

Multicast Routing

This chapter describes how to configure the ASA to use the multicast routing protocol.

- Multicast routing, on page 1
- Guidelines for multicast routing, on page 5
- Enable Multicast Routing, on page 5
- Customize Multicast Routing, on page 6
- Monitoring for PIM, on page 20
- Example for Multicast Routing, on page 21
- History for Multicast Routing, on page 22

Multicast routing

Multicast routing is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications include videoconferencing, corporate communications, distance learning, and distributing software, stock quotes, and news.

Multicast routing applications and protocols

Multicast routing protocols send source traffic to multiple receivers efficiently, without adding extra load on the source or receivers, and use less network bandwidth than other technologies. Multicast packets are replicated in the network by ASA enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols, which results in the most efficient delivery of data to multiple receivers possible.

The ASA supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single ASA.

Note The UDP and non-UDP transports are both supported for multicast routing. However, the non-UDP transport has no FastPath optimization.

Stub multicast routing

Stub multicast routing provides dynamic host registration and facilitates multicast routing.

When configured for stub multicast routing, the ASA acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the ASA forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for stub multicast routing, the ASA cannot be configured for PIM sparse or bidirectional mode. Enable PIM on the interfaces that participate in IGMP stub multicast routing.

The ASA supports both PIM-SM and bidirectional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees, each rooted at a single Rendezvous Point (RP) per multicast group. Optionally, it creates shortest-path trees for each multicast source.

PIM multicast routing

Bidirectional PIM is a variant of PIM-SM that builds bidirectional shared trees connecting multicast sources and receivers.

DF election process

Bidirectional trees are built using a Designated Forwarder (DF) election process operating on each link of the multicast topology. With the assistance of the DF, multicast data is forwarded from sources to the Rendezvous Point (RP) and then along the shared tree to receivers. This process does not require source-specific state. The DF election takes place during RP discovery and provides a default route to the RP.



Note If the ASA is the PIM RP, use the untranslated outside address of the ASA as the RP address.

PIM sparse mode

PIM Sparse Mode (PIM-SM) is a PIM mode that forwards traffic only when specifically requested by receivers. It uses a central Rendezvous Point (RP) to coordinate the multicast traffic forwarding between the multicast source and the destination. RP is a router that serves as the meeting point for the source and the receivers. Multicast sources register with the RP through their first hop router. They send a copy of the multicast traffic to the receivers through the RP.

PIM source specific multicast support

ASA can forward source specific multicast traffic (e.g., for groups in the 232.x.x.x range) even though they do not support PIM-SSM configuration or Internet Group Management Protocol version 3 (IGMPv3).

SSM is classified as a data delivery mechanism for one-to-many applications such as IPTV. The SSM model uses a concept of "channels" denoted by an (S,G) pair, where S is a source address and G is an SSM destination address. Subscribing to a channel is achieved by using a group management protocol such as IGMPv3. SSM enables a receiving client, once it has learned about a particular multicast source, to receive multicast streams directly from the source rather than receiving it from a shared Rendezvous Point (RP). Access control mechanisms are introduced within SSM, providing a security enhancement that is not available with current sparse or sparse-dense mode implementations.

Limitation:

- ASA cannot act as the last-hop router for SSM multicast because it does not support IGMPv3 (which receivers use to join SSM groups).

If the ASA is the last-hop, it will ignore IGMPv3 join messages from receivers for SSM groups, and SSM forwarding will not work.

- Static multicast routes on ASA do not work for SSM range (232.x.x.x).

Workaround:

For Cisco ASA firewall to forward SSM-related multicast traffic, you must add a multicast-capable layer 3 device (such as a router or switch) that supports PIM and IGMPv3 on the same network segment as the receivers.

How it Works:

- Receivers register their SSM group joins (IGMPv3) with this layer 3 device.
- This layer 3 device sends PIM join messages towards the ASA.
- The ASA receives these PIM messages and dynamically learns multicast routes.
- SSM multicast traffic is then properly forwarded by the ASA, since it is no longer the last-hop device.

PIM bootstrap router (BSR)

PIM Bootstrap Router (BSR) is a dynamic Rendezvous Point (RP) selection model that uses candidate routers for RP function and for relaying the RP information for a group.

The RP function includes RP discovery and provides a default route to the RP. It does this by configuring a set of devices as candidate BSRs (C-BSR) which participate in a BSR election process to choose a BSR amongst themselves. Once the BSR is chosen, devices that are configured as candidate Rendezvous Points (C-RP) start sending their group mapping to the elected BSR. The BSR then distributes the group-to-RP mapping information to all the other devices down the multicast tree through BSR messages that travel from PIM router to PIM router on a per-hop basis.

This feature allows networks to learn RPs dynamically. Dynamic RP discovery is essential in large, complex networks where an RP may occasionally go down and come up.

PIM bootstrap router (BSR) terminology

This reference provides definitions for key terminology used in PIM Bootstrap Router (BSR) configurations to help understand the roles and functions of different components in the BSR election and RP advertisement process.

These terms are frequently referenced in the PIM BSR configuration:

- Bootstrap Router (BSR) — A BSR advertises Rendezvous Point (RP) information to other routers with PIM on a hop-by-hop basis. Among multiple Candidate-BSRs, a single BSR is chosen after an election process. The primary purpose of this Bootstrap router is to collect all Candidate-RP (C-RP) announcements in to a database called the RP-set and to periodically send this out to all other routers in the network as BSR messages (every 60 seconds).
- Bootstrap Router (BSR) messages — BSR messages are multicast to the All-PIM-Routers group with a TTL of 1. All PIM neighbors that receive these messages retransmit them (again with a TTL of 1) out of all interfaces except the one in which the messages were received. BSR messages contain the RP-set and the IP address of the currently active BSR. This is how C-RPs know where to unicast their C-RP messages.

- Candidate Bootstrap Router (C-BSR) — A device that is configured as a candidate-BSR participates in the BSR election mechanism. A C-BSR with highest priority is elected as the BSR. The highest IP address of the C-BSR is used as a tiebreaker. The BSR election process is preemptive, for example if a new C-BSR with a higher priority comes up, it triggers a new election process.
- Candidate Rendezvous Point (C-RP) — An RP acts as a meeting place for sources and receivers of multicast data. A device that is configured as a C-RP periodically advertises the multicast group mapping information directly to the elected BSR through unicast. These messages contain the Group-range, C-RP address, and a hold time. The IP address of the current BSR is learned from the periodic BSR messages that are received by all routers in the network. In this way, the BSR learns about possible RPs that are currently up and reachable.

Note The ASA does not act as a C-RP, even though the C-RP is a mandatory requirement for BSR traffic. Only routers can act as a C-RP. So, for BSR testing functionality, you must add routers to the topology.

- BSR Election Mechanism — Each C-BSR originates Bootstrap messages (BSMs) that contain a BSR Priority field. Routers within the domain flood the BSMs throughout the domain. A C-BSR that hears about a higher-priority C-BSR than itself suppresses its sending of further BSMs for some period of time. The single remaining C-BSR becomes the elected BSR, and its BSMs inform all the other routers in the domain that it is the elected BSR.

Multicast group concept

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries. Hosts can be located anywhere on the Internet. Hosts that want to receive data sent to a group must join the group using IGMP.

Group membership requirements

Hosts must be a member of the group to receive the data stream. For information about how to configure multicast groups, see Configure a Multicast Group, on page 16.

Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

Clustering

Multicast routing supports clustering. In Spanned EtherChannel clustering, the control unit sends all multicast routing packets and data packets until fast-path forwarding is established.

After fast-path forwarding is established, data units may forward multicast data packets. All data flows are full flows. Stub forwarding flows are also supported. Because only one unit receives multicast packets in Spanned EtherChannel clustering, redirection to the control unit is common. In Individual Interface clustering, units do not act independently. All data and routing packets are processed and forwarded by the control unit. Data units drop all packets that have been sent.

Guidelines for multicast routing

Table 1: System requirements

Item	Description
Context mode	Supported in single context mode.
Firewall mode	Supported only in routed firewall mode. Transparent firewall mode is not supported.
IPv6	IPv6 is not supported.
Multicast group	The range of addresses from 224.0.0.0 to 224.0.0.255 is reserved for routing protocols and other topology discovery or maintenance protocols, such as gateway discovery and group membership reporting. Internet multicast routing from the 224.0.0/24 address range is not supported. When multicast routing is enabled for reserved addresses, an IGMP group is not created.
Clustering	In clustering, for IGMP and PIM, this feature is only supported on the primary unit.

Access control configuration

You must configure an access control rule on the inbound interface to allow traffic to the multicast host, such as 224.1.2.3. However, you cannot specify a destination interface for the rule, or it cannot be applied to multicast connections during initial connection validation.

Interface and protocol management

Ensure proper configuration management when working with PIM-enabled interfaces and multicast routing protocols.

- Multicast routing is not supported in ECMP.
- Do not configure ASA to simultaneously be a Rendezvous Point (RP) and a First Hop Router.
- The HSRP standby IP address does not participate in PIM neighborship. If the RP router IP is routed through the HSRP standby IP address, multicast routing does not work in ASA. To ensure multicast traffic passes through successfully, configure the route for the RP address to use an interface IP address rather than the HSRP standby IP address.

Enable Multicast Routing

Enabling multicast routing on the ASA, enables IGMP and PIM on all data interfaces by default, but not on the management interface for most models (see Management Slot/Port Interface for interfaces that do not allow through traffic). IGMP is used to learn whether members of a group are present on directly attached

subnets. Hosts join multicast groups by sending IGMP report messages. PIM is used to maintain forwarding tables to forward multicast datagrams.

To enable multicast routing on the management interface, you must explicitly set a multicast boundary on the management interface.

Note Only the UDP transport layer is supported for multicast routing.

The following list shows the maximum number of entries for specific multicast tables. Once these limits are reached, any new entries are discarded.

- MFIB—30,000
- IGMP Groups—30,000
- PIM Routes—72,000

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast**.

Step 2 In the Multicast pane, check the **Enable Multicast** routing check box.

Checking this check box enables IP multicast routing on the ASA. Unchecking this check box disables IP multicast routing. By default, multicast is disabled. Enabling multicast routing enables multicast on all interfaces. You can disable multicast on a per-interface basis.

Customize Multicast Routing

This section describes how to customize multicast routing.

Configure Stub Multicast Routing and Forward IGMP Messages

Note Stub multicast routing is not supported concurrently with PIM sparse and bidirectional modes.

An ASA acting as the gateway to the stub area does not need to participate in PIM sparse mode or bidirectional mode. Instead, you can configure it to act as an IGMP proxy agent and forward IGMP messages from hosts connected on one interface to an upstream multicast router on another interface. To configure the ASA as an IGMP proxy agent, forward the host join and leave messages from the stub area interface to an upstream interface. You must also enable PIM on the interfaces participating in stub mode multicast routing.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast**.

Step 2 In the Multicast pane, check the **Enable Multicast routing** check box.

Step 3 Click **Apply** to save your changes.

Step 4 Choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Protocol**.

Step 5 To modify the specific interface from which you want to forward IGMP messages, select the interface and click **Edit**.

The **Configure IGMP Parameters** dialog box appears.

Step 6 From the **Forward Interface** drop-down list, choose the specific interface from which you want to forward IGMP messages.

Step 7 Click **OK** to close this dialog box, then click **Apply** to save your changes.

Configure a Static Multicast Route

Configuring static multicast routes lets you separate multicast traffic from unicast traffic. For example, when a path between a source and destination does not support multicast routing, the solution is to configure two multicast devices with a GRE tunnel between them and to send the multicast packets over the tunnel.

When using PIM, the ASA expects to receive packets on the same interface where it sends unicast packets back to the source. In some cases, such as bypassing a route that does not support multicast routing, you may want unicast packets to take one path and multicast packets to take another.

Static multicast routes are not advertised or redistributed.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **MRoute**.

Step 2 Choose **Add** or **Edit**.

The Add or Edit Multicast Route dialog box appears.

Use the Add Multicast Route dialog box to add a new static multicast route to the ASA. Use the Edit Multicast Route dialog box to change an existing static multicast route.

Step 3 In the Source Address field, enter the IP address of the multicast source. You cannot change this value when editing an existing static multicast route.

Step 4 Choose the network mask for the IP address of the multicast source from the Source Mask drop-down list.

Step 5 In the Incoming Interface area, click either the **RPF Interface** radio button to choose RPF to forward the route or the **Interface Name** radio button, then enter the following:

- In the Source Interface field, choose the incoming interface for the multicast route from the drop-down list.

- In the Destination Interface field, choose the destination interface that the route is forwarded through from the drop-down list.

Note
You can specify the interface or the RPF neighbor, but not both at the same time.

Step 6 In the Administrative Distance field, choose the administrative distance of the static multicast route. If the static multicast route has the same administrative distance as the unicast route, then the static multicast route takes precedence.

Step 7 Click **OK**.

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

This section describes how to configure optional IGMP setting on a per-interface basis.

Disable IGMP on an Interface

You can disable IGMP on specific interfaces. This information is useful if you know that there are no multicast hosts on a specific interface and you want to prevent the ASA from sending host query messages on that interface.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Protocol**.

The Protocol pane displays the IGMP parameters for each interface on the ASA.

Step 2 Choose the interface that you want to disable and click **Edit**.

Step 3 To disable the specified interface, uncheck the **Enable IGMP** check box.

Step 4 Click **OK**.

The Protocol pane displays Yes if IGMP is enabled on the interface, or No if IGMP is disabled on the interface.

Configure IGMP Group Membership

You can configure the ASA to be a member of a multicast group. Configuring the ASA to join a multicast group causes upstream routers to maintain multicast routing table information for that group and keep the paths for that group active.

Note If you want to forward multicast packets for a specific group to an interface without the ASA accepting those packets as part of the group, see Configure a Statically Joined IGMP Group, on page 9.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Join Group**.

Step 2 Click **Add** or **Edit** > **in the** > **Join Group** > **pane**.

The Add IGMP Join Group dialog box allows you to configure an interface to be a member of a multicast group. The Edit IGMP Join Group dialog allows you to change existing membership information.

Step 3 In the Interface Name field, choose the interface name from the drop-down list. If you are editing an existing entry, you cannot change this value.

Step 4 In the Multicast Group Address field, enter the address of a multicast group to which the interface belongs. Valid group addresses range from 224.0.0.0 to 239.255.255.255.

Step 5 Click **OK**.

Configure a Statically Joined IGMP Group

Sometimes a group member cannot report its membership in the group because of some configuration, or there may be no members of a group on the network segment. However, you still want multicast traffic for that group to be sent to that network segment. You can have multicast traffic for that group sent to the segment by configuring a statically joined IGMP group.

In the main ASDM window, choose **Configuration > Routing > Multicast > IGMP > Static Group** to configure the ASA to be a statically connected member of a group. With this method, the ASA does not accept the packets itself, but only forwards them. Therefore, this method allows fast switching. The outgoing interface appears in the IGMP cache, but this interface is not a member of the multicast group.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Static Group**.

Step 2 Click **Add** or **Edit** in the **Static Group** pane.

Use the Add IGMP Static Group dialog box to statically assign a multicast group to an interface. Use the Edit IGMP Static Group dialog box to change existing static group assignments.

Step 3 In the Interface Name field, choose the interface name from the drop-down list. If you are editing an existing entry, you cannot change this value.

Step 4 In the Multicast Group Address field, enter the address of a multicast group to which the interface belongs. Valid group addresses range from 224.0.0.0 to 239.255.255.255.

Step 5 Click **OK**.

Control Access to Multicast Groups

You can control access to multicast groups by using access control lists.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Access Group**.

The Access Group pane appears. The table entries in the Access Group pane are processed from the top down. Place more specific entries near the top of the table and more generic entries further down. For example, place an access group entry that permits a specific multicast group near the top of the table and an access group entry below that denies a range of multicast groups, including the group in the permit rule. The group is permitted because the permit rule is enforced before the deny rule.

Double-clicking an entry in the table opens the Add or Edit Access Group dialog box for the selected entry.

Step 2 Click **Add** or **Edit**.

The Add Access Group or Edit Access Group dialog box appears. The Add Access Group dialog box lets you add a new access group to the Access Group Table. The Edit Access Group dialog box lets you change information for an existing access group entry. Some fields may be dimmed when editing existing entries.

Step 3 Choose the interface name with which the access group is associated from the Interface drop-down list. You cannot change the associated interface when you are editing an existing access group.

Step 4 Choose permit from the Action drop-down list to allow the multicast group on the selected interface. Choose deny from the Action drop-down list to filter the multicast group from the selected interface.

Step 5 In the Multicast Group Address field, enter the address of the multicast group to which the access group applies.

Step 6 Enter the network mask for the multicast group address, or choose one of the common network masks from the Netmask drop-down list.

Step 7 Click **OK**.

Limit the Number of IGMP States on an Interface

You can limit the number of IGMP states resulting from IGMP membership reports on a per-interface basis. Membership reports exceeding the configured limits are not entered in the IGMP cache, and traffic for the excess membership reports is not forwarded.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Protocol**.

Step 2 Choose the interface you want to limit from the table on the Protocol pane, and click **Edit**.

The Configure IGMP Parameters dialog box appears.

Step 3 Enter the maximum number of host that can join on an interface, in the Group Limit field.

The default value is 500.Valid values range from 0 to 5000.

Note
Setting this value to 0 prevents learned groups from being added, but manually defined memberships are still permitted.

Step 4 Click **OK**.



Note When you change the IGMP limit on the interface with active joins on it, the new limit is not applicable to the existing groups. ASA validates the limit only when a new group is added to the interface or when the IGMP join timers expire. To apply the new limit with immediate effect, you must disenable and re-enable IGMP on the interface.

Modify the Query Messages to Multicast Groups

The ASA sends query messages to discover which multicast groups have members on the networks attached to the interfaces. Members respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Query messages are addressed to the all-systems multicast group, which has an address of 224.0.0.1, with a time-to-live value of 1.

These messages are sent periodically to refresh the membership information stored on the ASA. If the ASA discovers that there are no local members of a multicast group still attached to an interface, it stops forwarding multicast packet for that group to the attached network, and it sends a prune message back to the source of the packets.

By default, the PIM designated router on the subnet is responsible for sending the query messages. By default, they are sent once every 125 seconds.

When changing the query response time, by default, the maximum query response time advertised in IGMP queries is 10 seconds. If the ASA does not receive a response to a host query within this amount of time, it deletes the group.

To change the query interval, query response time, and query timeout value, perform the following steps:

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Protocol**.

Step 2 Choose the interface you want to limit from the table on the Protocol pane, and click **Edit**.

The Configure IGMP Parameters dialog box appears.

Step 3 Enter the interval in seconds, at which the designated router sends IGMP host-query messages, in the **Query Interval** field.

Valid values range from 1 to 3600 seconds. The default value is 125 seconds.

Note
If the ASA does not hear a query message on an interface for the specified timeout value, then the ASA becomes the designated router and starts sending the query messages.

Step 4 Enter the period of time, in seconds, in the **Query Timeout** field before which the ASA takes over as the requester for the interface after the previous requester has stopped doing so.

Valid values range from 60 to 300 seconds. The default value is 255 seconds.

Step 5 In the **Response Time** field, enter the maximum query response time advertised in IGMP queries, in seconds.

Values range from 1 to 25 seconds. The default value is 10 seconds.

Step 6 Click **OK**.

Change the IGMP Version

By default, the ASA runs IGMP Version 2, which enables several additional features.

All multicast routers on a subnet must support the same version of IGMP. The ASA does not automatically detect Version 1 routers and switch to Version 1. However, a mix of IGMP Version 1 and 2 hosts on the subnet works; the ASA running IGMP Version 2 works correctly when IGMP Version 1 hosts are present.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Protocol**.

Step 2 Choose the interface whose version of IGMP you want to change from the table on the Protocol pane, and click **Edit**.

The Configure IGMP Interface dialog box appears.

Step 3 Choose the version number from the Version drop-down list.

Step 4 Click **OK**.

Configure PIM Features

Routers use PIM to maintain forwarding tables to use for forwarding multicast diagrams. When you enable multicast routing on the ASA, PIM and IGMP are automatically enabled on all interfaces.



Note PIM is not supported with PAT. The PIM protocol does not use ports, and PAT only works with protocols that use ports.

This section describes how to configure optional PIM settings.

Enable and Disable PIM on an Interface

You can enable or disable PIM on specific interfaces.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Protocol**.

Step 2 Choose the interface on which you want to enable PIM from the table on the Protocol pane, and click **Edit**.

The **Edit PIM Protocol** dialog box appears.

Step 3 Check the **Enable PIM** check box. To disable PIM, uncheck this check box.

Step 4 Click **OK**.

Configure a Static Rendezvous Point Address

All routers within a common PIM sparse mode or bidir domain require knowledge of the PIM RP address. The address is statically configured using the **pim rp-address** command.

Note The ASA does not support Auto-RP.

You can configure the ASA to serve as RP to more than one group. The group range specified in the ACL determines the PIM RP group mapping. If an ACL is not specified, then the RP for the group is applied to the entire multicast group range (224.0.0.0/4).

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Rendezvous Points**.

Step 2 Click **Add** or **Edit**.

The Add or Edit Rendezvous Point dialog box appears. The **Add Rendezvous Point** dialog box lets you add a new entry to the Rendezvous Point table. The Edit Rendezvous Point dialog box lets you change an existing RP entry. Additionally, you can click **Delete** to remove the selected multicast group entry from the table.

These restrictions apply to RPs:

- You cannot use the same RP address twice.
- You cannot specify All Groups for more than one RP.

Step 3 In the **Rendezvous Point Address** field, enter the IP address for the RP.

When editing an existing RP entry, you cannot change this value.

Step 4 Check the **Use bi-directional forwarding** check box if the specified multicast groups are to operate in bidirectional mode. The Rendezvous Point pane displays Yes if the specified multicast groups are to operate in bidirectional mode and displays No if the specified groups are to operate in sparse mode. In bidirectional mode, if the ASA receives a multicast packet and has no directly connected members or PIM neighbors present, it sends a prune message back to the source.

Step 5 Click the **Use this RP for All Multicast Groups** radio button to use the specified RP for all multicast groups on the interface, or the **Use this RP for the Multicast Groups as specified below** radio button to designate the multicast groups to use with the specified RP.

For more information about multicast groups, see Configure a Multicast Group, on page 16.

Step 6 Click **OK**.

Configure the Designated Router Priority

The DR is responsible for sending PIM register, join, and prune messages to the RP. When there is more than one multicast router on a network segment, selecting the DR is based on the DR priority. If multiple devices have the same DR priority, then the device with the highest IP address becomes the DR.

By default, the ASA has a DR priority of 1. You can change this value.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Protocol**.

Step 2 Choose the interface that you want to enable for PIM from the table on the Protocol pane, and click **Edit**.

The Edit PIM Protocol dialog box appears.

Step 3 In the DR Priority field, type the value for the designated router priority for the selected interface. The router with the highest DR priority on the subnet becomes the designated router. Valid values range from 0 to 4294967294. The default DR priority is 1. Setting this value to 0 makes the ASA interface ineligible to become the default router.

Step 4 Click **OK**.

Configure and Filter PIM Register Messages

When the ASA is acting as an RP, you can restrict specific multicast sources from registering with it to prevent unauthorized sources from registering with the RP. The Request Filter pane lets you define the multicast sources from which the ASA will accept PIM register messages.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Request Filter**.

Step 2 Click **Add**.

The Request Filter Entry dialog box lets you define the multicast sources that are allowed to register with the ASA when the ASA acts as an RP. You create the filter rules based on the source IP address and the destination multicast address.

Step 3 From the Action drop-down list, choose Permit to create a rule that allows the specified source of the specified multicast traffic to register with the ASA, or choose Deny to create a rule that prevents the specified source of the specified multicast traffic from registering with the ASA.

Step 4 Type the IP address for the source of the register message, in the Source IP Address field.

Step 5 Type or choose the network mask from the drop-down list for the source of the register message, in the Source Netmask field.

Step 6 Type the multicast destination address, in the Destination IP Address field.

Step 7 Type or choose the network mask from the drop-down list for the multicast destination address, in the Destination Netmask field.

Step 8 Click **OK**.

Configure PIM Message Intervals

Router query messages are used to select the PIM DR. The PIM DR is responsible for sending router query messages. By default, router query messages are sent every 30 seconds. Additionally, every 60 seconds, the ASA sends PIM join or prune messages.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Protocol**.

Step 2 Choose the interface that you want to enable for PIM from the table on the Protocol pane, and click **Edit**.

The Edit PIM Protocol dialog box appears.

Step 3 Type the frequency, in seconds, at which the interface sends PIM hello messages, in the Hello Interval field.

Step 4 Type the frequency, in seconds, at which the interface sends PIM join and prune advertisements, in the Prune Interval field.

Step 5 Click **OK**.

Configure a Route Tree

By default, PIM leaf routers join the shortest-path tree immediately after the first packet arrives from a new source. This method reduces delay, but requires more memory than the shared tree. You can configure whether or not the ASA should join the shortest-path tree or use the shared tree, either for all multicast groups or only for specific multicast addresses.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Route Tree**.

Step 2 Click one of the following radio buttons:

- **Use Shortest Path Tree for All Groups**—Choose this option to use the shortest-path tree for all multicast groups.
- **Use Shared Tree for All Groups**—Choose this option to use the shared tree for all multicast groups.
- **Use Shared Tree for the Groups specified below**—Choose this option to use the shared tree for the groups specified in the Multicast Groups table. The shortest-path tree is used for any group that is not specified in the Multicast Groups table.

  The Multicast Groups table displays the multicast groups to use with the shared tree.

  The table entries are processed from the top down. You can create an entry that includes a range of multicast groups, but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.

  To edit a multicast group, see Configure a Multicast Group, on page 16.

Configure a Multicast Group

Multicast groups are lists of access rules that define which multicast addresses are part of a group. A multicast group can include a single multicast address or a range of multicast addresses. Use the Add Multicast Group dialog box to create a new multicast group rule. Use the Edit Multicast Group dialog box to modify an existing multicast group rule.

To configure a multicast group, perform the following steps:

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Rendezvous Points**.

Step 2 The Rendezvous Point pane appears. Click the group that you want to configure.

The Edit Rendezvous Point dialog box appears.

Step 3 Click the **Use this RP for the Multicast Groups as specified below** radio button to designate the multicast groups to use with the specified RP.

Step 4 Click **Add** or **Edit**.

The Add or Edit Multicast Group dialog box appears.

Step 5 From the Action drop-down list, choose Permit to create a group rule that allows the specified multicast addresses, or choose Deny to create a group rule that filters the specified multicast addresses.

Step 6 In the Multicast Group Address field, type the multicast address associated with the group.

Step 7 From the Netmask drop-down list, choose the network mask for the multicast group address.

Step 8 Click **OK**.

Filter PIM Neighbors

You can define the routers that can become PIM neighbors. By filtering the routers that can become PIM neighbors, you can do the following:

- Prevent unauthorized routers from becoming PIM neighbors.
- Prevent attached stub routers from participating in PIM.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Neighbor Filter**.

Step 2 Choose the PIM neighbor that you want to configure from the table by clicking **Add**/**Edit**/**Insert**.

The **Add/Edit/Insert Neighbor Filter Entry** dialog box appears. It lets you create the ACL entries for the multicast boundary ACL. You can also delete a selected PIM neighbor entry.

Step 3 Choose the interface name from the **Interface Name** drop-down list.

Step 4 From the **Action** drop-down list, choose **Permit** or **Deny** for the neighbor filter ACL entry.

Choosing Permit allows the multicast group advertisements to pass through the interface. Choosing Deny prevents the specified multicast group advertisements from passing through the interface. When a multicast boundary is configured on an interface, all multicast traffic is prevented from passing through the interface unless permitted with a neighbor filter entry.

Step 5 Enter the IP address of the multicast PIM group being permitted or denied, in the **IP Address** field. Valid group addresses range from 224.0.0.0 to 239.255.255.255.

Step 6 From the **Netmask** drop-down list, choose the netmask for the multicast group address.

Step 7 Click **OK**.

Configure a Bidirectional Neighbor Filter

The Bidirectional Neighbor Filter pane shows the PIM bidirectional neighbor filters, if any, that are configured on the ASA. A PIM bidirectional neighbor filter is an ACL that defines the neighbor devices that can participate in the DF election. If a PIM bidirectional neighbor filter is not configured for an interface, then there are no restrictions. If a PIM bidirectional neighbor filter is configured, only those neighbors permitted by the ACL can participate in the DF election process.

When a PIM bidirectional neighbor filter configuration is applied to the ASA, an ACL appears in the running configuration with the name *interface-name*_multicast, in which the *interface-name* is the name of the interface to which the multicast boundary filter is applied. If an ACL with that name already exists, a number is appended to the name (for example, inside_multicast_1). This ACL defines which devices can become PIM neighbors of the ASA.

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled for bidir to elect a DF.

The PIM bidirectional neighbor filters enable the transition from a sparse-mode-only network to a bidir network by letting you specify the routers that should participate in the DF election, while still allowing all routers to participate in the sparse-mode domain. The bidir-enabled routers can elect a DF from among themselves, even when there are non-bidir routers on the segment. Multicast boundaries on the non-bidir routers prevent PIM messages and data from the bidir groups from leaking in or out of the bidir subset cloud.

When a PIM bidirectional neighbor filter is enabled, the routers that are permitted by the ACL are considered to be bidirectionally capable. Therefore, the following is true:

- If a permitted neighbor does not support bidir, then the DF election does not occur.
- If a denied neighbor supports bidir, then the DF election does not occur.
- If a denied neighbor does not support bidir, the DF election can occur.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Bidirectional Neighbor Filter**.

Step 2 Double-click an entry in the PIM Bidirectional Neighbor Filter table to access the Edit Bidirectional Neighbor Filter Entry dialog box for that entry.

Step 3 Choose the PIM neighbor that you want to configure from the table by clicking **Add**/**Edit**/**Insert**.

The **Add/Edit/Insert Bidirectional Neighbor Filter Entry** dialog box appears, which lets you create ACL entries for the PIM bidirectional neighbor filter ACL

Step 4 Choose the interface name from the **Interface Name** drop-down list. Select the interface for which you are configuring the PIM bidirectional neighbor filter ACL entry.

Step 5 From the **Action** drop-down list, choose **Permit** or **Deny** for the neighbor filter ACL entry.

Choose Permit to allow the specified devices to participate in the DF election process. Choose Deny to prevent the specified devices from participating in the DF election process.

Step 6 Enter the IP address of the multicast PIM group being permitted or denied. Valid group addresses range from 224.0.0.0 to 239.255.255.255, in the IP Address field.

Step 7 From the Netmask drop-down list, choose the netmask for the multicast group address.

Step 8 Click **OK**.

Configure the ASA as a Candidate BSR

You can configure the ASA as a candidate BSR. It also helps in the auto discovery of the RP.

Procedure

Step 1 In ASDM, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Bootstrap Router**.

Step 2 Check the **Configure this ASA as a candidate bootstrap router (CBSR)** check box to perform the CBSR set up.

a) Select the interface on the ASA from which the BSR address is derived to make it a candidate from the **Select Interface** drop-down list.

Note
This interface must be enabled with PIM.

b) Enter the length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called in the **Hash mask length** field. All groups with the same seed hash (correspond) to the same Rendezvous Point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups.

c) Enter the priority of the candidate BSR in the **Priority** field. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

Step 3 (Optional) Select an interface on which no PIM BSR messages will be sent or received, in the **Configure this ASA as a Border Bootstrap Router** section.

Step 4 Click **Apply**.

Configure a Multicast Boundary

Address scoping defines domain boundaries so that domains with RPs that have the same IP address do not leak into each other. Scoping is performed on the subnet boundaries within large domains and on the boundaries between the domain and the Internet.

You can set up an administratively scoped boundary on an interface for multicast group addresses. IANA has designated the multicast address range from 239.0.0.0 to 239.255.255.255 as the administratively scoped addresses. This range of addresses can be reused in domains administered by different organizations. The addresses would be considered local, not globally unique.

A standard ACL defines the range of affected addresses. When a boundary is set up, no multicast data packets are allowed to flow across the boundary from either direction. The boundary allows the same multicast group address to be reused in different administrative domains.

You can configure, examine, and filter Auto-RP discovery and announcement messages at the administratively scoped boundary. Any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL are removed. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Routing** > **Multicast** > **MBoundary**.

The MBoundary pane lets you configure a multicast boundary for administratively scoped multicast addresses. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains. When a multicast boundary is defined on an interface, only the multicast traffic permitted by the filter ACL passes through the interface.

Step 2 Click **Edit**.

The Edit Boundary Filter dialog box appears and displays the multicast boundary filter ACL. You can add and remove boundary filter ACL entries using this dialog box.

When the boundary filter configuration is applied to the ASA, the ACL appears in the running configuration with the name *interface-name*_multicast, where the *interface-name* is the name of the interface to which the multicast boundary filter is applied. If an ACL with that name already exists, a number is appended to the name (for example, inside_multicast_1).

Step 3 Choose the interface for which you are configuring the multicast boundary filter ACL from the Interface drop-down list.

Step 4 Check the **Remove any Auto-RP group range** check box to filter Auto-RP messages from sources denied by the boundary ACL. If the **Remove any Auto-RP group range** check box is unchecked, all Auto-RP messages are passed.

Step 5 Click **OK**.

Monitoring for PIM

To monitor or disable various PIM routing statistics, perform the following steps:

Procedure

Step 1 In the main ASDM window, choose **Monitoring** > **Routing** > **PIM** > **BSR Router**

The BSR Router configuration information is displayed.

Step 2 In the main ASDM window, choose **Monitoring** > **Routing** > **PIM** > **Multicast Routing Table**

The contents of the multicast routing table are displayed.

Step 3 In the main ASDM window, choose **Monitoring** > **Routing** > **PIM** > **MFIB**

The summary information about the number of IPv4 PIM multicast forwarding information base entries and interfaces are displayed.

Step 4 In the main ASDM window, choose **Monitoring** > **Routing** > **PIM** > **MFIB Active**

The summary information from the Multicast Forwarding Information Base (MFIB) about the rate at which active multicast sources are sending to multicast groups is displayed.

Step 5 In the main ASDM window, choose **Monitoring** > **Routing** > **PIM** > **Group Map**

The summary information from the Multicast Forwarding Information Base (MFIB) about the rate at which active multicast sources are sending to multicast groups is displayed.

a) Select **RP Timers** from the **Select PIM Group** drop-down list, to view the timer information for each group-to-PIM mode mapping.

Step 6 In the main ASDM window, choose **Monitoring** > **Routing** > **PIM** > **Neighbors**

The Protocol Independent Multicast (PIM) neighbor information is displayed.

Example for Multicast Routing

The following example shows how to enable and configure multicast routing with various optional processes:

1. In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast**.
2. In the Multicast pane, check the **Enable Multicast** routing check box, and click **Apply**.
3. In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **MRoute**.
4. Click **Add** or **Edit**.

   The Add or Edit Multicast Route dialog box appears.

   Use the Add Multicast Route dialog box to add a new static multicast route to the ASA. Use the Edit Multicast Route dialog box to change an existing static multicast route.
5. In the Source Address field, enter the IP address of the multicast source. You cannot change this value when editing an existing static multicast route.
6. Choose the network mask for the IP address of the multicast source from the Source Mask drop-down list.
7. In the Incoming Interface area, click either the **RPF Interface** radio button to choose RPF to forward the route or the **Interface Name** radio button, then enter the following:
   - In the Source Interface field, choose the incoming interface for the multicast route from the drop-down list.
   - In the Destination Interface field, choose the destination interface to which the route is forwarded through the selected interface from the drop-down list.

Note You can specify the interface or the RPF neighbor, but not both at the same time.

8. In the Administrative Distance field, choose the administrative distance of the static multicast route. If the static multicast route has the same administrative distance as the unicast route, then the static multicast route takes precedence.
9. Click **OK**.
10. In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **Multicast** > **IGMP** > **Join Group**.

    The Join Group pane appears.
11. Click **Add** or **Edit**.

    The Add IGMP Join Group dialog box allows you to configure an interface to be a member of a multicast group. The Edit IGMP Join Group dialog box allows you to change existing membership information.
12. In the Interface Name field, choose the interface name from the drop-down list. If you are editing an existing entry, you cannot change this value.

13. In the Multicast Group Address field, enter the address of a multicast group to which the interface belongs. Valid group addresses range from 224.0.0.0 to 239.255.255.255.
14. Click **OK**.

History for Multicast Routing

Table 2: Feature History for Multicast Routing

Feature Name	Platform Releases	Feature Information
Multicast routing over an Static Virtual Tunnel Interface tunnel	9.24(10)	You can securely deliver real-time multicast applications, such as video streaming, financial data feeds, and data replication over your VPN infrastructure by using IPsec tunnels configured with static VTI.
Multicast routing support	7.0(1)	Support was added for multicast routing data, authentication, and redistribution and monitoring of routing information using the multicast routing protocol. We introduced the following screen: Configuration > Device Setup > Routing > Multicast.
Clustering support	9.0(1)	Support was added for clustering.
Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) pass-through support	9.5(1)	Support was added to allow PIM-SSM packets to pass through when multicast routing is enabled, unless the ASA is the Last-Hop Router. This allows greater flexibility in choosing a multicast group while also protecting against different attacks; hosts only receive traffic from explicitly-requested sources. We did not change any screens.
Protocol Independent Multicast Bootstrap Router(BSR)	9.5(2)	Support was added for a new dynamic Rendezvous Point (RP) selection model that uses candidate routers for Rendezvous Point function and for relaying the Rendezvous Point information for a group. This feature provides a means of dynamically learning Rendezvous Points (RPs), which is very essential in large complex networks where an RP can periodically go down and come up. We introduced the following screens: Configuration > Device Setup > Routing > Multicast > PIM > Bootstrap Router
igmp limit increased	9.15(1) *Also in 9.12(4)*	igmp limit increased from 500 to 5000. We did not change any screens.