Configuration — IPv4 Multicast Routing Avaya Secure Router 2330/4134

Release 10.3.5
NN47263-504
Issue 04.02
July 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise,

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides information you need to configure IPv4 multicast routing.

Related Resources

Documentation

See the *Avaya Secure Router 2330/4134 Documentation Roadmap*, NN47263-103, for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following sections detail what is new in *Avaya Secure Router 2330/4134 Configuration — IPv4 Multicast Routing,* (NN47263-504) for Release 10.3.5.

Features

There is no new feature content added to *Avaya Secure Router 2330/4134 Configuration — IPv4 Multicast Routing,* (NN47263-504) for Release 10.3.5.

Other changes

Multicast traffic forwarding for PIM-SSM

A clarification is provided in PIM-SSM architecture on page 34 noting that you must add a static route when the source IP address is not in the same subnet as the IP address of the interface.

Chapter 3: Multicast routing fundamentals

IP Multicast extends the benefits of Layer 2 multicasting on LANs to WANs. Multicasting techniques are used on LANs primarily to help clients and servers to find each other. IP Multicast enables a source to send information to multiple destinations in a WAN with a single transmission. The source enjoys considerable efficiencies while a significant amount of bandwidth can be saved.

This section discusses the following topics and includes IP Multicast protocols that the Avaya Secure Router 2330/4134 supports:

- Distance Vector Multicast Routing Protocol (DVMRP)
- Protocol Independent Multicast-Sparse Mode (PIM-SM)
- Internet Group Management Protocol (IGMP)

Overview of IP Multicast

IP Multicast transmits messages to multiple recipients at the same time. This one-to-many delivery mechanism is similar to broadcasting, except that multicasting transmits to specific groups and broadcasting transmits to everybody. Since IP Multicast transmits only one stream of data to the network where it is replicated to many receivers, multicasting saves a considerable amount of bandwidth.

IP Multicast provides services such as the delivery of information to multiple destinations with a single transmission, and the solicitation of servers by clients. IP Multicast services benefit applications such as video conferencing, dissemination of datagram information, and dissemination of mail or news to a large number of recipients.

Multicast protocols use different techniques to discover delivery paths.

A Distribution Tree is a set of multicast routers and subnetworks that allow the members of the group to receive traffic from a source. The source of the tree depends on the algorithm used by the multicast protocol. Figure 1: Multicast distribution tree and broadcasting on page 14 is an example of a simple distribution tree where S is the multicast source and the arrows indicate the multicast broadcast procedure.

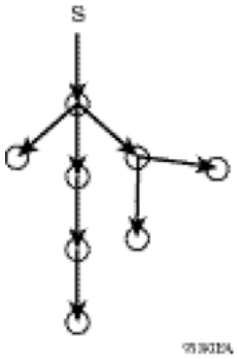

Figure 1: Multicast distribution tree and broadcasting

Broadcast and prune are methods to use multicast traffic to build the distribution tree. Periodically, data is sent out or broadcast from the source to the extremities of the internetwork to search for active group members. If there are no local members of the group, the router sends a message to the host, removing itself from the distribution tree, and thus pruning the router.

Figure 2: Pruning routers from a distribution tree on page 14 illustrates how routers are pruned from the distribution tree. First, a message is sent to the source, after which the pruned routers do not receive multicast data.

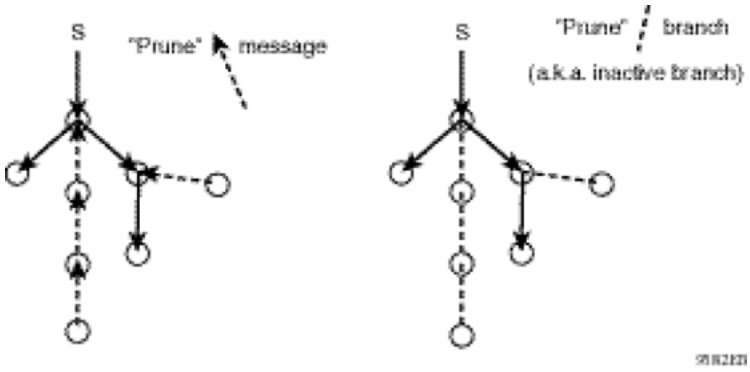

Figure 2: Pruning routers from a distribution tree

Reverse path multicast is based on the concept that a multicast distribution tree is built on the shortest path from the source to each (sub) network containing active receivers. When a datagram arrives on an interface, the router determines the reverse path to the source of the datagram by examining the routing table of known network sources. If the datagram is not on the optimal delivery tree, it is discarded.

Multicast host groups and their group members enable the IP Multicast router to transmit just to those groups interested in receiving the traffic. The Avaya Secure Router 2330/4134uses the Internet Group Membership Protocol (IGMP) to learn the existence of host group members on their directly attached subnets. A router communicates with the hosts on a local network by sending IGMP queries. Hosts respond by issuing IGMP reports. For more information about host groups, see Multicast host groups on page 15 and Multicast addresses on page 15. For more information about IGMP, see Internet Group Management Protocol on page 16.

Multicast traffic forwarding transmits frames to all interfaces/subnets from which IGMP reports are received for the multicast group indicated in the destination IP address. Packets are not

forwarded to networks which do not have members of the multicast group indicated in the destination IP address.

Multicast host groups

IP Multicast is a method for addressing, routing, and delivering a datagram to a collection of receivers called a host group.

Host groups can be permanent or transient, with the following characteristics:

- A permanent host group has a well-known, administratively-assigned IP Multicast group address. This address is permanent and defines the group. A permanent host group can consist of zero or more members.
- A transient host group exists only as long as it has members that need its services. IP addresses in the multicast range that are not reserved for permanent groups are available for dynamic assignment to transient host groups.

Any host system on any IP network can send a message to a multicast group using the IP Multicast address for the group. To receive a message addressed to a multicast group, however, the host must be a member of the group and must reside on a network where that group is registered with a local multicast router.

An IP Multicast host group can consist of zero or more members and places no restrictions on its membership. Host members can reside anywhere; they can join and leave the group at any time; and they can be members of more than one group at the same time.

In general, hosts that are members of the same group reside on different networks. However, a range of multicast addresses (224.0.0.x) is reserved for groups that are locally scoped. All message traffic for these hosts typically remains on the local network. Hosts that belong to a group in this address range and that reside in different networks do not receive message traffic for each other.

Important:

In the Avaya Secure Router 2330/4134, a special set of filters (global filters) can be applied to multicast packets. The user can create deny filters to configure the sources that can receive and send data.

Multicast addresses

Each host group is assigned a unique multicast address. To reach all members of the group, a sender uses the multicast address as the destination address of the datagram.

An IP version 4 multicast address is a Class D address (the high-order bits are set to 1110) from 224.0.1.0 to 239.255.255.255. These addresses are assigned statically for use by permanent groups and dynamically for use by transient groups.

The block of addresses from 224.0.0.1 to 224.0.0.255 is reserved for routing protocols and other low-level protocols. Multicast routers do not forward datagrams with addresses in this range because the time-to-live (TTL) value for the packet is usually set to 1.

Multicast protocols

This section describes several protocols you can use to enable multicasting on an Avaya Secure Router 2330/4134. These include:

- IP Multicast routers that use Internet Group Management Protocol (IGMP) to learn the existence of host group members on directly attached subnets.
- Distance Vector Multicast Routing Protocol (DVMRP) that is a dense-mode protocol suitable for implementation in networks that are densely populated by receivers.
- Protocol Independent Multicast (PIM)
  - Sparse Mode (PIM-SM) protocol is suitable for implementation on networks that are sparsely populated by receivers.
  - Source Specific Multicast (SSM) protocol uses a one-to-many model where members can only receive traffic from a single source. This is suitable for TV channels and other content-distribution applications.

Internet Group Management Protocol

Internet Group Management Protocol (IGMP) has the following characteristics:

- IGMP allows a host to register group memberships with the local querier router to receive any datagrams sent to this router which are targeted to a group with a specific IP Multicast address.
- IGMP allows a router to learn the existence of group members on networks to which it is directly attached. The router periodically sends a general query message to each of its local networks. Any host that is a member of any multicasting group identifies itself by sending a response.

IGMP is a protocol used by IP Multicast routers to learn the existence of host group members on their directly attached subnets. It allows hosts to communicate their desired group memberships to their local querier router, and to receive any datagrams sent to this router which are targeted to a group with a specific IP Multicast address. A router communicates with the hosts on a local network by sending IGMP queries. Hosts respond by issuing IGMP reports.

IGMP queries

When there are multiple IGMP routers on a network, one router is elected to send queries. This elected querier periodically sends host membership queries (also known as general

queries) to its attached local subnets. The Avaya Secure Router 2330/4134 supports queries from all three versions of IGMP.

IGMP host reports

A host that receives a membership query from a local router can respond with a host membership report, one for each multicast group that it joins. A host that receives a query delays its reply by a random interval and listens for a reply from any other host in the same host group. For example, consider a network that includes two host members—host A and host B—of the same multicast group. The router sends out a host membership query on the local network. Both host A and host B receive the query and listen on the network for a host membership report. The delay timer for Host B expires first, so it responds to the query with a membership report. Hearing the response, host A does not send a report of its own for the same group.

Each query from a router to a host includes a Maximum Response Time field. IGMP inserts a value n into this field specifying the maximum time in tenths of a second within which the host must issue a reply. The host uses this value to calculate a random value between 1 and 240 seconds for the period that it waits before sending a response. By default, this field is set to 10 seconds.

If at least one host on the local network specifies that it is a member of a given group, the router forwards to that network all datagrams bearing the multicast address for the group.

Upon initialization, the host can immediately issue a report for each of its supported multicast groups. The router accepts and processes these asynchronous reports the same way as requested reports.

After hosts and routers are in a steady state, they communicate in a way that minimizes the exchange of queries and reports. The designated routers set up a path between the IP Multicast stream source and the end stations and periodically query the end stations about whether or not to continue participation. As long as any client continues to participate, all clients, including nonparticipating end stations on the router port, receive the IP Multicast stream.

Host leave messages

When an IGMP version 2 host leaves a group, it issues a leave group message. The multicast router on the network then issues a group-specific query to determine whether there are other group members on the network. If no host responds to the query, the router assumes that no members belonging to that group exist on that interface and removes the interface from the multicast stream.

Fast leave feature

The Avaya Secure Router 2330/4134 supports a fast leave feature that is useful for multicast-based TV distribution applications. Fast leave relies on an alternative leave process where the router stops sending traffic for the group immediately after receiving a leave message, without issuing a query to check if other group members are present on the network. Fast leave alleviates the network from additional bandwidth demand when changing TV channels. This feature is useful in cases when no more than one host interested in the multicast traffic is present on the network segment.

Fast leave mode

The Avaya Secure Router 2330/4134 provides several fast leave processes for IP Multicast:

- Immediate leave
- Standard IGMP leave based on a Last Member Query Interval (LMQI), which is configurable in seconds

Fast leave modifies the IGMP leave processing mechanism on an IGMP interface. After receiving an IGMP leave on a fast leave-enabled interface, the router does not send a group-specific query and immediately stops sending traffic to the leaving member (IGMP host) port. Without fast leave, traffic is forwarded until the group-specific query times out. This wastes bandwidth if there is no receiver interested in the group traffic.

Fast leave mode applies to all fast leave-enabled IGMP interfaces.

IGMP snoop

The Avaya Secure Router 2330/4134 also provides IP Multicast capability when used as a switch. Functioning as a switch, it supports versions 1 and 2 of IGMP to prune group membership per port within a VLAN. This feature is called IGMP snoop.

Important:

IGMP snoop can optimize only local multicast data flow. IGMP snooping is not responsible for the forwarding state of the multicast tree. You cannot configure a port as a static receiver in an IGMP snoop-enabled VLAN that does not contain at least one dynamic receiver port and have multicast data forwarded.

The IGMP snoop feature allows you to optimize the multicast data flow, for a group within a VLAN, to only those ports that are members of the group. The switch builds a database of group members by listening to IGMP reports from each port. It suppresses the reports heard by not forwarding them to ports other than the one receiving the report, thus forcing the members to continuously send their own reports. The switch relays group membership from

the hosts to the multicast routers. It forwards queries from multicast routers to all port members of the VLAN. Furthermore, it forwards multicast data only to the participating group members and to the multicast routers within the VLAN.

Avaya Secure Router 2330/4134 implementation of IGMP

You can enable and disable multicast routing on an interface basis. If you disable multicast routing on an interface, IGMP queries are not generated.

IGMP snooping does not support the learning of mrouter ports using Multicast Extensions for OSPF (MOSPF).

IGMP proxy

If an Avaya Secure Router 2330/4134 receives multiple reports for the same multicast group, it does not transmit each report to the multicast upstream router. Instead, the switch consolidates the reports into a single report and forwards it. If there is new information that another multicast group has been added or that a query has been received since the last report was transmitted upstream, the report is forwarded onto the multicast router ports. This feature is known as IGMP proxy and is only available for ports in switching mode.

For more information on IGMP proxy configuration, see *Avaya Secure Router 2330/4134 Configuration—Layer 2 Ethernet, NN47263-501*.

IGMP versions

The Avaya Secure Router 2330/4134 supports IGMPv1, IGMPv2, and IGMPv3. All versions of IGMP are backward compatible and can exist together on a multicast network. The Avaya Secure Router 2330/4134 implementation of IGMPv3 for PIM-SSM is fully backward compatible with IGMPv1 or IGMPv2. The following describes the main purpose for each version:

- IGMPv1 provides the support for IP Multicast routing. IGMPv1 specifies the mechanism for communicating IP Multicast group membership requests from a host to its locally attached routers. For more information, see RFC 1112.
- IGMPv2 extends the features in IGMPv1 by quickly reporting group membership termination to the routing protocol. This feature is important for multicast groups with highly volatile group membership. For more information, see RFC 2236.
- IGMPv3 supports the PIM Source-Specific Multicast (SSM) protocol. IGMPv3 provides the ability for a host to selectively request or filter traffic from individual sources within a multicast group. For more information, see RFC 3376.

Static multicast routing support

Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. Multicast routing protocols use these routes to perform reverse-path forwarding (RPF) checks.

Distance Vector Multicast Routing Protocol

Distance Vector Multicast Routing Protocol (DVMRP) is a distance vector type of multicast routing protocol. It advertises shortest-path routes to multicasting source networks, that is, any network containing hosts that can issue multicast datagrams. In this respect, DVMRP is the opposite of RIP, which advertises all routes to destination networks. Coupled with IGMP, membership for a multicast stream is learned from both the routers and directly attached hosts.

DVMRP constructs a different distribution tree for each source and its destination host group. The distribution tree provides a shortest path between the source and each multicast receiver in the group, based on the number of hops in the path. A tree is constructed on demand, using a broadcast and prune technique, when a source begins to transmit messages to a multicast group.

DVMRP assumes that initially every host on the network is part of the multicast group. The designated router on the source subnet (the router that is selected to handle routing for all hosts on the subnet) begins transmitting a multicast message to all adjacent routers. Each of these routers then selectively forwards the message to downstream routers until the message is eventually passed to all multicast group members.

This section discusses the following topics:

- Reverse path forwarding on page 20
- Pruning and grafting on page 21
- DVMRP concepts and terminology on page 21
- Avaya Secure Router 2330/4134 implementation of DVMRP on page 23

Reverse path forwarding

In the selective forwarding process during the formation of the multicast tree, when a router receives a multicast stream, it checks its DVMRP routing tables to determine the interface that provides the shortest path back to the source. If that is the interface where the multicast stream arrived, the router enters state information to identify the multicast stream and its source in its internal tables, and forwards the multicast message to all adjacent routers except to those on the same interface. If the interface is not the optimal one receiving the multicast stream, the

stream is discarded. This mechanism, called reverse path forwarding, ensures that there are no loops in the tree and that the tree includes the shortest path from the source to all recipients.

Pruning and grafting

Pruning eliminates branches of the distribution tree that do not lead to any multicast group members. The IGMP running between hosts and their immediately neighboring multicast routers is used to maintain group membership data in the routers. When a router determines that no hosts beyond it belong to the multicast group, it sends a prune message to its upstream router. Routers update source and destination group state information in their tables to reflect the branches that are eliminated from the tree, resulting in a minimum multicast tree. If a router later learns of new group memberships from the hosts or downstream routers, it sends a graft message upstream to retract the prune sent earlier.

After the multicast tree is constructed, it is used to transmit multicast messages from the source to multicast members. Each router in the path forwards messages over only those interfaces that lead to group members. Because new members can join the group at any time and these members can depend on one of the pruned branches to receive the transmission, DVMRP periodically reinitiates the construction of the multicast tree.

DVMRP concepts and terminology

DVMRP is a multicasting protocol that provides a mechanism for routers to propagate multicast datagrams in a manner that minimizes the number of excess copies sent to any particular network.

Neighbor connections

In a DVMRP environment, neighbors are multicasting routers that have an interface to the same network.

At startup, a DVMRP multicasting router performs the following tasks:

- initializes its routing table with information on all of its local networks
- learns the existence of its neighbors by sending a probe for all routes on each of its multicast interfaces
- receives reports from its neighbors containing the routing information (including route costs)

Source route advertisements

A source network is any network containing hosts that can issue multicast datagrams. DVMRP advertises shortest-path routes to multicasting source networks. In this respect, DVMRP is the opposite of RIP, which advertises routes to destination networks.

Periodically, each multicasting router issues full or partial routing information on each DVMRP circuit using DVMRP report messages. This routing information represents the cost for the sending router to reach the specified source network. The cost is the sum of the hop metrics along the shortest path to the given source network.

Upon receiving a DVMRP report from another router, DVMRP reexamines its routing table to determine whether the shortest path information needs updating. Specifically, DVMRP looks in the routing table for an entry describing a route to the same source network. If one exists, DVMRP compares the cost of the two routes and stores the route with the lower cost in its routing table.

A router does not send route reports on an interface until it knows (by means of received probes or reports) that it has a neighboring multicast router on that interface. The Avaya Secure Router 2330/4134acknowledges implicit probes from neighboring multicast routers, and it sends probes periodically on the interface.

How DVMRP chooses a route

Each DVMRP interface is configured with a metric that indicates the cost of the hop. A router that receives multiple route reports for the same multicasting source network performs the following tasks:

- compares the cost specified in each route report (based on the metric field)
- stores information from the report with the lowest cost in its routing table

A route metric is the sum of all the interface (hop) metrics from a given route source to a given router. After a next-hop neighbor has been declared for a route, the route updates received from that neighbor for that route take precedence until either the route times out or another router advertises a better metric for that route.

Routing table

Table 1: Parts of a routing table entry on page 23 shows the principal items in a routing table entry.

Table 1: Parts of a routing table entry

Item	Description
Source subnet address and mask	The network address and mask that identify the source for this entry contains multicast routing information.
Upstream neighbor	The address of the upstream neighbor from where multicast datagrams are received.
Interface	The value of the interface index where IP datagrams sent by these sources are received.
Metric	The distance in hops to the source subnet.
Expiration Time	The maximum amount of time (in time ticks) remaining before this entry ages out.

Note that the source subnet and the previous-hop router in the DVMRP routing table are the opposite of the destination subnet and next-hop router in a RIP routing table.

Using this information, the router performs the following tasks:

- receives a multicast datagram and determines whether it has arrived on the interface that is on the shortest path to the source network
- drops the datagram if it has not arrived on the shortest-path interface
- floods the multicast stream to all active, nonpruned, downstream DVMRP neighbors

Shortest-path trees

Route information used by DVMRP is independent of any other routing information used by the router. This routing information creates a shortest-path tree entry in the routing table for the propagation of multicast datagrams.

The shortest-path tree entry indicates the interface that provides the shortest path to the network that is the source of the multicast datagram. A shortest-path tree also indicates those interfaces that are on the shortest path to that source network from a neighboring router.

In IGMP version 2, neighboring routers have the same metric to a given source network. The router with the lower IP address is responsible for propagating multicast traffic originating from that source network onto the network or tunnel that is common to these neighboring routers.

A network is considered a leaf network if it has no dependent downstream neighbors for a source.

Avaya Secure Router 2330/4134 implementation of DVMRP

In an Avaya Secure Router 2330/4134, DVMRP fully supports multiaccess networks. The forwarding entries for the receivers on multiaccess networks are port based rather than network

based. Therefore, on a multiaccess network, only ports interested in the data receive it. That is, IP multicast routing is supported on ports with port-based or IP subnet-based VLANs enabled.

The DVMRP router listens to all IGMP host membership reports even if it is not the designated querier and keeps a local group database of every host membership reporter.

When a multicast stream of UDP packets first enters the router, if DVMRP is enabled for the interface, then it processes these packets as necessary and creates a hardware cache entry to handle subsequent packets in the same stream for the same multicast destination. The packets are discarded if there are no members; otherwise they are forwarded.

The Avaya Secure Router 2330/4134 implementation does not support DVMRP tunneling, however, DVMRP over IP tunnels can be enabled. By doing so, you can tunnel between DVMRP clouds.

Protocol Independent Multicast-Sparse Mode

Protocol Independent Multicast-Sparse Mode (PIM-SM) supports multicast groups spread out across large areas of a company or the Internet. Unlike dense mode protocols, such as DVMRP, that initially flood multicast traffic to all routers over an entire internetwork, PIM-SM sends multicast traffic only to routers that have specifically joined a multicast group. This technique reduces traffic flow over WAN links and overhead costs for processing unwanted multicast packets.

Dense-mode protocols use a flood-and-prune technique, which is efficient where receivers are densely populated. However, for sparsely populated networks, PIM-SM is more efficient because it sends multicast traffic only to those routers that belong to a specific multicast group and that choose to receive the traffic.

PIM-SM is independent of any specific unicast routing protocol, but it does require the presence of a unicast routing protocol, such as RIP or OSPF. PIM-SM uses the information from the unicast routing table to create and maintain multicast trees that enable PIM-enabled routers to communicate.

PIM-SM concepts and terminology

Typically, a PIM-SM network consists of several multipoint data streams, each targeted to a small number of LANs in the internetwork. For example, customers whose networks consist of multiple hosts on different LANs can use PIM-SM to simultaneously access a video data stream, such as a video teleconference, on a different subnet.

Important:

In some cases, PIM stream initialization can take several seconds.

Hosts

A host can be a source, a receiver, or both.

- A source, also known as a sender, sends multicast data to a multicast group.
- A receiver receives multicast data from one or several sources that send data to a multicast group.

PIM-SM domain

PIM-SM operates in a domain of contiguous routers that have PIM-SM enabled. All these routers are configured to operate within a common boundary defined by PIM Multicast Border Routers (PMBRs).

Each PIM-SM domain requires the following routers:

- Designated router (DR)
- Rendezvous-point (RP) router
- Bootstrap router (BSR)

Although a PIM-SM domain can have only one active RP router and one active BSR, you can configure additional routers as candidate RP routers and as candidate BSRs. Candidate routers provide backup protection in case the primary RP or BSR router fails.

Designated router

The designated router (DR) is the router with the highest IP address on a LAN designated to perform the following tasks:

- sends register messages to the rendezvous-point (RP) router on behalf of directly connected sources
- sends join/prune messages to the RP router on behalf of directly connected receivers
- maintains information about the status of the active RP router for local sources in each multicast group

Important:

The DR is not a required configuration, and switches act automatically as such for directly attached sources and receivers.

Rendezvous-Point router

PIM-SM builds a shared multicast distribution tree within each domain, and the rendezvous point (RP) router is at the root of this shared tree. Although the RP can be physically located

anywhere on the network, it must be as close to the source as possible. There is only one active RP router for a multicast group.

At the RP router, receivers meet new sources. Sources use the RP to identify themselves to other routers on the network; receivers use the RP to learn about new sources.

The RP performs the following tasks:

- registers a source that wants to announce itself and send data to group members
- joins a receiver that wants to receive data for the group
- forwards data to the group

Candidate rendezvous-point router

You can configure a set of routers as candidate rendezvous-point (C-RP) routers that serve as backup to the RP router. If an RP fails, all the routers in the domain apply the same algorithm to elect a new RP from the group of C-RPs. To make sure that the routers have a complete list of C-RPs, the C-RP periodically sends unicast advertisement messages to the bootstrap router (BSR). The most common implementation is to configure a PIM-SM router as both a candidate RP and a candidate BSR.

Important:

Although you can configure a candidate RP on a DVMRP interface, no functionality is tied to this configuration.

Static rendezvous point router

You can configure a static entry for a rendezvous point (RP) with static RP. While configuring a PIM static RP in a router, consider that the next-hop of the unicast route towards PIM static RP must be a PIM neighbor. The PIM protocol fails to work if due to a route change the next-hop towards an already configured static RP becomes a non-PIM neighbor. The configured RP does not activate until it can be reached through a PIM neighbor, and its state remains invalid.

Static RP-enabled Avaya Secure Router 2330/4134 can communicate with devices from other vendors that do not use the BSR mechanism. Some vendors use either early implementations of PIM-SM v1 that do not support the BSR or proprietary mechanisms like the Cisco Auto-RP. For a network to work properly with static RP, you must have all the routers in the network (including routers from other vendors) map to the same RP or RPs, if several RPs are present in the network.

To avoid a single point of failure, you can also configure redundant static RPs.

You use the static RP feature when dynamic learning mode is not needed, typically in small networks or for security reasons, where RPs have to be forced to some devices in the network so that they do not learn other RPs.

Static RP configuration considerations

Before you can configure a static RP, you must enable PIM in sparse mode (SM) and enable Static RP.

After meeting these prerequisites, keep in mind the following configuration considerations:

- A static RP-enabled router cannot be configured as a BSR or as a C-RP.
- All dynamically learned BSR information is lost. However, if you disable static RP, the router loses the static RP information and regains the BSR functionality.
- Static RPs do not age, that is, they cannot time out.
- Routers do not advertise static RPs, so, if a new PIM neighbor joins the network, it does not know about the static RP unless it is configured with that static RP.
- Configure all the routers in the network (including routers from other vendors) to map to the same RP.
- In a PIM domain with both static and dynamic RP routers, the static RP routers cannot have one of their (local) interfaces configured as RP.
- To avoid a single point of failure, you can configure redundant static RPs for the same group prefix. If there is a mix of Avaya and other vendor's devices across the network, you must ensure that all switches/routers use the same active RP because other vendors can be using different algorithms to elect the active RP. Avaya Secure Router 2330/4134devices use the hash function defined in the PIM-SM standard to elect the active RP; other vendors can use the lowest IP address to break the tie.

  Important:

  To reduce convergence times, Avaya recommends you create only one static RP per group. The more static RPs you configure for redundancy, the more time PIM requires to rebuild the mroute table and associate RPs.
- Static RP configured on the router is always active. If the route is unreachable, it will still act as the RP, but may cause traffic disruption for any associated groups.

Bootstrap router

The BSR receives RP router advertisement messages from the candidate RPs. The BSR adds the RP router with its group prefix to the RP set. Only one BSR exists for each PIM-SM domain.

The BSR periodically sends bootstrap messages containing the complete RP set to all routers in the domain. The BSR ensures that all PIM-SM routers send join/prune and register packets.

Candidate bootstrap router

Within a PIM-SM domain, you can configure a small set of routers as candidate BSRs (C-BSRs). The candidate BSR with the highest configured priority becomes the BSR for the domain. If two candidate BSRs have equal priority, the candidate with the higher IP address becomes the BSR. If you add a new candidate BSR with a higher priority to the domain, it automatically becomes the new BSR.

Join/prune messages

The DR sends join/prune messages from a receiver toward a RP for the group to either join the shared tree or remove (prune) a branch from it. A single message contains both a join and a prune list. This list includes a set of source addresses indicating the shortest-path trees or the shared trees that the host wants to join. The DR sends join and prune messages hop by hop to each PIM router on the path to the source or the RP.

Register and register-stop messages

The DR sends register messages to the RP for a directly connected source. The register message informs the RP of a new source, causing the RP to send join or prune messages back toward the DR of the source which forwards the data down the RP tree after it gets the data natively. When the receiver DR gets the first packet, it switches to the shortest-path tree (SPT) and continues receiving data through the SPT path.

The DR stops sending encapsulated packets to the RP after receiving a register-stop message. This traffic stops without delay because the RP sends a register-stop message immediately after receiving the first multicast data packet, and joins the shortest-path tree.

Shared trees and shortest-path trees

In a PIM-SM domain, shared trees and shortest-path trees are used to deliver data packets to group members. This section describes both trees.

Shared trees

Group members in a PIM-SM domain receive the first packet of data from sources across a shared tree. A shared tree consists of a set of paths that connect all members of a multicast group to the RP. PIM creates a shared tree when sources and receivers send messages toward the RP.

Shortest-path trees

After receiving a certain number of packets from the RP, the DR switches from a shared tree to a shortest-path tree (SPT). Switching to a shortest-path tree creates a direct route between the receiver and the source. The Avaya Secure Router 2330/4134 switches to the SPT when it receives the first packet from the RP.

Figure 3: Shared tree and shortest-path tree on page 29 shows a shared tree and a shortest-path tree.

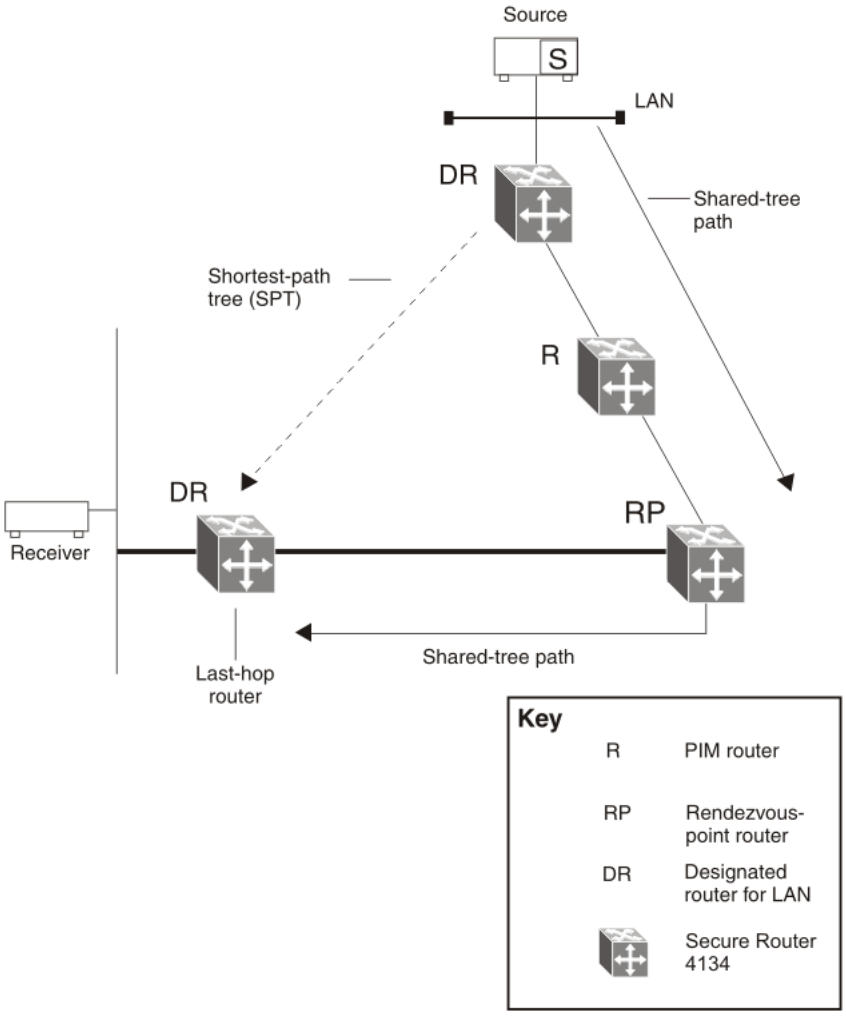

Figure 3: Shared tree and shortest-path tree

Receiver joining group

The following steps describe how a receiver joins a multicast group:

1. A receiver multicasts an IGMP host membership message to the group that it wants to join.
2. When the last-hop router (DR), normally the PIM router with the highest IP address, receives the IGMP message for a new group join, the router looks up the associated elected RP that is responsible for the group.

3. After it determines the RP router for the group, the last-hop router creates a (*,G) route entry in the multicast forwarding table and sends a (*,G) Join message to the RP. When the last-hop router receives data packets from the RP, if the multicast packet arrival rate exceeds the DR threshold, the last-hop router switches to the SPT by sending an (S,G) Join message to the source. (S denotes the source unicast IP address, and G denotes the multicast Group Address.)
4. If the switch to the SPT occurs:
   - All intermediate PIM routers along the path to the source create the (S,G) entry.
   - To trim the shared tree, the router sends an (S,G) Prune message to the RP.

Receiver leaving group

Before it leaves a multicast group, a receiver sends an IGMP leave message to the DR. If all directly connected members of a multicast group leave or time out, and no downstream members remain, the DR sends a prune message upstream and PIM-SM deletes the route entry after that entry times out.

Source sending packets to group

The following steps describe how a source sends multicast packets to a group:

1. A source directly attached to a VLAN bridges the multicast data to the DR. The DR for the VLAN (the router with the highest IP address) encapsulates each packet in a register message and sends a unicast message directly to the RP router to distribute to the multicast group.
2. If a downstream group member chooses to receive multicast traffic, the RP router sends a join/prune message towards the source DR and forwards the data down the RP tree after it gets the data natively.
3. When the receiver DR gets the first packet, it switches to the shortest-path tree (SPT) and continues receiving data through the SPT path.
4. If no downstream members want to receive multicast traffic, the RP router sends a register-stop message (for the source) to the DR.

   The DR starts the register suppression timer when it receives the first register-stop message. During the register suppression timeout period (the default is 60 seconds), the following events occur:

   - The DR for the source sends a probe packet to the RP router before the register suppression timer expires. The probe packet prompts the RP router to determine whether any new downstream receivers have joined the group.

- If no new receivers have joined the group, the RP router sends another register-stop message to the DR for the source, and its register suppression timer restarts.
- When the RP router no longer responds with a register-stop message to the source DR probe message, the register suppression timer expires and the DR sends encapsulated multicast packets to the RP router. The RP router uses this method to tell the DR that new members have joined the group.

The RP sends a register-stop message to the DR immediately after receiving the first multicast data packet.

Required elements for PIM-SM operation

For PIM-SM to operate, a number of elements must be present in the PIM-SM domain including the following:

- An underlying unicast routing protocol must be enabled for the router to provide routing table information to PIM-SM.
- In a PIM-SM domain, an active BSR must be in place to send bootstrap messages to all PIM-V2 configured switches and routers to enable them to learn group-to-RP mapping. If several BSRs are configured in a network, an active BSR is elected based on priority and IP address (if priority is equal, the BSR with the higher IP address is elected).
- An RP must be in place in the PIM-SM domain to perform the following tasks:
  - To manage one or several IP Multicast groups.
  - To become the root for the shared tree to these groups.
  - To accept join messages from receiver switches for groups that it manages.
  - If more than one RP have groups in common, the RPs elect an active RP based on priority and IP address (if priority is equal, the RP with the higher IP address is elected).

PIM-SM simplified example

Figure 4: PIM-SM simplified example on page 32 shows a simplified example of a PIM-SM configuration.

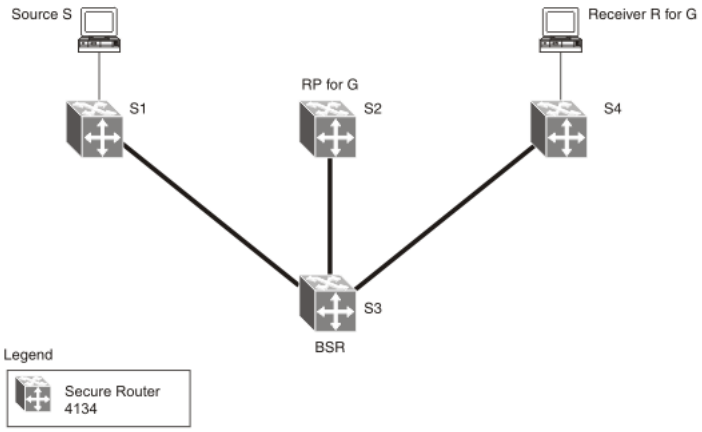

Figure 4: PIM-SM simplified example

In the sample configuration, the following events occur:

1. The BSR distributes RP information to all routers in the network.
2. R sends an IGMP membership report to S4.
3. Acting on this report, S4 sends a (*,G) join message to RP.
4. S sends data to G.
5. The DR (S1 in this example) encapsulates the data that it unicasts to RP (S2) in register messages.
6. S2 decapsulates the data which it forwards to S4.
7. S4 forwards the data to R.
8. If the packet rate exceeds the DR threshold, S4 sends S1 an (S,G) Join message.
9. S1 forwards data to S4. When S4 receives data from S1, it prunes the stream from the RP.

Important:

Figure 4: PIM-SM simplified example on page 32 is a simplified example and is not the best design for a network if the source and receiver are placed as shown. In general, RPs are placed as close as possible to sources.

PIM-SM Multipath

The duplication of packets in multicast is avoided by determining the reverse-path of a source S in a (S, G) entry and the IP address of the rendezvous point of the group G in case of a (*,

G) entry. It also ensures that the packet is not forwarded back on the interface on which it is received. For a source in (S, G) this is done by determining the interface through which a packet is sent with a destination IP address of S. Only if the packet is received on that particular interface, is that packet taken up for further processing.

In IP Multicast Multipath, the RPF interface for each (*, G) or (S, G) state is selected among the available equal cost paths depending on the RPF address to which the state resolves. For an (S, G) state, this is the address “S” of the source. For a (*, G) state, this is the address of the RP associated with the group G of the state. That results in multicast traffic for different states that can be received across more than just one equal-cost interface.

PIM-SM supports the multipath functionality. There are two methods for selecting the next hop if multiple ECMP routes exist:

- round-robin
- hashing

The first method selects the next hop in a round-robin manner, while the latter selects the next hop based on the key calculated using the source address, group address, and next hop address.

Anycast RP for PIM-SM

Anycast RP allows the mapping of a single group to multiple RPs. In Anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. The Anycast RP loopback address can be configured with a 32-bit mask, making it a host address. All the downstream routers can be configured to know that the Anycast RP loopback address is the IP address of their local RP. IP routing automatically selects the topologically-closest RP for each source and receiver.

PIM-SSM

Source Specific Multicast (SSM) optimizes PIM-SM by simplifying the many-to-many model. Since most multicast applications distribute content to a group in one direction, SSM uses a one-to-many model that only uses a subset of the PIM-SM features. This model is more efficient and puts less of a load on multicast routing devices.

SSM only builds source-based shortest path trees. Whereas PIM-SM always joins a shared tree first and then switches to the source tree, SSM eliminates the need for starting with a shared tree by immediately joining a source through the shortest path tree. This method enables SSM to avoid using a rendezvous point (RP) and RP-based shared trees, which can be a potential bottleneck.

Members of a SSM group can only receive from a single source. This is ideal for applications like TV channel distribution and other content-distribution businesses. Banking and trade

applications can also use SSM because it provides more control over the hosts receiving and sending data over their networks.

SSM applications use IP addresses reserved by the Internet Assigned Numbers Authority (IANA) in the 232/8 range (232.0.0.0 to 232.255.255.255). SSM recognizes packets in this range and controls the behavior of multicast routing devices and hosts that use these addresses. When a source S transmits IP datagrams to a SSM destination address G, a receiver can receive these datagrams by subscribing to the (S,G) channel.

A channel is a source-group (S,G) pair where S is the source sending to the multicast group and G is a SSM group address. SSM defines channels on a per-source basis, which enforces the one-to-many concept of SSM applications. In a SSM channel, each group is associated with one and only one source. However, another SSM channel can associate the same multicast group with a different source, which allows an efficient use of the SSM address range. For example, channel (192.1.3.4, 232.1.2.3) is different from channel (141.251.186.13, 232.1.2.3).

SSM features

SSM only uses a subset of the PIM-SM features such as the shortest path tree, designated router (DR), and some messages (Hello, Join/Prune, and Assert). However, there are also some features that are unique to SSM. These features, which are described in the following sections, are extensions of the IGMP and PIM protocols.

PIM requires a unicast protocol in order to forward multicast traffic within the network when performing the Reverse Path Forwarding (RPF) check. PIM-SM uses the information from the unicast routing table to create and maintain the shared and shortest multicast tree that enables PIM-enabled routers to communicate. The unicast routing table must contain a route to every multicast source in the network as well as to routes to PIM entities like the RPs and BSR.

PIM-SSM architecture

Figure 5: PIM-SSM architecture on page 35 illustrates how the PIM-SSM architecture requires routers to:

- support IGMPv3 source-specific host membership reports and queries at the edge routers
- initiate PIM-SSM (S,G) joins directly and immediately after receiving an IGMPv3 join report from the designated router
- restrict forwarding to shortest-path trees within the SSM address range by all PIM-SSM routers

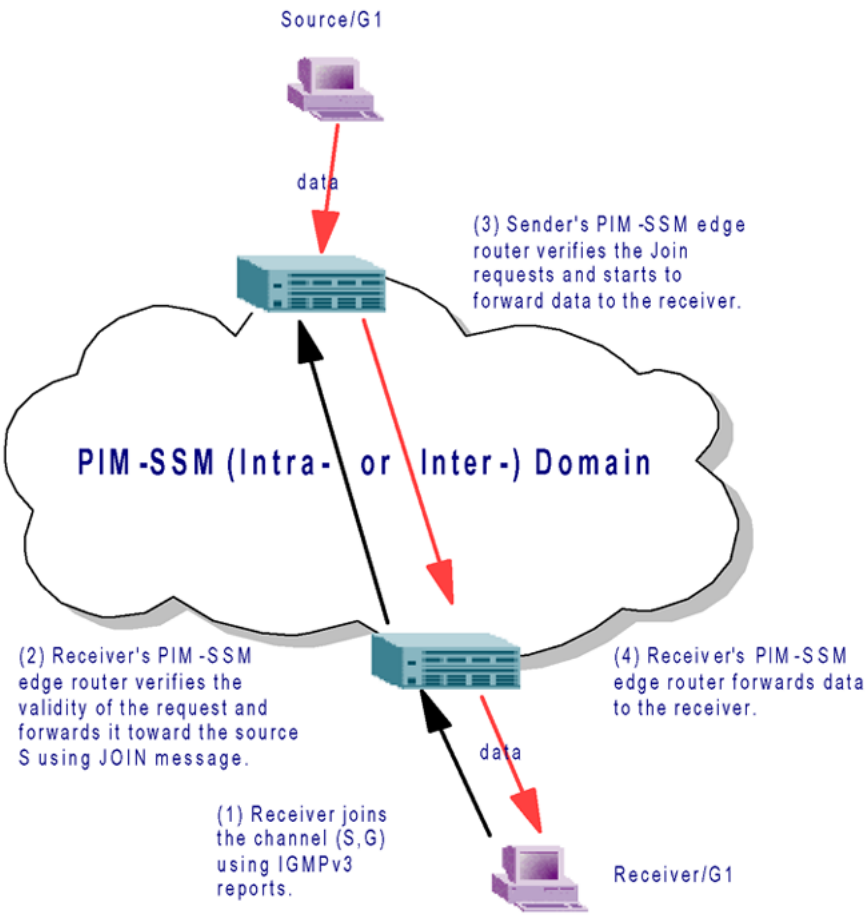

Figure 5: PIM-SSM architecture

The following rules apply to Layer 3 devices with SSM enabled:

- Receive IGMPv3 membership join reports in the SSM range and, if there is no entry (S,G) in the SSM channel table, creates one.
- Receive IGMPv2 membership join reports, but only for groups that already have a static (S,G) entry in the SSM channel table.
- Send periodic join messages to maintain a steady SSM tree state.
- Use standard PIM-SM SPT procedures for unicast routing changes, but ignore any rules associated with the SPT-bit for the (S,G) route entry.
- Receive prune messages and use standard PIM-SM procedures to remove interfaces from the source tree.
- Forward data packets to interfaces from the downstream neighbors that have sent an SSM join, or to interfaces with locally attached SSM group members.
- Drop data packets that do not have an exact-match lookup (S,G) in their forwarding database for S and G.
- When the source IP address is not in the same subnet as the IP address of the interface (Secure Router) connected to the source subnet, you must add a static route to the

interface, where the source-address/mask is set to the source subnet. Otherwise, the router cannot resolve a next-hop for RPF to this address.

Avaya Secure Router 2330/4134 implementation of SSM and IGMP

The following sections describe how PIM-SSM and IGMP are implemented in the Avaya Secure Router 2330/4134.

SSM range

The standard SSM range is 232/8, but you can extend the range to include any IP Multicast address with the Avaya Secure Router 2330/4134 implementation of SSM. Although you can configure the SSM range, configuring it for all multicast groups (224/4 or 224.0.0.0/240.0.0.0 or 224.0.0.0/255.0.0.0) is not allowed.

You can extend the SSM range to configure existing applications without changing their group configurations. This flexibility allows applications to take immediate advantage of SSM.

SSM and IGMPv2

SSM-configured devices can accept reports from IGMPv2 hosts on IGMPv2 interfaces if the group has a SSM channel table entry. However, the IGMPv2 host groups must be in the SSM range defined on the router, which is 232/8 by default.

- When the SSM router receives an IGMPv2 report for a group that is in the SSM channel table, it joins the specified source immediately.
- When the SSM router receives an IGMPv2 report for a group that has an enabled static SSM channel table entry, it triggers PIM-SSM processing as if it had received an equivalent IGMPv3 report.
- When the SSM router receives an IGMPv2 report for a group out of the SSM range, it processes the report as if it is in PIM-SM mode.

Configuration limitations

Avaya recommends running PIM-SSM on either all the routers in the domain or only on the edge routers. If there is a mix of PIM-SSM and PIM-SM routers in the domain, run PIM-SSM on all the edge routers and PIM-SM on all the core routers.

Important:

A PIM domain with edge routers running PIM-SM and core routers running PIM-SSM does not work properly.

SSM routers running IGMPv3 drop any reports that they receive out of the SSM range. The SSM router does not forward them to a PIM-SM router.

Static source groups cannot conflict with SSM channels and vice versa. When you configure a static source group or a SSM channel, the router performs a consistency check to make sure there are no conflicts. You cannot map one group (G) to different sources for both a static source group and a SSM channel.

PIM passive interfaces

You can specify whether you want a PIM interface to be active or passive. The default is active. With an active interface, you can configure transmit and receive PIM control traffic. A passive interface drops all PIM control traffic, thereby reducing the load on the system. This feature is useful when you have a high number of PIM interfaces and these interfaces are connected to end-users, not to other routers.

A PIM interface that is configured as passive does not transmit and drops any messages of the following type:

- Hello
- Join/Prune
- Register (see Note below)
- Register-Stop (see Note below)
- Assert
- Candidate-RP-Advertisement
- Bootstrap

If a PIM passive interface receives any of these types of messages, it drops them. These log messages help to identify the device that is performing routing on the interface, which is useful if you must disable a device that is not operating correctly.

Important:

A device can send Register and Register-Stop messages to a PIM passive interface, but these messages cannot be sent out of that interface.

The PIM passive interface maintains information about hosts, through the IGMP protocol, that are related to senders and receivers, but the interface does not maintain information about any PIM neighbors. You can configure a bootstrap router (BSR) or a rendezvous point (RP) on a PIM passive interface.

You can also use the PIM passive interface feature as a security measure to prevent routing devices from becoming attached and participating in the multicast routing of the network.

Important:

Before you change the state (active or passive) of a PIM interface, disable PIM on that interface. This prevents any instability in the PIM operations, especially when neighbors are present or streams are received.

Multicast routing over VLAN

With Release 10.2 and later, you can enable multicast routing on VLAN interfaces.

Features supported under multicast routing tree

The following table lists the features that are supported under multicast routing tree on Avaya Secure Router 2330/4134 Release 10.3.5.

Feature Name	Comments
IGMP	
Configurable support for version 1,2 or 3	
Backward compatibility support for older version of hosts and routers	
Fast leave support	
Access-list for groups	
Static group support	
Static SSM mapping support	
IGMP-MIB support (draft-ietf-magma-mgmd-mib-11.txt)	
IGMP Snoop	
Support for IGMP version 1 or 2	
Static mrouter port configuration per vlan	
Snooping Querier	
IGMP report suppression	
Dynamic learning of mrouter port from DVMRP or PIM control packets	
Supported only on VLAN interfaces.	

Feature Name	Comments
IGMP Proxy Supported only on ports in switching mode.	
DVMRP	
Version 3 mode of operations with backward compatibility with versions 1 and 2	
Interoperability with Cisco (non-standard) DVMRP implementation	
Configuration option for peering with non-prune/graft implementations	
PIM-SM	
Sparse mode operation as per draft specification (draft-ietf-pim-sm-v2-new-05)	
Source Specific Multicast with configurable range	
Bootstrap Router protocol support	
Static RP configuration	
Neighbor filter	
Access-list for filtering PIM Registers at RP	
Anycast-RP configuration	
Embedded-RP configuration	
Multipath configuration	
PIM-SM MIB support (RFC 5060)	
Multicast Forwarding Features	
Configurable TTL threshold per interface	
IP Multicast MIB support (RFC 5132)	
Supported Interface Types	
Ethernet, VLAN	
WAN bundles – PPP, ML-PPP, FR, ML-FR, HDLC	
IP-IP, GRE and IPSEC Tunnels	Operates over tunnels that are of a point-to-point nature only.
Configuration & Management	

Feature Name	Comments
Supports CLI for configuration, operational and debug commands	
Supports SNMP for configuration and operational commands	

Chapter 4: Multicast routing procedures

Enabling multicast routing

This procedures details the steps necessary to enable multicast routing on the Avaya Secure Router 2330/4134. Use the **no** form of this command to disable.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. In configuration mode, enter the command to enable multicast routing.

   ```
   [no] ip multicast-routing
   ```

Configuring multicast time-to-live

This procedure details the steps necessary to configure the minimum permissible time-to-live threshold value of packets being forwarded out of an interface. Use the **no** form of this command to return to the default threshold (0).

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to configure multicast time-to-live.

   ```
   [no] ip multicast ttl-threshold <ttl-value>
   ```

Table 2: Variable definition

Variable	Value
<ttl-value>	The time-to-live threshold. Valid range is 1–255.

Example of configuring multicast time-to-live

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. In Interface mode, enter the command to configure multicast time-to-live.

   ```
   ip multicast ttl-threshold 30
   ```

Configuring a multicast static route

Perform the following procedure to configure a multicast static route. Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. Multicast routing protocols use these routes to perform reverse-path forwarding (RPF) checks. By default, no multicast static routes are configured.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure a multicast static route:

   ```
   [no] ip mroute <source-prefix/mask> [<RPF-addr> | <RPF-
   ifname>] [<distance>]
   ```

Table 3: Variable definitions

Variable	Value
no	Removes the configure multicast static route.
<source-prefix/mask>	Specifies the multicast source IP prefix (A.B.C.D) and address mask length (0–32).
<RPF-addr>	Specifies the RPF neighbor address (A.B.C.D) for the multicast route. The host IP address can be a directly connected system or a remote system. When it is a remote system, a recursive lookup is done from the unicast routing table to find a directly connected system; the recursive lookup is done up to only one level.

Variable	Value
<RPF-ifname>	Specifies the incoming interface name. The interface can only be specified for nonbroadcast interfaces.
<distance>	Specifies a distance for the multicast route, which determines whether a unicast route or multicast static route is used for the RPF lookup. Lower distances take precedence. If the multicast static route has the same distance as other RPF sources, the multicast static route takes precedence. Default is 1. Range is 1–255.

Clearing multicast forwarding entries

Perform the following procedure to clear configured multicast forwarding entries. When you perform this procedure, the MRIB clears the multicast route entries in its multicast route table, and removes the entries from the multicast forwarder.

Procedure steps

Enter the following command to clear multicast forwarding entries:

```
clear ip mroute {all | <group-addr> [<source-addr>]}
```

Table 4: Variable definitions

Variable	Value
all	Deletes routes for all multicast groups.
<group-addr>	Specifies the group IP address of the forwarding entries to clear.
[<source-addr>]	Specifies the source IP address of the forwarding entries to clear.

Example of clearing multicast routing table entries

1. To delete all multicast routing table entries, enter:

   ```
   clear ip mroute all
   ```

2. To delete multicast entries by group, enter:

   ```
   clear ip mroute <group-adr>
   ```

Configuring multicast lookup in MRIB only

Perform the following procedure to configure the router to perform IP multicast lookups in the MRIB only. If this feature is not enabled, multicast route lookup is done in the URIB as well as in the MRIB. By default, this feature is disabled.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the multicast lookup in MRIB-only feature:

   ```
   [no] ip multicast-lookup-mrib-only
   ```

Table 5: Variable definitions

Variable	Value
[no]	Disables the multicast lookup in MRIB-only feature.

Displaying multicast interface information

This procedure describes how to display multicast interface information.

Procedure steps

To display multicast interface information, enter:

```
show ip mvif
```

Displaying the IP multicast routing table

This procedure describes how to display the IP multicast routing table.

Procedure steps

1. To display the multicast routing table in summary form, enter:

   ```
   show ip mroute summary
   ```

2. To display the multicast routing table entries for a specific source or group, enter

```
show ip mroute <address>
```

Table 6: Variable definition

Variable	Value
<address>	The source or group IP address.

Example of displaying the IP multicast routing table

To display the multicast routing table entries for a specific source or group, enter

```
show ip mroute 10.10.10.1
```

Chapter 5: DVMRP procedures

Enabling DVMRP

This procedure details the steps necessary to enable DVMRP on the current interface. Use the **no** form of this command to disable.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to enable DVMRP.

   ```
   [no] ip dvmrp enable
   ```

Assigning a metric value

This procedure details the steps necessary to assign a metric value to the current interface. Use the **no** form of this command to return to the default metric (1).

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to assign a metric value.

   ```
   [no] ip dvmrp metric <metric-value>
   ```

Table 7: Variable definition

Variable	Value
<metric-value>	Metric value for the interface. Valid range is 1–31.

Example of assigning a metric value

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to assign a metric value.

   ```
   ip dvmrp metric 10
   ```

Configuring route report burst interval

This procedure details the steps necessary to configure the DVMRP route report burst interval (in seconds) and to specify number of packets in a route report burst. Use the **no** form of this command to disable output-report-delay configuration on the interface.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to set the burst interval.

   ```
   [no] ip dvmrp output-report-delay <delay> [<num-reports>]
   ```

Table 8: Variable definition

Variable	Value
<delay>	The burst interval in seconds. Valid range is 1–5.
<num-reports>	Number of back-to-back reports sent after delay. Valid range is 1–65535.

Example of configuring route report burst interval

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to set the burst interval.

   ```
   ip dvmrp output-report-delay 5 2000
   ```

Rejecting non-pruners

This procedure details the steps necessary to configure the router such that it does not peer with a DVMRP neighbor that does not support pruning or grafting. Use the **no** form of this command to reverse the behavior and enable peering.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to reject non-pruners.

   ```
   [no] ip dvmrp reject-non-pruners
   ```

Configuring the global MFC timeout

Perform the following procedure to configure the timeout for negative entries in the multicast forwarding cache (MFC).

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the MFC timeout:

```
[no] ip dvmrp mfc-timeout <mfc-timeout>
```

Table 9: Variable definitions

Variable	Value
[no]	Resets the MFC timeout to the default value (2 minutes).
<mfc-timeout>	Specifies the MFC timeout. Range is 2–120 minutes.

Configuring neighbor change logging

Perform the following procedure to enable logging of the DVMRP neighbor changes to the console. By default, neighbor change logging is enabled.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure neighbor change logging:

   ```
   [no] ip dvmrp log-neighbor-changes
   ```

Table 10: Variable definitions

Variable	Value
[no]	Disables neighbor change logging value (2 minutes).

Configuring the global triggered updates interval

Perform the following procedure to specify the minimum amount of time between triggered DVMRP updates. The default value is 5 seconds.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the triggered updates interval:

```
[no] ip dvmrp triggered-update-interval <triggered-update-
interval>
```

Table 11: Variable definitions

Variable	Value
[no]	Resets the triggered update interval to the default value: 5 seconds.
<triggered-update-interval>	Specifies the triggered update interval. Range is 5–1000 seconds.

Configuring the status of the DVMRP holddown timer

Perform the following procedure to disable or reenable the DVMRP holddown timer. During the holddown period, the deleted route is advertised as unreachable, and all forwarding cache entries based on the route are flushed. If you disable the holddown timer, it does not affect timers that are already running. By default, the holddown timer is enabled.

If you enable the holddown timer for deleted routes, configure the full update interval to one half of the difference between the unconfirmed (garbage) route timeout value and the route expiration timeout value. The default values for these timer parameters comply with this requirement as follows:

Full update interval (60) * 2 = 120

Unconfirmed route timer – route expiration timer (260 – 140) = 120

If you enable the holddown timer and reset the full update timer, you are required to reset the route expiration timer and the unconfirmed route timer.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the status of the DVMRP holddown timer:

   ```
   [no] ip dvmrp holddown disable
   ```

Table 12: Variable definitions

Variable	Value
[no]	Reenables the DVMRP holddown timer.

Configuring the DVMRP route expiration timeout

Perform the following procedure to configure how long DVMRP waits for an update message indicating that a route is reachable. The default value is 140 seconds.

If the holddown timer is enabled and you change the value of the route expiration timer, then also change the value of the unconfirmed route timer accordingly.

If you enable the holddown timer for deleted routes, configure the full update interval to one half of the difference between the unconfirmed (garbage) route timeout value and the route expiration timeout value. The default values for these timer parameters comply with this requirement as follows:

Full update interval (60) * 2 = 120

Unconfirmed route timer – route expiration timer (260 – 140) = 120

If you enable the holddown timer and reset the full update timer, you must reset the route expiration timer and the unconfirmed route timer.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the DVMRP route expiration timeout:

   ```
   [no] ip dvmrp route-expiration-timeout <route-expiration-timeout>
   ```

Table 13: Variable definitions

Variable	Value
[no]	Resets to the default value: 140 seconds.
<route-expiration-timeout>	Specifies the route expiration timeout. Range is 21-4001 seconds.

Configuring the global DVMRP unconfirmed route timeout

Perform the following procedure to configure how long DVMRP advertises a route as unreachable before it removes the route from the routing table. The default value is 260 seconds.

If the holddown timer is enabled and you change the value of the unconfirmed route timer, then also change the value of the route expiration timer accordingly.

If you enable the holddown timer for deleted routes, configure the full update interval to one half of the difference between the unconfirmed (garbage) route timeout value and the route

expiration timeout value. The default values for these timer parameters comply with this requirement as follows:

Full update interval (60) * 2 = 120

Unconfirmed route timer – route expiration timer (260 – 140) = 120

If you enable the holddown timer and reset the full update timer, you must reset the route expiration timer and the unconfirmed route timer.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the DVMRP unconfirmed route timeout:

   ```
   [no] ip dvmrp unconfirmed-route-timeout <unconfirmed-route-timeout>
   ```

Table 14: Variable definitions

Variable	Value
[no]	Resets the unconfirmed route timeout to the default value: 260 seconds.
<unconfirmed-route-timeout>	Specifies the unconfirmed route timeout value. Range is 41–81001 seconds.

Configuring the global DVMRP neighbor timeout

Perform the following procedure to configure how long the router waits to receive a report from a neighbor before considering the connection inactive, if the neighbor is learned by report messages. The default value is 190 seconds.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the DVMRP neighbor timeout:

   ```
   [no] ip dvmrp neighbor-timeout <neighbor-timeout>
   ```

Table 15: Variable definitions

Variable	Value
[no]	Resets the DVMRP neighor timeout to the default value: 190 seconds.

Variable	Value
<neighbor-timeout>	Specifies the DVMRP neighbor timeout value. Range is 35–8000 seconds.

Configuring the global DVMRP neighbor probe interval

Perform the following procedure to configure how often DVMRP sends a probe on interfaces from which no neighbors have been heard. The default value is 10 seconds.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the DVMRP neighbor probe interval:

   ```
   [no] ip dvmrp neighbor-probe-interval <neighbor-probe-interval>
   ```

Table 16: Variable definitions

Variable	Value
[no]	Resets the DVMRP neighbor probe interval to the default value: 10 seconds.
<neighbor-probe-interval>	Specifies the DVMRP neighbor probe interval. Range is 5–30 seconds.

Configuring the global DVMRP switch timeout

Perform the following procedure to configure how long the router waits, without receiving a subsequent route update from the original neighbor, before switching to a different neighbor advertising equal cost for this route. The default value is 140 seconds.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the DVMRP switch timeout:

   ```
   [no] ip dvmrp switch-timeout <switch-timeout>
   ```

Table 17: Variable definitions

Variable	Value
[no]	Resets the DVMRP switch timeout to the default value: 140 seconds.
<switch-timeout>	Specifies the DVMRP switch timeout value. Range is 20–2000 seconds.

Configuring DVMRP default route advertisement on an interface

Perform the following procedure to advertise a default route (0.0.0.0) on this interface. By default, default route advertisement is disabled.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to specify the interface to configure:

   ```
   interface <if-name>
   ```

3. Enter the following command to configure default route advertisement:

   ```
   [no] ip dvmrp default-supply
   ```

Table 18: Variable definitions

Variable	Value
<if-name>	Specifies the interface to configure.
[no]	Disables default route advertisement on the interface.

Configuring DVMRP default route listening on an interface

Perform the following procedure to configure whether the router accepts default routes on this interface. By default, default route listening is disabled.

Procedure steps

1. Enter the following command for configuration mode:

```
configure terminal
```

2. Enter the following command to specify the interface to configure:

   ```
   interface <if-name>
   ```

3. Enter the following command to configure DVMRP default route listening:

   ```
   [no] ip dvmrp default-listen
   ```

Table 19: Variable definitions

Variable	Value
[no]	Disables DVMRP default route listening.

Configuring the DVMRP prune lifetime for an interface

Perform the following procedure to configure the lifetime of prune messages that are sent to upstream neighbors. By default, the value is 7200 seconds.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to specify the interface to configure:

   ```
   interface <if-name>
   ```

3. Enter the following command to configure the DVMRP prune lifetime:

   ```
   [no] ip dvmrp prune-lifetime <prune-lifetime>
   ```

Table 20: Variable definitions

Variable	Value
<if-name>	Specifies the interface to configure.
[no]	Resets the DVMRP prune lifetime to the default value: 7200 seconds.
<prune-lifetime>	Specifies the DVMRP prune lifetime value. Range is 0–86400 seconds.

Displaying DVMRP statistics

Perform the following procedure to display DVMRP statistics.

Procedure steps

Enter the following command to display DVMRP statistics:

```
show ip dvmrp statistics [<ifname>] [detail]
```

Table 21: Variable definitions

Variable	Value
[<ifname>]	Specifies the interface for which the statistics are to be displayed.
[detail]	Provides additional detail to the command output.

Showing interface information

This procedure details the steps necessary to display DVMRP information on all DVMRP-enabled interfaces or a specified interface.

Procedure steps

Enter the command to show interface information.

```
show ip dvmrp interface <ifname> [detail]
```

Table 22: Variable definition

Variable	Value
[detail]	Display detailed information (optional).
<ifname>	The interface name.

Example of showing interface information

Enter the command to show interface information.

```
show ip dvmrp interface ethernet0/1 detail
```

Showing neighbor information

This procedure details the steps necessary to display the DVMRP neighbor entry in detail indicated by interface <ifname> or neighbor IP address.

Procedure steps

Enter the command to show neighbor entry.

```
show ip dvmrp neighbor [detail] <ifname> <nbr-address>
```

Table 23: Variable definition

Variable	Value
[detail]	Display detailed information (optional).
<ifname>	The interface name.
<nbr-address>	The IP address of the neighbor.

Example of showing neighbor information

Enter the command to show neighbor entry.

```
show ip dvmrp neighbor detail ethernet0/1 10.10.10.1
```

Showing prune information

This procedure details the steps necessary to display the entire DVMRP prune table in detail. Use the [source] parameter to display the DVMRP prune table entry which matches both the multicast source network and subnet mask length. Use the [group] option to display DVMRP prune table entry for the multicast group.

Procedure steps

Enter the command to show prune information.

```
show ip dvmrp prune [detail] [group <group-address] [source
<source-address_mask>]
```

Table 24: Variable definition

Variable	Value
[detail]	Display detailed information (optional).
[group]	Show group information (optional).
<group-address>	The multicast group address.
[source]	Show matching source entry (optional).
<source-address_mask>	The source IP address.

Showing route information

This procedure details the steps necessary to display DVMRP route table entries in detail that have the upstream neighbor indicated by IP address.

Procedure steps

Enter the command to show DVMRP route table entries.

```
show ip dvmrp route [detail] <ipaddress_mask> [next-hop
<ipaddress>] [best-match <ipaddress>]
```

Table 25: Variable definition

Variable	Value
[best-match]	Show best-match (optional).
[detail]	Display detailed information (optional).
<ipaddress>	The address of the neighbor.
<ipaddress_mask>	The source network address and subnet mask.
[next-hop]	Show next hop (optional).

Example of showing route information

Enter the command to show DVMRP route table entries.

```
show ip dvmrp route next-hop 10.10.10.11
```

Showing statistics information

This procedure details the steps necessary to display DVMRP statistics information.

Procedure steps

Enter the command to show statistics.

```
show ip dvmrp statistics
```

Deleting DVMRP prune states

This procedure describes how to delete DVMRP prune states. You can delete all statistics, or you can delete by group or network prefix.

Procedure steps

To clear DVMRP prune states, enter:

```
clear ip dvmrp prune <all>|<network>|<groupIP>
```

Table 26: Variable definition

Variable	Value
<all>	Clear all prune states.
<groupIP>	Clear prune states by group address.
<network>	Clear prune states by network prefix.

Examples of deleting DVMRP prune states

1. To clear all DVMRP prune states, enter:

   ```
   clear ip dvmrp prune all
   ```

2. To clear DVMRP prune states by group address, enter:

   ```
   clear ip dvmrp prune group 10.10.10.1
   ```

3. To clear DVMRP prune states by network, enter:

   ```
   clear ip dvmrp prune 10.10.10.2/2
   ```

Deleting DVMRP unicast routes

This procedure describes how to delete DVMRP unicast routes. You can delete all unicast routes, or delete by network prefix.

Procedure steps

To delete DVMRP unicast routes, enter:

```
clear ip dvmrp route [all] <network>
```

Table 27: Variable definition

Variable	Value
[all]	Delete all DVMRP unicast routes.
<network>	Delete DVMRP unicast by network prefix.

Example of deleting DVMRP unicast routes

1. To delete all DVMRP unicast routes, enter:

   ```
   clear ip dvmrp route all
   ```

2. To delete DVMRP routes by network prefix, enter:

   ```
   clear ip dvmrp route 10.10.10.2/2
   ```

Chapter 6: PIM-SM procedures

Registering an accept filter

This procedure details the steps necessary to configure the ability to filter out multicast sources specified by the given access-list at the RP so that the RP will accept/refuse to perform Register mechanism for the packets sent by the specified sources. Use the **no** form of this command to revert to default (off).

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. In configuration mode, enter the command to configure the accept filter.

   ```
   [no] ip pim accept-register list {<accesslist>|<word>}
   ```

Table 28: Variable definition

Variable	Value
<accesslist>	The IP standard access list. Valid ranges are 1–99 for simple range value and 1300 to 1999 for expanded range value.
<word>	The IP named access-list.

Example of registering an accept filter

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter the command to configure the accept filter.

   ```
   ip pim accept-register list 50
   ```

Configuring candidate bootstrap router

This procedure details the steps necessary to enable BSR status using a specific interface name. Use the **no** form of this command to disable the function.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. In configuration mode, enter the command to enable BSR status.

   ```
   [no] ip pim bsr-candidate <ifname> [<hash>] [<priority>]
   ```

Table 29: Variable definition

Variable	Value
<ifname>	The name of the interface.
<hash>	The mask hash length for RP selection, in the range 0–32.
<priority>	The priority for a BSR candidate, in the range 0–255.

Example of configuring candidate bootstrap router

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter the command to enable BSR status.

   ```
   ip pim bsr-candidate fxp0 20 30
   ```

Calculate register checksum

This procedure details the steps necessary to configure the option to calculate register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions. Use the **no** form of this command to revert to the default setting (off).

Procedure steps

1. Enter configuration mode.

```
configure terminal
```

2. In configuration mode, enter the command to calculate register checksum.

```
[no] ip pim cisco-register-checksum
```

Setting the source address for PIM register

This procedure details the steps necessary to configure the source address of Register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host. Use the **no** form of this command to revert to the default source address.

Note:

The configured address must be reachable in order to be used by the RP to send corresponding Register-Stop messages in response. It can be either the loop back interface address or other physical addresses. This address must be advertised by unicast routing protocols on the DR. The configured interface does not require being PIM-SM enabled.

Procedure steps

1. Enter configuration mode.

```
configure terminal
```

2. In configuration mode, enter the command to configure the source address.

```
[no] ip pim register-source {<sourceaddress>|<ifname>}
```

Table 30: Variable definition

Variable	Value
<sourceaddress>	The IP address used as the source of register packets.
<ifname>	The interface name. The address of this interface is used as the source of register packets.

Example of setting the source address for PIM register

1. Enter configuration mode.

```
configure terminal
```

2. Enter the command to configure the source address.

```
ip pim register-source 10.1.1.1
```

Configuring source-specific multicast

This procedure details the steps necessary to configure the source-specific multicast (SSM) default value or access-list filter range. Use the **no** form of this command to disable source-specific multicast.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. In configuration mode, enter the command to configure SSM.

   ```
   [no] ip pim ssm [default] [range <accesslist> <word>]
   ```

Table 31: Variable definition

Variable	Value
<accesslist>	The IP standard access list. Valid range is 1–99 for simple range and 1300 to 1999 for expanded range. Access list variable must first be configured using access-list command.
[default]	To use 232/8 group range for SSM (optional).
[range]	To configure a range using access list or word (optional).
<word>	The IP named access list.

Example of configuring source-specific multicast

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter the command to configure SSM.

   ```
   ip pim ssm range ssmgrp
   ```

Configuring to ignore RP set priority value

This procedure describes how to configure the Avaya Secure Router 2330/4134 to ignore the RP set priority value. Use the **no** form of this command to revert to default.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. To ignore the RP set priority value, enter:

   ```
   [no] ip pim ignore-rp-set-priority
   ```

Configuring the PIM RP address

This procedure describes how to configure the PIM Rendezvous Point address. Use the **no** form of this command to revert to default.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. To configure the RP address, enter:

   ```
   [no] ip pim rp-address <address>
   ```

Table 32: Variable definition

Variable	Value
<address>	The address of the Rendezvous Point.

Example of configuring the PIM RP address

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. To configure the RP address, enter:

   ```
   ip pim rp-address 10.10.10.2
   ```

Configuring the PIMv2 RP candidate

This procedure describes how to configure the PIMv2 Rendezvous Point candidate. Use the **no** form of this command to revert to default behavior.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. To configure the RP candidate, enter:

   ```
   [no] ip pim rp-candidate <interface> [interval <1-16383>]
   [priority <0-255>] [group-list <listname>]
   ```

Table 33: Variable definition

Variable	Value
<interface>	The interface name of the RP candidate.
<interval>	The candidate RP advertisement interval.
<priority>	The candidate RP priority.
<group-list>	The group range for this candidate RP.

Example of configuring the PIMv2 RP candidate

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. To configure the RP candidate, enter:

   ```
   ip pim rp-candidate ethernet 6/2 interval 255 priority 100
   group-list testlist
   ```

Configuring a group to have no source-tree switching threshold

This procedure describes how to configure a group to have no source-tree switching threshold. Use the **no** form of this command to revert to default behavior.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. To have no source-tree switching threshold, enter:

   ```
   [no] ip pim spt-threshold-infinity [group-list <accesslist>]
   ```

Table 34: Variable definition

Variable	Value
<accesslist>	The IP access list name you want to remove the threshold from.

Example of configuring source-tree switching threshold

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. To have no source-tree switching threshold, enter:

   ```
   ip pim spt-threshold-infinity group-list testlist
   ```

Configuring PIM router DR priority

This procedure describes how to configure PIM router DR priority. Use the **no** form of this command to revert to default.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. To configure priority, enter:

   ```
   [no] ip pim dr-priority <priority>
   ```

Table 35: Variable definition

Variable	Value
<priority>	The PIM router DR priority, in the range 0–4294967294.

Example of configuring PIM router DR priority

1. Enter configuration mode.

```
configure terminal
```

2. Enter Interface mode.

```
interface ethernet 0/1
```

3. To configure priority, enter:

```
ip pim dr-priority 255
```

Configuring PIM to exclude Gen-id option

This procedure describes how to configure PIM to exclude Gen-id option from PIM hello packets on the specified interface. Use the **no** form of this command to revert to default behavior.

Procedure steps

1. Enter configuration mode.

```
configure terminal
```

2. Enter Interface mode.

```
interface <interface>
```

3. To exclude the Gen-id option, enter:

```
[no] ip pim exclude-genid
```

Configuring a PIM peer filter

This procedure describes how to configure a PIM peering filter. Use the **no** form of this command remove the peer filter.

Procedure steps

1. Enter configuration mode.

```
configure terminal
```

2. Enter Interface mode.

```
interface <interface>
```

3. To configure the peering filter, enter:

```
[no] ip pim neighbor-filter <accesslist>
```

Table 36: Variable definition

Variable	Value
<accesslist>	The IP access list name used in filtering.

Example of configuring a PIM peer filter

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. To configure the peering filter, enter:

   ```
   ip pim neighbor-filter testlist
   ```

Enabling a BSR border router

This procedure details the steps necessary to enable a BSR border router. Use the **no** form of this command to disable.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to enable a border router.

   ```
   [no] ip pim bsr-border
   ```

Setting Hello message interval

This procedure details the steps necessary to configure a hello interval value. Use the **no** form of this command to disable.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to configure the hello interval.

   ```
   [no] ip pim hello-interval <interval>
   ```

Table 37: Variable definition

Variable	Value
<interval>	The hello interval value in seconds. Valid range is 10 to 65535 (default is 30).

Example of setting Hello message interval

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to configure the hello interval.

   ```
   ip pim hello-interval 60
   ```

Enabling PIM sparse-mode operation

This procedure details the steps necessary to enable PIM-SM on the active interface. Use the no form of the command to disable PIM-SM on the interface.

Use the passive option to enable passive mode operation for local IGMP members on the interface. Passive mode stops PIM-SM transactions on the interface, allowing only IGMP mechanism to be active. Use the **no** form of this command to turn off passive mode.

Procedure steps

1. Enter configuration mode.

```
configure terminal
```

2. Enable multicast globally.

```
ip multicast-routing
```

3. Enter Interface mode.

```
interface <interface>
```

4. In Interface mode, enter the command to enable PIM-SM.

```
[no] ip pim sparse-mode
```

5. To enable passive mode, enter the following command:

```
[no] ip pim sparse-mode [passive]
```

Configuring PIM neighbor change logging

Perform the following procedure to enable logging of the PIM neighbor changes to the console. By default, PIM neighbor change logging is enabled.

Procedure steps

1. Enter the following command for configuration mode:

```
configure terminal
```

2. Enter the following command to configure PIM neighbor change logging to the console:

```
[no] ip pim log-neighbor changes
```

Table 38: Variable definitions

Variable	Value
[no]	Disables PIM neighbor change logging.

Configuring an Anycast member RP address

Perform the following procedure to configure an Anycast member RP address. By default, no Anycast members are configured.

Prerequisites

- To specify the Anycast RP address in this procedure, you must first configure the Anycast RP address as a static RP address.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the Anycast member RP address:

   ```
   [no] ip pim anycast-rp <anycast-RP-address> <anycast-member-RP-address>
   ```

Table 39: Variable definitions

Variable	Value
[no]	Removes the configured Anycast RP member.
<anycast-RP-address>	Specifies the IP address of the Anycast RP address.
<anycast-member-RP-address>	Specifies the IP address of the Anycast member RP address.

Configuring PIM multipath

Perform the following procedure to configure PIM multipath to enable the selection of different equal cost multipath (ECMP) next hops for a given destination. By default, PIM multipath is disabled.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure PIM multipath:

   ```
   [no] ip pim multipath [hashing]
   ```

Table 40: Variable definitions

Variable	Value
[no]	Disabes PIM multipath.
[hashing]	Enables the next hop selection based on key, which is calculated using source address,

Variable	Value
	group address and next-hop address. By default, round-robin mechanism is used to select the next hop.

Displaying PIM RPF

Perform the following procedure to display RPF information based on source address and, optionally, group address.

The router displays RPF information for all ECMP routes if

- Multipath (round-robin or hashing) is enabled and group address is not specified.
- Multipath (round-robin) is enabled and a matching (S,G) entry does not exist.

Procedure steps

Enter the following command to display the PIM RPF information:

```
show ip pim sparse-mode rpf <source-addr> [<group-addr>]
```

Table 41: Variable definitions

Variable	Value
<source-addr>	Specifies the IPv4 source address for which to display PIM RPF information.
<group-addr>	Specifies the IPv4 group address for which to display PIM RPF information.

Clearing PIM statistics

Perform the following procedure to clear PIM statistics. If no options are specified, the router clears the interface and global statistics counters.

Procedure steps

Enter the following command to clear PIM statistics:

```
clear ip pim sparse-mode statistics [interface [<ifname>] |
all ]
```

Table 42: Variable definitions

Variable	Value
[interface [<ifname>]	Clears statistics for the particular interface. If the interface name is not specified, the router clears statistics for all interfaces.
all	Clears the interface and global statistics counters and Tree Information Base (TIB) information.

Displaying bootstrap router information

This procedure details the steps necessary to show the bootstrap router address.

Procedure steps

Enter the command to show bootstrap router information.

```
show ip pim sparse-mode bsr-router
```

Displaying the PIM Tree Information Base

This procedure details the steps necessary to show the PIM Tree Information Base. Use group, source address (or both) to filter display between group, source, and group/source displays respectively.

Procedure steps

Enter the command to show the PIM Tree Information Base.

```
show ip pim sparse-mode database [<src-addr>|<grp-addr>]
```

Table 43: Variable definition

Variable	Value
<src-addr>	Filter by source address (optional).
<grp-addr>	Filter by group address (optional).

Example of displaying the PIM Tree Information Base

Enter the command to show the PIM Tree Information Base.

```
show ip pim sparse-mode database 10.1.1.2
```

Displaying PIM interface information

This procedure details the steps necessary to show PIM interface information.

Procedure steps

Enter the command to show PIM interface information.

```
show ip pim sparse-mode interface <ifname> [detail]
```

Table 44: Variable definition

Variable	Value
<ifname>	The interface name.
[detail]	Display detailed information (optional).

Example of displaying PIM interface information

Enter the command to show PIM interface information.

```
show ip pim sparse-mode interface ethernet 0/1 detail
```

Displaying PIM neighbor information

This procedure details the steps necessary to show PIM neighbor information.

Procedure steps

Enter the command to show neighbor information.

```
show ip pim sparse-mode neighbor <ifname> [detail]
```

Table 45: Variable definition

Variable	Value
<ifname>	The PIM-enabled interface name or number
[detail]	Show detailed PIM neighbor information (optional).

Example of displaying PIM neighbor information

Enter the command to show neighbor information.

```
show ip pim sparse-mode neighbor ethernet 0/1 detail
```

Displaying PIM Rendezvous Point information

This procedure details the steps necessary to display rendezvous-point (RP) information based on group.

Procedure steps

Enter the command to show RP information.

```
show ip pim sparse-mode rp-hash <group-address>
```

Table 46: Variable definition

Variable	Value
<group-address>	The IPv4 group address.

Example of displaying PIM Rendezvous Point information

Enter the command to show RP information.

```
show ip pim rp-hash 10.1.1.10
```

Clearing PIM bootstrap router information

This procedure describes how to clear all PIM bootstrap router information.

Procedure steps

To clear all PIM bootstrap router information, enter:

```
clear ip pim sparse-mode bsr rp-set all
```

Chapter 7: IGMP interface configuration procedures

Configuring an IGMP access group

Hosts on a subnet serviced by a particular interface have the access to join certain multicast groups. This procedure details the steps necessary to control the multicast groups on an interface. Use the **no** form of the command to disable groups on an interface.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to control multicast groups.

   ```
   [no] ip igmp access-group {<accesslist>|<word>}
   ```

Table 47: Variable definition

Variable	Value
<accesslist>	The IP standard access list. Valid range is 1–99 for simple range value and 1300 to 1999 for expanded range value.
<word>	The IP named access list.

Example of configuring an IGMP access group

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to control multicast groups.

```
ip igmp access-group 1350
```

Configuring leave behavior

This procedure details the steps necessary to minimize the leave latency of IGMP memberships for IGMPv2. Use the **no** form of this command to disable this feature.

Configure this command on an interface if only one IGMP-enabled neighbor is connected to the interface.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to configure immediate leave behavior.

   ```
   [no] ip igmp immediate-leave group-list <word>
   ```

Table 48: Variable definition

Variable	Value
<word>	The IP named access list.

Example of configuring leave behavior

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to configure immediate leave behavior.

   ```
   ip igmp immediate-leave group-list 1350
   ```

Configuring query interval

This procedure details the steps necessary to configure the frequency at which IGMP host query messages are sent. Use the **no** form of this command to return the frequency to default.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to set the query interval.

   ```
   [no] ip igmp query-interval <interval>
   ```

Table 49: Variable definition

Variable	Value
<interval>	The frequency, in seconds, at which IGMP group-specific host query message are sent. Valid range is 1–65535 (default is 125 seconds).

Example of configuring query interval

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to set the query interval.

   ```
   ip igmp query-interval 60
   ```

Configuring robustness variable

This procedure details the steps necessary to set the Robustness-Variable value. Use the **no** form of this command to return to the default value.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to set the Robustness Variable.

   ```
   [no] ip igmp robustness-variable <value>
   ```

Table 50: Variable definition

Variable	Value
<value>	The Robustness Variable value. Valid range is 2–7 (default is 2).

Example of configuring robustness variable

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to set the Robustness Variable.

   ```
   ip igmp robustness-variable 4
   ```

Configuring query maximum response time

This procedure details the steps necessary to configure the maximum response time advertised in IGMP queries. Use the **no** form of this command to restore the default value.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to set the maximum response time.

```
[no] ip igmp query-max-response-time <responsetime>
```

Table 51: Variable definition

Variable	Value
<responsetime>	The maximum response time, in seconds, advertised in IGMP queries. Valid range is 1–25 (default is 10 seconds).

Example of configuring query maximum response time

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to set the maximum response time.

   ```
   ip igmp query-max-response-time 10
   ```

Configuring querier timeout

This procedure details the steps necessary to configure the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying. Use the **no** form of this command to restore the default value.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to set the querier timeout.

   ```
   [no] ip igmp querier-timeout <timeout>
   ```

Table 52: Variable definition

Variable	Value
<timeout>	The number of seconds the router waits after the previous querier has stopped its query before it takes over. Valid range is 60 to 300 (default is 255 seconds).

Example of configuring querier timeout

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to set the querier timeout.

   ```
   ip igmp querier-timeout 125
   ```

Configuring the IGMP last member query count

This procedure describes how to configure the last member query counter. Use the **no** form of this command to return to the default.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. To configure the counter, enter:

   ```
   [no] ip igmp last-member-query-count <count>
   ```

Table 53: Variable definition

Variable	Value
<count>	The last member query count value, in the range 2–7.

Example of configuring the IGMP last member query counter

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

```
interface ethernet 0/1
```

3. To configure the counter, enter:

```
ip igmp last-member-query-count 5
```

Configuring the IGMP last member query interval

This procedures describes how to configure the interval between IGMP last member queries. Use the **no** form of this command to return to the default.

Procedure steps

1. Enter configuration mode.

```
configure terminal
```

2. Enter Interface mode.

```
interface <interface>
```

3. To configure the interval, enter:

```
[no] ip igmp last-member-query-interval <interval>
```

Table 54: Variable definition

Variable	Value
<interval>	The last member query interval, in the range 1–25.

Example of configuring the IGMP last member query interval

1. Enter configuration mode.

```
configure terminal
```

2. Enter Interface mode.

```
interface ethernet 0/1
```

3. To configure the interval, enter:

```
ip igmp last-member-query-interval 5
```

Setting the IGMP version

This procedure details the steps necessary to set the IGMP version to be used. Use the **no** form of this command to return to the default version.

Procedure steps

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface <interface>
   ```

3. In Interface mode, enter the command to set the IGMP version.

   ```
   [no] ip igmp version <version>
   ```

Table 55: Variable definition

Variable	Value
<version>	The IGMP version number to be used. Valid range is 1–3 (default is 3).

Example of setting the IGMP version

1. Enter configuration mode.

   ```
   configure terminal
   ```

2. Enter Interface mode.

   ```
   interface ethernet 0/1
   ```

3. Enter the command to set the IGMP version.

   ```
   ip igmp version 3
   ```

Configuring global IGMP state limit

Perform the following procedure to configure a maximum global limit to the number of allowable IGMP states (groups) on the router. By default, no IGMP limit exists.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following to configure the IGMP state limit:

   ```
   [no] ip igmp limit <limit>
   ```

Table 56: Variable definitions

Variable	Value
[no]	Removes the configured IGMP state limit.
<limit>	Specifies the maximum allowable IGMP states on the router.

Configuring IGMP group limit on an interface

Perform the following procedure to configure a maximum limit to the number of allowable states (groups) on an interface. By default, no IGMP limit exists.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to access the VLAN database:

   ```
   vlan database
   ```

3. Enter the following command to specify the VLAN to configure:

   ```
   vlan <vid>
   ```

4. Enter the following command to return to configuration mode:

   ```
   exit
   ```

5. Enter the following command for VLAN interface configuration mode:

   ```
   interface vlan vlan<vid>
   ```

6. Enter the following command to configure the IGMP group limit:

   ```
   [no] ip igmp limit <limit>
   ```

Table 57: Variable definitions

Variable	Value
<vid>	Specifies the ID of the VLAN interface to configure.
[no]	Removes the configured IGMP state limit.
<limit>	Specifies the maximum allowable IGMP states on the interface.

Configuring the SSM mapping status

Perform the following procedure to enable static source specific multicast (SSM) mapping. By default, SSM mapping is disabled.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the SSM mapping status:

   ```
   [no] ip igmp ssm-map enable
   ```

Table 58: Variable definitions

Variable	Value
[no]	Disables SSM mapping.

Configuring a static SSM map

Perform the following procedure to statically map a specified source address to an SSM group specified in the access list. The router applies the mapping after it receives an IGMPv1/v2 report for the specified group. By default, no static SSM maps are configured.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to configure the static SSM map:

   ```
   [no] ip igmp ssm-map static [<WORD>] <A.B.C.D>
   ```

Table 59: Variable definitions

Variable	Value
[no]	Removes the specified static SSM map.
<WORD>	Specifies the IP access-list name.
<A.B.C.D>	Specifies the source address to use for static map group.

Configuring a static IGMP group on an interface

Perform the following procedure to add a static IGMP group on an interface. By default, no static IGMP groups are configured.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to access the VLAN database:

   ```
   vlan database
   ```

3. Enter the following command to specify the VLAN to configure:

   ```
   vlan <vid>
   ```

4. Enter the following command to return to configuration mode:

   ```
   exit
   ```

5. Enter the following command for VLAN interface configuration mode:

   ```
   interface vlan vlan<vid>
   ```

6. Enter the following command to configure a static IGMP group:

   ```
   [no] ip igmp static-group <group-addr> [source {<source-addr>
   | ssm-map}] [interface <if-name>}]
   ```

Table 60: Variable definitions

Variable	Value
[no]	Removes the specified static group.
<group-addr>	Specifies the multicast group address to statically configure.
<source-addr>	Specifies the multicast source address to associate with this group.

Variable	Value
ssm-map	Specifies to use Source Specific Multicast (SSM) mapping to identify the source to associate with this group.
<if-name>	Specifies the interface name to associate with this group.

Displaying IGMP statistics

Perform the following procedure to display IGMP statistics.

Procedure steps

Enter the following command to display IGMP statistic:

```
show ip igmp statistics <if-name> [detail]
```

Table 61: Variable definitions

Variable	Value
<if-name>	Specifies the interface for which to display the IGMP statistics.
[detail]	Provides additional detail in the command output.

Clearing IGMP statistics

Perform the following procedure to clear IGMP statistics to set all the IGMP statistics counters to zero.

Procedure steps

Enter the following command to clear IGMP statistics:

```
clear ip igmp statistics <if-name>
```

Table 62: Variable definitions

Variable	Value
<if-name>	Specifies the interface for which to clear the IGMP statistics. If no interface is specified, all statistics information is set to zero.

Displaying IGMP group membership information

This procedure details the steps necessary to display the multicast groups with receivers directly connected to the router and learned through IGMP.

Procedure steps

Enter the command to show group membership information.

```
show ip igmp groups <groupaddress> <ifname> [detail]
```

Table 63: Variable definition

Variable	Value
<groupaddress>	The multicast group address.
<ifname>	The multicast group name.
[detail]	Show detailed information (optional).

Example of displaying IGMP group membership information

Enter the command to show group membership information.

```
show ip igmp groups 239.1.1.1
```

Displaying IGMP interface information

This procedure details the steps necessary to display multicast-related information about an interface. Use the command without parameters to display information for all interfaces or with an interface name for a specific interface.

Procedure steps

1. Enter the command to show interface information.

   ```
   show ip igmp interface
   ```

2. Show information about a specific interface.

   ```
   show ip igmp interface <interface>
   ```

Table 64: Variable definition

Variable	Value
<interface>	The name of the interface.

Example of displaying IGMP interface information

1. Enter the command to show interface information.

   ```
   show ip igmp interface
   ```

2. Show information about a specific interface.

   ```
   show ip igmp interface ethernet0/2
   ```

Displaying IGMP snooping information

This procedure details the steps necessary to display IGMP snooping information.

Procedure steps

Enter the command to show IGMP snooping information.

```
show ip igmp snooping
```

Clearing IGMP group cache entries

This procedure describes how to clear IGMP group cache entries.

Procedure steps

To clear group cache entries, enter:

```
clear ip igmp group [<all>|<A.B.C.D>]
```

Table 65: Variable definition

Variable	Value
<all>	Clear all IGMP group entries.
<A.B.C.D>	Clear IGMP group entries by multicast group address.

Example of clearing IGMP group cache entries

1. To clear all group cache entries, enter:

   ```
   clear ip igmp group all
   ```

2. To clear group cache entries by multicast address, enter:

   ```
   clear ip igmp group 239.1.1.1
   ```

Clearing IGMP interface entries

This procedure describes how to clear IGMP interface entries.

Procedure steps

To clear interface entries, enter:

```
clear ip igmp interface <interface>
```

Table 66: Variable definition

Variable	Value
<interface>	The interface from which to remove IGMP entries.

Example of clearing IGMP interface entries

To clear interface entries, enter:

```
clear ip igmp interface ethernet0/1
```

Chapter 8: IGMP snooping procedures

Configuring IGMP snooping status on a VLAN

Perform the following procedure to configure the status of IGMP snooping on a VLAN interface. By default, IGMP snooping is enabled on a VLAN.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to access the VLAN database:

   ```
   vlan database
   ```

3. Enter the following command to specify the VLAN to configure:

   ```
   vlan <vid>
   ```

4. Enter the following command to return to configuration mode:

   ```
   exit
   ```

5. Enter the following command for VLAN interface configuration mode:

   ```
   interface vlan vlan<vid>
   ```

6. Enter the following command to configure IGMP snooping:

   ```
   [no] ip igmp snooping
   ```

Table 67: Variable definitions

Variable	Value
<vid>	Specifies the ID of the VLAN interface to configure.
[no]	Disables IGMP snooping on the interface.

Configuring mrouter ports for IGMP snooping

Perform the following procedure to configure mrouter ports on a VLAN for IGMP snooping. By default, no mrouter ports are configured.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to access the VLAN database:

   ```
   vlan database
   ```

3. Enter the following command to specify the VLAN to configure:

   ```
   vlan <vid>
   ```

4. Enter the following command to return to configuration mode:

   ```
   exit
   ```

5. Enter the following command for VLAN interface configuration mode:

   ```
   interface vlan vlan<vid>
   ```

6. Enter the following command to configure mrouter ports:

   ```
   [no] ip igmp snooping mrouter interface <if-name>
   ```

Table 68: Variable definitions

Variable	Value
<vid>	Specifies the ID of the VLAN interface to configure.
[no]	Removes the specified mrouter port.
<if-name>	Specifies the name of the interface to configure as an mrouter port.

Configuring IGMP-snooping querier on a VLAN

If a VLAN receives no IGMP traffic from a multicast router, enable IGMP-snooping querier on the VLAN to provide multicast traffic support. With IGMP-snooping querier enabled, the interface uses its own IP address as the querier address. By default, IGMP-snooping querier is disabled.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to access the VLAN database:

   ```
   vlan database
   ```

3. Enter the following command to specify the VLAN to configure:

   ```
   vlan <vid>
   ```

4. Enter the following command to return to configuration mode:

   ```
   exit
   ```

5. Enter the following command for VLAN interface configuration mode:

   ```
   interface vlan vlan<vid>
   ```

6. Enter the following command to configure the IGMP-snooping querier:

   ```
   [no] ip igmp snooping querier
   ```

Table 69: Variable definitions

Variable	Value
<vid>	Specifies the ID of the VLAN interface to configure.
[no]	Disables the IGMP-snooping querier on the VLAN.

Configuring IGMP report suppression

Perform the following procedure to configure IGMP report suppression. IGMP report suppression, also known as IGMP proxy, forwards the first IGMP report for a group, and suppresses any subsquent reports for the same group. By default, IGMP report suppression is disabled.

Procedure steps

1. Enter the following command for configuration mode:

   ```
   configure terminal
   ```

2. Enter the following command to access the VLAN database:

   ```
   vlan database
   ```

3. Enter the following command to specify the VLAN to configure:

```
vlan <vid>
```

4. Enter the following command to return to configuration mode:

   ```
   exit
   ```

5. Enter the following command for VLAN interface configuration mode:

   ```
   interface vlan vlan<vid>
   ```

6. Enter the following command to configure IGMP report suppression:

   ```
   [no] ip igmp snooping report-suppression
   ```

Table 70: Variable definitions

Variable	Value
<vid>	Specifies the ID of the VLAN interface to configure.
[no]	Disables IGMP report suppression.

Displaying IGMP mrouter configuration

Perform the following procedure to display the IGMP snooping mrouter configuration.

Procedure steps

Enter the following command to display the IGMP snooping mrouter configuration:

```
show ip igmp snooping mrouter [vid]
```

Table 71: Variable definitions

Variable	Value
<vid>	Specifies the VLAN ID for which to display the IGMP snooping configuration.

Clearing the IGMP snooping mrouter configuration

Perform the following procedure to clear the IGMP snooping mrouter ports.

Procedure steps

Enter the following command to clear IGMP snooping mrouter ports:

```
clear ip igmp snooping mrouter
```

Clearing IGMP snooping statistics

Perform the following procedure to clear the IGMP snooping statistics.

Procedure steps

Enter the following command to clear IGMP snooping statistics:

```
clear ip igmp snooping statistics
```