autonomous system (AS) 375
  BGP 375
  multihop feature, EBGP 383
  multiple routing instances assigning access to 262
neighbor discovery
  configuring for IPv6 215
Netflow
collectors 463
  defining flows 463
  flow record versions 464
  metering modes 463
network access
  configuring 266
  enabling 267
network devices, configuring 22
network flow 463
network interface card (NIC) 22
network management station 196
network services
  chargen 267
  daytime 267
  discard 267
  echo 267
  enabling 267
  time 267
network throughput report 502
Network Voyager
  described
  navigating in 16
  overview 12
  setting session timeout 282
  troubleshooting access problems 269
  Web access options 269
  new password field 255
  NEXT_HOP path attribute 377
NMS 196
  notification
configuring failure 96
not-so-stubby areas 306
NSSA
  configuration parameters 311
  defined 306
NTP
  autokey authentication 479
  configuring 477
  description 477
  NTP MIB 191
OID registration MIB 188
opening Voyager 13
operating system (IPSO) 12
optional disk
  logging to 109
optional disks
  configuring logging to 111
  installing 104
  logging to 105
  removing 105
OSPF
  area configuration parameters 310
  configuring interfaces 316
  global settings 310, 315
  OSPFv3 221
  overview 303
  redistributing routes to 424
  route tags 418
  virtual links 313
  VRRP 155
  with clusters 308
  with VRRP 308
Other group 260
packages
  enabling 135
  installing 135
passwords
  changing 252
  complexity check 243
  disallowing reuse of 244
  expiration 245
forcing change of 245, 255
history check 244
palindrome check 243
setting strength policy 241
path attributes
BGP 377
path attributes (BGP) definitions 377
PC card
storing logs on 105
performance monitoring 494
physical interfaces 22
PIM
advanced options for dense mode 333
candidate bootstrap 339
configuring sparse mode 335
debugging 344
described 327
disabling 332
high-availability mode 337
rendezvous point 339
VRRP 155
with clustering 328
with VRRP 328
policy based routing
ACLs for 461
configuring 457
with clustering 462
with other routing 457
with VRRP 462
port numbers
SSL/TLS 269
ports
redirecting for HTTP tunnel over SSH 281
power supply
traps 199
power supply, monitoring 512
preempt mode 172
priority
VRRP parameter 155
priority delta, VRRP 164, 167
priority, VRRP 164, 165
private AS numbers 376
process
utilization 498, 499
process monitor 500

Q
Quality of service (QoS)
traffic shaping 445
Quality of service (QoS) 434
access control lists 434, 435
aggregation classes 434, 444
assured forwarding 439
cascade scheduling 448
DSfield 438
expedited forwarding 439
performance considerations 434
queue classes 434, 446
QueueSpec 438
strict priority scheduling 448
tail dropper 449
traffic shaping 445
weighted round robin scheduling 448
WRED constant 450
WRED drop rates 449
WRED dropper 449
queue classes 434
associating with interfaces 451
creating 450
QueueSpec 438, 444

R
RADIUS 290
RAID 93
rate shaping
example 452
rate-shape MIB 188
rate-shaping bandwidth report 502
configuring 133
RDI (routing domain identifier) 382
redistributing routes to IGRP 421
to RIP 421
redistributing
IGRP 421
RIP 421
redistributing routes described 418
inbound route filters 426
to BGP 419
to OSPF 424
refreshing pages 17
reject static routes 363
Reload button 17
reloading pages 17
reports
configuring 133
displaying 503
generating 502
Reset Routing button 16
RFC1583 compatibility 315
RIP
aggregating routes 325
auto-summarization 325
configuring 323
example 326
MIB 189
overview 303, 321
redistributing routes to 421
RIPv for IPv6 221
time tags 418
timers 325
VRRP 155
rlogin utility
vs. SSH 274
role-based administration
overview 262
roles 264
adding 263
assigning to users 264
cluster 262, 264
deleting 264
described 262
editing 263
overview 262
predefined system type 263
viewing list of 262
root user
controlling root access 260
in wheel group 260
route
precedence 371
rank 371
redistributing 421
route aggregation
described 368
example 369
route dampening 384
route filters 426
route maps
described 304
route rank 371
route redistribution
described 418
route reflection, BGP 381
route tags 418
route-based VPN 74
with BGP 374
with OSPF 306
with PIM 327
router alert IP option 138
router discovery 473
configuring 474
disabling 476
IPv6 225
server 473
router services
configuring 467
routes
flapping 384
redistributing 419
viewing settings 510
routing
configuring 301
configuring ranks 372
creating a default route 363
default protocol rank 371
disabling a static route 366
features 355
IGRP 352
OSPF 309
routing domain 382
routing information bases 387
Routing Information Protocol (RIP)
redistributing 421
routing protocols
displaying statistics 510
RPF algorithm 355
RSA
user identities 280
RSA host keys
generating 275
RSS (Resident Set Size) 499
S
S/Key 257
configuring 257
disabling 259
using 258
Save button 16
Secure Shell (SSH)
configuring 275, 278, 279
description 274
SecureXL
auto-expiry 137
delayed notification 137
sequence validation 137
seed, S/Key 257
Self-Signed X.509 Certificate 271
sequence number, S/Key 257
session management
described 282
enabling 269, 282
Log Off link 14
specifying timeout 269
session timeout
configuring 282
setting time/date 98
shell
inactivity timeout 254
users 254
show mcvr 181
show vrrp 181
slots
monitoring 512
SMTP 95
SNMP
agent address 196
contact information 202
daemon 194
described 188
enabling 194
enabling traps 196, 201
error messages 203
framework MIB 189
location information 202
managing users 207
MPD MIB 189
request messages 206
sending traps 200
trap definitions 196
user-based SM MIB 189
snmpd process 500
software
viewing summary
information 19
source platform (migrate configuration) 482
spanning tree protocol 185
sparse mode
described 327
in clusters 329
SPF delay 315
SSH
advanced options 276
authorized keys 278
configuring 274, 275
disabling 275
enabling 275
features 274
key pairs 279
obtaining SSH client 274
tunneling HTTP over 280
sshd process 500
SSL/TLS
about 270
certificate keys 270
connection testing 270
certificate 270
generating certificate 270
generating keys 270
private keys 270
specifying port number 269
troubleshooting 273
viewing certificate and private key 273
states, virtual router 181
static host
deleting 102
static mode
VMAC 169
static routes
backup 367
description 363
disabling 366
example 365
multicast 347
stub area
defined 306
swap space utilization 498
synchronization zone 94
syslog
configuring 107
message formats 111
system logs
monitoring 507
system message log 507
system processes
list of 500
system resources
monitoring 498
viewing summary 19
system roles 264
system state
saving 117
system time
setting 98
system utilization statistics 498
troubleshooting
SSL/TLS configuration 273
Tuning
advanced system 137
tunnels
configuring IPv6 in IPv4 217
GRE 48
IPv4 in IPv6 219
tunnel MIB 190
tunnels DVMRP 56
USM
described 206
V
virtual IP address, VRRP 167
virtual links
OSPF 313
virtual tunnel interfaces 74
VLAN interfaces 43
VMAC 168
VMAC mode 165
voltage sensors, monitoring 512
Voyager See Network Voyager
VRID 155
selecting 164
VRRP
accept mode 228
active-active
configuration 156
advertisements 155
authentication 165
authentication method 166
auto-deactivation 173
backup address 165, 167
changing backup address 172
Check Point configuration rules 179
Check Point Security Gateway 177
CLI commands 181
configuring VRRPv2 175
deleting IP address from interface 170
effective priority 164
election protocol 155
established master vs. equivalent priority 166
firewall state 182
full method 163, 170
hello interval 165, 166
hello messages 155
IPv6 227
IPv6 support 154
load sharing 157
location 181
MIB 189
monitored-circuit 163
monitored-circuit quick add method 174
T
TACACS+ 294
Telnet 449
target platform (migrate configuration) 482
TCP MD5 authentication 385
TCP MIB 189
TCP-establishment flag 443
telnet
configuring for 257
enabling access 266
vs. SSH 274
temperature
trap 200
temperature sensors
monitoring 512
TFTP access 266
time
setting system 98
time service 267
time setting 98
daylight savings time 99
timeout, session 269
token ring
MIB 190
TOS value
of GRE tunnel 50
traffic shaping 502
translator role, NSSA 311
transparent mode
configuring 68
described 63
limitations 63
neighbor learning 64
VPN 65
trap
sending 200
UDLD 28
UDP
UDP MIB 190
UDP packets
forwarding 471
UDP ports
IP Broadcast Helper 472
Unidirectional Link Detection 28
unit types MIB 189
USB modem configuration parameters 267
users
adding 256
attributes of 254
default 253
default privileges for new 262
group ID 254
home directory 254
ID 254
locking out
after failed logins 249, 245
for account inactivity 251
managing accounts of 253
name 254
nonlocal, RADIUS 292
nonlocal, TACACS+ 296
removing 256
removing directories 257
shell 254
SSH privileges 276
unlocking a locked account 255
viewing list of 253
viewing user activity 507
monitoring 181
OSPF 308
overview 154
preempt mode 166, 172
priority 155
priority delta 164, 167
priority parameter 164, 165
providing redundancy 157
removing VRRPv2 virtual
router 176
RFC 154
RIP 322
routing protocols 155
simplified method 163, 169
stats 182
switched environments 185
transparent mode 64
traps 198
troubleshooting failover 183
virtual IP address 167
VMAC mode 165, 168
VRID 164
with BGP 385
with HA Voyager 147
VSZ 499
VTI 74
with BGP 374
with OSPF 306
with PIM 327

W

watchdog timer 512
WCHAN (wait channel) 499
web servers
  access log 507
wheel group 260
WRED 449

X

xntpd process 500
xpand process 500