



SSM Channel Based Filtering for Multicast Boundaries

The SSM Channel Based Filtering for Multicast Boundaries feature enables the user to apply filtering policies based on Source Specific Multicast (SSM) channels for Source and Group (S,G) addresses, which is a combination of source and destination IP addresses.

Feature History for the SSM Channel Based Filtering for Multicast Boundaries Feature

Release	Modification
12.3(11)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for SSM Channel Based Filtering for Multicast Boundaries, page 2](#)
- [Restrictions for SSM Channel Based Filtering for Multicast Boundaries, page 2](#)
- [Information About the SSM Channel Based Filtering for Multicast Boundaries Feature, page 2](#)
- [How to Configure SSM Channel Based Filtering for Multicast Boundaries, page 3](#)
- [Configuration Examples for SSM Channel Based Filtering for Multicast Boundaries, page 4](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for SSM Channel Based Filtering for Multicast Boundaries

- IP multicast needs to be configured on the router.

Restrictions for SSM Channel Based Filtering for Multicast Boundaries

- The **filter-autorp** keyword does not support extended access lists.

Information About the SSM Channel Based Filtering for Multicast Boundaries Feature

To configure the SSM Channel Based Filtering for Multicast Boundaries feature, you should understand the following concepts:

- [Rules for Multicast Boundaries, page 2](#)
- [Benefits of SSM Channel Based Filtering for Multicast Boundaries, page 3](#)

Rules for Multicast Boundaries

The SSM Channel Based Filtering for Multicast Boundaries feature expands the **ip multicast boundary** command for control plane filtering support. More than one **ip multicast boundary** command can be applied to an interface.

The following rules govern the **ip multicast boundary** command:

- One instance of the **in** and **out** keywords can be configured on an interface.
- The **in** and **out** keywords can be used for standard or extended access lists.
- Only standard access lists are permitted with the use of the **filter-autorp** keyword or no keyword.
- A maximum of three instances of a command will be allowed on an interface: one instance of **in**, one instance of **out**, and one instance of **filter-autorp** or no keyword.
- When multiple instances of the command are used, the filtering will be cumulative. If a boundary statement with no keyword exists with a boundary statement with the **in** keyword, both access lists will be applied on the in direction and a match on either one will be sufficient.
- All instances of the command apply to both control and data plane traffic.
- Protocol information on the extended access list is parsed to allow reuse and filtering for IOS consistency. An (S,G) operation will be filtered by an extended access list under all conditions stated above for keywords if the access list filters (S,G) traffic for all protocols.

Benefits of SSM Channel Based Filtering for Multicast Boundaries

- This feature allows input on the source interface.
- The access control capabilities are the same for SSM and Any Source Multicast (ASM).

How to Configure SSM Channel Based Filtering for Multicast Boundaries

This section contains the following procedures:

- [Configuring the Multicast Boundaries, page 3](#)

Configuring the Multicast Boundaries

Perform this task to configure the multicast boundary.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list {standard | extended} *access-list-name***
4. **permit *protocol* *host address* *host address***
5. **deny *protocol* *host address* *host address***
6. Repeat Step 4 or Step 5 as needed.
7. **interface *type interface-number port-number***
8. **ip multicast boundary *access-list-name* [in |out | filter-autorp]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list {standard extended} access-list-name Example: Router(config)# ip access-list 101	Configures the standard or extended access list.
Step 4	permit protocol host address host address Example: Router(config-ext-nacl)# permit ip host 181.1.2.201 host 232.1.1.11	Permits specified ip host traffic.
Step 5	deny protocol host address host address Example: Router(config-acl-nacl)# deny ip host 181.1.2.203 host 232.1.1.1	Denies specified multicast ip group and source traffic.
Step 6	Repeat Step 4 or Step 5 as needed.	Permits and denies specified host and source traffic.
Step 7	interface type interface-number port-number Example: Router(config)# interface ethernet 2/3	Enables interface configuration mode.
Step 8	ip multicast boundary access-list-name [in out filter-autorp] Example: Router(config-if)# ip multicast boundary acc_grp1 out	Configures the multicast boundary.

Configuration Examples for SSM Channel Based Filtering for Multicast Boundaries

This section provides the following configuration examples for the multicast boundaries:

Configuring the Multicast Boundaries: Example

The following example permits outgoing traffic for (181.1.2.201, 232.1.1.1) and (181.1.2.202, 232.1.1.1) and denies all other (S,G)s.

```
configure terminal
 ip access-list extended acc_grp1
 permit ip host 0.0.0.0 232.1.1.1 0.0.0.255
 permit ip host 181.1.2.201 host 232.1.1.1
 permit udp host 181.1.2.202 host 232.1.1.1
 permit ip host 181.1.2.202 host 232.1.1.1
 deny igmp host 181.2.3.303 host 232.1.1.1
 interface ethernet 2/3
 ip multicast boundary acc_grp1 out
```

The following example permits outgoing traffic for (181.1.2.201, 232.1.1.5) and 181.1.2.202, 232.1.1.5).

```
configure terminal
 ip access-list extended acc_grp6
 permit ip host 0.0.0.0 232.1.1.1 5.0.0.255
 deny udp host 181.1.2.201 host 232.1.1.5
 permit ip host 181.1.2.201 host 232.1.1.5
 deny pim host 181.1.2.201 host 232.1.1.5
 permit ip host 181.1.2.202 host 232.1.1.5
 deny igmp host 181.2.3.303 host 232.1.1.1
 interface ethernet 2/3
 ip multicast boundary acc_grp6 out
```

The following example denies a group-range that is being announced by the candidate RP. Since the group range is denied, there will be no pim auto-rp mappings created.

```
configure terminal
 ip access-list standard acc_grp10
 deny 225.0.0.0 0.255.255.255
 permit any
 access-list extended acc_grp12
 permit pim host 181.1.2.201 host 232.1.1.8
 deny udp host 181.1.2.201 host 232.1.1.8
 permit pim host 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 0.0.0.0 host 227.7.7.7
 permit ip 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 181.1.2.201 host 232.1.1.7
 ip access-list extended acc_grp13
 deny ip host 181.1.2.201 host 232.1.1.8
 permit ip any any
 interface ethernet 2/3
 ip multicast boundary acc_grp10 filter-autorp
 ip multicast boundary acc_grp12 out
 ip multicast boundary acc_grp13 in
```

Additional References

The following sections provide references related to the Multicast VPN MIB feature.

Related Documents

Related Topic	Document Title
Multicast commands: complete syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IP Multicast Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Multicast Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

ip multicast boundary

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

