## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>vi</td>
</tr>
<tr>
<td>Introduction to Gaia Advanced Routing</td>
<td>7</td>
</tr>
<tr>
<td>DHCP Relay</td>
<td>8</td>
</tr>
<tr>
<td>Configuring DHCP Relay - WebUI</td>
<td>8</td>
</tr>
<tr>
<td>BOOTP/DHCP Parameters</td>
<td>9</td>
</tr>
<tr>
<td>BOOTP Interfaces</td>
<td>9</td>
</tr>
<tr>
<td>BOOTP Show Commands</td>
<td>9</td>
</tr>
<tr>
<td>BGP</td>
<td>11</td>
</tr>
<tr>
<td>Support for BGP-4</td>
<td>11</td>
</tr>
<tr>
<td>BGP Sessions (Internal and External)</td>
<td>12</td>
</tr>
<tr>
<td>Preventing Private AS Numbers from Propagating</td>
<td>12</td>
</tr>
<tr>
<td>BGP Route Refresh</td>
<td>12</td>
</tr>
<tr>
<td>BGP Path Attributes</td>
<td>13</td>
</tr>
<tr>
<td>BGP Multi-Exit Discriminator</td>
<td>14</td>
</tr>
<tr>
<td>BGP Interactions with IGPs</td>
<td>14</td>
</tr>
<tr>
<td>Inbound BGP Route Filters</td>
<td>14</td>
</tr>
<tr>
<td>Redistributing Routes to BGP</td>
<td>14</td>
</tr>
<tr>
<td>Communities</td>
<td>15</td>
</tr>
<tr>
<td>Route Reflection</td>
<td>15</td>
</tr>
<tr>
<td>Confederations</td>
<td>15</td>
</tr>
<tr>
<td>EBGP Multihop Support</td>
<td>16</td>
</tr>
<tr>
<td>Route Dampening</td>
<td>16</td>
</tr>
<tr>
<td>TCP MD5 Authentication</td>
<td>17</td>
</tr>
<tr>
<td>Configuring BGP - WebUI</td>
<td>17</td>
</tr>
<tr>
<td>BGP Global Settings</td>
<td>17</td>
</tr>
<tr>
<td>BGP Miscellaneous Settings</td>
<td>18</td>
</tr>
<tr>
<td>BGP AS Peer Groups</td>
<td>20</td>
</tr>
<tr>
<td>BGP Remote Peers</td>
<td>20</td>
</tr>
<tr>
<td>Configuring BGP - CLI (bgp)</td>
<td>26</td>
</tr>
<tr>
<td>External BGP</td>
<td>26</td>
</tr>
<tr>
<td>BGP Peers</td>
<td>27</td>
</tr>
<tr>
<td>BGP Confederations</td>
<td>29</td>
</tr>
<tr>
<td>BGP Route Reflection</td>
<td>30</td>
</tr>
<tr>
<td>BGP Route Dampening</td>
<td>31</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>33</td>
</tr>
<tr>
<td>BGP Communities</td>
<td>37</td>
</tr>
<tr>
<td>BGP Show Commands</td>
<td>37</td>
</tr>
<tr>
<td>IGMP</td>
<td>39</td>
</tr>
<tr>
<td>IGMP Version 3</td>
<td>39</td>
</tr>
<tr>
<td>Configuring IGMP - WebUI</td>
<td>40</td>
</tr>
<tr>
<td>Configuring IGMP - CLI (igmp)</td>
<td>41</td>
</tr>
<tr>
<td>Configure Interfaces for IGMP</td>
<td>41</td>
</tr>
<tr>
<td>Monitoring IGMP (show igmp)</td>
<td>43</td>
</tr>
<tr>
<td>IP Broadcast Helper</td>
<td>44</td>
</tr>
<tr>
<td>Configuring IP Broadcast helper - WebUI</td>
<td>44</td>
</tr>
<tr>
<td>Configuring IP Broadcast Helper - CLI (iphelper)</td>
<td>45</td>
</tr>
<tr>
<td>Forwarding Non-Local Packets</td>
<td>45</td>
</tr>
<tr>
<td>IP Broadcast Helper interfaces</td>
<td>45</td>
</tr>
<tr>
<td>Monitoring IP Broadcast Helper</td>
<td>45</td>
</tr>
<tr>
<td>RIP</td>
<td>47</td>
</tr>
<tr>
<td>RIP 2</td>
<td>47</td>
</tr>
<tr>
<td>Network Mask</td>
<td>47</td>
</tr>
</tbody>
</table>
Authentication ........................................................................................................... 47
RIP 1 .......................................................................................................................... 48
Network Mask ........................................................................................................... 48
Auto Summarization ................................................................................................. 48
Virtual IP Address Support for VRRP ................................................................. 48
Configuring RIP - WebUI ....................................................................................... 48
RIP Global Settings ................................................................................................. 49
RIP Interface Options .............................................................................................. 49
Configuring RIP - CLI (rip) .................................................................................... 50
RIP Global Commands ............................................................................................ 50
RIP Interface Commands ......................................................................................... 51
Monitoring RIP ............................................................................................................ 53
Monitoring RIP - WebUI ......................................................................................... 53
RIP Show Commands ............................................................................................... 53

OSPF ........................................................................................................................... 54
Types of Areas ............................................................................................................. 54
Area Border Routers ................................................................................................. 55
High Availability Support for OSPF ........................................................................... 55
Configuring OSPF - WebUI ....................................................................................... 56
Configuring Global Settings ..................................................................................... 56
Configuring OSPF Areas ......................................................................................... 57
Configuring OSPF Virtual Links .............................................................................. 59
Configuring OSPF Interfaces .................................................................................... 60
Configuring OSPF - CLI (ospf) ............................................................................... 62
OSPF Global Settings ............................................................................................... 63
OSPF Interfaces ......................................................................................................... 64
OSPF Virtual Links .................................................................................................... 66
OSPF Areas ................................................................................................................ 68
OSPF Show Commands ............................................................................................ 69

Route Aggregation .................................................................................................... 73
Configuring Route Aggregation - WebUI ............................................................... 73
Configuring Route Aggregation - CLI (aggregate) .................................................. 75

Routing Policy Configuration ..................................................................................... 77
Configuring Inbound Route Filters - WebUI ............................................................ 77
Add BGP Policy Window ......................................................................................... 78
Fine Tuning Policies .................................................................................................. 80
Configuring Route Redistribution - WebUI ............................................................ 81
Configuring Route Maps - CLI (route-map) ............................................................. 88
Set Routemap Commands ....................................................................................... 88
Show Routemap Commands .................................................................................... 93
Routemap Protocol Commands ................................................................................ 93
Supported Route Map Statements by Protocol ....................................................... 93
Route Map Examples ............................................................................................... 95

Routing Options ....................................................................................................... 97
Routing Options (Apply, Reset and Reload) - WebUI ............................................. 97
Equal Cost Path Splitting ......................................................................................... 97
Configuring Equal Cost Path Splitting - WebUI ..................................................... 97
Configuring Equal Cost Path Splitting - CLI (max-path-splits) .............................. 98
Kernel Options - Kernel Routes ............................................................................... 98
Configuring Kernel Routes - WebUI ....................................................................... 98
Configuring Kernel Routes - CLI (kernel-routes) .................................................. 98
Protocol Rank .......................................................................................................... 98
Default Ranks ........................................................................................................... 98
Configuring Protocol Rank - WebUI ....................................................................... 99
Configuring Protocol Rank - CLI (protocol-rank) .................................................. 99
Router Options - Wait for Clustering ...................................................................... 100
Configuring Wait for Clustering - WebUI .............................................................. 100
Configuring Wait for Clustering - CLI (router-options) ......................................... 100
Trace Options ........................................................................................................... 100
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace Options - WebUI</td>
<td>100</td>
</tr>
<tr>
<td>Trace Options - CLI</td>
<td>101</td>
</tr>
<tr>
<td><strong>Router Discovery</strong></td>
<td>109</td>
</tr>
<tr>
<td>How Router Discovery Works</td>
<td>109</td>
</tr>
<tr>
<td>Configuring Router Discovery - WebUI</td>
<td>109</td>
</tr>
<tr>
<td>Configuring Router Discovery - CLI (rdisc)</td>
<td>111</td>
</tr>
<tr>
<td>ICMP Router Discovery Interfaces</td>
<td>111</td>
</tr>
<tr>
<td>ICMP Router Discovery Show Commands</td>
<td>112</td>
</tr>
<tr>
<td><strong>Policy Based Routing</strong></td>
<td>113</td>
</tr>
<tr>
<td>Configuring Policy Based Routing - WebUI</td>
<td>113</td>
</tr>
<tr>
<td>Action Table Parameters</td>
<td>114</td>
</tr>
<tr>
<td>Policy Rule Parameters</td>
<td>115</td>
</tr>
<tr>
<td>Configuring Policy Based Routing - CLI</td>
<td>115</td>
</tr>
<tr>
<td>Monitoring Policy Based Routing</td>
<td>117</td>
</tr>
<tr>
<td><strong>PIM</strong></td>
<td>118</td>
</tr>
<tr>
<td>Dense Mode</td>
<td>118</td>
</tr>
<tr>
<td>Sparse Mode</td>
<td>118</td>
</tr>
<tr>
<td>Source-Specific multicast (SSM) Mode</td>
<td>118</td>
</tr>
<tr>
<td>PIM Dense Mode State Refresh</td>
<td>119</td>
</tr>
<tr>
<td>Configuring PIM - WebUI</td>
<td>119</td>
</tr>
<tr>
<td>PIM Global Settings</td>
<td>120</td>
</tr>
<tr>
<td>PIM Interfaces</td>
<td>120</td>
</tr>
<tr>
<td>Disabling PIM</td>
<td>121</td>
</tr>
<tr>
<td>Configuring PIM-DM Advanced Options (Optional)</td>
<td>121</td>
</tr>
<tr>
<td>Configuring PIM-SM Advanced Options (Optional)</td>
<td>121</td>
</tr>
<tr>
<td>Configuring PIM-SM Bootstrap and Rendezvous Point Settings</td>
<td>124</td>
</tr>
<tr>
<td>Configuring PIM - CLI (pim)</td>
<td>127</td>
</tr>
<tr>
<td>PIM Global Settings</td>
<td>127</td>
</tr>
<tr>
<td>PIM Interfaces</td>
<td>127</td>
</tr>
<tr>
<td>PIM Sparse Mode</td>
<td>128</td>
</tr>
<tr>
<td>Timer and Assert Rank Parameters for Dense Mode and Sparse Mode</td>
<td>132</td>
</tr>
<tr>
<td>Monitoring and Troubleshooting PIM</td>
<td>135</td>
</tr>
<tr>
<td>PIM Trace Options</td>
<td>135</td>
</tr>
<tr>
<td>PIM Show and MFC Commands</td>
<td>136</td>
</tr>
<tr>
<td><strong>Routing Monitor</strong></td>
<td>139</td>
</tr>
<tr>
<td>Monitoring Routes - WebUI</td>
<td>139</td>
</tr>
<tr>
<td>Monitoring Routes - CLI (show route)</td>
<td>139</td>
</tr>
<tr>
<td>Monitoring the Routing Daemon - CLI (show routed)</td>
<td>140</td>
</tr>
<tr>
<td>Monitoring the Multicast Forwarding Cache - CLI (show mfc)</td>
<td>141</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>143</td>
</tr>
</tbody>
</table>
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=22929

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the R76 home page (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 April 2013</td>
<td>PIM over unnumbered interfaces not supported. Corrected the virtual-address</td>
</tr>
<tr>
<td></td>
<td>parameter description (&quot;PIM Interfaces&quot; on page 127).</td>
</tr>
<tr>
<td>5 February 2013</td>
<td>First release of this document,</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Gaia Advanced Routing R76 Administration Guide).
Chapter 1

Introduction to Gaia Advanced Routing

Dynamic Routing is fully integrated into the Gaia WebUI and command-line shell. BGP, OSPF and RIP are supported.

Dynamic Multicast Routing is supported, using PIM (Sparse Mode (SM), Dense Mode (DM) and Source-Specific Multicast (SSM)) and IGMP.
Chapter 2

DHCP Relay

In This Chapter
- Configuring DHCP Relay - WebUI 8
- BOOTP Interfaces 9
- BOOTP Show Commands 9

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 Gaia 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 DHCP Relay - WebUI

Use the WebUI 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.

To enable BOOTP/DHCP relay on an Interface
1. Open the Advanced Routing > DHCP Relay page of the WebUI.
2. Click Add.
   The Add BOOTP/DHCP Relay window opens.
3. Select an Interface on which you want to enable BOOTP/DHCP.
4. Optional: Enter values for one or more of these parameters ("BOOTP/DHCP Parameters" on page 9):
   - Primary Address
   - Wait Time
5. Define the IPv4 address of each relay to which you want to forward BOOTP/DHCP requests ("BOOTP/DHCP Parameters" on page 9). For each relay:
   a) Click Add
   b) In the Add Relay window, enter the IPv4 address of the relay
   c) Click OK.
6. Click Save.
To disable BOOTP/DHCP relay on an interface
1. Open the Advanced Routing > DHCP Relay page of the WebUI.
2. Select an interface.
3. Click Delete.

**BOOTP/DHCP Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Address</td>
<td>The IP address to use as the BOOTP/DHCP router address. If you enter an IP address, 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>The minimum time to wait (in seconds) 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>Relay to Server</td>
<td>The IPv4 address of the BOOTP/DHCP configuration server to which to forward BOOTP/DHCP requests. 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 IPv4 address cannot be an address belonging to the local machine.</td>
</tr>
</tbody>
</table>

**BOOTP Interfaces**

Use these commands to configure BOOTP properties for specific interfaces.

```
set bootp interface <if_name>
  primary ip_address wait-time <0-65535> on
  relay-to ip_address <on | off>
  off
```

**Arguments**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary ip_address</td>
<td>The ip_address to stamp as the gateway address on all BOOTP requests. The wait-time value is the minimum seconds to wait before forwarding a bootp request. A client-generated bootp request includes the elapsed time after the client began to boot. The bootp relay does not forward the request until the indicated elapsed time at least equals the specified wait time. This delay lets a local configuration server reply, before it relays to a remote server.</td>
</tr>
<tr>
<td>wait-time &lt;0-65535&gt;</td>
<td></td>
</tr>
<tr>
<td>on</td>
<td></td>
</tr>
<tr>
<td>off</td>
<td></td>
</tr>
<tr>
<td>relay-to ip_address</td>
<td>The server to which BOOTP requests are forwarded. You can specify more than one server.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>off</td>
<td>Disables BOOTP on the specified interface.</td>
</tr>
</tbody>
</table>

**BOOTP Show Commands**

Use this group of commands to monitor and troubleshoot the BOOTP implementation.
show bootp
  interfaces
  interface if_name
  stats
  stats receive
  stats request
  stats reply
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.

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 IGP, 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).

### Support for BGP-4

Gaia implements BGP-4 to support multiprotocol extensions, 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.

On each peer you configure IPv4 unicast routes that should be exchanged between peers. For peering to be established, the routers must share a capability.
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. They do this by using the next hop received with a route from a peer as a forwarding address, and use this to look up an immediate next hop in IGP routes. Type internal groups support distant peers, but they need to be informed of the IGP whose routes they are using to determine immediate next hops.

Where possible, for internal BGP group types, a single outgoing message is built for all group peers based on the common policy. A copy of the message is sent to every peer in the group, with appropriate adjustments to the next hop field to each peer. This minimizes the computational load of running large numbers of peers in these types of groups.

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 Gaia to remove the private AS number from BGP update messages to external peers.

To configure Gaia 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

Gaia 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 in the:

- CLI - Run these commands:

  set bgp external remote-as as_number peer ip_address send-route-refresh
  set bgp internal peer ip_address send-route-refresh

- WebUI - Click the appropriate buttons in the Edit Peer page, in the section Advanced Settings > Route Refresh.
These options work only with peers that support the same capabilities. Gaia 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>
<tr>
<td>ATOMIC_AGGREGATE</td>
<td>Specifies to a BGP speaker that a less specific route was chosen over a more specific route. The BGP speaker attaches the ATOMIC_AGGREGATE attribute to the route when it reproduces it to other BGP speakers. The BGP speaker that receives this route cannot remove the ATOMIC_AGGREGATE attribute or make any Network Layer Reachability Information (NLRI) of the route more specific. This attribute is used only for debugging purposes.</td>
</tr>
</tbody>
</table>

All unreachable messages are collected into a single message and are sent before reachable routes during a flash update. For these unreachable announcements, the next hop is set to the local address on the connection, no metric is sent, and the path origin is set to incomplete. On external connections, the AS path in unreachable announcements is set to the local AS. On internal connections, the AS path length is set to zero.

Routing information shared between peers in BGP has two formats: announcements and withdrawals. A route announcement indicates that a router either learned of a new network attachment or made a policy decision to prefer another route to a network destination. Route withdrawals are sent when a router makes a new local decision that a network is no longer reachable.
BGP Multi-Exit Discriminator

Multi-exit Discriminator (MED) values are used to help external neighbors decide which of the available entry points into an AS are preferred. A lower MED value is preferred over a higher MED value and breaks the tie between two or more preferred paths.

*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

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, *routed* does not.

*Note* - To define a redistribution policy, use Advanced Routing > Route Distribution in the WebUI, or routemaps in the CLI.
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 (0xFFFFFFF01)</td>
<td>Not advertised outside a BGP confederation boundary. A stand-alone autonomous system that is not part of a confederation should be considered a confederation itself.</td>
</tr>
<tr>
<td>NO_ADVERTISE (0xFFFFFFF02)</td>
<td>Not advertised to other BGP peers.</td>
</tr>
<tr>
<td>NO_EXPORT_SUBCONFED (0xFFFFFFF03)</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 more about communities, see RFCs 1997 and 1998.

Route Reflection

Generally, all border routers in a single AS need to be internal peers of each other; all non-border 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** - We recommend 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).

Confederations

An alternative to route reflection is BGP confederations. As with route reflectors, you can partition BGP speakers into clusters where each cluster is typically a topologically close set of routers. With confederations, this is accomplished by subdividing the autonomous system into multiple, smaller ASes that
communicate among themselves. The internal topology is hidden from the outside world, which perceives the confederation to be one large AS.

Each distinct sub-AS within a confederation is referred to as a routing domain (RD). Routing domains are identified by using a routing domain identifier (RDI). The RDI has the same syntax as an AS number, but as it is not visible outside of the confederation, it does not need to be globally unique, although it does need to be unique within the confederation. Many confederations find it convenient to select their RDIs from the reserved AS space (ASes 64512 through 65535 (see RFC 1930). RDIs are used as the ASes in BGP sessions between peers within the confederation.

The confederation as a whole, is referred to by a confederation identifier. This identifier is used as the AS in external BGP sessions. As far as the outside world is concerned, the confederation ID is the AS number of the single, large AS. For this reason, the confederation ID must be a globally unique, normally assigned AS number.

**Note** - Do not nest confederations.

For further details, refer to the confederations specification document (RFC 1965).

### 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.

**Important** - 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.

### Route Dampening

Route dampening lessens the propagation of flapping routes. A flapping route is a route that repeatedly becomes available then unavailable. Without route dampening, autonomous systems continually send advertisement and withdrawal messages each time the flapping route becomes available or unavailable. As the Internet has grown, the number of announcements per second has grown as well and caused performance problems within the routers.

Route dampening enables routers to keep a history of the routes that are flapping and prevent them from consuming significant network bandwidth. This is achieved by measuring how often a given route becomes available and then unavailable. When a set threshold is reached, that route is no longer considered valid, and is no longer propagated for a given period of time, usually about 30 minutes. If a route continues to flap even after the threshold is reached, the time out period for that route grows in proportion to each additional flap. Once the threshold is reached, the route is dampened or suppressed. Suppressed routes are added back into the routing table once the penalty value is decreased and falls below the reuse threshold.

Route dampening can cause connectivity to appear to be lost to the outside world but maintained on your own network because route dampening is only applied to BGP routes. Because of increasing load on the backbone network routers, most NSPs (MCI, Sprint, UUNet etc.) have set up route suppression.
TCP MD5 Authentication

The Internet is vulnerable to attack through its routing protocols and BGP is no exception. External sources can disrupt communications between BGP peers by breaking their TCP connection with spoofed RST packets. Internal sources, such as BGP speakers, can inject bogus routing information from any other legitimate BGP speaker. Bogus information from either external or internal sources can affect routing behavior over a wide area in the Internet.

The TCP MD5 option allows BGP to protect itself against the introduction of spoofed TCP segments into the connection stream. To spoof a connection using MD5 signed sessions, the attacker not only has to guess TCP sequence numbers, but also the password included in the MD5 digest.

**Note** - TCP MD5 authentication for BGP is not supported on 64-bit Gaia or on a 32/64-bit Gaia VSX cluster.

Configuring BGP - WebUI

This section gives per-field help for the fields in the Advanced Routing > BGP section of the Gaia WebUI.

**Note** - Not all fields are shown in all cases.

### BGP Global Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The Router ID uniquely identifies the router in the autonomous system. The router ID is used by the BGP and OSPF protocols. We recommend setting the router ID rather than relying on the default setting. This prevents the router ID from changing if the interface used for the router ID goes down. Use an address on a loopback interface that is not the loopback address (127.0.0.1). In a cluster, you must select a router ID and make sure that it is the same on all cluster members.</td>
</tr>
<tr>
<td></td>
<td>• Range: Dotted-quad.([0-255],[0-255],[0-255],[0-255]). Do not use 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>• Default: The interface address of one of the local interfaces.</td>
</tr>
<tr>
<td>Cluster ID for Route Reflectors</td>
<td>The cluster ID used for route reflection. The default cluster ID is the router ID. You must override this default value if the cluster contains more than one route reflector.</td>
</tr>
<tr>
<td></td>
<td>Typically, a single router acts as the reflector for a set, or cluster, of clients. However, for redundancy two or more routers can also be configured as reflectors for the same cluster. In this case, you must select a cluster ID to identify all reflectors serving the cluster.</td>
</tr>
<tr>
<td></td>
<td>Gratuitous use of multiple redundant reflectors is not advised, for this situation can cause an increase in the memory required to store routes on the redundant reflectors peers.</td>
</tr>
<tr>
<td></td>
<td>• Range: Dotted-quad ([0-255],[0-255],[0-255],[0-255])</td>
</tr>
<tr>
<td></td>
<td>• Default: Router ID</td>
</tr>
<tr>
<td>Local Autonomous System Number</td>
<td>The local autonomous system number of the router.</td>
</tr>
</tbody>
</table>

### Change Local System Identification

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unconfigured</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Local Autonomous System Number** | The local autonomous system number of the router. This setting is mutually exclusive from the **Confederation** and **Routing Domain Identifier**. The router can be configured with either the autonomous system number or the member of confederation, not both. **Caution**: When you change the autonomous system number, all current peer sessions are reset and all BGP routes are deleted.  
- **Range**: 1-65535  
- **Default**: No default |
| **Confederation** | The identifier for the entire confederation system. This identifier is used as the AS in external BGP sessions. To the outside world, 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.  
- **Range**: 1-65535  
- **Default**: No default |
| **Number of loops permitted in AS_PATH** | For the confederation: The number of times the local autonomous system can appear in an AS path for BGP-learned routes. If the number of times the local autonomous system appears in an AS path is more than the number in this field, the corresponding routes are discarded or rejected.  
- **Range**: 1-10  
- **Default**: 1 |
| **Routing Domain Identifier** | The routing domain identifier (RDI) of this router. This value is required only if BGP confederations are in use. The RDI does not have to be globally unique since it is never used outside the domain of the confederation system. However, the configured RDI must be unique within the confederation. The routing-domain identifier and autonomous system number are mutually exclusive values; that is, the router can be configured with either the autonomous system number or the member of confederation, not both. If confederations are in use, the RDI is used wherever the autonomous system would be used to communicate with peers within the confederation, including group-type confederation peers and the various internal-type peers. For correct operation of the router in confederations you must configure both the routing-domain identifier and the confederation.  
- **Range**: 1-65535  
- **Default**: No default |
| **Number of loops permitted in AS_PATH** | For the routing domain identifier: The number of times the local autonomous system can appear in an AS path for BGP-learned routes. If the number of times the local autonomous system appears in an AS path is more than the number in this field, the corresponding routes are discarded or rejected.  
- **Range**: 1-10  
- **Default**: 1 |

**BGP Miscellaneous Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Default MED** | Defines the metric (MED) used when advertising routes through BGP. If you do not specify a value, no metric is propagated. A metric specified on the neighbor configuration or in the redistribution configuration might override the metric you configure.  
- **Range**: 0-65535 |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway:</td>
<td>A default route is generated when any BGP peer is up. This route has a higher rank than the default configured in the static routing page. If a specific BGP peer should not be considered for generating the default route, you should explicitly suppress the option in the peer-specific configuration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: Dotted-quad ([0-255].[0-255].[0-255].[0-255]).</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Default.</strong></td>
</tr>
<tr>
<td>Enable IGP Synchronization</td>
<td>Select this option to make internal and configured BGP peers check for a matching route from IGP protocols before installing a given route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Unselected</td>
</tr>
<tr>
<td>Enable communities</td>
<td>Enables communities-based policy options.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Unselected</td>
</tr>
<tr>
<td>Enable Weighted Route Dampening</td>
<td>Weighted route dampening minimizes the propagation of flapping routes across an internetwork. A route is considered to be flapping when it is repeatedly transitioning from available to unavailable or vice versa. Only routes learned through BGP are subjected to weighted route dampening.</td>
</tr>
<tr>
<td>Reuse-below metric</td>
<td>The value of the instability metric at which a suppressed route becomes unsuppressed if it is reachable but currently suppressed. The value assigned to the reuse-below metric must be less than the suppress-above value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-32</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 2</td>
</tr>
<tr>
<td>Suppress-above metric</td>
<td>The value of the instability metric at which a route is suppressed; a route is not installed in the FIB or announced even if it is reachable during the period that it is suppressed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 2-32</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 3</td>
</tr>
<tr>
<td>Max-flap metric</td>
<td>The upper limit of the instability. The value must be higher than one plus the suppress-above value. The metric assigned to the suppress-above, reuse-below, and max-flap metric values is a floating point number, in units of flaps. Each time a route becomes unreachable, one is added to the current instability metric.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 3-64</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 16</td>
</tr>
<tr>
<td>Reachable decay time</td>
<td>A value that determines the length of time it takes for the instability metric value to reach one half of its current value when the route is reachable. This half-life value determines the rate at which the metric value is decayed. A smaller half-life value makes a suppressed route reusable sooner than a larger value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-900</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 300</td>
</tr>
<tr>
<td>Unreachable decay time</td>
<td>The rate at which the instability metric is decayed when a route is unreachable. This value must be equal to or greater than the reach-decay value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-2700</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 900</td>
</tr>
</tbody>
</table>
### BGP AS Peer Groups

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer AS Number</td>
<td>The autonomous system number of the external peer group. Enter an integer from 1-65535.</td>
</tr>
</tbody>
</table>
| Peer Group Type    | One of  
  - Unconfigured  
  - Local Autonomous System Number  
  - Confederation |
| Description        | A free-text description of the peer group. |
| Virtual Address    | Note:  
  - Use this option only in a lab environment with the firewall turned off.  
  - Do not use in a cluster configuration. Select this option to force this router to use VRRP virtual IP address as the local endpoint for TCP connections. Only the VRRP master will establish BGP sessions. To enable this option, the local address must be configured.  
  - Default: Cleared |
| Local address      | The address used on the local end of the TCP connection with the peer. For external peers that do not have multihop enabled, the local address must be on an interface that is shared with the peer or with the peer’s gateway when the gateway parameter is used. A session with an external peer is opened only when an interface with a local address through which the peer or gateway address is directly reachable is operating. For other types of peers, a peer session is maintained when any interface with the specified local address is operating. In either case, incoming connections are recognized as matching a configured peer only if they are addressed to the configured local address.  
  - Note: If running BGP in a cluster you must not configure the local address.  
  - Default: None |
| Out Delay          | The length of time in seconds that a route must be present in the routing database before it is redistributed to BGP. This value applies to all neighbors configured in this group. The default value is zero, which means that this feature is disabled. This feature dampens route fluctuations.  
  - Range: 0-65535  
  - Default: 0 |
| Peer               | Configure peers. Each peer inherits as defaults all parameters configured on a group. To change the values of a peer's parameters, select the peer and click Edit. |

---

**BGP Remote Peers**
Parameter | Description
--- | ---
Peer | 
Comment | A free-text description of the remote peer.

**Advanced Settings**

**Multiprotocol Capabilities**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Unicast</td>
<td>Specifies if IPv4 unicast routes can be sent to and received from this peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> Selected</td>
</tr>
<tr>
<td>IPv6 Unicast</td>
<td>Specifies if IPv6 unicast routes can be sent to and received from this peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> Cleared</td>
</tr>
</tbody>
</table>

**Local Address**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Address</td>
<td>The address used on the local end of the TCP connection with the peer. For external peers that do not have multihop enabled, the local address must be on an interface that is shared with the peer or with the peer’s gateway when the gateway parameter is used. A session with an external peer is opened only when an interface with a local address through which the peer or gateway address is directly reachable is operating. For other types of peers, a peer session is maintained when any interface with the specified local address is operating. In either case, incoming connections are recognized as matching a configured peer only if they are addressed to the configured local address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If running BGP in a cluster you must not configure the local address.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> None</td>
</tr>
</tbody>
</table>

**Weight**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>The default weight associated with each route accepted from this peer. This value can be overridden by the weight specified in the import policy.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 0-65535</td>
</tr>
</tbody>
</table>

**MED**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept MED from External Peer</td>
<td>MED should be accepted from this external neighbor. MEDs are always accepted from routing-type and confederation neighbors. If this parameter is not used with an external neighbor, the MED is stripped before the update is added to the routing table. If this parameter is added or deleted and <strong>routed</strong> is reconfigured, the affected peering sessions are automatically restarted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> Cleared</td>
</tr>
<tr>
<td>MED Sent Out</td>
<td>The primary metric used on all routes sent to the specified peer. This metric overrides the default metric on any route specified by the redistribute policy.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 0-4294967294</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> 4294967294</td>
</tr>
</tbody>
</table>
### Next Hop and Time to Live

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EGP Multihop</strong></td>
<td>Multihop is used to set up EBGP peering connections with peers that are not directly connected. You can also use this option, which relies on an IGP to find the route to the peer, to set up peers to perform EBGP load balancing. You can refine the multihop session by configuring the TTL, that is, the number of hops to the EBGP peer. The TTL has a default value of 64.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Cleared</td>
</tr>
<tr>
<td><strong>Time to Live</strong></td>
<td>You can use the TTL (time to live parameter) to limit the number of hops over which the EBGP multihop session is established. You can configure the TTL only if multihop is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-255</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 64</td>
</tr>
</tbody>
</table>

### Aggregator

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No Aggregator ID</strong></td>
<td>Select to force this router to specify the router ID in the aggregator attribute as zero, rather than the actual router ID. This option prevents different routers in an AS from creating aggregate routes with different AS paths.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Cleared</td>
</tr>
</tbody>
</table>

### AS PATH

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASPATH prepend count</strong></td>
<td>The number of times this router adds to the AS path on EBGP external or CBGP confederation sessions. Use this setting to bias the degree of preference some downstream routers have for the routes originated by this router. Some implementations prefer to select routes with shorter AS paths. This parameter has no effect when used with IBGP peers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-25</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 1</td>
</tr>
</tbody>
</table>

### Private AS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remove Private AS</strong></td>
<td>Remove private AS numbers from the outgoing updates to this peer. Following conditions apply when this feature is enabled:</td>
</tr>
<tr>
<td></td>
<td>• If the AS path includes both public and private AS numbers, private AS numbers will not be removed.</td>
</tr>
<tr>
<td></td>
<td>• If the AS path contains the AS number of the destination peer, private AS numbers will not be removed.</td>
</tr>
<tr>
<td></td>
<td>• If the AS path contains only confederations and private AS numbers, private AS numbers will be removed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Cleared</td>
</tr>
</tbody>
</table>
### Timers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Alive Timer</td>
<td>An alternative way to specify a Hold Time value, in seconds, to use when negotiating the connection with this peer. The keepalive interval equals one-third the value of the holdtime. The keepalive interval is often used instead of the holdtime value, but you can specify both values, provided the value for the holdtime is three times the keepalive interval. The value must be 0, that is, no keepalives are sent, or at least 2.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 0, 2-21845</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 60</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The BGP holdtime value, in seconds, to use when negotiating a connection with this peer. According to the specification, if the BGP speaker does not receive a keepalive update or notification message from its peer within the period specified by the holdtime value in the BGP Open message, the BGP connection is closed. The value must be either 0, that is, no keepalives are sent, or at least 6.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 0, 6-65535</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 180</td>
</tr>
</tbody>
</table>

### Needed when Peering with Route Server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore First AS Hop</td>
<td>Select to force this router to ignore the first AS number in the AS_PATH for routes learned from the corresponding peer. Select this option only if you are peering with a route server in so-called transparent mode, that is, when the route server is configured to redistribute routes from multiple ASes without prepending its own AS number.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Cleared</td>
</tr>
</tbody>
</table>

### Keep Alive

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Alive Always</td>
<td>Select to force this router always to send keepalives even when an update can substitute. This setting allows interoperability with routers that do not completely adhere to the protocol specifications on this point.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Cleared</td>
</tr>
</tbody>
</table>

### Routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Routes Received From the Peer</td>
<td>Routes received from peer routes are accepted if there is an inbound BGP route policy. If an inbound policy to accept the route does not exist, you can select All or None.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All</strong> - Specifies to accept and install routes with an invalid preference. Depending on the local BGP inbound policy the routes could become active or inactive.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong> - Specifies to delete routes learned from a peer when no explicit local BGP inbound policy exists. This option is used to save memory overhead when many routes are rejected because there is no local policy. These routes can be relearned only by restarting the BGP session.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: All</td>
</tr>
</tbody>
</table>
# Allows Accept TCP Sessions from Your Peer

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive</td>
<td>Select to force this router to wait for the peer to issue an open. By default all explicitly configured peers are active and periodically send open messages until the peer responds. Modifying this option will reset the peer connection.</td>
</tr>
</tbody>
</table>

- Default: Cleared

## Authentication

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>The type of authentication scheme to use between given peers. In general peers must agree on the authentication configuration to form peer adjacencies. This feature guarantees that routing information is accepted only from trusted peers. If the Auth type selected is MD5 the Password field appears. When you enter a password, MD5 authentication is used with the given peer.</td>
</tr>
</tbody>
</table>

**Note** - TCP MD5 authentication for BGP is not supported on 64-bit Gaia or on a 32/64-bit Gaia VSX cluster.  
- Options: None / MD5  
- Default: None

## Limit BGP Updates Send to a Peer

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throttle count</td>
<td>Throttles the network traffic when there are many BGP peers. Throttle count determines the number of BGP updates sent at a time.</td>
</tr>
</tbody>
</table>

- Range: 0-65535  
- Default: No default

## Route Refresh

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Route Refresh | Route refresh is used to either re-learn routes from the BGP peer or to refresh the routing table of the peer without tearing down the BGP session. Both peers must support the BGP route refresh capability and should have advertised this at the time peering was established.  
Re-learning of routes previously sent by the peer is accomplished by sending a BGP route refresh message. The peer responds to the message with the current routing table. Similarly, if a peer sends a route refresh request the current routing table is re-sent.  
You can also trigger a route update without having to wait for a route refresh request from the peer.  
Both peers must support the same address and subsequent address families. For example a request for IPv6 unicast routes from a peer that did not advertise the capability during session establishment will be ignored.  
**Note:** Clicking a Route Refresh button sends a trigger to the routing daemon. It does not change the configuration of the router. |

## Graceful Restart

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helper</td>
<td>Routes received from peer are preserved if the peer goes down till either the session is re-established (OPEN message is received from the peer after it comes back up) or the graceful restart timer expires.</td>
</tr>
</tbody>
</table>

- Default: Cleared
### Stalepath Time

Maximum time for which routes previously received from a restarting router are kept unless they are re-validated. The timer is started after the peer sends indication that it is up again.

- **Range**: 60 - 65535
- **Default**: 360

### Logging

#### Log bgp peer transitions

Select to force this router to log a message whenever a BGP peer enters or leaves the ESTABLISHED state.

- **Default**: Cleared

#### Log warnings

Select to force this router to log a message whenever a warning scenario is encountered in the codepath.

- **Default**: Cleared

### Trace Options

The tracing options for BGP. The BGP implementation inherits the default values for global trace options. You can override these values on a group or neighbor basis. Log messages are saved in `var/log/routed.log`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Trace all message types.</td>
</tr>
<tr>
<td>General</td>
<td>Trace messages related to Route and Normal.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>Trace all the BGP keepalive messages to this peer, which are used to verify peer reachability.</td>
</tr>
<tr>
<td>Normal</td>
<td>Trace normal protocols occurrences. Abnormal protocol occurrences are always traced.</td>
</tr>
<tr>
<td>Open</td>
<td>Trace all the BGP open messages to this peer, which are used to establish a peer relationship.</td>
</tr>
<tr>
<td>Packets</td>
<td>Trace all the BGP packets to this peer.</td>
</tr>
<tr>
<td>Policy</td>
<td>Trace application of protocol and user-specified policy to routes being imported and exported.</td>
</tr>
<tr>
<td>Route</td>
<td>Trace routing table changes for routes installed by this peer.</td>
</tr>
<tr>
<td>State</td>
<td>Trace state machine transitions in the protocol.</td>
</tr>
<tr>
<td>Task</td>
<td>Trace system interface and processing associated with this peer.</td>
</tr>
<tr>
<td>Timer</td>
<td>Trace timer usage by this peer.</td>
</tr>
<tr>
<td>Update</td>
<td>Trace all the BGP update messages to this peer, which are used to pass network reachability information.</td>
</tr>
</tbody>
</table>
## Configuring BGP - CLI (bgp)

### External BGP

Use the following commands to configure external sessions of the protocol, that is, between routers in different autonomous systems.

```plaintext
set bgp external remote-as as_number  
  <on | off>  
  aspath-prepend-count <1-25 | default>  
  description text  
  local-address ip_address <on | off>  
  virtual-address <on | off>  
  outdelay <0-65535>  
  outdelay off
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as_number &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>aspath-prepend-count &lt;1-25</td>
<td>default&gt;</td>
</tr>
<tr>
<td>description text</td>
<td>You can enter a brief text description of the group.</td>
</tr>
<tr>
<td>local-address ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
| virtual-address <on | off>    | Note:  
  - Use this option only in a lab environment with the firewall turned off.  
  - Do not use in a cluster configuration.  
  Use the VRRP virtual IP address as the local endpoint for TCP connections, for this router. You must also configure a local address to enable this option. See the command above. You can configure this option only on a VRRP master. |
| outdelay <0-65535>          | The amount of time in seconds that a route must be present in the routing database before it is redistributed to BGP. The configured value applies to all peers configured in this group. This feature dampens route fluctuation. The value zero (0) disables this feature. **Default:** 0 |
| outdelay off                | Disables outdelay.                                                            |
**BGP Peers**

Use the following commands to configure BGP peers. Gaia supports IPv4 addresses for BGP peers.

```plaintext
set bgp external remote-as as_number peer ip_address
  <on | off>
  med-out <0-4294967294 | default>
  accept-med <on | off>
  multihop <on | off>
  no-aggregator-id <on | off>
  holdtime <6-65535 | default>
  keepalive <2-21845 | default>
  ignore-first-ashop <on | off>
  send-keepalives <on | off>
  send-route-refresh [request | route-update] [unicast]
  route-refresh <on | off>
  accept-routes <all | none>
  passive-tcp <on | off>
  removeprivateas <on | off>
  authtype none
  authtype md5 secret secret
  throttle-count <0-65535 | off>
  ttl <1-255 | default>
  suppress-default-originate <on | off>
  log-state-transitions <on | off>
  log-warnings <on | off>
  trace bgp_traceoption <on | off>
  graceful-restart-helper <on | off>
  graceful-restart-helper-stalepath-time seconds
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>med-out     &lt;0-4294967294</td>
<td>default&gt;</td>
</tr>
<tr>
<td>accept-med &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>multihop &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>no-aggregator-id &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>holdtime &lt;6-65535</td>
<td>default&gt;</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>keepalive</td>
<td>The keepalive option is an alternative way to specify a holdtime value in seconds when negotiating a connection with the specified peer. You can use the keepalive interval instead of the holdtime interval. You can also use both intervals, but the holdtime value must be 3 times the keepalive interval value.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 60 seconds</td>
</tr>
<tr>
<td>ignore-first-ashop</td>
<td>Specifies to ignore the first autonomous system number in the autonomous system path for routes learned from the corresponding peer. Set this option only if you are peering with a route server in transparent mode, that is, when the route server is configured to redistribute routes from multiple other autonomous systems without prepending its own autonomous system number.</td>
</tr>
<tr>
<td>send-keepalives</td>
<td>Specifies for this router always to send keepalive messages even when an update message is sufficient. This option allows interoperability with routers that do not strictly adhere to protocol specifications regarding updates.</td>
</tr>
<tr>
<td>send-route-refresh</td>
<td>Specifies that the router dynamically request BGP route updates from peers or respond to requests for BGP route updates.</td>
</tr>
<tr>
<td>route-refresh</td>
<td>Re-learns routes previously sent by the BGP peer or refreshes the routing table of the peer. The peer responds to the message with the current routing table. Similarly, if a peer sends a route refresh request the current routing table is re-sent. A user can also trigger a route update without having to wait for a route refresh request from the peer.</td>
</tr>
<tr>
<td>accept-routes</td>
<td>Specifies an inbound BGP policy route if one is not already configured. Enter <code>all</code> to specify accepting routes and installing them with an invalid preference. Depending on the local inbound route policy, these routes are then made active or inactive. Enter <code>none</code> to delete routes learned from a peer. This option saves memory overhead when many routes are rejected because no inbound policy exists.</td>
</tr>
<tr>
<td>passive-tcp</td>
<td>Specifies for the router to wait for the specified peer to issue an open message. No tcp connections are initiated by the router.</td>
</tr>
<tr>
<td>removeprivateas</td>
<td>Remove private AS numbers from BGP update messages to external peers.</td>
</tr>
<tr>
<td>authtype none</td>
<td>Specifies not to use an authentication scheme between peers. Using an authentication scheme guarantees that routing information is accepted only from trusted peers.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> none</td>
</tr>
<tr>
<td>authtype md5 secret secret</td>
<td>Specifies to use md5 authentication between peers. In general, peers must agree on the authentication configuration to and from peer adjacencies. Using an authentication scheme guarantees that routing information is accepted only from trusted peers.</td>
</tr>
<tr>
<td>throttle-count</td>
<td>Specifies number of BGP updates to send at one time. This option limits the number of BGP updates when there are many BGP peers. Off disables the throttle count option.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>ttl &lt;1-255</td>
<td>Specifies the value of the TTL (time to live) parameter, the number of hops over which the external BGP multihop session is established. Configure this value only if the multihop option is enabled. Default: 64</td>
</tr>
<tr>
<td>suppress-default-originate &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>log-state-transitions &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>log-warnings &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>trace bgp_traceoption &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>graceful-restart-helper &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>graceful-restart-helper-stalepath-time seconds</td>
<td>Specifies the maximum amount of time that routes previously received from a restarting router are kept so that they can be revalidated. The timer is started after the peer sends an indication that it has recovered.</td>
</tr>
</tbody>
</table>

**BGP Confederations**

Use the following commands to configure BGP confederations. You can configure a BGP confederation in conjunction with external BGP.
set bgp
  confederation identifier as_number
  confederation identifier off
  confederation aspath-loops-perMITTED <1-10>
  confederation aspath-loops-perMITTED default
  routing-domain identifier as_number
  routing-domain identifier off
  routing-domain aspath-loops-perMITTED <1-10>
  routing-domain aspath-loops-perMITTED default
  synchronization <on | off>

Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>confederation identifier as_number</td>
<td>Specifies the identifier for the entire confederation. This identifier is used as the autonomous system number in external BGP sessions. Outside the confederation, the confederation id is the autonomous system number of a single, large autonomous system. Thus the confederation id must be a globally unique, typically assigned autonomous system number.</td>
</tr>
<tr>
<td>confederation identifier off</td>
<td>Disables the confederation identifier.</td>
</tr>
<tr>
<td>confederation aspath-loops-perMITTED</td>
<td>Specifies the number of times the local autonomous system can appear in an autonomous system path for BGP-learned routes. If this number is higher than the number of times the local autonomous system appears in an autonomous system path, the corresponding routes are discarded or rejected.</td>
</tr>
<tr>
<td>routing-domain identifier as_number</td>
<td>Specifies a value of 1.</td>
</tr>
<tr>
<td>routing-domain identifier off</td>
<td>Disables the routing-domain identifier</td>
</tr>
<tr>
<td>routing-domain aspath-loops-perMITTED</td>
<td>Specifies the number of times the local autonomous system can appear in an autonomous system path for BGP-learned routes. If this number is higher than the number of times the local autonomous system appears in an autonomous system path, the corresponding routes are discarded or rejected.</td>
</tr>
<tr>
<td>routing-domain aspath-loops-perMITTED default</td>
<td>Specifies a value of 1.</td>
</tr>
<tr>
<td>synchronization &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

BGP Route Reflection

Use the following commands to configure BGP route reflection. You can configure route reflection as an alternative to BGP confederations. Route reflection supports both internal and external BGP routing groups.
set bgp
    cluster-id ip_address
    cluster-id off
    default-med <0-65535>
    default-med off
    default-route-gateway ip_address
    default-route-gateway off

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-id ip_address</td>
<td>Specifies the cluster ID used for route reflection. The cluster ID default is that of the router id. Override the default if the cluster has more than one route reflector.</td>
</tr>
<tr>
<td>cluster-id off</td>
<td>Disables the cluster ID.</td>
</tr>
<tr>
<td>default-med &lt;0-65535&gt;</td>
<td>Specifies the multi-exit discriminator (MED) metric used to advertise routes through BGP.</td>
</tr>
<tr>
<td>default-med off</td>
<td>Disables the specified MED metric.</td>
</tr>
<tr>
<td>default-route-gateway ip_address</td>
<td>Specifies the default route. This route has a higher rank than any configured default static route for this router. If you do not want a BGP peer considered for generating the default route, use the peer &lt;ip_address&gt; suppress-default-originate on command.</td>
</tr>
<tr>
<td>default-route-gateway off</td>
<td>Disables the configured default BGP route.</td>
</tr>
</tbody>
</table>

**BGP Route Dampening**

Use the following commands to configure BGP route dampening. BGP route dampening maintains a history of flapping routes and prevents advertising these routes. A route is considered to be flapping when it is repeatedly transitioning from available to unavailable or vice versa.
set bgp dampening
  <on | off>
suppress-above <2-32>
suppress-above default
reuse-below <1-32>
reuse-below default
max-flat <3-64>
max-flat default
reachable-decay <1-900>
reachable-decay default
unreachable-decay <1-2700>
unreachable-decay default
keep-history <2-5400>
keep-history default

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>suppress-above &lt;2-32&gt;</td>
<td>Specifies the value of the instability metric at which route suppression takes place. A route is not installed in the forwarding table or announced even if it reachable during the period that it is suppressed.</td>
</tr>
<tr>
<td>suppress-above default</td>
<td>Specifies an instability metric value for suppressing routes of 3.</td>
</tr>
<tr>
<td>reuse-below metric &lt;1-32&gt;</td>
<td>Specifies the value of the instability metric at which a suppressed route becomes unsuppressed if it is reachable but currently suppressed. The value assigned to the reuse-below metric must be lower than the suppress-above value.</td>
</tr>
<tr>
<td>reuse-below metric default</td>
<td>Specifies an instability metric value for announcing previously suppressed routes of 2.</td>
</tr>
<tr>
<td>max-flat &lt;3-64&gt;</td>
<td>Specifies the upper limit of the instability metric. The value must be greater than the suppress-above value plus 1. Each time a route becomes unreachable, 1 is added to the current instability metric.</td>
</tr>
<tr>
<td>max-flat default</td>
<td>Specifies the upper limit of the instability metric as 16.</td>
</tr>
<tr>
<td>reachable-decay &lt;1-900&gt;</td>
<td>Specifies the time for the instability metric to reach half of its value when the route is reachable. The smaller the value the sooner a suppressed route becomes reusable.</td>
</tr>
<tr>
<td>reachable-decay default</td>
<td>Specifies a value of 300.</td>
</tr>
<tr>
<td>unreachable-decay &lt;1-2700&gt;</td>
<td>Specifies the time for the instability metric to reach half its value when the route is NOT reachable. The value must be equal to or higher than the reachable-decay value.</td>
</tr>
<tr>
<td>unreachable-decay default</td>
<td>Specifies a value of 900</td>
</tr>
<tr>
<td>keep-history &lt;2-5400&gt;</td>
<td>Specifies the period for which route flapping history is maintained for a given route.</td>
</tr>
<tr>
<td>keep-history default</td>
<td>Specifies a value of 1800.</td>
</tr>
</tbody>
</table>
**Internal BGP**

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

```plaintext
set bgp internal
   <on | off>
description text
med <0-65535>
med default
outdelay <0-65535>
outdelay off
nexthop-self <on | off>
local-address ip_address <on | off>
virtual-address <on | off>
interface [all | if_name] <on | off>
protocol [all | bgp_internal_protocol] <on | off>
graceful-restart-helper <on | off>
graceful-restart-helper-stalepath-time seconds
route-refresh <on | off>
set bgp internal peer ip_address
   peer_type <on | off>
weight <0-65535>
weight off
no-aggregator id <on | off>
holdtime <6-65535>
holdtime default
keepalive <2-21845>
keepalive default
ignore-first-ashop <on | off>
send-keepalives <on | off>
send-route-refresh [request | route-update] [unicast]
accept-routes all
accept-routes none
passive-tcp <on | off>
authtype none
authtype md5 secret secret
throttle-count <0-65535>
throttle count off
log-state-transitions <on | off>
log-warnings <on | off>
trace bgp_traceoption <on | off>
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>description text</td>
<td>You can enter a brief text description of the group.</td>
</tr>
<tr>
<td>med &lt;0-65535&gt;</td>
<td></td>
</tr>
<tr>
<td>med default</td>
<td></td>
</tr>
</tbody>
</table>
| outdelay <0-65535>         | Specifies the amount of time in seconds that a route must be present in the routing database before it is redistributed to BGP. The configured value applies to all peers configured in this group. This feature dampens route fluctuation. Zero (0), which means that this feature is disabled.  
**Default:** 0                                                                 |
| outdelay off               | Disables outdelay.                                                                                                                                                                                          |
| nexthop-self <on | off>                                                                 | Specifies for this router to send one of its own IP addresses as the BGP next hop.                                                                                                                        |
|                           | **Default:** off                                                                                                                                                                                             |
| local-address              | The address used on the local end of the TCP connection with the peer. For external peers that do not have multihop enabled, the local address must be on an interface that is shared with the peer or with the peer’s gateway when the gateway parameter is used. A session with an external peer is opened only when an interface with a local address through which the peer or gateway address is directly reachable is operating.  
For other types of peers, a peer session is maintained when any interface with the specified local address is operating. In either case, incoming connections are recognized as matching a configured peer only if they are addressed to the configured local address.  
**Note:** If running BGP in a cluster you must not configure the local address.  
**Default:** Off                                                                 |
| ip_address <on | off>                                                                 |                                                                                                                                                                                                             |
| virtual-address            | **Note:**  
- Use this option only in a lab environment with the firewall turned off.  
- Do not use in a cluster configuration.  
Specifies for this router to use the VRRP virtual IP address as the local endpoint for TCP connections. You must also configure a local address to enable this option. See the command above. You can configure this option only on a VRRP master.  
**Default:** off.                                                                 |
<p>| &lt;on | off&gt;                                                                 |                                                                                                                                                                                                             |
| interface [all | if_name] &lt;on | off&gt;                                                                 | Specifies whether to enable the specified internal peer group on all interfaces or a specific interface.                                                                                                    |
| protocol [all bgp_internal_protocol] &lt;on | off&gt;                                                                 | Specifies whether to enable all internal routing protocols on the specified internal peer group or specific internal protocols. You can enter the following specific internal protocols: direct, rip, static, ospf, and ospfase. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer_ip_address</td>
<td>Specifies an internal peer address and peer type. Enter reflector-client to specify that the local router acts as a route reflector for the group of peers named. That is, the local router is the route reflection server, and the named peers are route reflection clients. Normally, the routing daemon readvertises, or reflects, routes it receives from one of its clients to all other IBGP peers, including the other peers in that client's group. Enter no-client-reflector to specify that a reflection client's routes are reflected only to internal BGP peers in other groups. Clients in the group are assumed to be direct IBGP peers of each other. Enter none if you do not want to specify route reflection.</td>
</tr>
<tr>
<td>peer_type &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>peer_ip_address weight &lt;0-65535&gt;</td>
<td>Specifies the weight associated with the specified peer. BGP implicitly stores any rejected routes by not mentioning them in a route filter. BGP explicitly mentions them within the routing table by using a restrict keyword with a negative weight. A negative weight prevents a route from becoming active, which prevents it from being installed in the forwarding table or exported to other protocols. This eliminates the need to break and reestablish a session upon reconfiguration if import route policy is changed.</td>
</tr>
<tr>
<td>peer_ip_address weight off</td>
<td>Disables the weight associated with the specified peer.</td>
</tr>
<tr>
<td>peer_ip_address aggregator_id &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>peer ip_address holdtime &lt;6-65535&gt;</td>
<td>Specifies the BGP holdtime interval, in seconds, when negotiating a connection with the specified peer. If the BGP speaker does not receive a keepalive update or notification message from its peer within the period specified in the holdtime field of the BGP open message, the BGP connection is closed.</td>
</tr>
<tr>
<td>peer ip_address holdtime default</td>
<td>Specifies a holdtime of 180 seconds.</td>
</tr>
<tr>
<td>peer ip_address keepalive &lt;2-21845&gt;</td>
<td>The keepalive option is an alternative way to specify a holdtime value in seconds when negotiating a connection with the specified peer. You can use the keepalive interval instead of the holdtime interval. You can also use both interval, but the holdtime value must be 3 times the keepalive interval value.</td>
</tr>
<tr>
<td>peer ip_address keepalive default</td>
<td>Specifies a keepalive interval of 60 seconds.</td>
</tr>
<tr>
<td>peer ip_address ignore-first-ashop &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>peer ip_address send-keepalives &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>send-route-refresh [request</td>
<td>route-update] [unicast]</td>
</tr>
<tr>
<td>peer ip_address accept-routes all</td>
<td>Specifies an inbound BGP policy route if one is not already configured. Enter all to specify accepting routes and installing them with an invalid preference. Depending on the local inbound route policy, these routes are then made active or inactive.</td>
</tr>
<tr>
<td>peer ip_address accept-routes none</td>
<td>Specifies an inbound BGP policy route if one is not already configured. Enter none to specify deleting routes learned from a peer. This option saves memory overhead when many routes are rejected because no inbound policy exists.</td>
</tr>
<tr>
<td>peer ip_address passive-tcp &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>peer ip_address authtype none</td>
<td>Specifies not to use an authentication scheme between peers. Using an authentication scheme guarantees that routing information is accepted only from trusted peers.</td>
</tr>
<tr>
<td>peer ip_address authtype md5 secret secret</td>
<td>Specifies to use md5 authentication between peers. In general, peers must agree on the authentication configuration to and from peer adjacencies. Using an authentication scheme guarantees that routing information is accepted only from trusted peers. <strong>Note</strong> - TCP MD5 authentication for BGP is not supported on 64-bit Gaia or on a 32/64-bit Gaia VSX cluster.</td>
</tr>
<tr>
<td>peer ip_address throttle-count &lt;0-65535&gt;</td>
<td>Specifies the number of BGP updates to send at one time. The throttle count option limits the number of BGP updates when there are many BGP peers.</td>
</tr>
</tbody>
</table>
### BGP Communities

Use the following command to configure BGP communities. A BGP community is a group of destinations that share the same property. However, a community is not restricted to one network or autonomous system. Use communities to simplify the BGP inbound and route redistribution policies. Use the BGP communities commands together with inbound policy and route redistribution.

```
set bgp communities <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

### BGP Show Commands

Use the following commands to monitor and troubleshoot your BGP implementation.
show bgp
    show bgp
groups
memory
errors
paths
stats
peers
peers detailed
peer ip_address detailed
peers established
peer ip_address advertise
peer ip_address received
summary
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 routed conforms to the traceroute facility for IP multicast draft specification.


**IGMP Version 3**

Gaia provides IGMP version 3 source filtering to support source-specific multicast (SSM), which enables the Gaia system to request traffic from specific sources via PIM join/prune messages without requiring the presence of a rendezvous point (RP). This enables the Gaia 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:

- **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 IGMP - WebUI**

IGMP is enabled by default.

**To configure IGMP:**
1. In the **Network Management > Network interfaces** page of the WebUI, configure Ethernet Interfaces and assign an IP address to the interface.
2. Configure a multicast routing protocol, such as PIM.
   IGMP supports IP multicast groups on a network. IGMP functions only in conjunction with a multicast routing protocol to calculate a multicast distribution tree. For more information on multicast routing protocols supported by Gaia, see PIM.
3. Open the **Advanced Routing > IGMP** page of the WebUI.
4. For each interface on which you enabled a multicast routing protocol:
   a) Select the interface and click **Add** or **Edit**.
      The **Edit IGMP on Interface** window opens.
   b) Configure the IGMP interface parameters. The parameters are optional.
   c) **Optional**: Add a local network Multicast Group or a static multicast group. Click **Add**.
      The **Add Multicast Group** window opens.
   d) Configure the IGMP multicast group parameters.

**Edit IGMP on Interface Window Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td>The version of the IGMP protocol to comply with.</td>
</tr>
<tr>
<td><strong>Note</strong> - 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Loss Robustness</strong></td>
<td>Allows tuning for the expected packet loss on a subnet. If the subnet is expected to be highly lossy, then the &quot;loss robustness&quot; value may be increased. IGMP protocol operation is robust to (lossrobustness - 1) packet loss.</td>
</tr>
<tr>
<td><strong>Range</strong>: 1-255.</td>
<td><strong>Default</strong>: 2.</td>
</tr>
<tr>
<td><strong>Query Interval</strong></td>
<td>The interval (in seconds) between IGMP general queries sent by the querier router. This parameter can be used to tune the IGMP messaging overhead and has a secondary effect on the timeout of idle IP multicast groups.</td>
</tr>
<tr>
<td><strong>Range</strong>: 1-3600.</td>
<td><strong>Default</strong>: 125.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Query Response Interval</strong></td>
<td>The maximum response time (in seconds) inserted into the periodic IGMP general queries. The query response interval may be used to tune the burstiness of IGMP messages; a larger value spreads the host IGMP reports over a larger interval, reducing burstiness. This value must always be less than the query interval.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-25.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 10.</td>
</tr>
<tr>
<td><strong>Last Member Query Interval</strong></td>
<td>The maximum response time (in seconds) inserted into IGMP group-specific queries. The last member query interval may be used to tune the &quot;leave latency.&quot; A smaller value results in a reduction in the time to detect the loss of the last member of a multicast group. This value must always be less than the query interval.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-25.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 1.</td>
</tr>
<tr>
<td><strong>Router Alert</strong></td>
<td>Allows the &quot;disable insertion of IP router alert&quot; option in all IGMP messages sent on the interface. This can be useful in interoperating with broken IP implementations that may discard the packet due to the use of this option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Options</strong>: Enabled, Disabled</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Enabled</td>
</tr>
</tbody>
</table>

**Add Multicast Group Window**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multicast Address</strong></td>
<td>The multicast address of the group</td>
</tr>
<tr>
<td><strong>Group Type</strong></td>
<td>• <strong>Local Group</strong> - Provides a mechanism to simulate the presence of local receivers for specific groups. When a multicast group is added to an interface, IGMP sends a membership report on the interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Static Group</strong> - Provides a mechanism to simulate the presence of local receivers on an interface. When a static group is configured on an interface that is also running a parent multicast protocol (such as PIM) IGMP informs the parent of the presence of a local receiver. In contrast to regular IGMP, no membership reports are sent on the corresponding interface.</td>
</tr>
<tr>
<td></td>
<td>If the same multicast group is configured as both a local and a static group, local group takes precedence, that is, membership reports are sent out on the interface.</td>
</tr>
</tbody>
</table>

**Configuring IGMP - CLI (igmp)**

Use the IGMP commands to configure parameters for the internet group management protocol.

**Configure Interfaces for IGMP**

Use these commands to configure IGMP for specific interfaces.
set igmp interface if_name
version <1 | 2 | 3>
last-member-query-interval <1-25>
loss-robustness <1-255>
query-interval <1-3600>
query-response-interval <1-25>
router-alert <on | off>
static-group address <on | off>
local-group address <on | off>

**Note**
IGMP version 2 runs by default.

In a gateway cluster, run commands on every cluster member. The configuration of each cluster member must be identical.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface if_name</td>
<td>The interface on which IGMP should be configured.</td>
</tr>
<tr>
<td>last-member-query-interval &lt;1-25&gt;</td>
<td>The maximum response time (in seconds) inserted into IGMP group-specific queries. The last member query interval may be used to tune the &quot;leave latency.&quot; A smaller value results in a reduction in the time to detect the loss of the last member of a multicast group. This value must always be less than the query interval.</td>
</tr>
<tr>
<td>last-member-query-interval default</td>
<td>A value of 1.</td>
</tr>
<tr>
<td>loss-robustness &lt;1-255&gt;</td>
<td>Allows tuning for the expected packet loss on a subnet. If the subnet is expected to be highly lossy, then the &quot;loss robustness&quot; value may be increased. IGMP protocol operation is robust to (lossrobustness - 1) packet loss</td>
</tr>
<tr>
<td>loss-robustness default</td>
<td>A value of 2.</td>
</tr>
<tr>
<td>query-interval &lt;1-3600&gt;</td>
<td>The interval (in seconds) between IGMP general queries sent by the querier router. This parameter can be used to tune the IGMP messaging overhead and has a secondary effect on the timeout of idle IP multicast groups.</td>
</tr>
<tr>
<td>query-interval default</td>
<td>A value of 125.</td>
</tr>
<tr>
<td>query-response-interval &lt;1-25&gt;</td>
<td>The maximum response time (in seconds) inserted into the periodic IGMP general queries. The query response interval may be used to tune the burstiness of IGMP messages; a larger value spreads the host IGMP reports over a larger interval, reducing burstiness. This value must always be less than the query interval.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>router-alert</td>
<td>Allows the &quot;disable insertion of IP router alert&quot; option in all IGMP messages sent on the interface. This can be useful in interoperating with broken IP implementations that may discard the packet due to the use of this option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> off</td>
</tr>
<tr>
<td>local-group address</td>
<td>A multicast group address. A local group provides a mechanism to simulate the presence of local receivers for specific groups. When a multicast group is added to an interface, IGMP sends a membership report on the interface.</td>
</tr>
<tr>
<td>static-group address</td>
<td>• A multicast group address. A static group provides a mechanism to simulate the presence of local receivers on an interface. When a static group is configured on an interface that is also running a parent multicast protocol (such as PIM) IGMP informs the parent of the presence of a local receiver. In contrast to regular IGMP, no membership reports are sent on the corresponding interface.</td>
</tr>
<tr>
<td></td>
<td>If the same multicast group is configured as both a local and a static group, local group takes precedence, that is, membership reports are sent out on the interface.</td>
</tr>
<tr>
<td>version &lt;1</td>
<td>2</td>
</tr>
</tbody>
</table>

**Monitoring IGMP (show igmp)**

Use these commands to monitor and troubleshoot IGMP.

```yaml
show igmp
  stats
  stats receive
  stats transmit
  stats error
  interfaces
  interfaces if_address
  groups [interface logical_interface] [local | static]
  group if_address
  if-stats
  if-stat if_address
  summary
```
Chapter 5

IP Broadcast Helper

In This Chapter
- Configuring IP Broadcast helper - WebUI 44
- Configuring IP Broadcast Helper - CLI (iphelper) 45
- Monitoring IP Broadcast Helper 45

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 more information, see RFC1542 section 4.

Configuring IP Broadcast helper - WebUI

To configure IP broadcast helper
1. Open the Advanced Routing > IP Broadcast Helper page of the WebUI.
2. Use the Forward Non-local Packets option to control whether to forward packets that are not locally originated by a source directly on the receiving interface.
3. In the Configure Relays section, click Add. The Add Relay window opens.
4. Select the Interface to which you want to add support for IP helper services.
5. Add a UDP Port number to the helper services.
6. Add a Relay (server) IPv4 address for the UDP port.

**Note** - To enable IP Broadcast Helper in a cluster, do the configuration on each cluster member

IP Broadcast helper configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Non-local Packets</td>
<td>Controls whether packets will be forwarded that are not locally originated by a source directly on the receiving interface. Enable to forward packets even if the source is not directly on the receiving interface. Clear the option to require that packets are generated by a source that is directly on the receiving interface to be eligible for relay.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface on which the IP helper service runs.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>The UDP service to be forwarded by the interface. Client UDP packets with the UDP port number are forwarded to the relay.</td>
</tr>
</tbody>
</table>
### Configuring IP Broadcast Helper - CLI (iphelper)

#### Forwarding Non-Local Packets

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-nonlocal</td>
<td>Select <strong>on</strong> to forward packets even if the source is not directly on the receiving interface. Select <strong>off</strong> to require that packets are generated by a source that is directly on the receiving interface to be eligible for relay.</td>
</tr>
<tr>
<td>Default</td>
<td><strong>off</strong></td>
</tr>
</tbody>
</table>

#### IP Broadcast Helper interfaces

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

```plaintext
set iphelper interface if_name
  off
  udp-port <1-65535> off
  udp-port <1-65535> relay-to ip_address <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;if_name&gt; off</td>
<td>Disable the interface configured for iphelper</td>
</tr>
<tr>
<td>udp-port &lt;1-65535&gt; off</td>
<td>Disable the UDP services configured for this interface.</td>
</tr>
<tr>
<td>udp-port &lt;1-65535&gt; relay-to ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

**Note** - To enable IP Broadcast Helper in a cluster, do the configuration on each cluster member.

### Monitoring IP Broadcast Helper

To monitor and troubleshoot IP Broadcast Helper in the WebUI:

1. Open the **Advanced Routing > IP Broadcast Helper** page of the WebUI.
2. Click the **Monitoring** tab.

**Note** - The page is static. To see the latest values, click **Reload**.
To monitor and troubleshoot IP Broadcast Helper in clih:

```
show iphelper services
show iphelper stats
```
Chapter 6

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 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**

Gaia 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 ("Configuring RIP - WebUI" on page 48). 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.

Note -

Gaia 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.

You must use Monitored Circuit mode when configuring virtual IP support for any dynamic routing protocol, including RIP.

**Configuring RIP - WebUI**

To configure RIP:

1. In the Network Management > Network interfaces page of the WebUI, configure Ethernet Interfaces and assign an IP address to the interface.
2. Open the Advanced Routing > RIP page of the WebUI.
3. Optional: In the RIP Global Settings section ("RIP Global Settings" on page 49):
   a) Configure the RIP Update Interval and Expire Interval. These timers allows you to vary the frequency with which updates are sent and when routes expire.
   b) Select Auto Summarization to aggregate and redistribute non-classful routes in RIP 1. Clear it to disable the option.
4. In the RIP Interfaces section, click Add.
   The Add Interface window opens
5. Configure the RIP Interfaces ("RIP Interface Options" on page 49).
6. Click Save.
## RIP Global Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Update Interval** | The amount of time, in seconds, between regularly scheduled RIP updates. To prevent synchronization of periodic updates, RIP updates are actually sent at a time from the uniform distribution on the interval (0.5T, 1.5T) where T corresponds to the Update Interval value.  
|                 | **Note** - Take care when you set this parameter, as RIP has no protocol mechanism to detect misconfiguration.  
|                 | • **Range**: 1-65535.  
|                 | • **Default**: 30. |
| **Expire Interval** | The amount of time, in seconds, that must pass without receiving an update for a given route before the route is considered to have timed out. This value should be 6 times the update interval in order to allow for the possibility that packets containing an update could be dropped by the network.  
|                 | • **Range**: 1-65535.  
|                 | • **Default**: 180. |
| **Auto Summarization** | Automatically aggregates and redistributes non-classful RIP Version 1 into RIP. This applies only to RIP Version 1. If the Auto summarization field option is unchecked, you must do the aggregation and redistribution manually by using route aggregation and route redistribution.  
|                 | **Note** - Take care when you set this parameter, as RIP has no protocol mechanism to detect misconfiguration.  
|                 | • **Default**: Selected. |

## RIP Interface Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>The interface on which RIP is enabled.</td>
</tr>
</tbody>
</table>
| **Version**    | The version of RIP to run. If you specify version 2, the default is to send full version 2 packets on the RIP multicast address.  
|                 | • **Options**: 1 or 2.  
|                 | • **Default**: 1. |
| **Metric**     | The RIP metric to be added to routes that are sent using the specified interface(s). The default is zero. This is used to make other routers prefer other sources of RIP routes over this router.  
|                 | • **Range**: 0-16.  
|                 | • **Default**: 0. |
| **Accept updates** | Whether RIP packets from other routers using the interface are accepted or ignored. Ignoring an update may result in suboptimal routing.  
|                 | • **Default**: Selected. |
| **Send updates** | Whether RIP packets should be sent via the interface. This causes the interface to be a passive RIP listener.  
<p>|                 | • <strong>Default</strong>: Selected |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Address</td>
<td>Make RIP run only on the VRRP Virtual IP address associated with this interface. If this router is not a VRRP Master then RIP will not run if this option is selected. It will only run on the VRRP Master. Make sure that VRRP is configured to Accept Connections to VRRP IPs.</td>
</tr>
<tr>
<td></td>
<td>• Default: Cleared.</td>
</tr>
<tr>
<td>Transport</td>
<td>Selecting Multicast specifies that RIP version 2 packets should be multicast on this interface. This is the default. Selecting Broadcast specifies that RIP version 1 packets that are compatible with version 2 should be broadcast on this interface.</td>
</tr>
<tr>
<td></td>
<td>• Options: Broadcast/Multicast.</td>
</tr>
<tr>
<td></td>
<td>• Default: Multicast.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The type of authentication scheme to use for the link. This option applies to rip version 2 only. In general, routers on a given link must agree on the authentication configuration in order to form neighbor adjacencies. This is used to guarantee that routing information is accepted only from trusted routers.</td>
</tr>
<tr>
<td></td>
<td>• None: There is no authentication scheme for the interface to accept routing information from neighboring routers.</td>
</tr>
<tr>
<td></td>
<td>• Simple: Implement a simple authentication scheme for the interface to accept routing information from neighboring routers. Enter the Simple Password, from 1 to 16 characters. Must contain alphanumeric characters only.</td>
</tr>
<tr>
<td></td>
<td>• MD5: Implement an authentication scheme that uses an MD5 algorithm for the interface to accept routing information from neighboring routers. Enter the password.</td>
</tr>
<tr>
<td></td>
<td>To ensure interoperability with Cisco routers running RIP MD5 authentication, enable Cisco Compatibility. By default, RIP MD5 is set to conform to the Check Point standard, and not for Cisco compatibility.</td>
</tr>
<tr>
<td></td>
<td>• Options: None/Simple/MD5.</td>
</tr>
<tr>
<td></td>
<td>• Default: None.</td>
</tr>
</tbody>
</table>

Configuring RIP - CLI (rip)

**RIP Global Commands**

Use these commands to configure RIP properties that apply to all interfaces configured for RIP.
set rip
  auto-summary <on | off>
  update-interval <1-65535>
  update-interval default
  expire-interval <1-65535>
  expire-interval default

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| auto-summary <on | off>                         | Automatically aggregates and redistributes non-classful RIP Version 1 into RIP. This applies only to RIP Version 1. If the Auto summarization field option is unchecked, you must do the aggregation and redistribution manually by using route aggregation and route redistribution.
  Note - Take care when you set this parameter, as RIP has no protocol mechanism to detect misconfiguration.
  Default: on                 |
| update-interval <1-65535>  | The amount of time, in seconds, between regularly scheduled RIP updates. To prevent synchronization of periodic updates, RIP updates are actually sent at a time from the uniform distribution on the interval (0.5T, 1.5T) where T corresponds to the Update Interval value.
  Note - Take care when you set this parameter, as RIP has no protocol mechanism to detect misconfiguration. |
| update-interval default    | A value of 30 seconds.                                                       |
| expire-interval <1-65535>  | The amount of time, in seconds, that must pass without receiving an update for a given route before the route is considered to have timed out. This value should be 6 times the update interval in order to allow for the possibility that packets containing an update could be dropped by the network. |
| expire-interval default    | A value of 180 seconds.                                                      |

**RIP Interface Commands**

Use these commands to configure RIP properties that apply to a RIP interface.

set rip interface if_name
  <off |on>
  version <1 | 2> on
  metric <0-16>
  metric default
  accept-updates <on | off>
  send-updates <on | off>
  transport <multicast | broadcast>
  authtype none
  authtype simple password
  authtype md5 secret secret [cisco-compatibility] <on | off>
  virtual address <on | off>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| interface if_name <off | on>                         | Turn on or turn off RIP on the interface.
  Default: off               |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1</td>
<td>2&gt;</td>
</tr>
<tr>
<td>metric &lt;0–16&gt;</td>
<td>The RIP metric to be added to routes that are sent using the specified interface(s). The default is zero. This is used to make other routers prefer other sources of RIP routes over this router.</td>
</tr>
<tr>
<td>metric default</td>
<td>A value of 0.</td>
</tr>
<tr>
<td>accept-updates &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>send-updates &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>transport &lt;multicast</td>
<td>broadcast&gt;</td>
</tr>
<tr>
<td>authtype none</td>
<td>There is no authentication scheme for the interface to accept routing information from neighboring routers. This option applies to rip version 2 only. In general, routers on a given link must agree on the authentication configuration in order to form neighbor adjacencies. This is used to guarantee that routing information is accepted only from trusted routers.</td>
</tr>
<tr>
<td>authtype simple password</td>
<td>Implement a simple authentication scheme for the interface to accept routing information from neighboring routers. Enter the Simple Password, from 1 to 16 characters. Must contain alphanumeric characters only. This option applies to RIP version 2 only.</td>
</tr>
<tr>
<td>authtype md5 secret secret</td>
<td>Implement an authentication scheme that uses an MD5 algorithm for the interface to accept routing information from neighboring routers. Enter the password.</td>
</tr>
<tr>
<td>interface if_name virtual &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>cisco-compatibility &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
Monitoring RIP

Monitoring RIP - WebUI

To monitor and troubleshoot RIP:
1. Open the Advanced Routing > RIP page of the WebUI.
2. Click the Monitoring tab.
3. In the Information table, click a line to see the current values.

   Note - The page is static. To see the latest values, reload your browser page.

RIP Show Commands

Use these commands to monitor and troubleshoot RIP.

```
show rip
show rip interfaces
   interface <if_name>
   packets
   errors
   neighbors
   summary
```
Chapter 7

OSPF

In This Chapter
Types of Areas 54
Area Border Routers 55
High Availability Support for OSPF 55
Configuring OSPF - WebUI 56
Configuring OSPF - CLI (ospf) 62

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.

Gaia supports OSPFv2, which supports IPv4 addressing.

You can run OSPF over a route-based VPN by enabling OSPF on a virtual tunnel interface (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.

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.
- **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

Gaia supports the OSPF protocol in clusters configured either via VRRP or ClusterXL.

In this configuration, the cluster becomes a virtual router, which is seen by neighboring routers as a single router that has an IP address that is the same as the virtual IP address of the cluster. Each member of the cluster runs the OSPF task, but only the member which is designated as primary or master actively participates in the network and exchanges routing information with neighbor routers. When a failover occurs, the standby member of the cluster becomes the master and its OSPF task becomes the active participant in protocol exchanges with neighbor routers.

Gaia also supports the OSPF protocol over VPN tunnels which terminate in the VRRP or ClusterXL cluster.

VRRP

Gaia 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 being active on the old master and then starts becoming active on the new master. Because the OSPF routes database of the master is not synchronized across all members of the cluster, a traffic break may occur during the time it takes the VRRP to become active and the OSPF protocol to learn routes again. The larger the network, the more time it takes OSPF to synchronize its database and install routes again.

Note - You must use monitored-circuit VRRP, not VRRP v2, when configuring virtual IP support for OSPF or any other dynamic routing protocol.
ClusterXL
Gaia ClusterXL advertises the virtual IP address of the ClusterXL virtual router. The OSPF routes database of the master is synchronized across all members of the cluster. The OSPF task of each standby member obtains routing state and information from the master and installs the routes in the kernel as the master does. On a failover, one of the standby members becomes the new master and then continues where the old master failed. During the time that the new master resynchronizes routes database with the neighbor routers, traffic forwarding continues using the old kernel routes until OSPF routes are fully synchronized and pushed into the kernel.

Configuring OSPF - WebUI
To configure OSPF:
1. In the Network Management > Network interfaces page of the WebUI, configure Ethernet Interfaces and assign an IP address to the interface.
2. Open the Advanced Routing > OSPF page of the WebUI.
3. Define other Global settings ("Configuring Global Settings" on page 56), including the Router ID.
4. Optional: Define additional OSPF areas ("Configuring OSPF Areas" on page 57) (in addition to the backbone area).
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 an address range from being advertised into the backbone, select Restrict for the address range.
6. Configure OSPF Interfaces ("Configuring OSPF Interfaces" on page 60).
7. Configure virtual links ("Configuring OSPF Virtual Links" on page 59) for any area that does not connect directly to the backbone area.

Configuring Global Settings
The following table 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.

Global Settings for OSPF

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The Router ID uniquely identifies the router in the autonomous system. The router ID is used by the BGP and OSPF protocols. We recommend setting the router ID rather than relying on the default setting. This prevents the router ID from changing if the interface used for the router ID goes down. Use an address on a loopback interface that is not the loopback address (127.0.0.1). In a cluster, you must select a router ID and make sure that it is the same on all cluster members.</td>
</tr>
<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>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: 2.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 1-60.</td>
</tr>
<tr>
<td>SPF Hold Time</td>
<td>Specifies the minimum time in seconds between recalculations of the OSPF routing table.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: 5.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>flap. It causes routes to be recomputed, updates to be generated, and unnecessary churn to the forwarding tables.</td>
</tr>
<tr>
<td></td>
<td>Enabling this option minimizes the negative effects caused by peer routers restarting by causing the Check Point system to maintain the</td>
</tr>
<tr>
<td></td>
<td>forwarding state advertised by peer routers even when they restart.</td>
</tr>
</tbody>
</table>

**Configuring OSPF Areas**

The following table 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.

- **Area**: Choose an IPv4 address (preferred) or an integer.

**OSPF Normal Type Area Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Address Range</td>
<td>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 IPv4 address aggregates a number of more specific IPv4 addresses within an area, you can configure an address that becomes the only IPv4 address advertised into the backbone. You must be careful when configuring an address range that covers parts of an IPv4 address not contained within the area. By definition, an address range consists of a IPv4 address and a mask length. <strong>Note</strong>: To prevent a specific IPv4 address from being advertised into the backbone, select Restrict.</td>
</tr>
</tbody>
</table>
Add Stub Network

OSPF can advertise reachability to IPv4 addresses that are not running OSPF using a stub network. The advertised IPv4 address appears as an OSPF internal route and can be filtered at area borders with the OSPF area ranges. The IPv4 address 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 IPv4 address to be included in the router-LSA. You configure stub hosts by specifying a mask length of 32.

This feature also supports advertising an IPv4 address 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 and a cost with a value other than zero.

Area Type

For descriptions of area types, see Types of Areas (on page 54).

Options: Normal/Stub/NSSA.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Stub Network</td>
<td>OSPF can advertise reachability to IPv4 addresses that are not running OSPF using a stub network. The advertised IPv4 address appears as an OSPF internal route and can be filtered at area borders with the OSPF area ranges. The IPv4 address 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 IPv4 address to be included in the router-LSA. You configure stub hosts by specifying a mask length of 32. This feature also supports advertising an IPv4 address 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 and a cost with a value other than zero.</td>
</tr>
<tr>
<td>Area Type</td>
<td>For descriptions of area types, see Types of Areas (on page 54). Options: Normal/Stub/NSSA.</td>
</tr>
</tbody>
</table>

Stub Area Parameters

The following table stub areas configuration parameters 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.</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-16777215.</td>
</tr>
<tr>
<td></td>
<td>• Default: 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.</td>
</tr>
<tr>
<td></td>
<td>• Default: Selected.</td>
</tr>
</tbody>
</table>

NSSA (Not So Stubby Area) Parameters

The following table 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Default: On.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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.</td>
</tr>
<tr>
<td>Default: 1</td>
<td></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.</td>
</tr>
<tr>
<td>Default: On</td>
<td></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.</td>
</tr>
<tr>
<td>Note: To prevent a specific prefix from being advertised, select On in the Restrict field next to the entry for that prefix.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring OSPF 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 a Normal Type area (which does not connect directly to the backbone area) and configure an interface to be in that area.
2. In the **Virtual Links** section, click **Add**.
3. In the **Add Virtual Link** window, enter the **Remote Router ID** of the remote endpoint of the virtual link.
4. Select the **Transit Area**. This is the area that connects both to the backbone and to the discontiguous area.
5. Configure the following parameters for the virtual link:
   - **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.

6. 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 **MD5 List** appears. Click Add and specify the MD5 Key ID and its corresponding 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.

7. Repeat this procedure on both the ABR for the discontiguous area and an ABR that connects to the backbone area.

**Configuring OSPF Interfaces**

To configure an OSPF interface:

1. In the **Edit Interface** window, assign the appropriate **Area** to each interface by selecting the OSPF area that this interface participates in.
   - 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.
   - **Note** - The hello interval, dead interval, and authentication method must be the same for all routers on the link.

**Configuration Parameters for OSPF Interfaces**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong></td>
<td>The drop-down list displays all of the areas configured and enabled on your platform. An entry for the backbone area is displayed even if it is disabled. An OSPF area defines a group of routers running OSPF that have the complete topology information of the given area. OSPF areas use an area border router (ABR) to exchange information about routes. Routes for a given area are summarized into the backbone area for distribution into other non-backbone areas. An ABR must have at least two interfaces in at least two different areas. For information on adding an area Configuring OSPF Areas and Global Settings.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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></td>
<td>- <strong>Range:</strong> 1-65535 in seconds</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> For broadcast interfaces, the default hello interval is 10 seconds. For point-to-point interfaces, the default hello interval is 30 seconds.</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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Recommended value:</strong> 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>
<tr>
<td></td>
<td>- <strong>Range:</strong> 1-65535 in seconds</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> For broadcast interfaces, the default dead interval is 40 seconds. For point-to-point interfaces, the default dead interval is 120 seconds.</td>
</tr>
<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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range:</strong> 1-65535 in seconds</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range:</strong> 1-65535.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> 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. A DR is not elected on point-to-point type interfaces. A router with priority 0 is not eligible to become the DR.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range:</strong> 0-255.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> 1.</td>
</tr>
<tr>
<td>Passive</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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Options:</strong> On or Off.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> Off.</td>
</tr>
</tbody>
</table>
### Parameter Description

**Use Virtual Address**  
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.

- **Options**: On or Off.
- **Default**: Off

**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 are:

- **None**: 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.

---

### Configuring OSPF - CLI (ospf)

Use the following group of commands to set and view parameters for OSPF. This syntax is shown below for each set of commands.

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

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

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

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router-id default</td>
<td>Selects the highest interface address when OSPF is enabled.</td>
</tr>
</tbody>
</table>
**Parameter** | **Description**
--- | ---
router-id ip_address | Specifies a specific IP address to assign as the router ID. Do not use 0.0.0.0 as the router ID address. Check Point recommends setting the router ID rather than relying on the default setting. Setting the router ID prevents the ID from changing if the default interface used for the router ID goes down.

The Router ID uniquely identifies the router in the autonomous system. The router ID is used by the BGP and OSPF protocols. We recommend setting the router ID rather than relying on the default setting. This prevents the router ID from changing if the interface used for the router ID goes down. Use an address on a loopback interface that is not the loopback address (127.0.0.1). In a cluster, you must select a router ID and make sure that it is the same on all cluster members.

- **Range:** Dotted-quad([0-255],[0-255],[0-255],[0-255]). Do not use 0.0.0.0
- **Default:** The interface address of one of the local interfaces.

**OSPF Global Settings**

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

For OSPFv2 use the following commands:

```bash
set ospf
  rfc1583-compatibility <on | off>
  spf-delay <1-60>
  spf-delay default
  spf-holdtime <1-60>
  spf-holdtime default
  default-ase-cost <1-677215>
  default-ase-type <1 | 2>
  graceful-restart-helper <on | off>
```

**Parameter** | **Description**
--- | ---
rfc1583-compatibility <on | off> | The Check Point implementation of OSPF is based on RFC 2178, which fixed some looping problems in an earlier specification of OSPF. If your implementation runs in an environment with OSPF implementations based on RFC 1583 or earlier, enable this option, which is on by default. Setting compatibility with RFC 1583 ensures backward compatibility.

on

spf-delay <1-60> | Specifies the time, in seconds, to wait before recalculating the OSPF routing table after a change in the topology.

spf-delay default | Specifies an spf-delay time of 2 seconds.

spf-holdtime <1-60> | Specifies the minimum time, in seconds, between recalculations of the OSPF routing table.

spf-holdtime default | Specifies an spf-holdtime of 5 seconds.

default-ase-cost <1-677215> | Specifies the cost assigned to routes from other protocols that are redistributed into OSPF as autonomous systems external. If the route has a cost already specified, that cost takes precedent.

1
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-ase-type &lt;1</td>
<td>2&gt;</td>
</tr>
<tr>
<td>graceful-restart-helper &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

**OSPF Interfaces**

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

For OSPFv2 use the following commands:

```plaintext
set ospf
  area <backbone | ospf_area> range ip_prefix <on | off>
  area <backbone | ospf_area> range ip_prefix restrict <on | off>
  stub-network ip_prefix <on | off>
  stub-network ip_prefix stub-network-cost <1-677722>

set ospf interface if_name
  area <backbone | ospf_area> <on | off>
  hello-interval <1-65535>
  hello-interval default
  dead-interval <1-65535>
  dead-interval default
  retransmit-interval <1-65535>
  retransmit-interval default
  cost <1-65535>
  priority <0-255>
  passive <on | off>
  virtual-address <on | off>
  auth-type none
  simple password
  md5 key authorization key id secret md5 secret
  md5 key authorization key id
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area &lt;backbone</td>
<td>ospf_area&gt; range ip_prefix &lt;on</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>area &lt;backbone</td>
<td>ospf_area&gt; range ip_prefix restrict &lt;on</td>
</tr>
<tr>
<td>stub-network ip_prefix &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>stub-network ip_prefix stub-network-cost &lt;1-677722&gt;</td>
<td>Configure a stub network to advertise reachability to prefixes that are not running OSPF. The advertised prefix appears as an OSPF internal route and is filtered at area borders with the OSPF area ranges. The prefix must be directly reachable on the router where the stub network is configured, that is, one of the router’s interface addresses must fall within the prefix range to be included in the router-link-state advertisement. Use a mask length of 32 to configure the stub host. The local address of a point-to-point interface can activate the advertised prefix and mask. To advertise reachability to such an address, enter an IP address for the prefix and a non-zero cost for the prefix.</td>
</tr>
<tr>
<td>interface if_name area &lt;backbone</td>
<td>ospf area&gt; &lt;on</td>
</tr>
<tr>
<td>interface if_name hello-interval &lt;1-65535&gt;</td>
<td>Specifies the interval, in seconds, between hello packets that the router sends on the specified interface. For a given link, this value must be the same on all routers or adjacencies do not form.</td>
</tr>
<tr>
<td>interface if_name hello-interval default</td>
<td>Specifies the default value for the hello interval, which is 10 seconds.</td>
</tr>
<tr>
<td>interface if_name dead-interval &lt;1-65535&gt;</td>
<td>Specifies the number of seconds after which a router stops receiving hello packets that it declares the peer down. Generally, you should set this value at 4 times the value of the hello interval. Do not set the value at 0. For a given link, this value must be the same on all routers or adjacencies do not form.</td>
</tr>
<tr>
<td>interface if_name dead-interval default</td>
<td>Specifies the default value for the dead interval, which is 40 seconds.</td>
</tr>
<tr>
<td>interface if_name retransmit-interval &lt;1-65535&gt;</td>
<td>Specifies the number of seconds between link state advertisement transmissions for adjacencies belonging to the specified interface. This value also applies to database description and link state request packets. Set this value conservatively, that is, at a significantly higher value than the expected round-trip delay between any two routers on the attached network.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>interface if_name retransmit-interval default</td>
<td>Specifies the default for the retransmit interval, which is 5 seconds.</td>
</tr>
<tr>
<td>interface if_name cost &lt;1-65535&gt;</td>
<td>Specifies the weight of the given path in a route. The higher the cost, the less preferred the link. To use one interface over another for routing paths, assign one a higher cost.</td>
</tr>
<tr>
<td>interface if_name priority &lt;0-255&gt;</td>
<td>Specifies the priority for becoming the designated router (DR) on the specified link. When two routers attached to a network attempt to become a designated router, the one with the highest priority wins. This option prevents the DR from changing too often. The DR option applies only to a share-media interface, such as Ethernet or FDDI; a DR is not elected on a point-to-point type interface. A router with a priority of 0 is not eligible to become the DR.</td>
</tr>
<tr>
<td>interface if_name passive &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>interface if_name authtype none</td>
<td>Specifies not to use an authentication scheme for the specified interface.</td>
</tr>
<tr>
<td>interface if_name authtype simple password</td>
<td>Specifies to use simple authentication for the specified interface. Enter an ASCII string that is 8 characters long. Generally, routers on a given link must agree on the authentication configuration to form peer adjacencies. Use an authentication scheme to guarantee that routing information is accepted only from trusted peers.</td>
</tr>
<tr>
<td>interface if_name authtype md5 key authorization key id secret md5 secret</td>
<td>Specifies to use MD5 authorization. Enter at least one key ID and its corresponding MD5 secret. If you configure multiple key IDs, the largest key ID is used for authenticating outgoing packets. All keys can be used to authenticate incoming packets. Generally, routers on a given link must agree on the authentication configuration to form peer adjacencies. Use an authentication scheme to guarantee that routing information is accepted only from trusted peers.</td>
</tr>
</tbody>
</table>

**OSPF Virtual Links**

Use the following commands to configure OSPF virtual links. Configure a virtual link if the router is a border router that does not have interfaces in the backbone area. The virtual link is effectively a tunnel across an adjacent non-backbone area whose endpoint must be any of the adjacent area’s border routers that has an interface in the backbone area.

For OSPFv2 use the following commands:
set ospf area backbone virtual-link ip_address
    transit-area ospf_area <on | off>
    transit-area ospf_area hello-interval <1-65535>
    transit-area ospf_area hello-interval default
    transit-area ospf_area dead-interval <1-4294967295>
    transit-area ospf_area dead-interval default
    transit-area ospf_area retransmit-interval <1-4294967295>
    transit-area ospf_area retransmit-interval default
    transit-area ospf_area authtype none
    transit-area ospf_area authtype simple password
    transit-area ospf_area authtype md5 key authorization key id secret md5 key
    transit-area ospf_area authtype md5 key authorization key id off

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address transit-area ospf_area &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area hello-interval &lt;1-65535&gt;</td>
<td>Specifies the interval, in seconds, between hello packets that the router sends on the specified interface. For a given link, this value must be the same on all routers or adjacencies do not form.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area hello-interval default</td>
<td>Specifies an interval of 10 seconds.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area dead-interval &lt;1-4294967295&gt;</td>
<td>Specifies the number of seconds after which a router stops receiving hello packets that it declares the neighbor down. Generally, you should set this value at 4 times the value of the hello interval. Do not set the value at 0. For a given link, this value must be the same on all routers or adjacencies do not form.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area dead-interval default</td>
<td>Specifies a value of 40 seconds.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area retransmit-interval &lt;1-4294967295&gt;</td>
<td>Specifies the number of seconds between link state advertisement transmissions for adjacencies belonging to the specified interface. This value also applies to database description and link state request packets. Set this value conservatively, that is, at a significantly higher value than the expected round-trip delay between any two routers on the attached network.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area retransmit-interval default</td>
<td>Specifies a value of 5 seconds.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area authtype none</td>
<td>Specifies not to use an authentication scheme for the specified interface.</td>
</tr>
</tbody>
</table>
### OSPF Areas

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

For OSPFv2, use the following commands.

```bash
set ospf area backbone <on | off>
set ospf area ospf_area
  <on | off>
  stub <on | off>
  stub default-cost <1-677215>
  stub summary <on | off>
  nssa <on | off>
  nssa default-cost <1-677215>
  nssa default-metric-type <1-2>
  nssa import-summary-routes <on | off>
  nssa translator-role <always | candidate>
  nssa translator-stability-interval <1-65535>
  nssa redistribution <on | off>
  nssa range ip_addr [restrict] <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backbone &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>stub &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>stub default-cost &lt;1-677215&gt;</td>
<td>Specifies a default route into the stub area with the specified cost.</td>
</tr>
<tr>
<td>stub summary &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>nssa &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>nssa default-cost &lt;1-677215&gt;</td>
<td>Specifies a default route into the stub area with the specified cost.</td>
</tr>
<tr>
<td>nssa default-metric-type &lt;1-2&gt;</td>
<td>Specifies the OSPF area as totally stubby, meaning that it does not have any AS external routes and its area border routers do not advertise summary routes.</td>
</tr>
<tr>
<td>nssa import-summary-routes &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>nssa translator-role &lt;always</td>
<td>candidate&gt;</td>
</tr>
<tr>
<td>nssa translator-stability-interval &lt;1-65535&gt;</td>
<td>Specifies the OSPF area as totally stubby, meaning that it does not have any AS external routes and its area border routers do not advertise summary routes.</td>
</tr>
<tr>
<td>nssa redistribution &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>nssa default-cost &lt;1-677215&gt;</td>
<td>Specifies the cost associated with the default route to the NSSA.</td>
</tr>
<tr>
<td>nssa default-metric-type &lt;1-2&gt;</td>
<td>Specifies the type of metric. The default, type 1, is equivalent to the <em>Default ASE Route Type</em> on the OSPF WebUI page. A type 1 route is internal and its metric can be used directly by OSPF for comparison. A type 2 route is external and its metric cannot be used for comparison directly.</td>
</tr>
<tr>
<td>nssa import-summary-routes &lt;on</td>
<td>Specifies if summary routes (summary link advertisements) are imported into the NSSA.</td>
</tr>
<tr>
<td></td>
<td>off&gt;</td>
</tr>
<tr>
<td>nssa translator-role &lt;always</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.</td>
</tr>
<tr>
<td></td>
<td>candidate&gt;</td>
</tr>
<tr>
<td>nssa translator-stability-interval &lt;1-65535&gt;</td>
<td>Specifies how long in seconds this elected Type-7 translator will continue to perform its translator duties once it has determined that its translator status has been assumed by another NSSA border router. Default: 40 seconds.</td>
</tr>
<tr>
<td>nssa redistribution &lt;on</td>
<td>Specifies if both Type-5 and Type-7 LSAs or only Type-7 LSAs will be originated by this NSSA border router.</td>
</tr>
<tr>
<td></td>
<td>off&gt;</td>
</tr>
<tr>
<td>nssa rangeip_addr[restrict] &lt;on</td>
<td>Specify the range of addresses to reduce the number of Type-5 LSAs for the NSSA border router. To prevent a specific prefix from being advertised, use the restrict argument.</td>
</tr>
<tr>
<td></td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

**OSPF Show Commands**

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

To view a summary of your OSPF implementation, including the number of areas configured and the number of interfaces configured within each area, use:

- For OSPFv2: `show ospf`

For OSPFv2 use the following commands:
show ospf
  neighbors
  neighbor ip_address
  interfaces
  interfaces stats
  interfaces detailed
  interface ifname
  interface ifname stats
  interface ifname detailed
  packets
  errors
  errors dd
  errors hello
  errors ip
  errors lsack
  errors lsr
  errors lsu
  errors protocol
  events
  border-routers
  database
  database areas
  database area ospf_area
  database asbr-summary-lsa
  database checksum
  database database-summary
  database detailed
  database external-lsa
  database network-lsa
  database router-lsa
  database summary-lsa
  database type <1 | 2 | 3 | 4 | 5 | 7> [detailed]
  database nssa-external-lsa [detailed]
  summary

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbors</td>
<td>The IP addresses of neighboring interfaces, their priority and status, and the number of errors logged for each interface.</td>
</tr>
<tr>
<td>neighbor ip_address</td>
<td>The priority, status, and number of errors logged for the specified IP address.</td>
</tr>
<tr>
<td>interface ifname &lt;on</td>
<td>The use of the VRRP virtual link-local address as the source of its control packets</td>
</tr>
<tr>
<td>off&gt;</td>
<td>off&gt;</td>
</tr>
<tr>
<td>interfaces</td>
<td>The names of all configured logical interfaces, their corresponding IP addresses, to area to which each interface is assigned, each interface’s status and the IP addresses of each logical interface’s designated router and backup designated router.</td>
</tr>
<tr>
<td>interfaces stats</td>
<td>The number of each type of error message logged for each OSPF interface as well as the number of link state advertisements sent by each interface.</td>
</tr>
<tr>
<td>interfaces detailed</td>
<td>Displays detailed information about each OSPF interface, including the authentication type configured if any, the router IDs and IP addresses of the designated router and backup designated router, the timer intervals configured for hello wait, dead, and retransmit messages, and the number of neighbors for each interface.</td>
</tr>
<tr>
<td>interface if_name</td>
<td>The IP address, area ID, status, number of errors logged, and the IP address of the designated router and backup designated router for the specified interface.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>neighbors</td>
<td>The IP addresses of neighboring interfaces, their priority and status, and the number of errors logged for each interface.</td>
</tr>
<tr>
<td>interface if_name stats</td>
<td>The number of each type of error message logged by the specified interface as well as the number of link-state advertisements sent by the specified interface.</td>
</tr>
<tr>
<td>interface if_name detailed</td>
<td>Displays detailed information about the specified interface, including the authentication type configured if any, the router IDs and IP addresses of the designated router and backup designated router, the timer intervals configured for hello wait, dead, and retransmit messages, and the number of neighbors for each interface</td>
</tr>
<tr>
<td>packets</td>
<td>The number of each type of packet sent, including hello packets, link-state update packets, and link-state acknowledgment and link-state request packets.</td>
</tr>
<tr>
<td>errors</td>
<td>The number of each type of error message sent, including hello protocol errors, database description errors, protocol errors, link-state acknowledgment errors, link-state request errors, link-state update errors, and IP errors.</td>
</tr>
<tr>
<td>errors dd</td>
<td>The number of each type of database- description error messages only.</td>
</tr>
<tr>
<td>errors hello</td>
<td>The number of each type of hello- error message only.</td>
</tr>
<tr>
<td>errors ip</td>
<td>The number of each type of IP-errors message only.</td>
</tr>
<tr>
<td>errors lsack</td>
<td>The number of each type of link-state acknowledgment error message only.</td>
</tr>
<tr>
<td>errors lsu</td>
<td>The number of each type of link-state update error message only</td>
</tr>
<tr>
<td>errors lsr</td>
<td>The number of each type of link-state request error messages only.</td>
</tr>
<tr>
<td>errors protocol</td>
<td>The number of each type of protocol error message only.</td>
</tr>
<tr>
<td>border-routers</td>
<td>The IP address of each area border router, the OSPF area of each border router, and the cost associated with each IP address.</td>
</tr>
<tr>
<td>database</td>
<td>Router-link state and network-link state statistics for each OSPF area. Also The checksum, sequence number, and link count of each OSPF interface.</td>
</tr>
<tr>
<td>database areas</td>
<td>Router-link state, network-link state, AS-border-router link state, AS-external link state, and summary-link state statistics for each OSPF area. Also The checksum, sequence number, and link count of each OSPF interface.</td>
</tr>
<tr>
<td>database area ospf_area</td>
<td>Displays router-link state, network-link state, AS-border-router-link state, AS- external-link state, and summary-link state statistics for the specified OSPF area. Also The checksum, sequence number, and link count of each IP address configured within the specified OSPF area.</td>
</tr>
<tr>
<td>database asbr-summary</td>
<td>A summary of AS-border-router link state statistics for each OSPF area. For OSPFv2 only.</td>
</tr>
<tr>
<td>database external</td>
<td>Displays AS-external-link state statistics for each OSPF area.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>neighbors</td>
<td>The IP addresses of neighboring interfaces, their priority and status, and the number of errors logged for each interface.</td>
</tr>
<tr>
<td>database network</td>
<td>Network-link-state statistics, including the advertised router, sequence number, and checksum of each OSPF interface. For OSPFv2 only.</td>
</tr>
<tr>
<td>database nssa-external-lsa</td>
<td>Type 7 LSAs (NSSA). This argument applies only to OSPF v2.</td>
</tr>
<tr>
<td>database router-lsa</td>
<td>Displays router-link-state statistics, including the advertised router, sequence number, checksum, and link count, of each OSPF interface. For OSPFv2 only.</td>
</tr>
<tr>
<td>database summary-lsa</td>
<td>A summary of link-state statistics for each OSPF area. For OSPFv2 only.</td>
</tr>
</tbody>
</table>
| database type <1 | 2 | 3 | 4 | 5 | 7> [detailed] | Displays link-state statistics associated with the specified number:  
1—router-link-state statistics.  
2—network-link-state statistics.  
3—summary-link-state statistics.  
4—AS-border-router-link-state statistics.  
5—AS-external-link-state statistics.  
7—NSSA. This option applies only to OSPF v2. |
| events                          | The number of interface up/down events; virtual interface up/down events; designated router election events; router ID changes; area border router changes; AS border router changes, and link state advertisement messages. |
Chapter 8

Route Aggregation

In This Chapter

Configuring Route Aggregation - WebUI 73
Configuring Route Aggregation - CLI (aggregate) 75

Route aggregation is a method of generating a more general route, given the presence of a specific route. Use this method to reduce the number of routes advertised for a given protocol. For example, if a router has many stub interface routes subnetted from a class C and is running RIPv2 on another interface, you can use interface routes to create an aggregate route of the class C that can then be redistributed into RIP. This action reduces the number of routes advertised through RIP. Be careful when aggregating if there are "holes" in the route that is aggregated.

The interface that originates the aggregate routes does not use aggregate routes to forward packets. Only the router receiving data can use the Aggregate routes to forward traffic. A router that receives a packet that does not match one of the component routes that generated an aggregate route should respond with an ICMP network unreachable message. This action prevents packets for unknown component routes from following a default route into another network, where they are continually forwarded back to the border router until their TTLs expire.

Create an aggregate route by specifying the network address and mask length and then providing a set of contributing routes. Define a contributing route by specifying a source, such as, a routing protocol, a static route, an interface route, and a route filter, which is either a prefix or the keyword all. An aggregate route can have many contributing routes, but at least one of the routes must be present to generate an aggregate route.

Configuring Route Aggregation - WebUI

To create aggregate routes
1. Go to the Advanced Routing > Route Aggregation page of the WebUI.
2. Click Add.
   The Add Aggregate Route window opens.
3. Enter the IPv4 address for the new contributing route.
4. Enter the Subnet mask.
   The IPv4 address and subnet mask correspond to a single routing table entry.
5. In the Contributing Protocol section, click Add.
   The Add Contribution Setting window opens.
7. Optional: Select Contribute All Routes.
8. Optional: To specify a prefix, fill in the Address and Subnet mask.
9. Select the Match Type (None, Refines or Exact).
10. Click Save.
Add Aggregate Route Window

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 address</td>
<td>The IPv4 address of a route that activates the aggregate route, if contributed by the protocol.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: Dotted-quad ([0-255].[0-255].[0-255].[0-255])</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: No default.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>The mask length of the route that activates the aggregate route, if contributed by the protocol.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 0-32.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: No default.</td>
</tr>
<tr>
<td>Rank</td>
<td>The routing system uses rank when there are routes from different protocols to the same destination. For each route, the route from the protocol with the lowest rank is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 0-255.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Each routing protocol has a default rank value. Aggregate routes have a default rank of 130. The default value for OSPF is 10, and the default value for RIP is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>A second tie breaker after the rank. It selects routes going to the same destination. The route with the highest weight is an active route and is installed in the kernel forwarding table and redistributed to other routing protocols.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 0-65535.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 0.</td>
</tr>
<tr>
<td>AS Path Truncate</td>
<td>When selected, the AS path is truncated to the longest common AS path.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Options</strong>: Select / Clear</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Clear. Build an AS path consisting of SETs and SEQUENCEs of all contributing AS paths.</td>
</tr>
<tr>
<td>Contributing Protocol</td>
<td>Contributing protocols whose routes activate the aggregate routes.</td>
</tr>
</tbody>
</table>

Add Contribution Setting window

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>A contributing protocol whose routes activate the aggregate route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: All routing protocols, as well as interface routes, aggregate routes, and static routes. Select one of the following: All / Direct / Static / Aggregate / OSPF2 / OSPF2ASE / RIP / BGP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: No default</td>
</tr>
<tr>
<td>Contribute All Routes</td>
<td>When selected, lets any routes contributed by the protocol activate the aggregate route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Options</strong>: Select / Clear</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Clear.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the aggregate route being created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: Dotted-quad ([0-255].[0-255].[0-255].[0-255])</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: No default.</td>
</tr>
</tbody>
</table>
### Configuring Route Aggregation - CLI (aggregate)

Create aggregate routes using these commands.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>contributing protocol</td>
<td>The IP address and mask length of the new aggregate route and the contributing protocol or interface route. To specify a protocol, enter direct, static, ospf2, ospf2ase, bgp, rip, igrp, rip, or aggregate. To specify a contributing route, enter all to contribute all the routes for a specific protocol or enter the IP address and mask length to contribute a specific route.</td>
</tr>
<tr>
<td>contributing-route</td>
<td>The contributing route is limited to the specified IP address and mask length only. You cannot enable both exact on and refines on at the same time. If you enable refines on when exact on is enabled, exact on is automatically disabled.</td>
</tr>
<tr>
<td>&lt;ip_prefix&gt; exact on</td>
<td>The contributing route is based on addresses with a greater value than the specified mask length of the specified IP address. You cannot enable both exact on and refines on at the same time. If you enable refines on when exact on is enabled, exact on is automatically disabled.</td>
</tr>
<tr>
<td>&lt;ip_prefix&gt; refines on</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet mask</td>
<td>The mask length of the aggregate route being created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 0-32</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> No default</td>
</tr>
<tr>
<td>Match Type</td>
<td>The routes that are filtered for the <em>Address</em> and <em>Subnet mask</em>. These are the ways to compare other routes against it:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong> - matches any route that equals the specified route or is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exact</strong> - matches a route only if it equals the <em>From Address</em> and <em>Subnet mask</em> of the specified route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Refines</strong> - matches a route only if it is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Options:</strong> None, Exact, Refines.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> None.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rank default</td>
<td>The rank to assign to the aggregate route when routes from different protocols to the same destination are present. For each route, the route from the protocol with the lowest rank is used. Each routing protocol has a different default rank value. Aggregate routes have a default rank of 130.</td>
</tr>
<tr>
<td>rank &lt;0-255&gt;</td>
<td>The rank to assign to the aggregate route when routes from different protocols to the same destination are present. For each route, the route from the protocol with the lowest rank is used. Each routing protocol has a different default rank value. Aggregate routes have a default rank of 130.</td>
</tr>
<tr>
<td>weight default</td>
<td>A value that breaks a tie if select routes going to the same destination have the same rank value. The route with the highest weight is the active route. The active route is installed in the kernel forwarding table and redistributed to the other routing protocols.</td>
</tr>
<tr>
<td>weight &lt;0-65535&gt;</td>
<td>A value that breaks a tie if select routes going to the same destination have the same rank value. The route with the highest weight is the active route. The active route is installed in the kernel forwarding table and redistributed to the other routing protocols.</td>
</tr>
<tr>
<td>aspath-truncate &lt;on</td>
<td>Specifies that the autonomous system (AS) path be truncated to the longest common AS path. The default behavior is to build an AS path that consists of sets and sequences of all contributing AS paths.</td>
</tr>
<tr>
<td>off&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: off</td>
</tr>
</tbody>
</table>
Chapter 9

Routing Policy Configuration

In This Chapter

<table>
<thead>
<tr>
<th>Routing Policy Configuration</th>
<th>Description</th>
<th>Configured Using</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound Route filters</td>
<td>Restrict or constrain the set of routes accepted by a given routing protocol. Inbound Route filters are similar to route maps for an import policy.</td>
<td>WebUI</td>
</tr>
<tr>
<td>Route Redistribution</td>
<td>Allow routes learned from one routing protocol to be propagated to another routing protocol. It is also useful for advertising static routes, such as the default route, or aggregates into a protocol. Route Redistribution are similar to route maps for an export policy.</td>
<td>WebUI</td>
</tr>
<tr>
<td>Routemaps</td>
<td>Control which routes are accepted and announced. Used to configure inbound route filters, outbound route filters, and to redistribute routes from one protocol to another. Route maps offer more configuration options than the WebUI options. However, they are not functionally equivalent. If one or more route maps are assigned to a protocol (for import or export), any corresponding WebUI configuration is ignored.</td>
<td>cli/sh</td>
</tr>
</tbody>
</table>

You can configure routing policy for RIP, OSPFv2 and BGP in these ways:

**Configuring Inbound Route Filters - WebUI**

Inbound route filters allow you to restrict or constrain the set of routes accepted by a given routing protocol. By default, all RIP and OSPF external routes are accepted. BGP requires an explicit policy to accept routes.

The filters let an operator include or exclude ranges of prefixes from the routes that are accepted into RIP, 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.

You can define Inbound route filters only using the WebUI. Inbound route filters are not available in the CLI. However, you can configure the same functionality in the CLI using routemaps.

**To configure a policy for OSPF routes:**
1. Go to the Advanced Routing > Inbound Route Filters page of the WebUI.
2. In the Inbound Route Protocols and BGP Policies section, select OSPF External Routes.
3. Click Edit.
4. In the Configure OSPF External All Routes window, select the Action:
   - Options: Accept or Restrict
   - Default: Accept
5. If you selected Accept, change the Rank:
   - Range: 0-255
   - Default: 150

**To configure a policy for RIP routes:**
1. Go to the Advanced Routing > Inbound Route Filters page of the WebUI.
2. In the Inbound Route Protocols and BGP Policies section, select RIP Routes.
3. Click Edit.
4. In the Configure RIP All Routes window, select the Action:
   - Options: Accept or Restrict
   - Default: Accept
5. If you selected Accept, change the Rank:
   - Range: 0-255
   - Default: 100
6. You can fine tune the policy for RIP routes. In the Individual Routes section click Add. The Add Route window opens ("Fine Tuning Policies" on page 80).

**To configure a policy for BGP routes:**
1. Go to the Advanced Routing > Inbound Route Filters page of the WebUI.
3. You can fine tune the policy for BGP routes. In the Individual Routes section click Add. The Add Route window opens ("Fine Tuning Policies" on page 80).

**Note** - For BGP, no routes are accepted from a peer by default. You must configure an explicit Inbound BGP Route Filter to accept a route from a peer.

### Add BGP Policy Window

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Type: Based on AS_PATH Regular Expression (1-511)</td>
<td>An autonomous system can control BGP importation. BGP supports propagation control through the use of AS-PATH regular expressions. BGP version 4 supports the propagation of any destination along a contiguous network mask.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>BGP Type:</strong> Based on Autonomous System Number (512-1024)**</td>
<td>An autonomous system can control BGP importation. BGP can accept routes from different BGP peers based on the peer AS number.</td>
</tr>
<tr>
<td><strong>Import ID</strong></td>
<td>The order in which the import lists are applied to each route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range for BGP Type based on AS_PATH Regular Expression:</strong> 1-511</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range for BGP Type based on Autonomous System Number:</strong> 512-1024</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> No default</td>
</tr>
<tr>
<td><strong>AS Number</strong></td>
<td>Autonomous system number of the peer AS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 0-65535</td>
</tr>
<tr>
<td><strong>AS-PATH Regular Expression</strong></td>
<td>The following definitions describe how to create regular expressions. AS-PATH operators are one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>aspath_term (m n)</strong> A regular expression followed by (m n), where m and n are both non-negative integers and m is less than or equal to n. This expression means that there are at least m, and at most, n repetitions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aspath_term m</strong> A regular expression followed by m, where m is a positive integer and means exactly m repetitions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aspath_term (m)</strong> A regular expression followed by m, where m is a positive integer. This expression means that there are exactly m repetitions.</td>
</tr>
<tr>
<td></td>
<td>• **aspath_term *** A regular expression followed by *, which means zero or more repetitions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aspath_term +</strong> A regular expression followed by +, which means one or more repetitions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aspath_term ?</strong> A regular expression followed by ?, which means zero or one repetition.</td>
</tr>
<tr>
<td></td>
<td>• **aspath_term</td>
</tr>
<tr>
<td><strong>Origin</strong></td>
<td>The completeness of AS-PATH information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any</strong> -</td>
</tr>
<tr>
<td></td>
<td>• <strong>IGP</strong> - A route was learned from an interior routing protocol and is probably complete.</td>
</tr>
<tr>
<td></td>
<td>• <strong>EGP</strong> - The route was learned from an exterior routing protocol that does not support AS-PATHs, and the path is probably incomplete.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Incomplete</strong> - The path information is incomplete.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Options:</strong> Any / IGP / EGP / Incomplete</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> No default</td>
</tr>
</tbody>
</table>
Parameter | Description
--- | ---
Weight | BGP stores any routes that are rejected by not mentioning them in a route filter. BGP explicitly mentions these rejected routes in the routing table and assigns them a restrict keyword with a negative weight. A negative weight prevents a route from becoming active, which means that it is not installed in the forwarding table or exported to other protocols. This feature eliminates the need to break and re-establish a session upon reconfiguration if importation policy is changed.
  - **Range:** 0-65535
  - **Default:** No default

Local Pref. | The BGP local preference to the imported route. Check Point recommends that you configure this value to bias the preference of `routed` for BGP routes.
  
  **Note:** Do not use the local preference parameter when importing BGP.

  The local preference value is sent automatically when redistributing external BGP routes to an internal BGP route. The local preference parameter is ignored if used on internal BGP import statements.
  
  - **Range:** 0-65535. Larger values are preferred
  - **Default:** No default

All Routes: Action | Whether the routing protocol should accept or restrict the All Routes route, equivalent to 0.0.0.0/0, from the given AS-Path or AS. If set to Accept, you can specify a Rank for all routes.
  
  - **Options:** Accept / Restrict
  - **Default:** Restrict

All Routes: Rank | If All Routes: Action is set to Accept, you can specify a Rank for all routes.
  
  - **Range:** 0-65535
  - **Default:** no default.

**Fine Tuning Policies**

To fine tune your OSPF, RIP or BGP Policy:

1. Specify which routes should be filtered by:
   
   - IP address
   - Subnet mask
   - Match type
   - Optional: Parameters that depend on the match type. For routes that match a filter, you can select Accept or Restrict. If the route is accepted, you can specify its rank.

2. Specify what actions to perform on a route if it matches the route filter.

Do these steps by configuring the parameters in the **Add Route** window.

**Add Route Window**

Parameter | Description
--- | ---
Protocol | The protocol for which you want to create the inbound route filter.

Address Subnet mask | A baseline route that specifies a route filter. This route is the **specified route** in the context of a single route filter.
Routing Policy Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matchtype</td>
<td>The routes that are filtered for the From Address and Subnet mask. These are the ways to compare other routes against it:</td>
</tr>
<tr>
<td></td>
<td>- Normal - matches any route that equals the specified route or is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>- Exact - matches a route only if it equals the From Address and Subnet mask of the specified route.</td>
</tr>
<tr>
<td></td>
<td>- Refines - matches a route only if it is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>- Range - matches any route whose ip prefix equals the specified route's From Address and whose Subnet Mask falls within the specified Subnet Mask length range.</td>
</tr>
<tr>
<td></td>
<td>- Options: Normal, Exact, Refines, Range.</td>
</tr>
<tr>
<td></td>
<td>- Default: Normal.</td>
</tr>
<tr>
<td>Action</td>
<td>What to do with the routes that match the filter that is defined by the From Address, Subnet mask and Matchtype.</td>
</tr>
<tr>
<td></td>
<td>- Options: Accept, Restrict.</td>
</tr>
<tr>
<td></td>
<td>- Default: Accept.</td>
</tr>
<tr>
<td>Weight</td>
<td>BGP stores any routes that are rejected by not mentioning them in a route filter. BGP explicitly mentions these rejected routes in the routing table and assigns them a restrict keyword with a negative weight. A negative weight prevents a route from becoming active, which means that it is not installed in the forwarding table or exported to other protocols. This feature eliminates the need to break and re-establish a session upon reconfiguration if importation policy is changed.</td>
</tr>
<tr>
<td></td>
<td>- Range: 0-65535</td>
</tr>
<tr>
<td></td>
<td>- Default: No default</td>
</tr>
<tr>
<td>Local Pref</td>
<td>The BGP local preference to the imported route. Check Point recommends that you configure this value to bias the preference of routed for BGP routes.</td>
</tr>
<tr>
<td></td>
<td>- Note: Do not use the local preference parameter when importing BGP.</td>
</tr>
<tr>
<td></td>
<td>The local preference value is sent automatically when redistributing external BGP routes to an internal BGP route. The local preference parameter is ignored if used on internal BGP import statements.</td>
</tr>
<tr>
<td></td>
<td>- Range: 0-65535. Larger values are preferred</td>
</tr>
<tr>
<td></td>
<td>- Default: No default</td>
</tr>
</tbody>
</table>

Configuring Route Redistribution - WebUI

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, OSPF, or BGP need to be advertised into another protocol. Route redistribution is also useful for advertising static routes, such as the default route, or aggregates into a protocol.

You can define Route Redistribution only using the WebUI. Route Redistribution is not available in clish. To configure Route Redistribution using the CLI use routemaps.

To Configure Route Redistribution
1. Go to the Advanced Routing > Route Redistribution page of the WebUI.
2. In the relevant section:
   - To add a redistributed route, click Add.
   - To edit a redistributed route, select it and click Edit.
## Redistributed Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Protocol</strong></td>
<td>The destination protocol.</td>
</tr>
<tr>
<td><strong>From Interface</strong></td>
<td>The interface from which to distribute the routes</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>The cost of the created routes in the destination protocol.</td>
</tr>
</tbody>
</table>

## Redistributed Static Routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Protocol</strong></td>
<td>The destination protocol.</td>
</tr>
<tr>
<td><strong>From Static Route</strong></td>
<td>The static route to be distributed to the protocol</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>The cost of the created routes in the destination protocol.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This is mandatory when configuring redistributions to RIP.</td>
</tr>
</tbody>
</table>

## Redistributed Aggregate Routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Protocol</strong></td>
<td>Redistribute all active aggregate routes into the selected protocol.</td>
</tr>
<tr>
<td><strong>From Aggregate Route</strong></td>
<td>The aggregate route to be distributed to the protocol</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>The cost of the created routes in the destination protocol.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This is mandatory when configuring redistributions to RIP.</td>
</tr>
</tbody>
</table>

## Redistributed RIP Routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Protocol</strong></td>
<td>The destination protocol.</td>
</tr>
<tr>
<td><strong>All RIP Routes</strong></td>
<td>Choose which RIP routes to redistribute into the To Protocol.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>• Select - All active RIP routes.</td>
</tr>
<tr>
<td></td>
<td>• Clear - The RIP routes that match the From Address, Subnet Mask</td>
</tr>
<tr>
<td></td>
<td>and Matchtype filter.</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Cleared</td>
</tr>
<tr>
<td><strong>From Address</strong></td>
<td>The network for the destination to redistribute.</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>IP address format.</td>
</tr>
<tr>
<td><strong>Subnet mask</strong></td>
<td>The subnet mask for the destination to redistribute.</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>the mask of the specified route.</td>
</tr>
</tbody>
</table>
## Routing Policy Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Matchtype</strong></td>
<td>The routes that are filtered for the <em>From Address</em> and <em>Subnet mask</em>. These are the ways to compare other routes against it:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normal</strong> - matches any route that equals the specified route or is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Exact</strong> - matches a route only if it equals the <em>From Address</em> and <em>Subnet mask</em> of the specified route.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Refines</strong> - matches a route only if it is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong> - matches any route whose Ip prefix equals the specified route’s <em>From Address</em> and whose <em>Subnet Mask</em> falls within the specified Subnet Mask length range.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Options</strong>: Normal, Exact, Refines, Range.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: Normal.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>What to do with the routes that match the filter that is defined by the <em>From Address</em>, <em>Subnet mask</em> and <em>Matchtype</em>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Options</strong>: Accept, Restrict.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: Accept.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>The cost of the created routes in the destination protocol.</td>
</tr>
</tbody>
</table>

### Redistributed OSPF2 Routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Protocol</strong></td>
<td>The destination protocol.</td>
</tr>
<tr>
<td><strong>All OSPF2 Routes</strong></td>
<td>Choose which OSPFv2 routes to redistribute into the <em>To Protocol</em>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Options</strong>:</td>
</tr>
<tr>
<td></td>
<td>- Select - All active OSPFv2 routes.</td>
</tr>
<tr>
<td></td>
<td>- Clear - The OSPFv2 routes that match the From Address, Subnet Mask and Matchtype filter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: Cleared</td>
</tr>
<tr>
<td><strong>From Address</strong></td>
<td>The network for the destination to redistribute.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: IP address format.</td>
</tr>
<tr>
<td><strong>Subnet mask</strong></td>
<td>The subnet mask for the destination to redistribute.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: the mask of the specified route.</td>
</tr>
<tr>
<td><strong>Matchtype</strong></td>
<td>The routes that are filtered for the <em>From Address</em> and <em>Subnet mask</em>. These are the ways to compare other routes against it:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normal</strong> - matches any route that equals the specified route or is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Exact</strong> - matches a route only if it equals the <em>From Address</em> and <em>Subnet mask</em> of the specified route.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Refines</strong> - matches a route only if it is more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong> - matches any route whose Ip prefix equals the specified route’s <em>From Address</em> and whose <em>Subnet Mask</em> falls within the specified Subnet Mask length range.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Options</strong>: Normal, Exact, Refines, Range.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: Normal.</td>
</tr>
</tbody>
</table>
### Routing Policy Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>What to do with the routes that match the filter that is defined by the From Address, Subnet mask and Matchtype.</td>
</tr>
<tr>
<td></td>
<td>• Options: Accept, Restrict.</td>
</tr>
<tr>
<td></td>
<td>• Default: Accept.</td>
</tr>
<tr>
<td>Metric</td>
<td>The cost of the created routes in the destination protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This is mandatory when configuring redistributions to RIP.</td>
</tr>
</tbody>
</table>

#### Redistributed OSPF2 External Routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Protocol</td>
<td>The destination protocol.</td>
</tr>
<tr>
<td>All OSPF2 Ex Routes</td>
<td>Choose which OSPFv2 External routes to redistribute into the To Protocol.</td>
</tr>
<tr>
<td></td>
<td>• Options:</td>
</tr>
<tr>
<td></td>
<td>• Select - All active OSPFv2 External routes.</td>
</tr>
<tr>
<td></td>
<td>• Clear - The OSPFv2 External routes that match the From Address,</td>
</tr>
<tr>
<td></td>
<td>Subnet Mask and Matchtype filter.</td>
</tr>
<tr>
<td></td>
<td>• Default: Cleared</td>
</tr>
<tr>
<td>From Address</td>
<td>The network for the destination to redistribute.</td>
</tr>
<tr>
<td></td>
<td>• Range: IP address format.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>The subnet mask for the destination to redistribute.</td>
</tr>
<tr>
<td></td>
<td>• Default: the mask of the specified route.</td>
</tr>
<tr>
<td>Matchtype</td>
<td>The routes that are filtered for the From Address and Subnet mask.</td>
</tr>
<tr>
<td></td>
<td>These are the ways to compare other routes against it:</td>
</tr>
<tr>
<td></td>
<td>• Normal - matches any route that equals the specified route or is</td>
</tr>
<tr>
<td></td>
<td>more specific than the specified route.</td>
</tr>
<tr>
<td></td>
<td>• Exact - matches a route only if it equals the From Address and</td>
</tr>
<tr>
<td></td>
<td>Subnet mask of the specified route.</td>
</tr>
<tr>
<td></td>
<td>• Refines - matches a route only if it is more specific than the</td>
</tr>
<tr>
<td></td>
<td>specified route.</td>
</tr>
<tr>
<td></td>
<td>• Range - matches any route whose Ip prefix equals the specified</td>
</tr>
<tr>
<td></td>
<td>route's From Address and whose Subnet Mask falls within the</td>
</tr>
<tr>
<td></td>
<td>specified Subnet Mask length range.</td>
</tr>
<tr>
<td></td>
<td>• Options: Normal, Exact, Refines, Range.</td>
</tr>
<tr>
<td></td>
<td>• Default: Normal.</td>
</tr>
<tr>
<td>Action</td>
<td>What to do with the routes that match the filter that is defined by the From Address, Subnet mask and Matchtype.</td>
</tr>
<tr>
<td></td>
<td>• Options: Accept, Restrict.</td>
</tr>
<tr>
<td></td>
<td>• Default: Accept.</td>
</tr>
<tr>
<td>Metric</td>
<td>The cost of the created routes in the destination protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This is mandatory when configuring redistributions to RIP.</td>
</tr>
</tbody>
</table>

#### Redistributed BGP AS Path Routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Protocol</td>
<td>The destination protocol.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>AS Path RegEx</strong></td>
<td>The following definitions describe how to create regular expressions. AS-PATH operators are one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <code>aspath_term (m n)</code> A regular expression followed by <code>(m n)</code>, where <code>m</code> and <code>n</code> are both non-negative integers and <code>m</code> is less than or equal to <code>n</code>. This expression means that there are at least <code>m</code>, and at most, <code>n</code> repetitions.</td>
</tr>
<tr>
<td></td>
<td>- <code>aspath_term m</code> A regular expression followed by <code>m</code>, where <code>m</code> is a positive integer and means exactly <code>m</code> repetitions.</td>
</tr>
<tr>
<td></td>
<td>- <code>aspath_term (m)</code> A regular expression followed by <code>m</code>, where <code>m</code> is a positive integer. This expression means that there are exactly <code>m</code> repetitions.</td>
</tr>
<tr>
<td></td>
<td>- <code>aspath_term *</code> A regular expression followed by <code>*</code>, which means zero or more repetitions.</td>
</tr>
<tr>
<td></td>
<td>- <code>aspath_term +</code> A regular expression followed by <code>+</code>, which means one or more repetitions.</td>
</tr>
<tr>
<td></td>
<td>- <code>aspath_term ?</code> A regular expression followed by <code>?</code>, which means zero or one repetition.</td>
</tr>
<tr>
<td></td>
<td>- `aspath_term</td>
</tr>
<tr>
<td><strong>Origin</strong></td>
<td>The completeness of AS-PATH information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Any</strong> -</td>
</tr>
<tr>
<td></td>
<td>- <strong>IGP</strong> - A route was learned from an interior routing protocol and is probably complete.</td>
</tr>
<tr>
<td></td>
<td>- <strong>EGP</strong> - The route was learned from an exterior routing protocol that does not support AS-PATHs, and the path is probably incomplete.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Incomplete</strong> - The path information is incomplete.</td>
</tr>
<tr>
<td></td>
<td><strong>Options:</strong> Any / IGP / EGP / Incomplete</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> No default</td>
</tr>
<tr>
<td><strong>All Routes</strong></td>
<td>Choose which BGP AS Path routes to redistribute into the <strong>To Protocol</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Options:</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Select</strong> - All active BGP AS Path routes.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Clear</strong> - The BGP AS Path routes that match the From Address, Subnet Mask and Matchtype filter.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Cleared</td>
</tr>
<tr>
<td><strong>From Address</strong></td>
<td>The network for the destination to redistribute.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> IP address format.</td>
</tr>
<tr>
<td><strong>Subnet mask</strong></td>
<td>The subnet mask for the destination to redistribute.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> the mask of the specified route.</td>
</tr>
</tbody>
</table>
## Routing Policy Configuration

### Parameter | Description
--- | ---
**Matchtype** | The routes that are filtered for the From Address and Subnet mask. These are the ways to compare other routes against it:
- **Normal** - matches any route that equals the specified route or is more specific than the specified route.
- **Exact** - matches a route only if it equals the From Address and Subnet mask of the specified route.
- **Refines** - matches a route only if it is more specific than the specified route.
- **Range** - matches any route whose Ip prefix equals the specified route’s From Address and whose Subnet Mask falls within the specified Subnet Mask length range.
- **Options**: Normal, Exact, Refines, Range.
- **Default**: Normal.

**Action** | What to do with the routes that match the filter that is defined by the From Address, Subnet mask and Matchtype.
- **Options**: Accept, Restrict.
- **Default**: Accept.

**Metric** | The cost of the created routes in the destination protocol.

### Redistributed BGP AS Routes

| Parameter | Description |
--- | ---|
**To Protocol** | The destination protocol. |
**From BGP AS** | The BGP AS routes to be distributed to the protocol. |
**All Routes** | Choose which BGP AS routes to redistribute into the To Protocol. |
- **Options**:
  - **Select** - All active BGP AS routes.
  - **Clear** - The BGP AS routes that match the From Address, Subnet Mask and Matchtype filter.
- **Default**: Cleared |
**From Address** | The network for the destination to redistribute. |
- **Range**: IP address format. |
**Subnet mask** | The subnet mask for the destination to redistribute. |
- **Default**: the mask of the specified route. |
### Parameter | Description
---|---
**Matchtype** | The routes that are filtered for the *From Address* and *Subnet mask*. These are the ways to compare other routes against it:
  - **Normal** - matches any route that equals the specified route or is more specific than the specified route.
  - **Exact** - matches a route only if it equals the *From Address* and *Subnet mask* of the specified route.
  - **Refines** - matches a route only if it is more specific than the specified route.
  - **Range** - matches any route whose Ip prefix equals the specified route’s *From Address* and whose *Subnet Mask* falls within the specified Subnet Mask length range.
  - **Options**: Normal, Exact, Refines, Range.
  - **Default**: Normal.

**Action** | What to do with the routes that match the filter that is defined by the *From Address*, *Subnet mask* and *Matchtype*.
  - **Options**: Accept, Restrict.
  - **Default**: Accept.

**Metric** | The cost of the created routes in the destination protocol.

### Redistribute BGP Default Routes

**Parameter** | **Description**
---|---
**To Protocol** | The destination protocol.

**Redistribute All** | Choose which BGP default routes to redistribute into the *To Protocol*.
  - **Options**:
    - **Select** - All active BGP default routes.
    - **Clear** - The BGP Default routes that match the BGP Redistribution Settings
  - **Default**: Cleared

**Metric** | The cost of the created routes in the destination protocol.

### BGP Redistribution Settings

**Parameter** | **Description**
---|---
**To Protocol** | The destination protocol.

**MED** | BGP 4 metrics (Multi-Exit Discriminator or MED) are 32-bit unsigned quantities (that is they range from 0 to 4294967295 inclusive, with 0 being the most attractive). If the metric is specified as IGP, any existing metric on the route is sent as the MED. This setting can allow, for example, OSPF costs to be exported as BGP MEDs. Note: If this capability is used, any change in the metric causes a new BGP update.

The MED is a metric that defines the cost of using this route. The range of values is 1 to 16.
### Configuring Route Maps - CLI (routemap)

Each route map includes a list of match criteria and set statements. You can apply route maps to inbound, outbound, or redistribution routes. Routes are compared to the match criteria, and all the actions specified in the set criteria are applied to those routes which meet all the match conditions. You can specify the match conditions in any order. If you do not specify any match conditions in a route map, the route map matches all routes.

You define route maps, then assign them to protocols for export or import policy for that protocol. Route maps take precedence over WebUI based configuration.

To create a route map, use CLI commands to specify a set of criteria that must be matched for the command to take effect. If the criteria are matched, then the system executes the actions you specify. A route map is identified by name and an identifying number, an Allow or Restrict clause, and a collection of match and set statements.

There can be more than one instance of a route map (same name, different ID). The lowest numbered instance of a route map is checked first. Route map processing stops when either all the match criteria of some instance of the route map are satisfied, or all the instances of the particular route map are exhausted. If the match criteria are satisfied, the actions in the set section are performed.

Routing protocols can use more than one route map when you specify distinct preference values for each. The appropriate route map with lowest preference value is checked first.

### Set Routemap Commands

To set a route map:

```
set routemap rm_name id <1-65535>
   <off|on>
   allow
   inactive
   restrict
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routemap  rm_name</td>
<td>The name of the routemap.</td>
</tr>
<tr>
<td>id &lt;1-65535&gt;</td>
<td>The ID of the routemap. You can enter the keyword default or the default value 10.</td>
</tr>
<tr>
<td>&lt;off</td>
<td>on&gt;</td>
</tr>
<tr>
<td>allow</td>
<td>Allow routes that match the routemap.</td>
</tr>
<tr>
<td>inactive</td>
<td>Temporarily disable a routemap. To activate the routemap, use the allow or restrict arguments.</td>
</tr>
</tbody>
</table>
Routing Policy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restrict</td>
<td>Routes that match the routemap are not allowed.</td>
</tr>
</tbody>
</table>

To specify actions for a routemap:

- **Note** - Some statements affect only a particular protocol ("Supported Route Map Statements by Protocol" on page 93).
- The same parameter cannot appear both as a match and action statement in a routemap. These include Community, Metric, and Nexthop.

```plaintext
set routemap rm_name id id_number action
aspath-prepend-count <1-25>
community <append | replace | delete> [on|off]
community <1-65535> as <1-65535> [on|off]
community no-export [on|off]
community no-advertise [on|off]
community no-export-subconfed [on|off]
community none [on|off]
localpref <1-65535>
metric <add|subtract> <1-16>
metric igp [ <add | subtract> ] <1-4294967295>
metric value <1-4294967295>
nexthop <ip ipv4_address>
precedence <1-65535>
preference <1-65535>
route-type <type-1 | type-2>
remove action_name
ospfautomatictag tag
ospfmanualtag tag
riptag tag
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routemap rm_name</td>
<td>Specifies the name of the routemap.</td>
</tr>
<tr>
<td>id id_number</td>
<td>Specifies the ID of the routemap. You can enter the keyword default or the default value 10.</td>
</tr>
<tr>
<td>aspath-prepend-count</td>
<td>Specifies to affix AS numbers at the beginning of the AS path. It indicates the number of times the local AS number should be prepended to the ASPATH before sending out an update. BGP only.</td>
</tr>
<tr>
<td>community &lt;append</td>
<td>replace</td>
</tr>
<tr>
<td>community &lt;1-65535&gt; as &lt;1-65535&gt; [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-export [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-advertise [on</td>
<td>off]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>community no-export-subconfed [on</td>
<td>off]</td>
</tr>
<tr>
<td>community none [on</td>
<td>off]</td>
</tr>
<tr>
<td>localpref &lt;1-65535&gt;</td>
<td>Set the local preference for BGP route. BGP only.</td>
</tr>
<tr>
<td>metric [&lt;add</td>
<td>subtract&gt;] &lt;1-16&gt;</td>
</tr>
<tr>
<td>metric igp [&lt;add</td>
<td>subtract&gt;] &lt;1-4294967295&gt;]</td>
</tr>
<tr>
<td>metric value &lt;1-4294967295&gt;</td>
<td>Set the metric value. For RIP the metric is metric, for OSPF the metric is cost, and for BGP the metric is MED.</td>
</tr>
<tr>
<td>nexthop &lt;ip ipv4_address&gt;</td>
<td>Set IPv4 Nexthop Address. BGP only. <strong>Note:</strong> The ipv6 address should not be a link-local address.</td>
</tr>
<tr>
<td>precedence &lt;1-65535&gt;</td>
<td>Sets the rank of the route. Precedence works across protocols. Use this setting to bias routes of one protocol over the other. The lower value has priority.</td>
</tr>
<tr>
<td>preference &lt;1-65535&gt;</td>
<td>Applies only to BGP. This is equivalent to the bgp weight (in Cisco terms) of the route. However, unlike Cisco, the route with lower value will be preferred. This value is only relevant for the local router.</td>
</tr>
<tr>
<td>route-type &lt;type-1</td>
<td>type-2&gt;</td>
</tr>
<tr>
<td>remove action_name</td>
<td>Remove the specified action from the routemap. For community, it removes all community statements. Allowed values for action_name are: aspath-regexp community ifaddress interface metric neighbor network next-hop protocol route-type</td>
</tr>
<tr>
<td>ospfautomaticntag tag</td>
<td>Creates an automatic OSPF route tag.</td>
</tr>
<tr>
<td>ospfmanualtag tag</td>
<td>Creates a manual OSPF route tag.</td>
</tr>
<tr>
<td>riptag tag</td>
<td>Creates a RIP route tag.</td>
</tr>
</tbody>
</table>
To specify the criteria that must be matched for the routemap to take effect:

Note: Some statements affect only a particular protocol ("Supported Route Map Statements by Protocol" on page 93). The same parameter cannot appear both as a match and action statement in a routemap. These include Community, Metric, and Nexthop.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as 1-65535 [on</td>
<td>off]</td>
</tr>
<tr>
<td>aspath-regex [&quot;regular_expression&quot;</td>
<td>empty] origin &lt;any</td>
</tr>
<tr>
<td>community 1-65535 as 1-65535 [on</td>
<td>off]</td>
</tr>
<tr>
<td>community exact [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-export [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-advertise [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-export-subconfed [on</td>
<td>off]</td>
</tr>
</tbody>
</table>
## Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community none</td>
<td>Matches an empty community string, i.e. a route which does not have any communities associated with it.</td>
</tr>
<tr>
<td></td>
<td>The CLI returns an error if you turn &quot;none&quot; on and other community values already defined, or if &quot;none&quot; is defined and you add some other community value.</td>
</tr>
<tr>
<td>ifaddress IPv4_addr</td>
<td>Match the specified interface address. There can be multiple if address statements.</td>
</tr>
<tr>
<td>interface interface_name</td>
<td>Match the route if the nexthop lies on the specified interface name. There can be multiple interface statements.</td>
</tr>
<tr>
<td>metric value</td>
<td>Match the specified metric value.</td>
</tr>
<tr>
<td>neighbor IPv4_addr</td>
<td>Match the neighbors IP address. BGP or RIP. There can be multiple neighbor statements.</td>
</tr>
<tr>
<td>network IPv4_network / masklength</td>
<td>Use with the following keywords:</td>
</tr>
<tr>
<td></td>
<td>- all: Match all networks belonging to this prefix and masklength. This is a combination of exact and refines.</td>
</tr>
<tr>
<td></td>
<td>- between masklength and masklength: Specify a range of masklengths to be accepted for the specified prefix.</td>
</tr>
<tr>
<td></td>
<td>- exact: Match prefix exactly.</td>
</tr>
<tr>
<td></td>
<td>- off: Delete the network match statement.</td>
</tr>
<tr>
<td></td>
<td>- refines: Match networks with more specific mask lengths only. Matches only subnets.</td>
</tr>
<tr>
<td></td>
<td>There can be multiple network match statements in a route map.</td>
</tr>
<tr>
<td>nexthop IPv4_addr</td>
<td>Match the specified nexthop address.</td>
</tr>
<tr>
<td>protocol {ospf2</td>
<td>ospf2ase</td>
</tr>
<tr>
<td>route-type {type-1</td>
<td>type-2</td>
</tr>
<tr>
<td>remove match_condition_name</td>
<td>Remove the specified match condition from the routemap. For match conditions which can have multiple match statements (such as network, neighbor), this argument removes all of them.</td>
</tr>
</tbody>
</table>
Show Routemap Commands
show routemap rm_name <all | id VALUE>
show routemaps

Routemap Protocol Commands
To assign routemaps to protocols:
The preference value specifies which order the protocol will use each routemap.

set <ospf | rip>
    export-routemap rm_name preference VALUE on
    import-routemap rm_name preference VALUE on

To turn a routemap off:
set <ospf | rip>
    export-routemap rm_name off
    import-routemap rm_name off

To view routemaps assigned to protocols:
show <ospf | rip> routemap

To set BGP routemaps for export and import policies:
set bgp external remote-as <1-65535>
    export-routemap rm_name
    off
    preference <1-65535> [family inet] on

set bgp external remote-as <1-65535>
    import-routemap rm_name
    off
    preference <1-65535> [family inet] on

set bgp internal export-routemap rm_name
    off
    preference <1-65535> [family inet] on

set bgp internal import-routemap rm_name
    off
    preference <1-65535> [family inet] on

show bgp routemap

Note - You cannot use routemaps in BGP confederations. To configure route filters and redistribution for BGP confederations, use the Inbound Route Filters and Route Redistribution pages in the WebUI.

Supported Route Map Statements by Protocol
Some statements affect only a particular protocol, for example, matching the Autonomous System Number is applicable only to BGP. If such a condition is in a routemap used by OSPF, the match condition is ignored. Any non-applicable match conditions or actions are ignored and processing is done as if they do not exist. A log message is generated in /var/log/messages for any such statements.

Note - The same parameter cannot appear both as a match and action statement in a routemap. These include Community, Metric, and Nexthop.

RIP
- Import Match conditions: Neighbor, Network, Interface, Ifaddress, Metric, Neighbor, Nexthop.
- Import Actions: Precedence, Metric Add/Subtract
- Export Match conditions when exporting from RIP - Interface, Ifaddress, Metric, Network, Nexthop
- Export Match Conditions when redistributing using Protocol match: According to the protocol from which route is being redistributed.
- Export Actions when exporting from RIP - Metric Add/Subtract
- Export Actions when redistributing - Metric Set

**OSPFv2**

- Import Match conditions: Network (Route Prefix)
- Import Actions: Precedence
- Export Match conditions when other protocols redistribute OSPF routes: Network, Interface, Ifaddress, Metric, Route-type, Nexthop
- Export Match conditions when OSPF redistributes routes from other protocols: Conditions supported by that protocol
- Export Actions when redistributing to AS External: Metric, Route-type

**BGP**

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Selects the highest interface address when OSPF is enabled.</td>
</tr>
<tr>
<td>ip_address</td>
<td>The Router ID uniquely identifies the router in the autonomous system. The router ID is used by the BGP and OSPF protocols. We recommend setting the router ID rather than relying on the default setting. This prevents the router ID from changing if the interface used for the router ID goes down. Use an address on a loopback interface that is not the loopback address (127.0.0.1). In a cluster, you must select a router ID and make sure that it is the same on all cluster members.</td>
</tr>
</tbody>
</table>

- **Range:** Dotted-quad([0-255].[0-255].[0-255].[0-255]). Do not use 0.0.0.0
- **Default:** The interface address of one of the local interfaces.

Use the following group of commands to set and view parameters for BGP.

```
set as as_number
set as off
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as as_number</td>
<td>The local autonomous system number of the router. This number is mutually exclusive from the confederation and routing domain identifier. The router can be configured with either the autonomous system number or confederation number, not both. Caution: When you change the autonomous system number, all current peer sessions are reset and all BGP routes are deleted.</td>
</tr>
<tr>
<td>as off</td>
<td>Disables the configured local autonomous system number.</td>
</tr>
</tbody>
</table>
Routing Policy Configuration

Redistributing Static, Interface, or Aggregate Routes
When redistributing static routes into BGP, OSPFv2 or RIP the following match conditions are supported:

- Network Prefix,
- Nexthop
- Interface
- Ifaddress
- Protocol (proto = static)

When redistributing interface/direct routes into BGP, OSPFv2 or RIP the following match conditions are supported:

- Network Prefix
- Interface
- Ifaddress
- Protocol (proto = direct)

When redistributing aggregate routes into BGP, OSPFv2 or RIP the following match conditions are supported:

- Network Prefix
- Protocol (proto = aggregate)

Route Map Examples

Example 1
Redistribute interface route for eth3c0 into ospf, and set the ospf route-type to AS type-2 with cost 20.

```bash
set routemap direct-to-ospf id 10 on
set routemap direct-to-ospf id 10 match interface eth3c0
set routemap direct-to-ospf id 10 match protocol direct
set routemap direct-to-ospf id 10 action route-type type-2
set routemap direct-to-ospf id 10 action metric value 20

set ospf export-routemap direct-to-ospf preference 1 on
```

Example 2
Do not accept routes from RIP neighbor 192.0.2.3, accept routes from neighbor 192.0.2.4 as is, and for all other routes increment the metric by 2.

```bash
set routemap rip-in id 10 on
set routemap rip-in id 10 restrict
set routemap rip-in id 10 match neighbor 192.0.2.3

set routemap rip-in id 15 on
set routemap rip-in id 15 match neighbor 192.0.2.4

set routemap rip-in id 20 on
set routemap rip-in id 20 action metric add 2

set rip import-routemap rip-in preference 1 on
```

Example 3
Redistribute all static routes into BGP AS group 400. Set the MED value to 100, prepend our AS number to the aspath 4 times. If the route belongs to the prefix 192.0.2.0/8, do not redistribute. Send all BGP routes whose aspath matches the regular expression (100 200+) and set the MED value to 200.
set routemap static-to-bgp id 10 on
set routemap static-to-bgp id 10 restrict
set routemap static-to-bgp id 10 match protocol static
set routemap static-to-bgp id 10 match network 192.0.2.0/8 all

set routemap static-to-bgp id 15 on
set routemap static-to-bgp id 15 match protocol static
set routemap static-to-bgp id 15 action metric 100
set routemap static-to-bgp id 15 action aspath-prepend-count 4

set routemap bgp-out id 10 on
set routemap bgp-out id 10 match aspath-regex "(100 200+)" origin any
set routemap bgp-out id 10 action metric 200

set bgp external remote-as 400 export-routemap bgp-out preference 1 family inet on
set bgp external remote-as 400 export-routemap static-to-bgp preference 2 family inet on

*Note* - There is no need for a match protocol statement for routes belonging to the same protocol.
Chapter 10

Routing Options

In This Chapter
Routing Options (Apply, Reset and Reload) - WebUI 97
Equal Cost Path Splitting 97
Kernel Options- Kernel Routes 98
Protocol Rank 98
Router Options - Wait for Clustering 100
Trace Options 100

This chapter describes routing options that apply to all dynamic routing protocols.

Routing Options (Apply, Reset and Reload) - WebUI

In the Advanced Routing > Routing Options page of the WebUI, clicking these buttons has this effect:

- **Apply** - Save changes in this page.
- **Reload** - Discard unsaved changes. This is the same as navigating away from the page, discarding changes, and returning to the page.
- **Reset** - Restart the routed routing daemon on the Gaia appliance or computer.

Equal Cost Path Splitting

You can configure the maximum number of equal-cost paths that will be used when there is more than one equal-cost path to a destination. You can specify a value for the maximum number of equal-cost paths that will be used when there is more than one equal-cost path to a destination. Only OSPF routes and Static routes are able to use more than one "next hop"

- Range: 1 to 8
- Default: 8

The "next hop" algorithm that is used for forwarding when there is more than one "next hop" to a destination is Source/destination hash: A hash function is performed on the source and destination IP address of each packet that is forwarded to a multipath destination. This result is used to determine which next hop to use.

!! Important - Changing this option causes all routes to be reinstalled.

Configuring Equal Cost Path Splitting - WebUI

To configure equal cost path splitting using the WebUI:
1. In the tree view, click Advanced Routing > Routing Options.
2. In the Equal Cost Multipath section, select the Maximum Paths.
3. Click Apply.
Configuring Equal Cost Path Splitting - CLI (max-path-splits)

To configure equal cost path splitting using the CLI:
1. Run: `set max-path-splits <1-8>`
   - For example: `set max-path-splits 2`
2. Run: `save config`

Kernel Options - Kernel Routes

Route Injection Mechanism (RIM) enables a Security Gateway to use dynamic routing protocols to propagate the encryption domain of a VPN peer Security Gateway to the internal network and then initiate back connections. When a VPN tunnel is created, RIM updates the local routing table of the Security Gateway to include the encryption domain of the VPN peer.

In Gaia, the Route Injection Mechanism adds routes directly to the kernel. For the routes to remain in the Kernel, you must configure this option.

For more about configuring RIM, see the VPN Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Configuring Kernel Routes - WebUI

To set kernel routes using the WebUI:
1. In the tree view, click Advanced Routing > Routing Options.
2. In the Kernel Options area, select the Kernel Routes option.
3. Click Apply.

Configuring Kernel Routes - CLI (kernel-routes)

To set kernel routes using the CLI:
1. Run: `set kernel-routes on`
2. Run: `save config`

Protocol Rank

The protocol rank is the value that the routing daemon uses to order routes from different protocols to the same destination. It is an arbitrarily assigned value used to determine the order of routes to the same destination. 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 daemon. In the case where the same route is contributed by more than one protocol, the one with the lowest rank becomes the active route.

Rank cannot be used 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. Instead, rank is used to select routes from the same external gateway protocol (EGP) learned from different peers or autonomous systems.

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.

Default Ranks

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 default rank values are:

<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>RIP routes</td>
<td>100</td>
</tr>
<tr>
<td>Aggregate routes</td>
<td>130</td>
</tr>
<tr>
<td>OSPF AS external routes</td>
<td>150</td>
</tr>
<tr>
<td>BGP routes</td>
<td>170</td>
</tr>
</tbody>
</table>

These numbers do not generally need to be changed from their defaults. Use caution when modifying the default route ranks. Rank affects the route selection process, so unexpected consequences may occur throughout the network. Such a change should be planned carefully and take into account both the protocols being used and the location of the router in the network.

**Configuring Protocol Rank - WebUI**

**To set route rank:**

1. Open the Advanced Routing > Routing Options page of the WebUI.
2. In the Protocol Rank section, enter the route rank for each protocol.
3. Click Apply.

**Configuring Protocol Rank - CLI (protocol-rank)**

Rank is used by the routing system when there are routes from different protocols to the same destination. For each route, the route from the protocol with lowest rank number is used.

**Syntax**

```plaintext
set protocol-rank protocol
    bgp rank <0-255>
    bgp rank default
    rip rank <0-255>
    rip rank default
    ospf rank <0-255>
    ospf rank default
    ospfase rank <0-255>
    ospfase rank default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rank &lt;0-255&gt;</td>
<td>The protocol rank value.</td>
</tr>
<tr>
<td>ospf rank default</td>
<td>The default rank value for OSPF is 10.</td>
</tr>
<tr>
<td>rip rank default</td>
<td>The default rank value for RIP is 100.</td>
</tr>
<tr>
<td>bgp rank default</td>
<td>The default rank value for BGP is 170.</td>
</tr>
<tr>
<td>ospfase rank default</td>
<td>The default rank value for OSPF ASE routes is 150.</td>
</tr>
</tbody>
</table>
Router Options - Wait for Clustering

In a clustering environment, *Wait for Clustering* has this effect on RIP, PIM and OSPF routing:

<table>
<thead>
<tr>
<th>WebUI</th>
<th>CLI</th>
<th>The routed routing daemon</th>
</tr>
</thead>
</table>
| Selected | on | • Does not start the routing protocols if the cluster state is down.  
|         |     | • Turns on the routing protocols after the cluster goes up.         |
| Cleared | off | Ignores the state of the cluster. The state of the routing protocols does not depend on the state of the cluster.  
|         |     | This is the default. |

⚠️ *Important* - Changing the setting of this option restarts the *routed* routing daemon. Do not change it unless instructed by Support

Configuring Wait for Clustering - WebUI

To set the Wait for Clustering routing option:
1. In the tree view, click **Advanced Routing > Routing Options**.
2. In the **Router Options** area, select **Wait for Clustering**.
3. Click **Apply**.

Configuring Wait for clustering - CLI (router-options)

To turn on Wait for Clustering:
1. Run: `set router-options wait for clustering on`
2. Run: `save config`

To turn off Wait for Clustering:
1. Run: `set router-options wait for clustering off`
2. Run: `save config`

To show the state of the Wait for Clustering option:
`show router-options`

Trace Options

The routing system can optionally log information about errors and events. Logging is configured for each protocol or globally. Logging is not generally turned on during normal operations, as it can decrease performance. Log messages are saved in `/var/log/routed.log`

Trace Options - WebUI

To Enable Trace options:
1. In the tree view, click **Advanced Routing > Routing Options**.
2. In the **Configuration** tab, in the **Trace Options** area, configure:
   - Maximum Trace File Size
   - Number of Trace Files
   - Filter Visible Tables Below
3. In the option variables area, do one of:
   - Double-click an option.
   - Select an option (to select multiple options, use Shift-Click) and click **Activate**.
4. Click **Apply** at the top of the page
Trace Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Trace File Size</td>
<td>Limit the maximum size of the trace file to the specified size. When the trace file reaches the specified size, it is renamed to file.0, then file.1, file.2.</td>
</tr>
<tr>
<td></td>
<td>• Range: Integer 1-4095 (in megabytes).</td>
</tr>
<tr>
<td></td>
<td>• Default: 1</td>
</tr>
<tr>
<td>Maximum Number of Trace Files</td>
<td>• Limit the number of trace files.</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-4294967295.</td>
</tr>
<tr>
<td></td>
<td>• Default: 10</td>
</tr>
<tr>
<td>Filter Visible Tables Below</td>
<td>Select a table to show only that table.</td>
</tr>
</tbody>
</table>

Tips for Enabling Trace Options

You can enable

<table>
<thead>
<tr>
<th>For example, to enable the BGP Normal option, select</th>
</tr>
</thead>
<tbody>
<tr>
<td>An option.</td>
</tr>
<tr>
<td>All options for a protocol.</td>
</tr>
<tr>
<td>An option for all protocols.</td>
</tr>
<tr>
<td>All options for all protocols</td>
</tr>
</tbody>
</table>

For an explanation of each trace option, see the Trace Options - CLI (on page 101).

To monitor an Option:

You can see the most recent trace log messages in the /var/log/routed.log log file.

1. In the tree view, click Advanced Routing > Routing Options.
2. In the Configuration tab, enable the trace options you need.
3. Click the Monitoring tab.
4. Configure the Number of lines that you want to show at the end (the "tail") of the log file.
   The minimum number of lines is 5. The maximum is 100, regardless of value entered.
5. Click Get Tail.
   The log messages show.

Trace Options - CLI

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

```
set tracefile
  size <1-4095>
  size default
maxnum <1-4294967295>
maxnum default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>size &lt;1-4095&gt;</td>
<td>Limits the maximum size of the trace file to the specified size, in megabytes.</td>
</tr>
<tr>
<td>size default</td>
<td>The default maximum trace file size is 1 MB.</td>
</tr>
</tbody>
</table>
Parameter | Description
---|---
maxnum \(<1-4294967295>\) | When the trace file reaches the specified size, it is renamed to file.0, then file.1, file.2, up to the maximum number of files.
maxnum default | The default maximum number of trace files is 10.

Global Trace options

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

```bash
set trace global
    adv <on | off>
    parse <on | off>
    traceoptions <on | off>
```

While there are trace options specific to each protocol, many protocols share a set of options. These common trace options are specified in the `traceoptions` variable. The following table lists the `traceoption` parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceoptions</td>
<td>One or more of these values: `&lt;all</td>
</tr>
<tr>
<td>all</td>
<td>Trace all of the options in <code>traceoptions</code>.</td>
</tr>
<tr>
<td>adv</td>
<td>Trace the allocation of and freeing of policy blocks.</td>
</tr>
<tr>
<td>general</td>
<td>Trace both <code>normal</code> and <code>route</code>.</td>
</tr>
<tr>
<td>normal</td>
<td>Trace normal protocol occurrences. Abnormal protocol occurrences are always traced.</td>
</tr>
<tr>
<td>parse</td>
<td>Trace the lexical analyzer and parser.</td>
</tr>
<tr>
<td>policy</td>
<td>Trace the application of protocol- and user-specified policy to routes being imported and exported.</td>
</tr>
<tr>
<td>route</td>
<td>Trace routing table changes for routes installed by this protocol or peer.</td>
</tr>
<tr>
<td>state</td>
<td>Trace state machine transitions in the protocols.</td>
</tr>
<tr>
<td>task</td>
<td>Trace system interface and processing associated with this protocol or peer.</td>
</tr>
<tr>
<td>timer</td>
<td>Trace timer usage by this protocol or peer.</td>
</tr>
</tbody>
</table>

BGP Trace Options

Use the following command to turn BGP trace options on or off.
**Routing Options**

```
set trace bgp
    keepalive <on | off>
    open <on | off>
    update <on | off>
    packets <on | off>
    traceoptions <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive</td>
<td>Trace BGP keepalive messages</td>
</tr>
<tr>
<td>open</td>
<td>Trace BGP open packets. These packets are sent between peers when they are establishing a connection.</td>
</tr>
<tr>
<td>update</td>
<td>Trace update packets. These packets provide routing updates to BGP systems.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace all BGP protocol packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

**ICMP Trace Options**

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

```
set trace icmp
    error <on | off>
    info <on | off>
    routerdiscovery <on | off>
    packets <on | off>
    traceoptions <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Trace only ICMP error packets, which include:</td>
</tr>
<tr>
<td></td>
<td>- time exceeded</td>
</tr>
<tr>
<td></td>
<td>- parameter problem</td>
</tr>
<tr>
<td></td>
<td>- unreachable</td>
</tr>
<tr>
<td></td>
<td>- source quench</td>
</tr>
<tr>
<td>info</td>
<td>Trace only ICMP informational packets, which include:</td>
</tr>
<tr>
<td></td>
<td>- mask request/response</td>
</tr>
<tr>
<td></td>
<td>- info request/response</td>
</tr>
<tr>
<td></td>
<td>- echo request/response</td>
</tr>
<tr>
<td></td>
<td>- time stamp request/response</td>
</tr>
<tr>
<td>routerdiscovery</td>
<td>Trace only ICMP router discovery packets.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace all ICMP packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

**IGMP Trace Options**

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

```
set trace igmp
    error <on | off>
    info <on | off>
    packets <on | off>
    traceoptions <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Trace only IGMP error packets, which include:</td>
</tr>
<tr>
<td></td>
<td>- time exceeded</td>
</tr>
<tr>
<td></td>
<td>- parameter problem</td>
</tr>
<tr>
<td></td>
<td>- unreachable</td>
</tr>
<tr>
<td></td>
<td>- source quench</td>
</tr>
<tr>
<td>info</td>
<td>Trace only IGMP informational packets, which include:</td>
</tr>
<tr>
<td></td>
<td>- mask request/response</td>
</tr>
<tr>
<td></td>
<td>- info request/response</td>
</tr>
<tr>
<td></td>
<td>- echo request/response</td>
</tr>
<tr>
<td></td>
<td>- time stamp request/response</td>
</tr>
</tbody>
</table>
set trace igmp
    group <on | off>
    leave <on | off>
    mtrace <on | off>
    query <on | off>
    report <on | off>
    request <on | off>
    packets <on | off>
    traceoptions <on | off>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Trace multicast group add, delete, refresh and accelerated leave.</td>
</tr>
<tr>
<td>leave</td>
<td>Trace IGMP “leave group” messages.</td>
</tr>
<tr>
<td>mtrace</td>
<td>Trace details of IGMP multicast traceroute request processing.</td>
</tr>
<tr>
<td>query</td>
<td>Trace IGMP membership query packets (both general and group-specific).</td>
</tr>
<tr>
<td>report</td>
<td>Trace IGMP membership report packets (both IGMPv1 and IGMPv2).</td>
</tr>
<tr>
<td>request</td>
<td>Trace IGMP multicast traceroute request packets.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace all IGMP packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

IP Broadcast Helper Trace Options

Use the following command to turn IP broadcast helper trace options on or off.

set trace iphelper
    packets <on | off>
    traceoptions <on | off>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>Trace all IP broadcast helper packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

Kernel Trace Options

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

set trace kernel
    iflist <on | off>
    interface <on | off>
    packets <on | off>
    remnants <on | off>
    request <on | off>
    routes <on | off>
    traceoptions <on | off>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iflist</td>
<td>Trace iflist, the interface list scan.</td>
</tr>
<tr>
<td>interface</td>
<td>Trace interface status messages that are received from the kernel.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace packets that are read from the kernel.</td>
</tr>
</tbody>
</table>
## Routing Options

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

### MFC Trace Options

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

```
set trace mfc
  alerts <on | off>
  cache <on | off>
  interface <on | off>
  mcastdist <on | off>
  packets <on | off>
  resolve <on | off>
  wrongif <on | off>
  traceoptions <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alerts</td>
<td>Trace multicast protocol alert callback functions.</td>
</tr>
</tbody>
</table>
| cache | Trace log details of cache maintenance. These include:  
  - addition or deletion of orphan entries (in other words, entries with no route to source).  
  - addition or deletion of normal entries.  
  - cache state aging and refresh. |
| interface | Trace log changes requested by external routed modules (IGMP and multicast routing protocols) affecting the forwarding dependencies on an interface. These include:  
  - addition or deletion of a forwarding interface due to routing changes.  
  - changing of the parent (reverse path forwarding) interface due to routing changes. |
| mcastdist | Trace kernel multicast distribution entries. Both generic and PIM register encapsulation and decapsulation types. |
| packets | Trace all MFC related packets. |
| resolve | Trace kernel external resolve requests (both normal and PIM register types). |
| wrongif | Trace kernel multicast incoming interface violation notifications (both physical interface and PIM register types). |
| traceoptions | <all | general | normal | policy | route | state | task | timer> |
**OSPF Trace Options**

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ack</td>
<td>Trace link-state acknowledgment packets.</td>
</tr>
<tr>
<td>dd</td>
<td>Trace all database description packets.</td>
</tr>
<tr>
<td>dr</td>
<td>Trace designated router packets.</td>
</tr>
<tr>
<td>hello</td>
<td>Trace hello packets.</td>
</tr>
<tr>
<td>lsa</td>
<td>Trace link-state announcement packets.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace OSPF packets.</td>
</tr>
<tr>
<td>request</td>
<td>Trace link-state request packets.</td>
</tr>
<tr>
<td>spf</td>
<td>Trace shortest-path-first (SPF) calculations.</td>
</tr>
<tr>
<td>trap</td>
<td>Traces OSPF trap packets.</td>
</tr>
<tr>
<td>update</td>
<td>Trace link-state updates packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

**PIM Trace Options**

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

```
set trace pim
  assert <on | off>
  bootstrap <on | off>
  crp <on | off>
  graft <on | off>
  hello <on | off>
  join <on | off>
  mfc <on | off>
  mrt <on | off>
  packets <on | off>
  rp <on | off>
  register <on | off>
  trap <on | off>
  traceoptions <on | off>
```

The following trace options apply both to dense-mode and sparse-mode implementations:

```plaintext
The following trace options apply both to dense-mode and sparse-mode implementations:
```
## Routing Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assert</td>
<td>Trace PIM assert messages.</td>
</tr>
<tr>
<td>hello</td>
<td>Trace PIM router hello messages.</td>
</tr>
<tr>
<td>join</td>
<td>Trace PIM join/prune messages.</td>
</tr>
<tr>
<td>mfc</td>
<td>Trace calls to or from the multicast forwarding cache</td>
</tr>
<tr>
<td>mrt</td>
<td>Trace PIM multicast routing table events.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace all PIM packets.</td>
</tr>
<tr>
<td>trap</td>
<td>Trace PIM trap messages.</td>
</tr>
<tr>
<td>all</td>
<td>Trace all PIM events and packets.</td>
</tr>
</tbody>
</table>

The following trace options apply to sparse-mode implementations only:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootstrap</td>
<td>Trace bootstrap messages.</td>
</tr>
<tr>
<td>crp</td>
<td>Trace candidate-RP-advertisements.</td>
</tr>
<tr>
<td>rp</td>
<td>Trace RP-specific events, including RP set-specific and bootstrap-specific events.</td>
</tr>
<tr>
<td>register</td>
<td>Trace register and register-stop packets.</td>
</tr>
</tbody>
</table>

The following trace option applies to dense-mode implementations only:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graft</td>
<td>Trace graft and graft acknowledgment packets.</td>
</tr>
</tbody>
</table>

### Other Trace Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

## RIP Trace Options

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

```
set trace rip
    packets <on | off>
    traceoptions <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>Trace all RIP packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>
### Router Discovery Trace Options

Use the following command to turn ICMP router discovery trace options on or off.

```
set trace router-discovery option <on | off>
 traceoptions
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

### VRRP Trace Options

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

```
set trace vrrp
   advertise <on | off>
   traceoptions <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertise</td>
<td>Trace all VRRP packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>
Chapter 11

Router Discovery

In This Chapter

How Router Discovery Works 109
Configuring Router Discovery - WebUI 109
Configuring Router Discovery - CLI (rdisc) 111

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.

Gaia 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.

How Router Discovery Works

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. They 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. However, if a multicast or broadcast advertisement is due in a moment, the router does not respond with a unicast advertisement.

Each router advertisement contains an advertisement lifetime field indicating the length of time that 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. All IP addresses configured on the physical interface are included in the router advertisement when:

- Router advertisements are sent to the all-hosts multicast address, or
- An interface is configured for the limited-broadcast address 255.255.255.255.

When the router advertisements are sent to a net or subnet broadcast, only the address associated with that net or subnet is included.

Configuring Router Discovery - WebUI

To enable router discovery services:
1. Open the Advanced Routing > Router Discovery page of the WebUI.
2. Click Add.
The Add Interface window opens.

3. Select the Interface on which to enable Router Discovery.

4. Optional: Enter values for the Router Discover Configuration parameters.
   - Enable Router Discovery
   - Min. Advertise Interval
   - Max. Advertise Interval
   - Advertisement Lifetime

5. Optional: For each IP address on the interface, define the Router Discover Configuration parameters:
   - Advertise
   - Eligibility
   - Preference

6. Click OK.

7. Click Save.

To disable router discovery service on an interface:
1. Open the Advanced Routing > Router Discovery page of the WebUI.
2. Select an Interface and click Edit.
3. Clear Enable Router Discovery.
4. Click Save.

Router Discover Configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface on which Router Discovery occurs.</td>
</tr>
<tr>
<td>Enable Router Discovery</td>
<td>Whether ICMP router discovery is running on the interface. After you enable ICMP router discovery, configuration options for the interface appear.</td>
</tr>
<tr>
<td></td>
<td>- Default: Unselected</td>
</tr>
<tr>
<td>Min. Advertise Interval</td>
<td>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 in the Max advertise interval.</td>
</tr>
<tr>
<td></td>
<td>- Default: 0.75 times the value in the Max advertise interval.</td>
</tr>
<tr>
<td>Max. Advertise Interval</td>
<td>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>The lifetime (in seconds) of the advertisements sent from the interface.</td>
</tr>
<tr>
<td></td>
<td>- Range: Max. Advertise Interval-9000</td>
</tr>
<tr>
<td></td>
<td>- Default: 3 x Max. Advertise Interval</td>
</tr>
<tr>
<td>Advertise</td>
<td>Whether the address should be advertised in the Router Advertisement packets. This applies to each address on the interface and not to the interface itself.</td>
</tr>
<tr>
<td></td>
<td>- Default: Selected</td>
</tr>
<tr>
<td>Eligibility</td>
<td>You can make an IP address ineligible as a default router address. A router address that is not to be used as a default router has a Preference of 0.</td>
</tr>
<tr>
<td></td>
<td>- Options: Eligible/ineligible</td>
</tr>
<tr>
<td></td>
<td>- Default: Eligible.</td>
</tr>
</tbody>
</table>
### Parameter Description

**Preference**

The level of preference of the IP address as a default router address, relative to other router addresses on the same subnet. The minimum value corresponds to `ineligible` and indicates that the address is not to be used as a default router.

- **Range:** 0 (`ineligible`) - 2147483648 ($2^{31}$)
- **Default is 0**

---

### ICMP Router Discovery Interfaces

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

```plaintext
set rdisc interface if_name
   <on | off>
   min-adv-interval <3-1800>
   min-adv-interval default
   max-adv-interval <4-1800>
   max-adv-interval default
   adv-lifetime integer
   adv-lifetime default
   advertise ip_address <on | off>
   advertise ip_address preference ineligible
   advertise ip_address preference integer
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`&lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><code>min-adv-interval &lt;3-1800&gt;</code></td>
<td>The minimum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMP router advertisements on the interface.</td>
</tr>
<tr>
<td><code>min-adv-interval default</code></td>
<td>A value of 450 seconds.</td>
</tr>
<tr>
<td><code>max-adv-interval &lt;4-1800&gt;</code></td>
<td>The maximum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMP router advertisements on the interface.</td>
</tr>
<tr>
<td><code>max-adv-interval default</code></td>
<td>A value of 600 seconds.</td>
</tr>
<tr>
<td><code>adv-lifetime integer</code></td>
<td>The lifetime (in seconds) of the advertisements sent from the interface. An integer value between the configured value for the maximum advertisement interval and 9000.</td>
</tr>
<tr>
<td><code>adv-lifetime default</code></td>
<td>A value of 1800 or 3 times the maximum advertisement interval.</td>
</tr>
<tr>
<td>`advertise ip_address &lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><code>advertise ip_address preference ineligible</code></td>
<td>Do not use the specified IP address as a default router.</td>
</tr>
<tr>
<td><code>advertise ip_address preference integer</code></td>
<td>The preferability of the specified IP address as a default router address relative to other router addresses on the same subnet.</td>
</tr>
</tbody>
</table>
**ICMP Router Discovery Show Commands**

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

```
show rdisc
    interfaces
    interface if_name
    stats
    summary
```
Chapter 12

Policy Based Routing

In This Chapter

- Configuring Policy Based Routing - WebUI
- Configuring Policy Based Routing - CLI
- Monitoring Policy Based Routing

You can control traffic forwarding in great detail using policy based routing (PBR). When you use PBR, you create routing tables of static routes (Action Tables), and direct traffic to the appropriate tables using Policy Rules.

Policy Rules

The Policy Rules specify what traffic is matched. You can route traffic by matching on one or more of the following:

- Security Gateway interface.
- Source IPv4 address and subnet mask.
- Destination IPv4 address and subnet mask.

The Policy Rules also specify the action to take if the traffic is matched:

- Prohibit: Send a Prohibit message to the sending host.
- Unreachable: Send an Unreachable message to the sending host.
- Table: Do the actions defined in an Action Table

You can define many Policy Rules. Traffic is matched to all the rules, one rule at a time, according to the priority that is configured for the rule.

Action Tables

The Action Tables define the static routes, that is, where the traffic is sent. You define the destination of the route and the next hop gateway to that destination.

Static Route Priorities

PBR static routes have priority over static routes in the routing table. When a packet arrives at the Gaia Security Gateway, the packet is checked for a match to a PBR static route. If it matches, the packet is forwarded according to the priority of the PBR static route. If the packet does not match a PBR static route, the packet is forwarded according to the priority of the static routes in the routing table.

Configuring Policy Based Routing - WebUI

The workflow for configuring Policy Based Routing (PBR) is

1. In the Gaia WebUI, go to the Advanced Routing > Policy Based Routing page.
2. Configure one or more Action Tables. The Action Tables define the static routes, that is, where the traffic is sent. You define the destination of the route and the next hop gateway to that destination.
3. Configure Policy Rules. Define the traffic to match and the action to take if the traffic is matched. One of the possible Actions is to forward traffic to the static routes defined in an Action Table.
To Add an Action Table:

Note - For the meaning of the parameters, see Action Table Parameters (on page 114).

1. In the Action Tables section of the Policy Based Routing page, click Add.
2. In the Add Policy Table with Static Route window, define the Table Name.
3. Define the route to the destination. Choose one of:
   - Default Route.
   - Destination IPv4 address and Subnet mask.
4. Select the Next Hop Type. One of:
   - Normal
   - Blackhole
   - Reject
5. Add one or more Gateways to a normal destination. Click Add Gateway. You can select:
   - IP Address. Define the Gateway Priority.
   - Network interfaces. Define the Gateway Priority.
6. Click Save.

To Add a Policy Rule:

Note - For the meaning of the parameters, see Policy Rule Parameters (on page 115).

1. In the Policy Rules section of the Policy Based Routing page, click Add.
2. In the Add Policy Rule window, configure the Priority of the rule.
3. Configure the Action to take on the traffic that is matched. Choose one of:
   - Prohibit
   - Unreachable
   - Table. Select the Action Table.
4. Configure the traffic to match. Choose one or more of the following:
   - Interface
   - Source IPv4 address and subnet mask.
   - Destination IPv4 address and subnet mask.
5. Click Save.

To Delete a Policy Rule:

1. In the Policy Rules section of the Policy Based Routing page, select a rule.
2. Click Delete.

To Delete an Action Table:

1. In the Action Tables section of the Policy Based Routing page, select a static route table.
2. Click Delete.

### Action Table Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Name</td>
<td>The name of the table.</td>
</tr>
<tr>
<td>Table ID</td>
<td>A numerical ID for the table. Assigned by the system.</td>
</tr>
<tr>
<td>Default route</td>
<td>The default static route in the system routing table.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination of the route.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask for the destination of the route.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Table Name</td>
<td>The name of the table.</td>
</tr>
<tr>
<td>Next Hop Type</td>
<td>Choose one of:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normal</strong>: Accept and forward packets.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reject</strong>: Drop packets and send <em>unreachable</em> messages.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Black Hole</strong>: Drop packets but don’t send <em>unreachable</em> messages.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Next hop gateway IPv4 address.</td>
</tr>
<tr>
<td>Gateway Interface</td>
<td>Security Gateway interface that leads to the next hop gateway.</td>
</tr>
<tr>
<td>Gateway Priority</td>
<td>The preference of the particular route.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 1-8</td>
</tr>
</tbody>
</table>

### Policy Rule Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>You can define many Policy Rules. Traffic is matched to all the rules, one</td>
</tr>
<tr>
<td></td>
<td>rule at a time, according to the priority that is configured for the rule.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to take if the traffic is matched</td>
</tr>
<tr>
<td>Prohibit</td>
<td>Send a Prohibit message to the sending host.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Send an Unreachable message to the sending host.</td>
</tr>
<tr>
<td>Table</td>
<td>Do the actions defined in an Action Table.</td>
</tr>
<tr>
<td>Match</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Match by: Interface through which the packets enter the Security Gateway</td>
</tr>
<tr>
<td></td>
<td>from the source host.</td>
</tr>
<tr>
<td>Source, subnet mask</td>
<td>Match by: Source IPv4 address and subnet mask.</td>
</tr>
<tr>
<td>Destination, Subnet mask</td>
<td>Match by: Destination IPv4 address and subnet mask.</td>
</tr>
</tbody>
</table>

### Configuring Policy Based Routing - CLI

Create routing tables of static routes (Action Tables) and direct traffic to the appropriate tables by using Policy Rules.

#### To configure Action Tables:

<table>
<thead>
<tr>
<th>Description</th>
<th>The Action Tables define the static routes, that is, where the traffic is sent. You define the destination of the route and the next hop gateway to that destination.</th>
</tr>
</thead>
</table>
| Syntax        | set pbr table VALUE static-route VALUE  
nexthop blackhole  
nexthop reject  
nexthop gateway address VALUE <on | off>  
nexthop gateway logical VALUE <on | off>  
<on | off> |
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>table VALUE</td>
<td>The name of the table.</td>
</tr>
<tr>
<td>static-route VALUE</td>
<td>Choose one of:</td>
</tr>
<tr>
<td></td>
<td>• The default static route in the system routing table. VALUE is default.</td>
</tr>
<tr>
<td></td>
<td>• The destination of the route. VALUE is IPv4 address /mask length. For example 192.0.2.0/24</td>
</tr>
<tr>
<td>nexthop blackhole</td>
<td>Drop packets but don't send <em>unreachable</em> messages.</td>
</tr>
<tr>
<td>nexthop reject</td>
<td>Drop packets and send <em>unreachable</em> messages.</td>
</tr>
<tr>
<td>gateway address VALUE</td>
<td>Accept and forward packets to the Next hop gateway IPv4 address.</td>
</tr>
<tr>
<td>gateway logical VALUE</td>
<td>Accept and forward packets to the Security Gateway interface that leads to the next hop gateway.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

### Example

```
set pbr table PBRtable2 static-route 192.0.2.0/24
nexthop gateway logical eth0 on
```

### To configure Policy Rules

**Description**

Define the traffic to match and the action to take if the traffic is matched. One of the possible Actions is to forward traffic to the static routes defined in an Action Table.

**Syntax**

```
set pbr rule priority VALUE
    action prohibit
    action unreachable
    action table VALUE
    match from VALUE to VALUE interface VALUE <on | off>
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority VALUE</td>
<td>You can define many Policy Rules. Traffic is matched to all the rules, one rule at a time, according to the priority that is configured for the rule. VALUE is a number. The highest priority is 1.</td>
</tr>
<tr>
<td>action prohibit</td>
<td>Send a Prohibit message to the sending host.</td>
</tr>
<tr>
<td>action unreachable</td>
<td>Send an Unreachable message to the sending host.</td>
</tr>
<tr>
<td>action table VALUE</td>
<td>Do the actions defined in an Action Table. You must specify one or more match parameters.</td>
</tr>
<tr>
<td>from VALUE</td>
<td>Match by: Source IPv4 address and subnet mask.</td>
</tr>
<tr>
<td>to VALUE</td>
<td>Match by: Destination IPv4 address and subnet mask.</td>
</tr>
<tr>
<td>interface VALUE</td>
<td>Match by: Interface through which the packets enter the Security Gateway from the source host.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

### Example

```plaintext
corp_fw> set pbr rule priority 3 match interface eth2
corp_fw> set pbr rule priority 3 action table PBRtable2
```

---

**Monitoring Policy Based Routing**

To monitor Policy Based Routing - WebUI

1. In the Gaia WebUI, go to the Advanced Routing > Policy Based Routing page.
2. Click the Monitoring tab.

To monitor Policy Based Routing - CLI

Run these commands:

```plaintext
show pbr tables
show pbr rules
show pbr summary
```
Protocol-Independent Multicast (PIM) gets its name from the fact that it can work with any existing unicast protocol to perform multicast forwarding. PIM efficiently routes multicast traffic for groups that may span wide area (and inter-domain) networks. It works with all existing unicast routing protocols. PIM supports three modes: dense, sparse and Source-Specific Multicast (SSM). Only one mode of PIM can be enabled at a time.

**Dense Mode**

Dense mode is most useful when:
- Senders and receivers are in close proximity to one another.
- There are few senders and many receivers.
- The volume of multicast traffic is high.
- The stream of multicast traffic is constant.

**Sparse Mode**

Sparse mode is most useful when:
- There are few receivers in a group.
- Senders and receivers are separated by WAN links.
- The type of traffic is intermittent.

**Source-Specific multicast (SSM) Mode**

Source-specific multicast (SSM) is most useful when:
- Most multicast traffic is from well-known sources.
- It is desirable to avoid the overhead of shared tree and rendezvous point processing associated with sparse mode.

SSM is a version of PIM sparse-mode. It is used in conjunction with IGMP version 3 to request or block multicast traffic from specific sources. For example, when a host requests traffic for a multicast group from a specific source, SSM sends PIM join/prune messages towards the source.

The multicast group range 232/8 is reserved for SSM. When SSM is enabled, sparse-mode accepts only IGMPv3 reports for groups that fall within this range. Sparse-mode ignores IGMP v1 and v2 reports in this range.
range. In addition, only shortest-path-tree (SPT) join/prune messages for these groups are accepted from neighboring routers. All other multicast groups are processed as in native sparse mode.

SSM does not need a rendezvous-point (RP). The presence of an RP for any of the SSM groups does not have any influence on the processing of join/prune messages.

**PIM Dense Mode State Refresh**

The State Refresh option can be used in conjunction with dense mode to eliminate the periodic flood-and-prune of multicast data with no active receivers. All PIM routers must have State Refresh enabled to take advantage of this feature.

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.

**Configuring PIM - WebUI**

To configure PIM using the WebUI:
1. Open the Advanced Routing > PIM page of the WebUI.
2. Configure the PIM Global Settings ("PIM Global Settings" on page 120). In the PIM Global Settings section, select the PIM Protocol. One of:
   - Sparse Mode (SM)
   - Dense Mode (DM). Enable State Refresh, if appropriate.
   - Source Specific Multicast (SSM)
3. In the PIM Interfaces section, click Add.
   The Add Interface window opens.
4. In the Add Interface ("PIM Interfaces" on page 120) window
   a) Select the Interface on which you want to run PIM.
   b) Optional: For each interface that is running PIM, enter the Local Address.
   c) Optional: To configure this interface to use the VRRP virtual IP address, click Use Virtual address.
   d) Optional: Enter a new DR Priority (Designated Router priority).
5. Click Save.
### PIM Global Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Protocol</td>
<td>The PIM mode to use. One of:</td>
</tr>
<tr>
<td></td>
<td>• Sparse Mode (SM)</td>
</tr>
<tr>
<td></td>
<td>• Dense Mode (DM)</td>
</tr>
<tr>
<td></td>
<td>• Source-Specific Multicast (SSM)</td>
</tr>
<tr>
<td>State Refresh</td>
<td>In Dense Mode, use state refresh messages to delay timing out prune state of multicast traffic that has no active receivers. This helps suppress the flood-and-prune cycle inherent to dense mode.</td>
</tr>
</tbody>
</table>

### PIM Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select the interface on which to enable PIM</td>
</tr>
<tr>
<td>Local Address</td>
<td>Use the specified local address for all advertisements sent on the interface. This is useful on interfaces with multiple IP addresses (aliases). The local address must match one of the addresses configured on the interface. If a local address is specified while the virtual address option enabled, the local address must match a virtual address on the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - Each router must have at least one interface address with a subnet prefix shared by all neighboring PIM routers. If any neighboring routers choose advertisement addresses that do not appear to be on a shared subnet all messages from those neighbors will be rejected. This holds true even when the virtual address option is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Range: Dotted-quad ([0-255].[0-255].[0-255].[0-255]).</td>
</tr>
<tr>
<td></td>
<td>• Default: Selects one of the IP addresses configured on the interface. If the virtual address option is enabled, PIM will use the virtual address configured on the interface after the router transitions to master state with respect to VRRP.</td>
</tr>
<tr>
<td>Use Virtual Address</td>
<td>Use the VRRP virtual IP address on this interface. If enabled, PIM runs on this interface only after the router transitions to become a VRRP master after a failover.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - You cannot configure a local address or a virtual address when ClusterXL is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Range: Enabled, cleared</td>
</tr>
<tr>
<td></td>
<td>• Default: Cleared</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DR Priority</td>
<td>The dr-priority advertised in the PIM hello messages sent on the interface. This is used for DR election on a LAN. The router with the highest priority is elected the designated router. To break a tie, the DR is selected on the basis of the highest IP address. If even one router does not advertise a dr-priority, the DR election is based on the IP address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range:</strong> 0-4294967295 (2^32 - 1).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default:</strong> 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - To verify whether a PIM neighbor supports DR Priority, use the following command:</td>
</tr>
<tr>
<td></td>
<td>show pim neighbor &lt;ip_address&gt;</td>
</tr>
<tr>
<td></td>
<td>For neighbors that advertise a DR election priority value, the following message appears in the summary:</td>
</tr>
<tr>
<td></td>
<td>DRPriorityCapable Yes.</td>
</tr>
</tbody>
</table>

**Disabling PIM**

You can disable PIM on one or more interfaces configured on the WebUI platform.

1. Open the Advanced Routing > PIM page of the WebUI.
2. In the PIM Interfaces section, select the interface on which to disable PIM and click Delete.
   To disable PIM entirely, delete all PIM interfaces.

**Configuring PIM-DM Advanced Options (Optional)**

To configure PIM Dense Mode Advanced Options:

1. Open the Advanced Routing > PIM page of the WebUI.
2. Select the PIM Protocol: Dense Mode (DM).
3. Click Edit Settings. The Advanced Options window opens.
4. In the General Timers section ("PIM Advanced Options- General Timers" on page 122), enter values for the:
   • **Hello interval** (in seconds).
   • **Data Interval** (in seconds).
   • **Assert Interval** (in seconds).
   • **Assert-rate Limit**.
   • **Join Prune Interval** (in seconds).
   • **Join Prune Delay Interval** (in seconds).
   • **Join Prune Suppress Interval** (in seconds).
5. In the Assert Ranks section ("PIM Advanced Options- Assert Ranks" on page 123), enter values for the routing protocol(s) you are using.
6. Click Save.

**Configuring PIM-SM Advanced Options (Optional)**

To configure PIM Simple Mode Advanced options:

1. Open the Advanced Routing > PIM page of the WebUI.
2. Select the PIM Protocol. One of:
   • **Sparse Mode (SM)**
   • **Source Specific Multicast (SSM)**
3. Click Edit Settings.
   The Advanced Options window opens.
4. In the Sparse Mode Timers ("PIM Advanced Options- Sparse Mode Timers" on page 124) section, enter a value for the
5. In the Shortest Path First Threshold section, click Add. The Shortest Path First Threshold: Add Multicast Group window opens.

6. In the SPT: Add Multicast Group window ("PIM Advanced Options- Shortest First Path Threshold - Add Multicast Group" on page 124), enter a value for the:
   a) Multicast Group to which the SPT threshold applies.
   b) Subnet mask for the group multicast address.
   c) Threshold to Switch (in kilobits per second).
   d) Click OK.

7. In the General Timers section ("PIM Advanced Options- General Timers" on page 122), enter values for the:
   - Hello interval (in seconds).
   - Data Interval (in seconds).
   - Assert Interval (in seconds).
   - Assert-rate Limit.
   - Join Prune Interval (in seconds).
   - Join Prune Delay Interval (in seconds).
   - Join Prune Suppress Interval (in seconds).

8. In the Assert Ranks section ("PIM Advanced Options- Assert Ranks" on page 123), enter values for the routing protocol(s) you are using.

9. Click Save.

**PIM Advanced Options- General Timers**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello interval</td>
<td>Interval between which PIM hellos are sent on a multicast-capable interface. Hello messages are addressed to the All-PIM-Routers multicast group (224.0.0.13) so that PIM routers may discover neighbors on a multi-access network.</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-21845 seconds</td>
</tr>
<tr>
<td></td>
<td>• Default: 30</td>
</tr>
<tr>
<td>Data Interval</td>
<td>The life-time of a new PIM forwarding entry. Subsequently the life of the entry will be extended in different ways depending on the location of this router in the network. For example, in some cases the receipt of PIM control messages (e.g. periodic join/prune messages) will extend the life of the entry and in others the presence of local senders of multicast traffic will prevent the entry from being deleted.</td>
</tr>
<tr>
<td></td>
<td>• Range: 11-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• Default: 210</td>
</tr>
<tr>
<td>Assert Interval</td>
<td>If an assert battle on an upstream interface results in a PIM neighbor other than the unicast reverse-path-forwarding (RPF) neighbor towards the source of the data traffic (for which the assert battle was generated) getting elected as the designated forwarder on that interface, the winner is used as the upstream neighbor for all subsequent join/prune messages. This change is timed-out after expiry of the assert interval (measured in seconds).</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• Default: 180</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assert-rate Limit.</td>
<td>The number of asserts to send per second. Asserts are generated by the router when data from a source is detected on an interface other than the incoming interface (based on the unicast routing table) towards the source. These messages are rate-limited and the router should not originate more than a fixed number of assert messages per second. If the limit is set to 0, rate-limiting is disabled.</td>
</tr>
<tr>
<td></td>
<td>- Range: 0, 10-10000</td>
</tr>
<tr>
<td></td>
<td>- Default: 10</td>
</tr>
<tr>
<td>Join Prune Interval</td>
<td>Interval between sending Join/Prune messages.</td>
</tr>
<tr>
<td></td>
<td>- Range: 1-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>- Default: 60</td>
</tr>
<tr>
<td>Join Prune Delay Interval</td>
<td>The maximum interval from the time when the unicast Reverse Path Forwarding (RPF) neighbor (towards a source or the RP) changes, and a triggered Join/Prune message is sent.</td>
</tr>
<tr>
<td></td>
<td>- Range: 1-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>- Default: 5</td>
</tr>
<tr>
<td>Join Prune Suppress Interval</td>
<td>Mean interval from receiving a Join/Prune with a higher Holdtime (with ties broken by higher network layer address) and allowing duplicate Join/Prunes to be sent again. Set this interval to 1.25 times the join/prune interval.</td>
</tr>
<tr>
<td></td>
<td>- Range: 2-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>- Default: 75</td>
</tr>
</tbody>
</table>

**PIM Advanced Options- Assert Ranks**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>Used to compare the cost of protocols in order to determine which router will forward multicast data packets on a multi-access LAN. These values are used in assert messages sent out on a LAN when a router detects data packets on an interface other than the incoming interface towards the source of the data. These values must be the same for all routers on a multi-access LAN that are running the same protocol. Hence, the default values have been specifically configured to match that of other implementations.</td>
</tr>
<tr>
<td>OSPF</td>
<td></td>
</tr>
<tr>
<td>Kernel</td>
<td></td>
</tr>
<tr>
<td>Static</td>
<td></td>
</tr>
<tr>
<td>RIP</td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Range: 0-255</td>
</tr>
<tr>
<td></td>
<td>- Defaults:</td>
</tr>
<tr>
<td></td>
<td>- Direct: 0</td>
</tr>
<tr>
<td></td>
<td>- OSPF: 10</td>
</tr>
<tr>
<td></td>
<td>- Kernel: 40</td>
</tr>
<tr>
<td></td>
<td>- Static: 60</td>
</tr>
<tr>
<td></td>
<td>- RIP: 100</td>
</tr>
<tr>
<td></td>
<td>- BGP: 170</td>
</tr>
</tbody>
</table>

**PIM Advanced Options- State Refresh Parameters (DM)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Refresh Interval</td>
<td>For Dense Mode, the interval at which state refresh messages are sent for multicast traffic originated by directly-connected sources.</td>
</tr>
<tr>
<td></td>
<td>- Range: 1-255</td>
</tr>
<tr>
<td></td>
<td>- Default: 60</td>
</tr>
</tbody>
</table>
Parameter | Description
--- | ---
State Refresh TTL | For Dense Mode, the time-to-live (TTL) placed in the state refresh messages originated for multicast traffic from directly-connected sources. This value can be used to limit the forwarding of state refresh messages in the network. In the absence of user configuration it is derived from the multicast data.
- **Range:** 1-255
- **Default:** None

### PIM Advanced Options - Sparse Mode Timers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Register Suppression Interval | The mean interval between receiving a register-stop and allowing registers to be sent again. A lower value means more frequent register bursts at the rendezvous point. A higher value means a longer join latency for new receivers.
- **Range:** 60-3600 seconds
- **Default:** 60 seconds
| CRP Advertise Interval | The interval between which candidate-rendezvous point routers send candidate-rendezvous point advertisements to the elected bootstrap router.
- **Range:** 1-3600 seconds
- **Default:** 60 seconds

### PIM Advanced Options - Shortest First Path Threshold - Add Multicast Group

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Multicast Group | The multicast group address to apply to the shortest path tree (spt) threshold.
- **Range:** Dotted-quad ([224-239],[0-255],[0-255],[0-255])
- **Default:** None
| Subnet mask | Mask length.
- **Range:** 1-32
- **Default:** None
| Use Infinity | Specifies that there is no spt switch. |
| Use Integer | The data rate threshold in Kbits/sec to trigger the spt switchover. 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.
- **Range:** 0-1000000 Kbits/s, or infinity (for no switchover)
- **Default:** None

### Configuring PIM-SM Bootstrap and Rendezvous Point Settings

To configure this router as a Bootstrap router, Candidate Rendezvous Point and Static Rendezvous Point:
1. Open the **Advanced Routing > PIM** page of the WebUI.
2. Select the **PIM Protocol.** One of:
3. In the *Bootstrap and Rendezvous Point Settings* section, click *Edit Settings*. The *Bootstrap and Rendezvous Point Settings* window opens.
4. To enable the router as a Bootstrap Router (*"PIM Bootstrap Settings" on page 125*):
   a) Select *Enable Bootstrap Router*.
   b) Optional: Enter the *Local Address* of the bootstrap router.
   c) Optional: Enter the *Local Preference*.
5. To enable the router as a Candidate Rendezvous Point (*"PIM Candidate Rendezvous Point" on page 126*):
   a) Select *Enable Candidate RP*.
   b) Optional: Enter the *Local Address* of the Candidate Rendezvous Point router.
   c) Optional: Enter the *Local Preference*.
   d) Optional: Click *Add* to Configure a *Multicast Group* and *Subnet mask* for which this router is designated as the candidate rendezvous point.
6. To enable a Static Rendezvous Point (*"PIM Static Rendezvous Point" on page 126*):
   a) Select *Enable Static RP*.
   b) Optional: Click *Add* to enter the *Static Rendezvous Point* IP address.
   c) Optional: Click *Add* to configure a *Multicast Group* and *Subnet mask* for which this router is designated as the static rendezvous point.

**PIM Bootstrap Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Bootstrap Router</strong></td>
<td>If enabled, this router is a candidate bootstrap router (C-BSR). All candidate RPs (C-RPs) send C-RP-Advertisements to the elected bootstrap router (BSR). The BSR then disseminates this information in bootstrap messages across the PIM domain. To avoid a single point of failure, configure more than one router in a domain as a candidate BSR.</td>
</tr>
<tr>
<td><strong>Local Address</strong></td>
<td>Address used for the C-BSR state machine and the bootstrap messages. If PIM clustering is enabled, then this address must be configured and must match that of one of the PIM interfaces. If PIM clustering is not enabled, this address can either be that of the PIM interfaces or an address configured on the loopback interface. If an address from the loopback interface is used, take care not select an address in the 127/8 address range.</td>
</tr>
<tr>
<td><strong>Local Preference</strong></td>
<td>The priority advertised in C-BSR messages. The candidate bootstrap router with the highest priority value is elected as the bootstrap router for the domain. The C-RP with the lowest priority has the highest preference. The highest priority value is 0.</td>
</tr>
</tbody>
</table>

- **Default**: Cleared
- **Range**: Address of PIM interface or a non 127.0.0.0/8 loopback address.
- **Default**: The IP address of one of the interfaces on which PIM is enabled. The default does not apply if PIM clustering is enabled.
## PIM Candidate Rendezvous Point

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Candidate RP</td>
<td>Specifies that the platform is a candidate rendezvous point router.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Address used for the C-RP state machine and in the C-RP-Advertisements sent to the elected bootstrap router.</td>
</tr>
<tr>
<td></td>
<td>If PIM clustering is enabled, then this address must be configured and must match that of one of the PIM interfaces.</td>
</tr>
<tr>
<td></td>
<td>If clustering is not enabled, this address can either be that of one of the PIM interfaces or an address configured on the loopback interface. If an address from the loopback interface is used, take care not select an address in the 127/8 address range.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: Address of PIM interface or a non 127.0.0.0/8 loopback address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: Selects the IP address of one of the interfaces on which PIM is enabled. The default does not apply if PIM clustering is enabled.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>The priority of this C-RP. All PIM routers select the same RP for a multicast group address from the list of C-RPs received in the bootstrap messages from the elected BSR. The lower the Local Preference of the C-RP, the higher the priority.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 0-255</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 0</td>
</tr>
<tr>
<td>Multicast Group</td>
<td>The multicast group(s) for which this rendezvous point is responsible. Enter the group multicast IP address and mask length.</td>
</tr>
<tr>
<td></td>
<td>Multicast group address</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: Dotted-quad ([224-239],[0-255],[0-255],[0-255])</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 224.0.0.0/4</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Mask length:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-32</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: None</td>
</tr>
</tbody>
</table>

## PIM Static Rendezvous Point

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Static RP</td>
<td>Enables or disables the static rendezvous point.</td>
</tr>
<tr>
<td>Static Rendezvous Point</td>
<td>A static rendezvous point. If an associated multicast group and prefix is not configured, the static-rp is considered to be responsible for all multicast groups (224.0.0.0/4). This needs to be consistent with the RP information at other routers in a multicast domain irrespective of the RP-dissemination mechanism (bootstrap or autoRP) used.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - The static RP overrides the RP information received from other RP-dissemination mechanisms, such as bootstrap routers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: Any IP address</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: None</td>
</tr>
</tbody>
</table>
### Configuring PIM - CLI (pim)

Use the commands in this section to configure PIM via the CLI.

#### PIM Global Settings

```
set pim mode
  dense
  sparse
  ssm

set pim state-refresh <on | off>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;dense</td>
<td>sparse</td>
</tr>
<tr>
<td>• Sparse Mode (SM)</td>
<td></td>
</tr>
<tr>
<td>• Dense Mode (DM)</td>
<td></td>
</tr>
<tr>
<td>• Source-Specific Multicast (SSM)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state-refresh &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

#### PIM Interfaces

After you set PIM to run dense mode, sparse mode or SSM, use the following commands to configure PIM for specific interfaces.

```
set pim interface if_name
  <on | off>
  virtual-address <on | off>
  local-address ip_address
  dr-priority <0-4294967295>
  dr-priority default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface if_name &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| virtual-address <on | off>                                                                                                                                         | Use the VRRP virtual IP address on this interface. If enabled, PIM runs on this interface only after the router transitions to become a 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.  
**Note** - You cannot configure a local address or a virtual address when ClusterXL is enabled.  
- **Default:** Off                                                                                                                   |
| local-address ip_address  | Use the specified local address for all advertisements sent on the interface. This is useful on interfaces with multiple IP addresses (aliases). The local address must match one of the addresses configured on the interface. If a local address is specified while the virtual address option enabled, the local address must match a virtual address on the interface.  
**Note** - Each router must have at least one interface address with a subnet prefix shared by all neighboring PIM routers. If any neighboring routers choose advertisement addresses that do not appear to be on a shared subnet all messages from those neighbors will be rejected. This holds true even when the virtual address option is enabled.  
- **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255]).  
- **Default:** Selects one of the IP addresses configured on the interface. If the virtual address option is enabled, PIM will use the virtual address configured on the interface after the router transitions to master state with respect to VRRP. |
| dr-priority <0-4294967295> | The dr-priority advertised in the PIM hello messages sent on the interface. This is used for DR election on a LAN. The router with the highest priority is elected the designated router. To break a tie, the DR is selected on the basis of the highest IP address. If even one router does not advertise a dr-priority, the DR election is based on the IP address.  
- **Range:** 0-4294967295 ($2^{32} - 1$).  
- **Default:** 1.  
- **Note** - To verify whether a PIM neighbor supports DR Priority, use the following command:  
  show pim neighbor <ip_address>  
  For neighbors that advertise a DR election priority value, the following message appears in the summary:  
  DRPriorityCapable Yes. |
| dr-priority default | A value of 1.                                                                                                                                                                                                                                                                                                                                 |

**PIM Sparse Mode**  
Use the following commands to configure parameters for sparse mode PIM only.
set pim
  bootstrap-candidate <on | off>
  bootstrap-candidate local-address ip_address
  bootstrap-candidate priority <0-255>
  bootstrap-candidate priority default
  candidate-rp <on | off>
  candidate-rp local-address ip_address
  candidate-rp priority <0-255>
  candidate-rp priority default
  candidate-rp multicast group mcast_ip_prefix <on | off>
  static-rp off
  static-rp rp-address ip_address < on | off>
  static-rp rp-address ip_address multicast-group
  register-suppress-interval <60-3600>
  register-suppress-interval default
  candidate-rp advertise-interval <1-3600>
  candidate rp-advertise-interval default
  spt-threshold multicast <mcast_address>/<mask_length> threshold
  <0-1000000> <on | off>
  spt-threshold multicast <mcast_address>/<mask_length> threshold infinity
  <on | off>

Bootstrap and Rendezvous Point Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootstrap-candidate &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td>• Default: off</td>
</tr>
<tr>
<td>bootstrap-candidate local-address ip_address</td>
<td>Address used for the C-BSR state machine and the bootstrap messages. If PIM clustering is enabled, then this address must be configured and must match that of one of the PIM interfaces. If PIM clustering is not enabled, this address can either be that of the PIM interfaces or an address configured on the loopback interface. If an address from the loopback interface is used, take care not select an address in the 127/8 address range.</td>
</tr>
<tr>
<td></td>
<td>• Range: Address of PIM interface or a non 127.0.0.0/8 loopback address.</td>
</tr>
<tr>
<td></td>
<td>• Default: The IP address of one of the interfaces on which PIM is enabled. The default does not apply if PIM clustering is enabled.</td>
</tr>
<tr>
<td>bootstrap-candidate priority &lt;0-255&gt;</td>
<td>The priority advertised in C-BSR messages. The candidate bootstrap router with the highest priority value is elected as the bootstrap router for the domain. The C-RP with the lowest priority has the highest preference. The highest priority value is 0.</td>
</tr>
<tr>
<td></td>
<td>• Range: 0-255</td>
</tr>
<tr>
<td></td>
<td>• Default: 0</td>
</tr>
<tr>
<td>bootstrap-candidate priority default</td>
<td>Specifies a value of 0.</td>
</tr>
</tbody>
</table>

Gaia Advanced Routing Administration Guide R76 | 129
## Candidate Rendezvous Point

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>candidate-rp &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: off</td>
</tr>
<tr>
<td>candidate-rp local-address ip_address</td>
<td>Address used for the C-RP state machine and in the C-RP-Advertisements sent to the elected bootstrap router.</td>
</tr>
<tr>
<td></td>
<td>If PIM clustering is enabled, then this address must be configured and must match that of one of the PIM interfaces.</td>
</tr>
<tr>
<td></td>
<td>If clustering is not enabled, this address can either be that of one of the PIM interfaces or an address configured on the loopback interface. If an address from the loopback interface is used, take care not select an address in the 127/8 address range.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: Address of PIM interface or a non 127.0.0.0/8 loopback address.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: Selects the IP address of one of the interfaces on which PIM is enabled. The default does not apply if PIM clustering is enabled.</td>
</tr>
<tr>
<td>candidate-rp priority &lt;0-255&gt;</td>
<td>The priority of this C-RP. All PIM routers select the same RP for a multicast group address from the list of C-RPs received in the bootstrap messages from the elected BSR. The lower the Local Preference of the C-RP, the higher the priority.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 0-255</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: 0</td>
</tr>
<tr>
<td>candidate-rp priority default</td>
<td>A value of 0.</td>
</tr>
</tbody>
</table>

## Candidate Rendezvous Point

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>candidate-rp multicast-group &lt;mcast_address&gt;/&lt;mask_length&gt; &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: Dotted-quad ([224-239].[0-255].[0-255].[0-255]).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: None.</td>
</tr>
<tr>
<td></td>
<td>Mask length:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 1-32</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: None</td>
</tr>
</tbody>
</table>

## Static Rendezvous Point

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static-rp off</td>
<td>Disables the static rendezvous point option.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| static-rp rp-address ip_address <on | off>                                                                                                                                  | A static rendezvous point. If an associated multicast group and prefix is not configured, the static-rp is considered to be responsible for all multicast groups (224.0.0.0/4). This needs to be consistent with the RP information at other routers in a multicast domain irrespective of the RP-dissemination mechanism (bootstrap or autoRP) used.  
**Note** - The static RP overrides the RP information received from other RP-dissemination mechanisms, such as bootstrap routers.  
- **Range**: Any IP address  
- **Default**: None                                                                                                                   |
| static-rp rp-address ip_address multicast-group <mcast_address>/<mask_length> <on | off>                                                                         | The multicast group(s) for which this rendezvous point is responsible. Enter the group multicast IP address and mask length.  
Multicast group address  
- **Range**: Dotted-quad ([224-239],[0-255],[0-255],[0-255])  
- **Default**: 224.0.0.0/4  
Mask length:  
- **Range**: 1-32  
- **Default**: None                                                                                                                   |

**Sparse Mode Timers**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| register-suppress-interval <60-3600>    | The mean interval between receiving a register-stop and allowing registers to be sent again. A lower value means more frequent register bursts at the rendezvous point. A higher value means a longer join latency for new receivers.  
- **Range**: 60-3600 seconds  
- **Default**: 60 seconds |
| register-suppress-interval default       | A value of 60 seconds.                                                                              |
| candidate-rp advertise-interval <1-3600> | The interval between which candidate-rendezvous point routers send candidate-rendezvous point advertisements to the elected bootstrap router.  
- **Range**: 1-3600 seconds  
- **Default**: 60 seconds |
| candidate-rp advertise-interval default  | A value of 60 seconds.                                                                              |
### Shortest Path First Threshold

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| spt-threshold multicast &lt;mcast_address&gt;/&lt;mask_length&gt; threshold &lt;0-1000000&gt; | The multicast group address to apply to the shortest path tree (spt) threshold.  
  - **Range**: Dotted-quad ([224-239],[0-255],[0-255],[0-255])  
  - **Default**: None  
  
  Mask length.  
  - **Range**: 1-32  
  - **Default**: None  
  
  The data rate threshold in Kbits/sec to trigger the spt switchover.  
  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.  
  - **Range**: 0-1000000 Kbits/s, or infinity (for no switchover)  
  - **Default**: None  |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| spt-threshold multicast &lt;mcast_address&gt;/&lt;mask_length&gt; threshold infinity &lt;on | off&gt; | Specifies that there is no spt switchover.  
  Multicast group address  
  - **Range**: Dotted-quad ([224-239],[0-255],[0-255],[0-255])  
  - **Default**: 224.0.0.0/4  
  
  Mask length:  
  - **Range**: 1-32  
  - **Default**: None |

**Timer and Assert Rank Parameters for Dense Mode and Sparse Mode**

Use these commands to change or restore default values for timers and assert ranks.
set pim
  hello-interval <1-21845>
  hello-interval default
  data-interval <11-3600>
  data-interval default
  assert-interval <1-3600>
  assert-interval default
  assert-limit <10-10000>
  assert-limit default
  assert-limit <0>
  jp-interval <1-3600>
  jp-interval default
  jp-delay-interval <1-3600>
  jp-delay-interval default
  jp-suppress-interval <2-3600>
  jp-suppress-interval default
  assert-rank protocol protocol name rank <0-255>
  assert-rank protocol protocol name rank default
  state-refresh-interval <1 - 255>
  state-refresh-ttl <1 - 255>

### General Timers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello interval</td>
<td>Interval between which PIM hellos are sent on a multicast-capable interface. Hello messages are addressed to the All-PIM-Routers multicast group (224.0.0.13) so that PIM routers may discover neighbors on a multi-access network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-21845 seconds</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 30</td>
</tr>
<tr>
<td>hello interval default</td>
<td>A value of 30.</td>
</tr>
<tr>
<td>data-interval</td>
<td>The life-time of a new PIM forwarding entry. Subsequently the life of the entry will be extended in different ways depending on the location of this router in the network. For example, in some cases the receipt of PIM control messages (e.g. periodic join/prune messages) will extend the life of the entry and in others the presence of local senders of multicast traffic will prevent the entry from being deleted.</td>
</tr>
<tr>
<td>assert-interval</td>
<td>If an assert battle on an upstream interface results in a PIM neighbor other than the unicast reverse-path-forwarding (RPF) neighbor towards the source of the data traffic (for which the assert battle was generated) getting elected as the designated forwarder on that interface, the winner is used as the upstream neighbor for all subsequent join/prune messages. This change is timed-out after expiry of the assert interval (measured in seconds).</td>
</tr>
<tr>
<td>assert-interval default</td>
<td>A value of 180.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Range</strong>: 1-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>: 180</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>assert-limit &lt;10-10000&gt;</td>
<td>The number of asserts to send per second. Asserts are generated by the router when data from a source is detected on an interface other than the incoming interface (based on the unicast routing table) towards the source. These messages are rate-limited and the router should not originate more than a fixed number of assert messages per second. If the limit is set to 0, rate-limiting is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Range: 0, 10-10000</td>
</tr>
<tr>
<td></td>
<td>• Default: 10</td>
</tr>
<tr>
<td>assert-limit default</td>
<td>A value of 10.</td>
</tr>
<tr>
<td>assert-limit &lt;0&gt;</td>
<td>Disables the limit placed on the number of asserts that can be sent per second.</td>
</tr>
<tr>
<td>jp-interval &lt;1-3600&gt;</td>
<td>Interval between sending Join/Prune messages.</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• Default: 60</td>
</tr>
<tr>
<td>jp-interval default</td>
<td>A value of 60.</td>
</tr>
<tr>
<td>jp-delay-interval &lt;1-3600&gt;</td>
<td>The maximum interval from the time when the unicast Reverse Path Forwarding (RPF) neighbor (towards a source or the RP) changes, and a triggered Join/Prune message is sent.</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• Default: 5</td>
</tr>
<tr>
<td>jp-delay-interval default</td>
<td>A value of 5.</td>
</tr>
<tr>
<td>jp-suppress-interval &lt;2-3600&gt;</td>
<td>Mean interval from receiving a Join/Prune with a higher Holdtime (with ties broken by higher network layer address) and allowing duplicate Join/Prunes to be sent again. Set this interval to 1.25 times the join/prune interval.</td>
</tr>
<tr>
<td></td>
<td>• Range: 2-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• Default: 75</td>
</tr>
<tr>
<td>jp-suppress-interval default</td>
<td>A value of 75.</td>
</tr>
</tbody>
</table>

**Assert Ranks**

<table>
<thead>
<tr>
<th>assert-rank protocol protocol name rank &lt;0-255&gt;</th>
<th>Used to compare the cost of protocols in order to determine which router will forward multicast data packets on a multi-access LAN. These values are used in assert messages sent out on a LAN when a router detects data packets on an interface other than the incoming interface towards the source of the data. These values must be the same for all routers on a multi-access LAN that are running the same protocol. Hence, the default values have been specifically configured to match that of other implementations.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Range: 0-255</td>
</tr>
</tbody>
</table>
assert-rank protocol protocol name rank <0-255>

Used to compare the cost of protocols in order to determine which router will forward multicast data packets on a multi-access LAN. These values are used in assert messages sent out on a LAN when a router detects data packets on an interface other than the incoming interface towards the source of the data. These values must be the same for all routers on a multi-access LAN that are running the same protocol. Hence, the default values have been specifically configured to match that of other implementations.

- **Range**: 0-255

---

assert-rank protocol protocol name rank default

Default assert-rank values for supported protocols that match other implementations.

- **Defaults**:
  - Direct: 0
  - OSPF: 10
  - Kernel: 40
  - Static: 60
  - RIP: 100
  - BGP: 170

---

### State Refresh Parameters - Dense Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state-refresh-interval &lt;1 – 255&gt;</td>
<td>For Dense Mode, the interval at which state refresh messages are sent for multicast traffic originated by directly-connected sources.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 1-255</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: 60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state-refresh-ttl &lt;1 – 255&gt;</td>
<td>For Dense Mode, the time-to-live (TTL) placed in the state refresh messages originated for multicast traffic from directly-connected sources. This value can be used to limit the forwarding of state refresh messages in the network. In the absence of user configuration it is derived from the multicast data.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Range</strong>: 1-255</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default</strong>: None</td>
</tr>
</tbody>
</table>

---

**Monitoring and Troubleshooting PIM**

**PIM Trace Options**

To log information about PIM errors and events using the WebUI:

1. In the tree view, click **Advanced Routing > Routing Options**.
2. In the **Configuration** tab, select **Filter Visible Tables Below** and select **PIM**.
3. In the option variables area, do one of:
   - Double-click an option.
   - Select an option (to select multiple options, use Shift-Click) and click **Activate**.
4. Click **Apply** at the top of the page
To log information about PIM errors and events using the CLI:

```bash
set trace pim
    assert <on | off>
    bootstrap <on | off>
    crp <on | off>
    graft <on | off>
    hello <on | off>
    join <on | off>
    mfc <on | off>
    mrt <on | off>
    packets <on | off>
    rp <on | off>
    register <on | off>
    trap <on | off>
    traceoptions <on | off>
```

The following trace options apply both to dense-mode and sparse-mode implementations:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assert</td>
<td>Trace PIM assert messages.</td>
</tr>
<tr>
<td>hello</td>
<td>Trace PIM router hello messages.</td>
</tr>
<tr>
<td>join</td>
<td>Trace PIM join/prune messages.</td>
</tr>
<tr>
<td>mfc</td>
<td>Trace calls to or from the multicast forwarding cache</td>
</tr>
<tr>
<td>mrt</td>
<td>Trace PIM multicast routing table events.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace all PIM packets.</td>
</tr>
<tr>
<td>trap</td>
<td>Trace PIM trap messages.</td>
</tr>
<tr>
<td>all</td>
<td>Trace all PIM events and packets.</td>
</tr>
</tbody>
</table>

The following trace options apply to sparse-mode implementations only:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootstrap</td>
<td>Trace bootstrap messages.</td>
</tr>
<tr>
<td>crp</td>
<td>Trace candidate-RP-advertisements.</td>
</tr>
<tr>
<td>rp</td>
<td>Trace RP-specific events, including RP set-specific and bootstrap-specific events.</td>
</tr>
<tr>
<td>register</td>
<td>Trace register and register-stop packets.</td>
</tr>
</tbody>
</table>

The following trace option applies to dense-mode implementations only:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graft</td>
<td>Trace graft and graft acknowledgment packets.</td>
</tr>
</tbody>
</table>

**PIM Show and MFC Commands**

Use these commands to monitor and troubleshoot PIM.
These commands apply to both dense-mode and sparse-mode PIM:

```
show pim
  interfaces
  interfaces if_address
  neighbors
  neighbor ip_address
  memory
  timers
  stats
  summary
```

These commands apply only to sparse-mode PIM:

```
show pim
  bootstrap
  candidate-rp
  joins
  rps
  sarse-mode-stats
  group-rp-mapping <mcast_address>
```

### Dense Mode and Sparse Mode Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The interfaces that are running PIM, their status, and their mode. This</td>
</tr>
<tr>
<td></td>
<td>command also displays the interface and its DR priority and the number of</td>
</tr>
<tr>
<td></td>
<td>PIM neighbors on the interface.</td>
</tr>
<tr>
<td>neighbors</td>
<td>The IP address of each PIM neighbor and the interface on which the neighbor</td>
</tr>
<tr>
<td></td>
<td>is present. This command also displays the neighbor’s DR priority,</td>
</tr>
<tr>
<td></td>
<td>generation ID, holdtime and the time the neighbor is set to expire based on</td>
</tr>
<tr>
<td></td>
<td>the holdtime received in the most recent hello message.</td>
</tr>
<tr>
<td>neighbor ip_address</td>
<td>Use this command to verify whether a PIM neighbor supports DR Priority.</td>
</tr>
<tr>
<td></td>
<td>For neighbors that advertise a DR election priority value, the following</td>
</tr>
<tr>
<td></td>
<td>message appears in the summary:</td>
</tr>
<tr>
<td></td>
<td>DRPriorityCapable Yes.</td>
</tr>
<tr>
<td>stats</td>
<td>The number of different types of PIM packets received and transmitted and</td>
</tr>
<tr>
<td></td>
<td>any associated errors.</td>
</tr>
<tr>
<td>memory</td>
<td></td>
</tr>
<tr>
<td>timers</td>
<td></td>
</tr>
<tr>
<td>summary</td>
<td></td>
</tr>
</tbody>
</table>

### Sparse Mode Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootstrap</td>
<td>The IP address and state of the Bootstrap router.</td>
</tr>
<tr>
<td>candidate-rp</td>
<td>The state of the Candidate Rendezvous Point state machine.</td>
</tr>
<tr>
<td>joins</td>
<td>PIM’s view of the join-prune (*, G and S, G) state, including RP for the</td>
</tr>
<tr>
<td></td>
<td>group, incoming, and outgoing interface(s), interaction with the multicast</td>
</tr>
<tr>
<td></td>
<td>forwarding cache and the presence of local members. To view the equivalent</td>
</tr>
<tr>
<td></td>
<td>information for dense-mode PIM, use the show mfc cache command.</td>
</tr>
<tr>
<td>rps</td>
<td>The active RP-set, including the RP addresses, their type (or source of</td>
</tr>
<tr>
<td></td>
<td>information about them) and the groups for which they are configured to act</td>
</tr>
<tr>
<td></td>
<td>as RP.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>group-rp-mapping &lt;group-address&gt;</td>
<td>The RP selected for a particular group based on information from the active RP-set.</td>
</tr>
<tr>
<td>sparse-mode stats</td>
<td>Error statistics for multicast forwarding cache (MFC); Bootstrap Router (BSR) messages; Candidate Rendezvous Point (CRP) advertisements; and the Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>

**MFC Commands and Trace Options**

To log multicast errors and events, use the `show mfc` commands or the MFC Trace options in the WebUI or the CLI (“MFC Trace Options” on page 105).

```plaintext
show mfc
  cache
  interface
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache</td>
<td>Multicast source and group forwarding state by prefix.</td>
</tr>
<tr>
<td>interface</td>
<td>Multicast source and group forwarding state by interface.</td>
</tr>
</tbody>
</table>
Chapter 14

Routing Monitor

In This Chapter

- Monitoring Routes - WebUI 139
- Monitoring Routes - CLI (show route) 139
- Monitoring the Routing Daemon - CLI (show routed) 140
- Monitoring the Multicast Forwarding Cache - CLI (show mfc) 141

Use the routing monitor to show summary information about routes on the Gaia system.

Monitoring Routes - WebUI

To show the routes on the Gaia system using the WebUI:
1. In the tree view, click Advanced Routing > Routing Monitor.
2. Optional: In the Filter Protocols column, select the protocol whose routes you want to see. Shift-click to select multiple items.

Monitoring Routes - CLI (show route)

Use these commands to show information about active, inactive or all (both active and inactive) routes on your system for BGP, OSPF and RIP protocols:

```
show route
  rip
  bgp <aspath | communities | detailed | metrics | suppressed>
  inactive <bgp | rip>
  all <bgp | rip | ospf>
```

Use these commands to show information about active, inactive, or all routes on your system for OSPF:

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

Use these commands to show information about active, inactive and all aggregate routes on your system:

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

Use these commands to show additional information about routes on your system:
show route
  all
  all direct
  all static
  all kernel
direct
inactive
inactive direct
inactive static
inactive kernel
kernel
static
summary
destination ip_address
exact ip_prefix
less-specific ip_prefix
more-specific ip_prefix

Monitoring the Routing Daemon - CLI (show routed)

Use the following commands to view general information recorded by the Gaia routing daemon (`routed`).

show routed
memory
resources
krt
version

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>Show the memory usage of the routing daemon, for each routing protocol running on the system.</td>
</tr>
<tr>
<td></td>
<td>- Total memory usage.</td>
</tr>
<tr>
<td></td>
<td>- Memory used by each routing protocol.</td>
</tr>
<tr>
<td></td>
<td>- MFC - memory used for the multicast forwarding cache (MFC).</td>
</tr>
<tr>
<td></td>
<td>- Core - memory used by routed for internal purposes.</td>
</tr>
<tr>
<td>resources</td>
<td>Show the following system information:</td>
</tr>
<tr>
<td></td>
<td>- Total uptime</td>
</tr>
<tr>
<td></td>
<td>- Total user time</td>
</tr>
<tr>
<td></td>
<td>- Total system time</td>
</tr>
<tr>
<td></td>
<td>- Page faults</td>
</tr>
<tr>
<td></td>
<td>- Page reclaims</td>
</tr>
<tr>
<td></td>
<td>- File system writes</td>
</tr>
<tr>
<td></td>
<td>- File system reads</td>
</tr>
<tr>
<td></td>
<td>- Message writes</td>
</tr>
<tr>
<td></td>
<td>- Message reads</td>
</tr>
<tr>
<td></td>
<td>- Signals received</td>
</tr>
<tr>
<td></td>
<td>- Total swaps</td>
</tr>
<tr>
<td></td>
<td>- Voluntary context switches</td>
</tr>
<tr>
<td></td>
<td>- Involuntary context switches</td>
</tr>
</tbody>
</table>
### krt

Show statistical information about the messages sent and received on the raw sockets between the kernel and `routed`.

- KRT interface message count
- KRT interface message length
- KRT route message count (rx)
- KRT route message length (rx)
- KRT route message count (tx)
- KRT route message length (tx)
- KRT route adds
- KRT route changes
- KRT route deletes

### version

Shows the following system information:

- `routed` version
- System start time
- Current time
- System uptime

---

**Monitoring the Multicast Forwarding Cache - CLI (show mfc)**

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

```
show mfc
  cache
  summary
  interface
  orphans
  stats
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache</td>
<td>Shows MFC state information.</td>
</tr>
<tr>
<td>summary</td>
<td>Shows the following MFC state information:</td>
</tr>
<tr>
<td></td>
<td>Number of interfaces enabled</td>
</tr>
<tr>
<td></td>
<td>Number of cache entries</td>
</tr>
<tr>
<td></td>
<td>Kernel forwarding entry limit</td>
</tr>
<tr>
<td></td>
<td>Number of kernel forwarding entries</td>
</tr>
<tr>
<td></td>
<td>Cache entry average lifetime</td>
</tr>
<tr>
<td></td>
<td>Prune average lifetime</td>
</tr>
<tr>
<td></td>
<td>Cache age cycle</td>
</tr>
<tr>
<td></td>
<td>Data rate update interval</td>
</tr>
<tr>
<td></td>
<td>Multicast protocol (instance)</td>
</tr>
<tr>
<td>interface</td>
<td>Shows MFC interface state information.</td>
</tr>
<tr>
<td>orphans</td>
<td>Shows MFC orphan state information.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| `stats`   | Shows various information about the following MFC properties:  
- Resolve task summary  
- Resolve requests  
- RPF failure notifications  
- MFC maintenance |
Index

A

Action Table Parameters • 114
Add BGP Policy Window • 78
Area Border Routers • 55
Authentication • 47
Auto Summarization • 48

B

BGP • 11, 94
BGP AS Peer Groups • 20
BGP Communities • 37
BGP Confederations • 29
BGP Global Settings • 17
BGP Interactions with IGPs • 14
BGP Miscellaneous Settings • 18
BGP Multi-Exit Discriminator • 14
BGP Path Attributes • 13
BGP Peers • 27
BGP Remote Peers • 20
BGP Route Dampening • 31
BGP Route Reflection • 30
BGP Route Refresh • 12
BGP Sessions (Internal and External) • 12
BGP Show Commands • 37
BGP Trace Options • 102
BOOTP Interfaces • 9
BOOTP Show Commands • 9
BOOTP/DHCP Parameters • 9

C

Communities • 15
Confederations • 15
Configure Interfaces for IGMP • 41
Configuring BGP - CLI (bgp) • 26
Configuring BGP - WebUI • 17
Configuring DHCP Relay - WebUI • 8
Configuring Equal Cost Path Splitting - CLI (max-path-splits) • 98
Configuring Equal Cost Path Splitting - WebUI • 97
Configuring Global Settings • 56
Configuring IGMP - CLI (igmp) • 41
Configuring IGMP - WebUI • 40
Configuring Inbound Route Filters - WebUI • 77
Configuring IP Broadcast Helper - CLI (iphelper) • 45
Configuring IP Broadcast helper - WebUI • 44
Configuring Kernel Routes - CLI (kernel-routes) • 98
Configuring Kernel Routes - WebUI • 98
Configuring OSPF - CLI (ospf) • 62
Configuring OSPF - WebUI • 56
Configuring OSPF Areas • 57
Configuring OSPF Interfaces • 60
Configuring OSPF Virtual Links • 59
Configuring PIM - CLI (pim) • 127
Configuring PIM - WebUI • 119
Configuring PIM-DM Advanced Options (Optional) • 121

Configuring PIM-SM Advanced Options (Optional) • 121
Configuring PIM-SM Bootstrap and Rendezvous Point Settings • 124
Configuring Policy Based Routing - CLI • 115
Configuring Policy Based Routing - WebUI • 113
Configuring Protocol Rank - CLI (protocol-rank) • 99
Configuring Protocol Rank - WebUI • 99
Configuring RIP - CLI (rip) • 50
Configuring RIP - WebUI • 48
Configuring Route Aggregation - CLI (aggregate) • 75
Configuring Route Aggregation - WebUI • 73
Configuring Route Maps - CLI (routemap) • 88
Configuring Route Redistribution - WebUI • 81
Configuring Router Discovery - CLI (rdisc) • 111
Configuring Router Discovery - WebUI • 109
Configuring Wait for clustering - CLI (router-options) • 100
Configuring Wait for Clustering - WebUI • 100

D

Default Ranks • 98
Dense Mode • 118
DHCP Relay • 8
Disabling PIM • 121

E

EBGP Multihop Support • 16
Equal Cost Path Splitting • 97
Example 1 • 95
Example 2 • 95
Example 3 • 95
External BGP • 26

F

Fine Tuning Policies • 80
Forwarding Non-Local Packets • 45

G

Global Trace options • 102

H

High Availability Support for OSPF • 55
How Router Discovery Works • 109

I

ICMP Router Discovery Interfaces • 111
ICMP Router Discovery Show Commands • 112
ICMP Trace Commands • 103
IGMP • 39
IGMP Trace Options • 103
IGMP Version 3 • 39
Important Information • vi
Inbound BGP Route Filters • 14
Internal BGP • 33
Introduction to Gaia Advanced Routing • 7
IP Broadcast Helper • 44
IP Broadcast Helper interfaces • 45
IP Broadcast Helper Trace Options • 104
K
Kernel Options - Kernel Routes • 98
Kernel Trace Options • 104

M
MFC Trace Options • 105
Monitoring and Troubleshooting PIM • 135
Monitoring IGMP (show igmp) • 43
Monitoring IP Broadcast Helper • 45
Monitoring Policy Based Routing • 117
Monitoring RIP • 53
Monitoring RIP - WebUI • 53
Monitoring Routes - CLI (show route) • 139
Monitoring Routes - WebUI • 139
Monitoring the Multicast Forwarding Cache - CLI (show mfc) • 141
Monitoring the Routing Daemon - CLI (show routed) • 140

N
Network Mask • 47, 48

O
OSPF • 54
OSPF Areas • 68
OSPF Global Settings • 63
OSPF Interfaces • 64
OSPF Show Commands • 69
OSPF Trace Options • 106
OSPF Virtual Links • 66
OSPFv2 • 94

P
PIM • 118
PIM Advanced Options - Assert Ranks • 123
PIM Advanced Options - General Timers • 122
PIM Advanced Options - Shortest First Path Threshold - Add Multicast Group • 124
PIM Advanced Options - Sparse Mode Timers • 124
PIM Advanced Options - State Refresh Parameters (DM) • 123
PIM Bootstrap Settings • 125
PIM Candidate Rendezvous Point • 126
PIM Dense Mode State Refresh • 119
PIM Global Settings • 120, 127
PIM Interfaces • 120, 127
PIM Show and MFC Commands • 136
PIM Sparse Mode • 128
PIM Static Rendezvous Point • 126
PIM Trace Options • 106, 135
Policy Based Routing • 113
Policy Rule Parameters • 115
Preventing Private AS Numbers from Propagating • 12
Protocol Rank • 98

R
Redistributing Routes to BGP • 14
Redistributing Static, Interface, or Aggregate Routes • 95
RIP • 47, 93
RIP 1 • 48