Current IP Multicast Commands

Change history

03/10/03 Added description for the "threshold" argument to "ip multicast route-limit" [12.0(23)S, 12.2(13)T, 12.2(14)S, CSCdy16803].

03/02/03 Subsecond convergence feature: Added description for "msec" option to "ip pim query-interval" and "debug ip pim hello". Updated description of "ip pim version".

01/03/03 Added description for commands introduced or modified by the SSM mapping feature: "ip igmp ssm-map enable", "ip igmp ssm-map query dns", "ip domain multicast <domain-prefix>", "ip igmp ssm-map static <acl> <source>", "ip igmp static-group <group> [... source ssm-map]", "show ip igmp ssm-mapping [<group>]"

10/13/02 Added desription for "priority <n>" option for the "ip pim rp-candidate" command. See notes below for version numbering. [CSCdx59801, 12.0(23)S, 12.2S, 12.2(PI5)T]

10/13/02 Added desription on AutoRP and BSR interworking in Cisco IOS. See description of "ip pim bsr-candidate" and "ip pim send-rp-discovery".

08/16/02 Added description for "ip multicast route-limit <routes>" [12.1(2), 12.0(11)S, CSCdm84653]

08/05/02 Added description for CISCO-PIM-MIB feature, "snmp-server enable traps pim ...", "snmp-server host ..." [CSCdr38615, 12.0(15)S, 12.2(4)T]

08/05/02 Added description for IP multicast heartbeat feature, "ip multicast heartbeat", "debug ip mhbeat", and "snmp-server enable traps ipmulticast"[CSCdr40842, 12.1(3)T, 12.2].

07/22/02 - Added "ip pim bidir-neighbor-filter" [CSCdx11884, 12.2(10) 12.2(10)S 12.2(10)T]

07/02/02 - Added "filter-autorp" to "ip multicast boundary" command and "debug ip pim autorp" [12.0(22)S, 12.2(8)]

05/23/02 - Added "show ip msdp sa-cache [rejected-sa [detail] [read-only]]" / "ip msdp cache-rejected-sa" (CSCdv13858)

05/03/02 - Added "ip pim sparse-mode-register"

10/06/01 - Added pointer to configuration note for "ip pim rp-announce-filter"

10/10/01 - Added description for IGMP immediate-leave (CSCdk29405, CSCdr27925)
ip igmp immediate-leave (global, interface)

09/20/01 - Added description for CSCdm73649 commands:
ip pim dense-mode proxy-register
ip pim bsr-border

09/17/01 - Added description for "ip msdp sa-limit", updated documentation for "show ip msdp count", "show ip msdp peer", "show ip msdp count" [CSCdt19258].

09/17/01 - Updated information on "ip msdp cache-sa-state" - mandatory now [CSCdr93446].

08/29/01 - Added description about UDP/IGMPv3lite port number change 659 -> 465 due to CSCdr53615.

07/12/01 - Added documentation for "ip pim register-source", added notes

06/29/01 - Corrected documentation for ip multicast multipath

06/27/01 - Added documentation for ip pim bidir-enable

05/28/01 - Added documentation for ip pim dr-priority

05/28/01 - Added documentation for Bidir-PIM commands
ip pim rp-address ... bidir

```
          ip pim send-rp-announce ... bidir
        ip pim rp-candidate ... bidir
05/17/01 - Added description for ip msdp sa-filter RP matching options
05/09/01 - Added documentation for source option to "ip igmp static-group"
05/09/01 - ip pim spt-threshold note added.
05/09/01 - Added SSM / IGMP version 3 feature documentation:
         ip igmp version 3, ip pim ssm, ip urd, ip igmp v3lite,
         show ip igmp group detail, debug ip urd
```

Notes:

The text in brackets after the description of a command details the releases and sometimes also the ddts number in which this command appeared. The versions shown are only those where a command was explicitly added to the code, but in addition to that, the command will also be available on all further IOS version that inherit from one one the shown IOS versions:

```
   12.0S, 12.0T  inherits from 12.0
   12.1          inherits from 12.0T
   12.1E, 12.1T  inherits from 12.1
   12.2          inherits from 12.1T
   12.2T         inherits from 12.2
   12.2T         inherits from 12.2
   12.2S         inherits from 12.2 and 12.1E
   12.3          inherits from 12.2T
```

For features documented here before they are released on CCO (in support of EFT testers), the final CCO version numbers are not always known. The following abbreviations are used:

```
   12.X(PIy)T - the y'th maintenance release of Cisco IOS 12.XT on CCO
                Example: 12.2(PI5)T is the fifth maintenance release of
                 12.2T after the first four which are 12.2(2), 12.2(4)T,
                 12.2(8)T, 12.2(11)T)

   12.2S      - Release numbers for 12.2S images will be added later.
```

Global commands:

```
  [no] ip multicast-routing [distributed]
      Enables IP multicast forwarding. If disabled, group addressed IP
      packets that the router is not a member will be discarded. The
      default value is IP multicast routing disabled. [10.2]

      The distributed keyword will enable distributed fastswitching for the
      router. The interface command described below will enable
      individual interfaces for distributed fastswitching. [11.1(20)CC].

  [no] ip multicast route-limit <routes> [<threshold>]
      Configure this command to limit the total number of (*,G) and
      (S,G) multicast routing table entries as shown in
    "show ip mroute" to <routes>. Use this command to limit the
    impact of Denial of Service attacks based on creating useless
    IP multicast routing state. Valid arguments are 1... 2,147,483,646.
    "no ip multicast route-limit" establishes a multicast route-limit of
    2,147,483,647 (the maximum 32-bit integer value). This is
```

also the default configuration and it will not show up in the configuration.

If the router needs to create a new multicast routing table entry but has exceeded the number of configured <routes>, a warning level log messae will be emitted:

"<current-routes> routes exceeded multicast route-limit of <routes>"

<current-routes> can be larger than <routes> if you configured "ip multicast route-limit <routes>" when he router already had more routes than <routes> installed. In that case the router will not remove already existing routes (you can force deletion of routes with "clear ip mroute"). The currently configured value <routes> is also displayed in the "show ip mroute count" command. [12.1(2), 12.0(11)S, CSCdm84653]

If the optional <thres> argmument is configured, Cisco IOS will start emitting warning messages as soon as at least <thresh> mroutes are established:

"multicast route-limit warning (curr <n> threshold <thresh>) - VRF <name>",

Establishing a lower threshold than limit allows for the network operator to be alerted before the actual user will see any limitation [12.0(23)S, 12.2(13)T, 12.2(14)S, CSCdy16803].

[no] ip multicast cache-headers [rtp] [<entries>]

Allocates a circular buffer to store IP multicast packet headers that are received by the router. This command will allocate approximately a 32 kilobyte buffer. If you are low on memory, this command should not be used. Use the "show ip mpacket" command to display this buffer. This feature is used to determine 1) who is sending to what groups, 2) what the inter-packet delay and 3) if there are any duplicates or multicast forwarding loops in your network. [11.1]

When the keyword "rtp" is used, RTP headers will also be saved. This is used in conjuction with the "show ip mpacket <group> quality" command. [11.1(20)CC]

<entries> is the power-of-2 number of cache entries maintained in the circular buffer. Valid values are 10 through 20. Use caution when setting this value greater than 10 because you can use up all the memory in the router. The default value is 10, which means 1024 entry circular buffer is maintained. [11.1(22)CC, 12.0S]

ip multicast heartbeat <group> <minimum> <window> <interval>

[no] ip multicast heartbeat <group>

This featurette allows you to monitor existing ip multicast traffic via SNMP traps. It command is a simple but effective alternative to MRM.

ionfigure this command to receive an SNMP traps when ip multicast group <group> has not been forwarding traffic during at least <minimum> out of the last <window> intervals of length <interval>

<interval> should be set to multiple of 10 seconds on platforms that

use MDFS because on those platforms, the packet counters are only updated once every 10 seconds (Cisco-7500, Cisco-12000). Other platforms may have other increments (Cisco-6500).

This command will not create a heartbeat if no multicast forwarding state exists for <group> at all in the router.

This command will not create state in the router. Use "ip igmp static-group" on this or a downstream router to force forwarding of ip multicast traffic.

You need to enable trap generation for ip multicast globally via the "snmp-server enable traps ipmulticast" for this command to be effective. Use the "snmp-server host ... ipmulticast" command to enable sending of ipmulticast traps to specific receiver hosts.

Use "debug ip mhbeat" to debug operations of this command.

Example:

```
snmp-server enable traps ipmulticast
ip multicast heartbeat 224.0.1.53 2 5 10
```

The router will sample the packets forwarded for group 224.0.1.53 in intervals of 10 seconds. If at least one packet was forwarded during 2 out of the last 5 intervals, no trap will be generated. Only if the router did not see packets being forwarded during 4 or more of these 10 second intervals will a trap be generated.

The SNMP trap triggered by this command is ciscoIpMRouteMissingHeartBeats defined in CISCO-IPMROUTE-MIB. See ftp://ftpeng.cisco.com/ipmulticast/config-notes/mib-info.txt for more information about the MIB. See ftp://ftpeng.cisco.com/ipmulticast/mibs for the MIBs themselves.
[CSCdr40842, 12.1(3)T, 12.2]

[no] ip multicast multipath

By default, this command is not enabled, and the RPF neighbor for all (*,Gi) with a certain RP and all (Si,G) with a certain Si is the PIM neihgbor with the highest IP address if there are multiple equal-cost alternatives for RP or Si. If this command is enabled, then the RPF neighbor will be selected pseudo-randomnly from the available equal-cost RPF neighbors, resulting in load splitting of traffic from different sources amongst the available equal cost paths (or neighbors). All traffic from a single source is still received from a single neighbor [12.0, 12.0S, 12.0T]

[no] ip pim bidir-enable

This global configuration command enables support for Bidir PIM on the router. If not enabled, then The router will behave like a legacy IOS router that does not support Bidir-PIM: The PIM Hello messages will not contain the Bidir option, the bidir options to the rp configuration commands will not be allowed, no Bidir-PIM DF election messages will be sent and received messages will be ignored, CLI commands for bidir will not work. This command exists to avoid potential issues when upgrading routers to images supporting Bidir-PIM. The default for this command in 12.0ST

is "no ip pim bidir-enable", the default for 12.2 and 12.2T is "ip pim bidir-enable". [CSCdu53264, 12.0(18)ST, 12.2(2), 12.2(3)T]

[no] ip pim ssm [default | range <acl>]
Configure the SSM-range. If the argument default is configured, then the range 232.0.0.0...232.255.255.255 will be used as the SSM-range. If range <acl> is configured than <acl> must be a numeric or named standard ip access list defining the SSM-range - all ip addresses permitted by <acl> will be considered to be within the SSM-range. The SSM-range is the range of addresses, in which the router will support Source Specific Multicast (SSM) operations: Receiver hosts use IGMP version 3, URD or IGMP v3lite to explicitly join to an (S,G) channel to receive traffic directly via the shortest path from the source. [12.1(5)T, 12.2, 12.0(15)S, 12.1(8)E]

[no] ip pim register-source <interface-unit>
By default this command is not configured and routers who are DR and need to send PIM sparse mode register messages will use the ip address of the interface towards the RP as the source address for these register messages. If that interface address is one that the RP can not reach (scoped or anycast address), then the PIM sparse mode registration process will malfunction because the RPs register-stop messages will not reach the DR. Configure ip pim register-source in global configuration command to make this router use the ip address of <interface-unit> as the source address of PIM sparse-mode register messages if you need to avoid such problem. [CSCdm95268, 12.1(1)]

[no] ip pim rp-address <ip-address> [<group-access-list>] [override] [bidir]
Configures the PIM Rendezvous Point (RP) address for a particular group. The RP address is used by first-hop routers to send Register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send Join and Prune messages toward the RP. A single RP can be configured for multiple groups described by the access-list pointer. [10.2]

If keyword "bidir" is supplied, the group range will be used for bidirectional shared-tree forwarding otherwise it will be used for sparse mode forwarding. A single <ip-address> can only be configured to be RP for either bidir or sparse mode group ranges. [12.1(2)T, 12.2]

If there is no RP configured for a group, the router will treat the group as dense using the dense-mode PIM techniques. If the RP for a group is learned through a dynamic mechanism, such as Auto-RP, then this command may not be required. If there is a conflict between the RP configured with this command and one learned by Auto-RP, the Auto-RP information is used. Unless, the "override" keyword is specified. [11.1]

[no] ip pim accept-rp {<address> | auto-rp} [<acl>]
When this command is entered, the router will only accept (*,G) Joins with an RP address of <address> if G is in the group range specified by <acl>. When this command is entered with an address equal to one of the system's addresses, the system will be the RP only for the specified group range specified in <acl>. When not in the group range,

the RP will not accept Joins or Register messages and will respond immediately to Registers with Register-Stop messages. There is no default setting for this command. [10.2]

When the keyword "auto-rp" is specified, Join and Register messages will only be accepted for RPs that are in the Auto-RP cache. [11.1]

If <address> is 0.0.0.0, the filter will accept any RP for any group accepted by <acl>, and deny any RP rejected by <acl>.

When multiple "ip pim accept-rp" filters are configured, they must be configured in the following order (in 11.3(4.5), 12.0(1) and newer images the following order is guaranteed by the IOS, irrespective of the configuration sequence):

```
ip pim accept-rp <specific RP address> <acl>
ip pim accept-rp auto-rp
ip pim accept-rp 0.0.0.0 <acl>
```

The following example will accept 171.69.58.88 as the RP for groups in 239.0.0.0/8, and RPs for groups in the Auto-RP cache. If the RP and group don't match the first two filters, the 3rd filter is in effect, i.e. any RP is accepted for groups permitted by ACL 2, and no RP for 224.0.1.39 and 224.0.1.40 is accepted.

```
ip pim accept-rp 171.69.58.88 1
ip pim accept-rp auto-rp
ip pim accept-rp 0.0.0.0 2

access-list 1 permit 239.0.0.0 0.255.255.255

access-list 2 deny 224.0.1.39
access-list 2 deny 224.0.1.40
access-list 2 permit any
```

```
[no] ip pim send-rp-announce <interface-unit> scope <ttl> group-list <acl>
                             [interval <num-seconds>] [bidir]
```

This command sends an Auto-RP RP annoucement message to the well known group CISCO-RP-ANNOUNCE (224.0.1.39). This command should be used in a router you want to be the RP. The RP address field inside the announcement message will contain the IP address from the <interface-unit>. <ttl> is the time-to-live in the IP header which is set. This allows for the announcements to stay inside a ttl scoped boundary. <group-list> is an access-list describing the group ranges this system is willing to be the RP for. Note that the deny clauses in the <group-list> are ignored. [11.1]

If keyword "bidir" is supplied, the group range will be used for bidirectional shared-tree forwarding otherwise it will be used for sparse mode forwarding. In AutoRP, a single IP address can only be RP for one type of groups, bidir or sparse mode. Use different <interface-unit> arguments if you want to use a single router as an RP for both bidir-PIM and sparse mode group ranges and want to use Auto-RP to announce these mappings. [12.1(2)T, 12.2]

Starting with IOS versions [12.0(1.1)], if the access-list contains a "deny" entry, auto-rp will maintain a negative entry for those group

ranges. This will make it easier to configure group ranges to be dense-mode only groups. An RP announcement with a denied group prefix overrides any positive announcements for the same prefix from other RPs. However, IOS versions prior to this required a deny clause. The access-list must be changed to remove these deny clauses to obtain the correct RP map.

When "interval" is specified, the interval between RP announcements is set to <number of seconds>. The total holdtime of the RP announcements is automaticly set to 3 times <interval>. The default interval is 60 seconds. Tuning this interval down can reduce the time required to fail over to a secondary RP, at the expense of generating more Auto-RP messages through the entire region covered by the ttl scope. [11.2(18), 11.3(8), 12.0(3.1)]

[no] ip pim send-rp-discovery [<interface>] scope <ttl>
By entering this command, an AutoRP RP-mapping agent is started on the router. The RP-mapping agent listens on well-known group address CISCO-RP-ANNOUNCE for announcements from candidate RPs. The RP-mapping agent will send RP-to-group mappings in an Auto-RP RP discovery message to the well known group CISCO-RP-DISCOVERY (224.0.1.40). PIM DRs will listen to this group and use the RPs they learn from the RP discovery message. <ttl> is the time-to-live in the IP header which is set. This allows for the discovery messages to stay inside a ttl scoped boundary. [11.1]

When <interface> is specified, RP discovery messages will be sourced from the IP address assigned to <interface>, otherwise the source address will be that of the outgoing interface from which the packet is sourced. If you do not specify this option and the mapping agent has multiple interfaces, and in addition, the network is also redundant then DR routers will see mappipng agent messages from multiple different interface addresses of the mapping agent - which can be confusing in troubleshooting (but is otherwise uncritical) [12.0]

Am AutoRP RP mapping agent will only sends out announcements from RPs learned via announcements from routers using AutoRP (eg: with "ip pim send-rp-announce" discovered). It will not redistribute BSR learned candidate RP information. On the other hand, a Cisco IOS router configured as a BSR will redistribute AutoRP learned information (see description of "ip pim bsr-candidate"). We do only redistribute learned mappings in one direction (AutoRP to BSR) to avoid otherwise endlessly looping C-RP announcements between AutoRP and BSR.

[no] ip pim rp-announce-filter rp-list <acl> group-list <acl>
This command is entered in the PIM RP-mapping agent. This command configures an incoming filter for RP announcement messages. Parameter "rp-list <acl>" configures an access-list of RP addresses that, if permitted, will be filtered for the group ranges denies by the parameter "group-list <acl>". If this command is not configured, all RP announcements are accepted. If you are going to use more than one RP-mapping agent, the filters should be consistent among them so there is no conflicts between different mapping agents. [11.1]

For more detailed explanations and examples see:
ftp://ftpeng.cisco.com/ipmulticast/config-notes/rp-announce-filter.txt

[no] ip pim spt-threshold <kbps> | infinity [group-list <acl>]
Configures when a PIM leaf router should join the shortest path source-tree for the specified group. <kbps> is the traffic rate in kilobits per second. If a source sends at a rate greater than or equal to <kbps>, a PIM Join message is triggered towards the source to construct a source-tree. If "infinity" is used, all sources for the specified group will use the shared-tree. Specifying a "group-list" indicates what groups the spt-threshold applies to. <acl> is a reference to a simple IP access-list. When a value of 0 is specified or the group-list parameter is not used, the threshold applies to all groups. The default setting (when this command is not used), is to join the shortest path tree immediately after the first packet arrives from a new source. [11.1]

The ability to define an spt threshold value other than 0 or infinity is deprecated. It should not be used and may not be supported in further releases [05/01].

[no] ip pim bsr-candidate <interface> <hash-mask-len> [<priority>]
Configures the router to send bootstrap messages with <interface>'s address as the bootstrap-router (BSR) address, if no better bootstrap router is found. <interface> must be a PIM enabled interface. <hash-mask-len> is the mask length used by the PIMv2 hash function. This hash mask length is accepted by all routers within the same PIM domain when selecting an RP. <priority> is an integer whose value is between 0 and 255. It is 0 by default. BSRs with larger preference values are preferred over those with smaller values.

This command should only be used in "backbone" routers with good connectivities to all parts of the PIM region. E.g. a stub router that relies on an on-demand dial-up link to connect to the rest of the PIM domain is not a good candidate BSR. [11.3T]

The BSR mechanism is specified in RFC2362. Candidate RP routers unicast C-RP-Advertisement packets to the BSR. The BSR aggregates these advertisements into Bootstrap messages which it regularily multicasts. Multicasting of these messages is special, they are hop-by-hop RPF-flooded, so they do not require any pre-existing IP multicast routing setup (unlike AutoRP). The BSR does not preselect the designated RP for a particular group range (unlike AutoRP), but instead, each router receiving Bootstrap messages will elect RPs for group ranges based on the information in the Bootstrap messages. Cisco IOS routers (12.0 and later) always accept and process Bootstrap messages. There is no command to disable this function.

Cisco IOS routers perform the following steps to determine which RP for a group is actually to be used:

1. Longest match lookup on the C-RPs announced group prefix
   (This is incompatible with RFC2362 but in compliance with the new PIM v2 spec, eg: draft-ietf-pim-sm-v2-new-05, 4.8.1 (p100))
2. If there are both AutoRP and a BSR learned C-RPs for the prefix found in 1., prefer the AutoRP learned C-RP.
   The following steps will then not be exercised as they are

specific to BSR C-RPs.
3. If more than one BSR-learned C-RP are found in 1., prefer the one with the highest priority (lowest numerical <prio> configured via "ip pim rp-candidate ... priority <prio>").
3. If more than one BSR learned C-RP have the same priority, use the BSR hash function to select the RP for a group.
4. If more than one BSR learned C-RP return the same hash value from 3., use the C-RP with the highest IP address from them.

Note: Step 3. was defect before CSCdx59801. See description of "ip pim rp-candidate" below.

A Cisco IOS BSR router will redistribute AutoRP learned prefixes in Bootstrap messages. If the BSR router knows for a given group prefix both AutoRP and BSR C-RPs, then it will only announce the (best) AutoRP RP via Bootstrap messages but not any BSR learned C-RPs (for this group prefix). In result, the router consistenly announces via BSR the same C-RPs that it also uses for itself (as explained in the previous paragraph). This behavior is independent of wether or not the BSR router is also an AutoRP mapping agent.

[no] ip pim rp-candidate <interface> [group-list <acl>] [priority <prio>] [bidir]

Configures to send pim version 2 candidate RP advertisement to the bootstrap RP. The IP address associated with <interface> will be advertised as the candidate RP address. The group prefixes defined by simple access-list <acl> will also be advertised in association with the RP address. RP-candidates should also be placed in the well-connected "backbone" part of the PIM domain. [11.3T]

If the keyword "bidir" is supplied, the group range will be used for bidirectional shared-tree forwarding otherwise it will be used for sparse mode forwarding. A single interface can only be RP for one type of groups, bidir or sparse mode. Use different <interface> arguments if you want to use a single router as an RP for both bidir-PIM and sparse mode group ranges. [12.1(2)T, 12.2]

If the option "priority <prio>" is used, then the router will announce himself to be a candidate RP with priority <prio>. The default for <prio> is 0 and is not NVgened. For this option to work, the candidate BSRs must also run a Cisco IOS version supporting this option. BSR routers running previous Cisco IOS versions ignored the priority field in candidate RP announcements and forwarded a priority of 0 for all candidate RPs in their Bootstrap messages. 0 is the highest priority, 255 is the lowest priority. See "ip pim bsr-candidate" for a description of the selection process on the BSR. [CSCdx59801, 12.0(23)S, 12.2(PI5)T, 12.2S].

[no] ip pim register-rate-limit <pps>

Sets a limit on the maximum number of data registers/second sent for each (S,G). If this is configured on a PIM domain border, a recommended <pps> is 2. [11.3T, 11.1(20)CC]

[no] ip pim accept-register list <acl> | route-map <map>

Configures where Register messages are accepted from. This command is

used only in candidate RPs. If "list <acl>" is used, you can configure an extended access-list <acl> which determines which (source, group) pairs will be permitted or denied when seen in a Register message. If "route-map <map>" is used, you can apply typical route-map operations on the route for the source address which appears in a Register message. Both keywords "list" and "route-map" are not allowed together.

When a Register message is denied, an immediate Register-Stop is sent back to the originator of the Register. [12.0, 12.0S, 12.0T]

[no] ip dvmrp routehog-notification <route-count>
This configures the number of routes allowed within an approximate one minute interval before a syslog message is isssued warning that there maybe a route surge going on in the MBONE. This is typically used to detect quickly when someone has misconfigured their routers to inject a large number of routes into the MBONE. The default value is 10,000. You can find a running count in the "show ip igmp interface" display. When the count is exceeded, you'll see an "*** ALERT ***" string appended to the line. [10.2]

[no] ip dvmrp route-limit <route-count>
This command limits the number of DVMRP routes advertised over an interface enabled to run DVMRP. That is a DVMRP tunnel, an interface where a DVMRP neighbor has been discovered, or an interface configured to run "ip dvmrp unicast-routing". The default value is 7000. This command will be automatically generated to the configuration file when at least one interface is enabled for multicast routing. This command is necessary so misconfigured "ip dvmrp metric" commands don't cause massive route injection into the MBONE. The "no" version of the command configures no limit. [11.0]

[no] ip dvmrp distance <admin-distance>
Configures the default adminstrative distance for received DVMRP routes. This command should be used so routes advertised from the unicast routing table that are reflected back through DVMRP cause the original unicast routes to continue to be advertised. The "ip dvmrp accept-filter" command may override this value when specified on an interface. [11.2]

[no] ip mroute <source> <mask> [<protocol><as-number>] [route-map <map>]
<rpf-address> | <interface> [<distance>]
Configures a multicast static route (called a "static mroute"). When a source range is specified, the mroute applies only to those sources. When <protocol><as-number> is specified, the mroute applies to those sources that have been learned by the corresponding routing process. If route-map <map> is specified, further classification can be accomplished by the match clauses from <map>. If the mroute is selected, the <rpf-address> address dictates the incoming interface for the source that matches the mroute. If the <rpf-address> is a PIM neighbor, PIM Joins, Grafts, and Prunes will be sent to it. The <rpf-address> can be a host address of a directly connected router or a route. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected neighbor. If <rpf-address> is not specified, <interface> is used as the incoming interface. <distance> is used to decide if a unicast route, a DVMRP route, or a static mroute should be used for the RPF lookup. The lower distances have better preference. If the static mroute has the

same distance as the other two RPF sources, the static mroute will take precedence. There are only two exceptions to this rule, directly connected routes and the default unicast route. Default <distance> is 0. Static mroutes are local to the router and are not redistributed by any dynamic routing protocol. [11.0]

[no] ip sdr cache-timeout <minutes>
The amount of time an sdr cache entry stays active in the cache. A value a 0 indicates the entry will never timeout. The default value is 24 hours. [11.2]

[no] ip pim state-refresh disable
Disables PIM-DM State-Refresh message processing and forwarding. A router configured with this command will behave like a non-State Refresh capable router and will not advertise the SR-capability in PIM Hello messages. By default, State-Refresh processing and forwarding is enabled. [12.1(3)T]

ip igmp immediate-leave group-list <acl>
no ip igmp immediate-leave
Use this command to reduce the leave latency of IGMP memberships to zero when IGMP version 2 is in use and only a single receiver host is connected to each interface:

If this command is not configured, the router will operate the normal IGMP version 2 leave process: It will send out a group specific query upon receipt of an IGMP version 2 leave message to learn if more hosts are interested in receiving this group. The router can then only stop forwarding traffic for the group if no host replies within the timeout resulting in a leave latency of around 2 to 3 seconds. If this command is configured, then the router assumes that only one host was joined to the group and stops forwarding the groups traffic immediately.

Forwarding for only those groups is affected by this commands which are allowed by the standard or named standard access list <acl>. Use <acl> to limit the effect of this command to group ranges known to be receivable by only one host on each interface even if there may be multiple hosts.

This command does not change the leave latency if IGMP version 3 is in effect for the group. To reduce the the leave latency with IGMP version 3, use the explicit tracking support for IGMP version 3.

This command will take no effect on interfaces where IGMPv1 hosts are present.

The global version of the immediate-leave command can not be used together with the per-interface immediate-leave command. You must either use one global configuration command or per-interface commands. When the global command is configured, the per-interface immediate-leave commands will be removed from the configuration and newly entered interface immediate-leave commands will silently be ignored. [CSCdr27925, 12.2(4)]

This command was available in pre-IOS 12.2 versions as a hidden

command and is thus unsupported in those releases. [CSCdk29405, 12.0(4)]

[no] ip igmp ssm-map enable
Configuring this global command enables the SSM mapping feature for groups in the configured SSM range. By default, this command is not enabled. SSM mapping is a feature that takes IGMP version 1 or IGMP version 2 membership reports for a group G and converts them into IGMP version 3 (S,G) membership reports by looking up one or more sources associated with the group G via DNS or static configured entries. Default is to use DNS. SSM mapping is compatible with the other two Cisco IOS SSM transition solutions URD and IGMP v3lite.

See also ftp://ftpeng.cisco.com/ipmulticast/config-notes/ssm-map.txt for more information. [CSCdx32173, 12.3(1)T].

[no] ip igmp ssm-map query dns
This global configuration command enabled DNS based SSM mapping. It is by default enabled whenever "ip igmp ssm-map enable" is configured. Disable this command to inhibit DNS based SSM mapping If disabled, only statically mapped SSM sources via "ip igmp ssm-map static" will be determined. The domain used to look up mappings is determined by the command "ip domain multicast <domain-prefix>".

See also ftp://ftpeng.cisco.com/ipmulticast/config-notes/ssm-map.txt for more information. [CSCdx32173, 12.3(1)T].

[no] ip domain multicast <domain-prefix>
Configure this command to change the domain prefix used by IOS for the DNS based SSM mapping. By default this prefix is "in-addr.arpa".

When a Cisco IOS router tries to do DNS based SSM mapping for an IP group address G = G1.G2.G3.G4, it queries the name server for IP address ressource records ("IP A" RR's) for the following fully qualified domain name: G4.G3.G2.G1.<domain-prefix>

See also ftp://ftpeng.cisco.com/ipmulticast/config-notes/ssm-map.txt for more information. [CSCdx32173, 12.3(1)T].

[no] ip igmp ssm-map static <acl> <source>
Use this command to configure static SSM mappings. If SSM mapping is globally enabled via the "ip igmp ssm-map enable" command and the router receives an IGMP membership for group G in the SSM range, it will try to determine the source address(es) associated with G by walking the configured "ip igmp ssm-map static commands". If G is permitted by <acl>, then <source> is taken. If multiple configured "ip igmp ssm-map static" lines are configured and G is permitted by multiple <acl>, then the <source> arguments of all matching <acl> will be used (up to a limit of 20).

Only if no matching "ip igmp ssm-map static" lines matched, will SSM mapping query the DNS for address mapping (see "ip domain multicast" and "ip igmp ssm-map query dns").

See also ftp://ftpeng.cisco.com/ipmulticast/config-notes/ssm-map.txt

for more information. [CSCdx32173, 12.3(1)T].

[no] snmp-server enable traps ipmulticast
Configure this command globally to enable generation of SNMP traps for ip multicast. Currently, this is only qassociated with the traps generated by the "ip multicast heartbeat" command. [CSCdr40842, 12.1(3)T, 12.2].

[no] snmp-server enable traps pim [{ neighbor-change | rp-mapping-change | invalid-pim-message }]
Configure this command globally to enable generation of SNMP traps for the CISCO-PIM-MIB. If the "neighbor-change" option is included, traps will be generated when a PIM interface is enabled or disabled or when a PIM neighbor adjacency expires or is established. If the "rp-mapping-change" option is included, traps will be generated if changes in the RP mapping state happen due to AutoRP or BSR messages. If the "invalid-pim-message" option is included, traps will be generated if invalid PIM messages are received. Use the "snmp-server host ... pim" command to enable sending of PIM traps to specific receiver hosts.

See CISCO-PIM-MIB.my definition file for the format of the traps. ftp://ftpeng.cisco.com/ipmulticast/config-notes/mib-info.txt. [CSCdr38615, 12.0(15)S, 12.2(4)T]

[no] snmp-server host <ipaddr> traps [...] [ipmulticast | pim | ...]
Use this command to configure which host <ipaddr> will receive which type of SNMP traps. [CSCdr40842, 12.1(3)T, 12.2], [CSCdr38615, 12.0(15)S, 12.2(4)T]

IS-IS and OSPF Router commands:

[no] mpls traffic-eng multicast-intact
MPLS TE (traffic engineering) tunnels can not be used to convey PIM protocol traffic because theses tunnels are unidirectional in nature. This command allows for coexistance of PIM and MPLS TE tunnels by using native hop-by-hop transport for PIM protocol packets, even though the unicast routing is using MPLS TE tunnels.

Configure this command under router IS-IS or router OSPF to enable the MPLS TE and PIM interworking for routes of the appropriate routing protocol (OSPF and/or IS-IS). By default, this command is disabled. [12.0(7)S,12.1(2)T, 12.1(2) via CSCdm63234]

Interface subcommands:

ip igmp immediate-leave group-list <acl>
no ip igmp immediate-leave
Use this command to reduce the leave latency of IGMP memberships to zero when IGMP version 2 is in use and only a single receiver host is connected to each interface. Please refer to the documentation for the global configuration command

"ip igmp immediate-leave" for more details

[no] ip igmp join-group <group-address>
Informs the router to join group <group-address> on the interface. IP packets that are addressed to this group address will be passed up to the IP client process in the router as well forwarded out the interface. If you do not want packets forwarded out the interface, join the group on a loopback interface. Packets are not sent on the loopback interface. [10.2]

[no] ip igmp [vrf <name>] static-group <group>
[source <source> | source ssm-map]
[no] ip igmp [vrf <name>] static-group <group> "*"
Use this interface configuration command to statically forward traffic for the multicast group <group> onto this interface. Using this commands, packets to the group will get fastswitched or hardware switched (whatever is available on the platform), unlike the "ip igmp join-group" command which will cause packets for the group to become process switched. [11.2]

If the "*" keyword is present, then the interface will be placed by default into all newly created mroute entries. It will not create new state where there was none before. Note that this means that prunes will be ignored when received on the interface. This option is mostly meant to flood triffc to certain interfaces without join signalling like on a satellite headend router. [12.0T]

The "source <source>" option is in support of SSM. It allows to statically forward a (<source>,<group>) channel out of the interface. This option does require for <group> to be within the configured SSM range. [12.0(15)S, 12.2(1)].

The "source ssm-map" option was introduced for the SSM mapping feature. If configured, then SSM mapping will be used to determine the source(s) associated with this group and the resulting (<source>, <group>) channels will then statically be forwarded. Like "source <source>" this option also requires <group> to be n the configured SSM range. Use this command if you want to statically forward SSM traffic for certain group(s), but you want to let the DNS based SSM mapping determine the source addresse(s) of the channels. [CSCdx32173, 12.3(1)T]

[no] ip igmp query-interval <time-in-seconds>
Configures the frequency of IGMP Host-Query packets transmitted. A designated router for a LAN is the only router that transmits queries. For IGMPv1, the designated router is elected according to the multicast routing protocol that runs on the LAN. For IGMPv2, the designated querier is the lowest IP addressed multicast router on the subnet. The default value is 60 seconds. [10.2]

[no] ip igmp last-member-query-interval <interval>
Configures the "last member query interval" to be <interval>, in milliseconds. The default value is 1000 ms, or 1 second. A value below 1 second can result in faster IGMP leave actions. [12.0]

[no] ip igmp access-group <access-list>
Configures what groups are allowed on the interface. The

default is all groups are allowed. [10.2]

[no] ip igmp version 3 | 2 | 1

Interface subcommand to change IGMP version. Default is version 2. [11.1]

IGMP version 3 enabled receiver applications to signal (S,G) channel membership in support of SSM. Enable IGMP version 3 on all interfaces connected to receivers, if SSM is needed [12.1(5)T, 12.0(15)S, 12.2]

[no] ip igmp v3lite

Configure this command on interfaces connected to receiver hosts if you are using SSM and users may run applications on older host operating systems that do not yet support IGMP version 3 directly. IGMP v3lite enables the router to accept UDP (port 659) encapsulated IGMP version 3 application specifically compiled to support older operating systems (like IP/TV 3.2 and later). [12.1(5)T, 12.0(15)S, 12.2].

See the following URL for library needed to compile applications for IGMPv3lite. This is called the HSIL (Host Side IGMP Library):

http://www.talarian.com/products/multicastlite/index.shtml

The port used by igmp v3lite was changed to UDP port 465 via CSCdt68756 (See Release Notes for the ddts on CCO for more explanations). The HSIL will default to this new port in version 1.1 and later [12.2(4)M/B/T, 12.0(19)S/ST, 12.1(8a)E02].

[no] ip urd [proxy]

Configure this command on interfaces connected to receiver hosts if you are using SSM and users may run applications that by themselves do not support IGMP version 3 yet. URD is a mechanism that allows web-started applications (like typical streaming media players) to be SSM augmented from an appropriately written web page. With URD enabled, the router will intercept TCP connections to port 659, act like a HTTP server on that port and interpret URLs requested from the clients browser to contain SSM channel information:

http://arbitrary:659/arbitrary?group=<group>&source=<source>&

If the router intercepts such a URL, it will join to the (<source>,<group>) SSM channel as soon if or as soon as it also sees that the legacy application is simply trying to join to the group <group>. In the URL, <source> and <group> can either be IP addresses or fully qualified domain names (you need to have domain name resolution enabled on the router to support domain names). [12.1(5)T, 12.0(15)S, 12.2(1)]

If the proxy option is not given, intercepted TCP connections are only considered to be valid, if they originate from directly connected hosts. If the proxy option is given, requests will be honored from any TCP connection arriving on this interface. Never enable the proxy option on a backbone interface because this would allow people from the backbone to create URD state in your router. This option is meant to be used with unnumbered interfaces towards users or stub networks with IGMP proxy routers downstream of your router. [12.2(1), 12.0(16)S]

The port used by URD was changed to TCP port 465 via CSCdt68756 (See Release Notes for the ddts on CCO for more explanations). [12.2(4)M/B/T, 12.0(19)S/ST, 12.1(8a)E02].

[no] ip igmp query-timeout [timeout value in secs]
This command is valid when IGMP v2 is running. This command specifies the timeout for the router to take over as the querier for the interface, after the previous querier has stopped querying. The default value is 2 * query-interval. If the router hears no queries for the "timeout" period, it becomes the querier. [11.1]

[no] ip igmp query-max-response-time [secs]
This command is valid when IGMP v2 is running. This command specifies the maximum query response time advertised in the IGMP queries. Default value is 10 secs. Configuring a value less than 10 seconds enables the router to prune groups faster. [11.1]

[no] ip igmp helper-address <ip-address>
This command causes all IGMP host report and leave message received on the interface to be forwarded toward the given ip-address. The reports are resent out the next-hop interface towards the ip-address with that interface's source address. This command can enable a sort of "dense-mode" join, allowing stub sites not participating in PIM to indicate membership in multicast groups. [11.3]

[no] ip cgmp
Enables the Cisco Group Management Protocol (CGMP) for IP multicast on a LAN. The command triggers a CGMP Join message. This should only be enabled on 802 media (i.e. Ethernet, Fddi, and Token Ring) or ATM. When a "no" is issued, a triggered CGMP Leave message is sent for the router's MAC address on the interface for group 0000.0000.0000. CGMP can only run on an interface if PIM is configured on the same interface. [11.1]

A cisco will send CGMP Join messages in response to receiving IGMP reports from multicast capable members. Only the IGMP querier cisco router sends these CGMP Join messages on behalf of hosts.

[no] ip cgmp proxy
Enables CGMP for IP multicast as well as a proxy function. Initially supported is DVMRP proxying. If a DVMRP Report is received from a router that is not a PIM router, a cisco IGMP querier will advertise the MAC address of the DVMRP router in a CGMP Join with group address 0000.0000.0000. [11.1]

To perform CGMP proxy, a cisco must be the IGMP querier. An IGMPv2 querier is selected based on the lowest IP addressed router on the interface. An IGMPv1 querier is selected based on the multicast routing protocol used on the interface.

When multiple cisco routers are connected to a switched network and "ip cgmp [proxy]" is needed, it is recommended that all of them are configured 1) with the same CGMP option and 2) to have precedence of becoming IGMP querier over non-cisco routers.

[no] ip pim version 1
By default, this command is not configured on an interface and

the router uses PIM version 2 but will automatically fall back using PIM version 1 if it detects PIM version 1 routers.

If you configure this command, the router will only use PIM version 1 on an interface. You should never need to configure this command, it was only introduced to allow disabling PIM version 2 to troubleshoot PIM version 2 problems in early IOS images (around 1998).

Note: There is no specific command to disable PIM version 1 backward compatibility in Cisco IOS, but you can inhibit recognizing individual routers via the "ip pim neighbor-filter" command.

See description under "ip pim query-interval" for further information about automatic PIM version 1 backward compatibility. [11.3T, 12.0].

Cisco IOS images prior to 11.3T, 12.0 do only support PIM version 1.

[no] ip pim dr-priority <value>
Configures the neighbor priority used for PIM Designated Router (DR) election. The router with the largest <value> on an interface will become the PIM DR. If multiple routers have the same priority, then the largest IP addressed system on the interface becomes DR. If a router doesn't include the DR-Priority Option in it's Hello messages, the router is regarded highest priority router and will become DR. If multiple of such routers exist, the largest IP addressed router will become DR. This allows interoperation with older systems. [12.1(2)T, 12.2, feature available in IOS images with Bidir-PIM]

[no] ip pim [dense-mode | sparse-mode]
Enables the PIM multicast routing protocol on the interface. Configures the interface to operate in dense or sparse mode. The default mode is dense-mode. A dense-mode interface is subject to multicast flooding by default. A sparse-mode interface is only used for multicast forwarding if a join is received from a downstream router or their are directly connected members on the interface. When "no ip pim" is entered, it disables PIM on the interface. [10.2]

[no] ip pim sparse-dense-mode
Enables the PIM multicast routing protocol on the interface. In this mode, the interface will be treated as dense-mode if the group is in dense-mode. If the group is in sparse-mode, the interface will be treated in sparse-mode. When an interface is treated in dense-mode, it will be populated in a multicast routing table's outgoing interface list when 1) there are members or DVMRP neighbors on the interface, or 2) any of the PIM neighbors on the interface have not pruned for the group. When an interface is treated in sparse-mode, it will be populated in a multicast routing table's outgoing interface list when 1) there are members or DVMRP neighbors on the interface or 2) an explicit Join has been received by a PIM neighbor on the interface. [11.1]

[no] ip pim dense-mode proxy-register [list <eacl> | route-map <rmap>]
Enable this command on an interface connecting to a dense-mode region to enable registering for sources in that dense-mode region.

For multicast groups in PIM sparse mode, the router will normally

do the PIM sparse mode registering if it is the first-hop DR, directly connected to the source. If the router receives a packet from a non-directly connected source on an interface it will only register for this if either a DVMRP neighbor is active on an interface, or if this command is configured. Configuring this command will thus allow to get traffic from a source in a PIM dense-mode region to be correctly received by a receiver in the sparse mode region.

In addition to a dense mode border, this command also needs to be configured on interfaces connecting to a stub region with IGMP proxying routers to allow for sources from that region to be correctly registered for when sending to PIM sparse mode groups. Because the "proxy-register" option is only supported together with the "ip pim dense-mode" interface mode, one should avoid putting further PIM or DVMRP routers on that interface (only IGMP proxy routers) to avoid that the border router starts to flood traffic (as long as there is no DVMRP or PIM router connected, a dense-mode interface does not behave different from a sparse-mode or sparse-dense-mode interface).

Use the "list <eacl>" or "route-map <rmap>" options to limit the (S,G) packets arriving at this interface for which the router will do registering. These filtering options will only affect (S,G) for which S is not directly connected.
[12.0(7), CSCdm73649]

[no] ip pim query-interval <time> [msec]
Configures the frequency of PIM neighbor discovery messages. By default these messages are sent once every 30 seconds.

In PIM version 1 these messages are called Query messages. A Cisco IOS version 11.3F/12.0 or later router supports by default PIM version 2 with auto-fallback to PIM version 1. Such a router will by default send PIM version 2 Hello messages. It will change to PIM version 1 and sending of PIM Query messages on an interface if it detects a neighboring router that only supports PIM version 1 but not PIM version 2. As soon as the last PIM version 1 router is removed from a network, the router reverts to PIM version 2. A router can be made to only use PIM version 1 on an interface via the "ip pim version 1" command.

PIM neighbor discovery messages are used to determine which router on a network is the Designated Router (DR) for PIM-SM and SSM. The DR is responsible for joining to multicast traffic on sparse-mode and SSM groups that is requested from hosts via IGMP - so called local receivers. In addition, in PIM-SM the DR is also responsible to register local sources with the RP. If the DR fails, a possible backup router will start becoming the DR and then forward traffic for local receivers and register for local sources.

Each router announces (3 * <time>) as it's holdtime in its Query/Hello messages. If this time expires and another router has not received another Query/Hello message from this router, it will time out the PIM neighbor. If the timed out router was the DR, this will trigger DR election. By default, this so called DR_failover will thus happen after 3 * 30 = 90 seconds. To reduce DR-failover in redundant networks, configure a lower <time> on all routers. The minimum DR_failover

time is 3 seconds with <time> configured to be 1 seconds.

Notes: If IGMP version 1 is being used on a network, then the DR is also the IGMP querier - if at least IGMP version 2 is being used, then the router with the lowest IP address becomes the IGMP querier. In PIM version 2, PIM Hello messages do also contain a variety of options that allow PIM routers on the network to learn about the other routers capabilities - for example their ability to support Bidir-PIM.
[10.2]

If the msec option is used, the DR-failover time can be reduced to below 3 seconds. <time> is interpreted as a value in milliseconds instead of seconds. The minimum value for <time> is 10 msec. If a value of less than one second is configured, the router will announce the holdtime in a new PIM Fast-Hello option in milliseconds. It will still announce the rounded holdtime in the standard PIM Hello holdtime field (which only ha seconds resolution).
[CSCdv33013, 12.0(22)S, 12.1(11b)E, 12.2(15)T, 12.2(11)S]

[no] ip pim neighbor-filter <acl>
This command filters all PIM control messages based on the given access-list. It can be used to administratively deny a misconfigured PIM neighbor from participating in PIM, or in conjunction with "ip igmp helper-address" to be the basis for a simple stub IP multicast setup. Note: this command does not filter Auto-RP announcents and is only intended to filter neighbor-to-neighbor packets. [11.3]

[no] ip pim bidir-neighbor-filter <acl>
Configures a list of bidir capable neighbors on an interface. Normally DF election would only occur on interfaces where all the PIM neighbors are Bidir capable. To allow for a smoother transition from a sparse-mode only network to a hybrid bidir/sparsemode network, this command enables the operator to explicitly specify what routers should be participating on the DF election, while still allowing all routers to participate in the sparsemode domain. [This commands was introduced by CSCdx11884 in the following releases: 12.2(10) 12.2(10)S 12.2(10)T]

[no] ip pim multipoint-signalling
Enables PIM to open ATM multipoint VCs for each multicast group that is joined. This command is only accepted on an ATM interface. This command allows optimal multicast trees to be built down to ATM switch granularity. This can enhance router performance and link utilization since packets are not replicated and sent multiple times over the ATM interface. The default setting is disabled. That is, all multicast traffic goes to the static map multipoint VC as long as "atm multipoint-signalling" is configured. [11.3]

[no] ip pim vc-count <number>
Configures the maximum number of VCs PIM opens. The default value is 200. When the router hits this maximum limit it will delete inactive VCs so it may open VCs for new groups that might have activity. [11.3]

[no] ip pim minimum-vc-rate <pps>
Configures the minimum traffic rate to keep VCs active. When the

maximum number of VCs are opened and a new VC needs to be opened, the router will scan existing VCs. VCs that have a current 1 second rate less than or equal to <pps> are eligible for deletion. If a VC is deleted, it means that packets for its respective group do not have its own multipoint VC. However, packets will flow over a shared multipoint VC which delivers packets to all PIM neighbors. If all VCs have a 1 minute rate more than <pps>, the new group will use the shared multipoint VC. The default value is 0 packets per second. [11.3]

[no] ip pim bsr-border
Configures the interface to be the PIM domain border. Bootstrap messages will not be able to pass through this border in either directions. Thus effectively partitions the network into regions using different bootstrap routers. No other PIM messages are dropped by this domain border setup. Please also note that this command does not set up any multicast boundaries. [12.0(7), CSCdm73649]

Prior to renaming in 12.0(7) and all later IOS releases, this command was called "ip pim border". This old syntax is still accepted on input but will be NV generated as "ip pim bsr-border".

[no] ip pim border
See "ip pim bsr-border". [11.3T, 11.1(20)CC]

[no] ip dvmrp metric <metric> [list <access-list>]
{[<protocol> <process-id>] | dvmrp]
When PIM is configured on an interface and DVMRP neighbors are discovered, the router will, by default, send DVMRP Report messages. Under certain circumstances, it may be desirable to tailor the metric used for various unicast routes. This command allows one to configure the metric associated with a set of destinations for Reports sent out this interface. The acceptable <metric> value is between 0 and 32, where 0 means that the route will not be advertised and 32 means infinity and the route is advertised unreachable. If an <access-list> is specified, only the destinations that match the access-list will be reported with the configured metric. <access-list> can be a simple or extended access-list. When extended access-lists are used, you have both address and netmask granularity. Any destinations not advertised due to split horizon will not use the configured metric.

If the <protocol><process-id> is configured, only routes learned by the specified routing protocol will be advertised in DVMRP Report messages. This parameter can be used in conjunction with <access-list> so a selective list of destinations learned from a given routing protocol may be reported. If this command is not used, only directly connected networks are advertised when DVMRP neighbors are discovered.

If the "dvmrp" keyword is configured, only routes from the DVMRP routing table will be selected to be advertised with <metric>.

This command can be used multiple times on an interface. [10.2]

[no] ip dvmrp metric <metric> route-map <map-name>
This command has existed since release 10.2. What has been added is the route-map keyword. Now unicast routes can be subject to route-map conditions before being injected into DVMRP. Note, route-maps

cannot be used for DVMRP routes. [11.1]

[no] ip dvmrp metric <metric> [route-map <map-name>] mbgp
Configures redistribution of MBGP routes into DVMRP. If you supply a route-map, you can specify various match criteria options for the MBGP routes. [11.1(20)CC]

[no] ip dvmrp accept-filter <access-list> [neighbor-list <nbr-acl>] [<distance>]
Configures an acceptance filter for incoming DVMRP Reports. Any destinations that match <access-list> received in DVMRP reports from neighbors in the <nbr-acl> are stored in the DVMRP routing table with <distance>. The distance is used to compare with the same destination in the unicast routing table. The lower distance route (either from the unicast routing table or DVMRP routing table) will take precedence when computing the RPF interface for a source of a multicast packet. When no filters are configured on an interface, all destinations are accepted with distance configured from the "ip dvmrp distance" global command. An <access-list> value of 0, accepts all destinations. <access-list> can be a simple or extended access-list. If extended access-lists are used, you have both address and netmask granularity. An <nbr-acl> value of 0 means accept from all neighbors on interface. [10.2]

[no] ip dvmrp default-information originate | only
Indicates network 0.0.0.0 is advertised to DVMRP neighbors on this interface. By default, metric 1 will be used. This command can be used with the "ip dvmrp metric" command to tailor the metric used when advertising default. This command only takes effect when peering with mrouted 3.4 machines. When keyword "only" is used, no other DVMRP routes are reported. When keyword "originate" is used, other more specific routes may be advertised. Do not advertise the DVMRP default route into the MBONE. [10.2]

[no] ip dvmrp metric-offset [in | out] <increment>
This is the value added to the metric of a DVMRP route advertised in a Report message. When "in" (or no keyword is supplied, the <increment> applies (is added) to incoming DVMRP reports and is reported in mrinfo replies. When the "out" keyword is supplied, the <increment> applies (is added) to outgoing DVMRP reports for routes from the DVMRP routing table. This is similar to the metric keyword in mrouted configuration files. The default value for "in" is 1. The default value for "out" is 0. [11.0]

[no] ip dvmrp unicast-routing
Enables DVMRP unicast routing on the interface. This means that routes in DVMRP Report messages are cached by the cisco in a DVMRP routing table. When PIM is running, these routes get preference over routes in the unicast routing table. This allows PIM to run on the MBONE topology, when it is different (or deviates) from the unicast topology. The default setting is off. DVMRP unicast routing can run on all interfaces including GRE tunnels. On DVMRP tunnels, it runs by virtue of doing DVMRP multicast routing. This command does not enable DVMRP multicast routing among ciscos. However, if there is a DVMRP capable multicast router, the cisco will do PIM/DVMRP multicast routing interaction. [10.3]

[no] ip dvmrp reject-non-pruners
    This command will cause the router not to peer with a DVMRP neighbor if the neighbor doesn't support DVMRP Pruning/Grafting. If a DVMRP Probe or Report message is received without the Prune-Capable flag set, a syslog message will be logged and the message will be discarded. The default setting of this command is that all DVMRP neighbors will be accepted, regardless of capability (or lack there of). This command only prevents peering with neighbors. If there are any non-pruning routers multiple hops away (downstream towards potential receivers) that are not rejected, then a non-pruning DVMRP network may still exist. [11.0]

[no] ip dvmrp summary-address <address> <mask> metric <value>
    Configures a summary address to be advertised out the interface. If there is at least one more specific route in the unicast routing table that matches the <address>/<mask>, the summary will be advertised. Routes in the DVMRP routing table are not candidates for summarization. When the metric keyword is supplied, the summary will be advertised with metric <value>. The default metric <value> is 1. Multiple summary addresses can be configured on an interface. When multiple overlapping summary addresses are configured on an interface, the one with the longest mask takes preference. [11.2]

[no] ip dvmrp auto-summary
    Enables/disables DVMRP auto-summarization. DVMRP auto-summarization occurs when a unicast subnet route is collasped into a classful network number route. This occurs then the subnet is a different network number than the IP address of the interface (or tunnel) the advertisement is sent over. If the interface is unnumbered, the network number of the numbered interface the unnumbered interface points to is compared. The default setting for this command is enabled. [11.2]

[no] ip dvmrp output-report-delay <delay-time> [<burst>]
    Configures an inter-packet delay between DVMRP reports. <delay-time>, in milliseconds, is the amount of time that elaspes between transmission of a set of <burst> number packets. For example, at the periodic DVMRP report interval, if 6 packets are built, and the <delay-time> is 200 with <burst> of 2, 2 packets will be sent, then a delay of 200 milliseconds occurs, then another 2 packets are sent, then another delay of 200 milliseconds, then the final 2 packets are sent. The default value for <burst> is 2. The default value for <delay-time> is 100 milliseconds. [11.2]

[no] tunnel mode dvmrp
    Configures a cisco tunnel to encapsulate IP in IP using protocol number 4. This mode can be used when a cisco connects to a mrouted machine to run DVMRP over a tunnel. This is a popular way to connect to the MBONE. It is required to configure PIM and an IP address on a DVMRP tunnel. This mode is not used to construct a tunnel between a pair of cisco routers. [10.2]

[no] ip multicast ttl-threshold <ttl-value>
    Configures a packet TTL threshold for traffic going out the interface. Any multicast packets with a TTL less than the threshold are not forwarded out the interface. The default value is 0 which means all multicast packets are forwarded out interface. [10.2]

[no] ip multicast rate-limit in | out [video] | [whiteboard]
[group-list <acl>] [source-list <acl>]
[<kbps>]

Controls the rate a sender from the source-list can send to a multicast group in group-list. Any packets greater than <kbps> are silently discarded. The default value for <kbps> is 0, meaning all packets are discarded. If "in" is used, only <kbps> will be accepted on the interface. IF "out" is used, only a maximum of <kbps> kilobits per second will transmitted on the interface. If keywords "video" or "whiteboard" are used, then rate-limiting is performed based on the UDP port number used for the respective media. For this to work, "ip sdr listen" must be enabled so the port number can be obtained from the sdr cache. If sdr is not enabled, or the group address is not in the sdr cache, no rate-limiting is done for the group. The default setting of this command is disabled, meaning there is no rate-limiting in effect. [11.0]

[no] ip multicast boundary <acl> [filter-autorp]

Configures an administratively scoped boundary on the interface for multicast group addresses in the range defined by the simple IP access-list <acl>. No multicast data packets will be allowed to flow across the boundary from either directions. This allows reuse of the same multicast group address in different administrative domains or simply to inhibit access to that range between the two sides of the boundary.

The multicast address range 239.0.0.0 to 239.255.255.255 is designated as administratively scoped addresses by the IANA. Refer to RFC2365 for more information. For example, to configure a boundary for all administratively scoped address, do:

```
access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 15.255.255.255
interface ethernet 0
ip multicast boundary 1
```

If this interface is also a PIM interdomain link, the access-list that also stops unwanted Auto-RP packets would be:

```
access-list 1 deny 224.0.1.40
access-list 1 deny 224.0.1.39
access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 15.255.255.255
```

If the RPF interface for a multicast route has a multicast boundary configured for that group, its outgoing interfaces will not be populated. Joins received on other interfaces will be ignored as long as the boundary remains on the RPF interface. If the RPF interface changes and the boundary no longer applies to the new RPF interface, there will be join latency introduced because of the delay in populating outgoing interfaces. [11.1]

If the "filter-autorp" option is configured, the boundary will also examine RP-discovery and RP-announcement messages and filter (remove) group-range announcements from them if they are denied by the boundary acl. A group-range announcement is only permitted and passed

by the boundary if ALL addresses in the group-range are permitted by the boundary acl, otherwise the whole group-range announcement is filtered and removed from the message before the message is passed on. Refer to the configuration note
ftp://ftpeng.cisco.com/ipmulticast/config-notes/filter-autorp.txt
for more information on how to use this feature. Use "debug ip pim auto-rp" to troubleshoot this option [12.0(22)S, 12.2(12)].

[no] ip multicast helper-map {<group-address> | broadcast} {<broadcast-address> | <multicast-address>} <acl>

When a multicast-capable cloud is between two broadcast-only clouds, this command helps to convert broadcast traffic to multicast at the first hop router, and convert it back to broadcast at the last hop router to deliver the packets to the broadcast clients. This command utilizes the multicast capability of the intermediate multicast cloud. It prevents unnecessary replication at the intermediate routers and can take advantage of multicast fastswitching in the multicast cloud. <acl> is an extended access-list, when specified you can selectively configure what broadcast packets are translated based on the UDP port number. [11.1]

[no] ip mroute-cache [distributed]

Configures IP multicast fast-switching. If fast-switching is disabled on an incoming interface for a multicast routing table entry, the packet will be sent at process level for all interfaces in the outgoing interface list. If fast-switching is disabled on an outgoing interface for a multicast routing table entry, the packet is process level switched for that interface but may be fast-switched for other interfaces in the outgoing interface list. The default setting is all interfaces are multicast fastswitched. [11.0]

The "distributed" keyword will enable the interface to perform distributed fastswitching on incoming packets. This command applies to the configuration of the physical interface and not to subinterfaces. Once this command is configured on the interface, all packets coming in this interface will be distributed switched. The command "ip route-cache distributed" should be configured before this command is configured on a 7500 (and not on the 12000). [11.1(20)CC]

[no] ip sdr listen

Enables/disables accepting sdr Session Directory Protocol V2 packets. The router joins group 224.2.127.254 on the interface. If "ip multicast-routing" is configured, packets arriving on any interface will be accepted. In this case, it is sufficient to enable this command only on a single interface. Otherwise, you must use this command on all interfaces. [11.1]

[no] ip pim nbma-mode

This configures a multi-access WAN interface to be in Non-Broadcast Multi-Access mode. In this case, each PIM Join message is kept track of in the outgoing interface list of a multicast routing table entry. Therefore, only PIM WAN neighbors that have joined for the group will get packets sent to as data link unicasts. This command should only be used when "ip pim sparse-mode" is configured on the interface. This is not recommended for LANs that have natural

multicast capabilities. The default setting is NBMA mode disabled. [11.0]

[no] ip multicast use-functional
Enables the use of the RFC 1469 mandated MAC-level address, 0xc000.0004.0000, for transmission and reception of IP Multicast traffic. Valid only on Token Ring interfaces. [11.1]

[no] ip pim state-refresh origination-interval [<interval>]
Configures the PIM-DM State-Refresh origination interval. By default a router will process and forward State-Refresh messages but will not originate them. This command is required on first-hop routers directly connected to multicast sources to originate State-Refresh messages. It is required that all routers attached to the same LAN have the same value for <interval>. The value for <interval> is in units of seconds. The default value is 60 seconds. [12.1(3)T]

Platform specific IOS Multicast commands:

[no] ip pim sparse-mode-register

This interface level configuration command is available on Cisco-12000 POS interfaces on Engine-4 and Engine4+ linecards. By default, this command is enabled and NVgen'ed, and the router will perform normally. If "no ip pim sparse-mode-register" is configured, the router will not do registering for directly connected sources. This only affects sparse-mode groups but not dense-mode groups or source-specific-mode groups.

It is recommended that you configure "no ip pim sparse-mode-register" to save memory in HW-forwarding database of Engine-4 linecards if you do not have directly connected sources (like in typical backbone links). [CSCdt72742, 12.0(18)S]

Debug commands:

debug ip packet
Logs IP packets received and transmitted. This generates lots of messages. Use with caution. [Since the beginning of day]

debug ip mhbeat
Use this command to debug the operations of the "ip multicast heartbeat" command. If enabled, the router will generate a debug message in every interval and if a loss of heartbeat is detected.

debug ip mpacket [detail] [<acl>] [<group-name-or-address>]
Logs only IP multicast packets received and transmitted. This generates lots of messages. Use with caution. An optional group address is allowed to monitor a single group's packet activity. If <acl> is specified, only multicast packets from sources described by the access-list will be logged. When "detail" is used, the packet's IP header information as well as MAC address information will be

display. [10.2]

debug ip igmp <group>
Logs IGMP packets received and transmitted as well as IGMP host related events. Specifically IGMP protocol messages and mtrace messages. [10.2]

When <group> is specified, logging for the single group is performed. [11.3T]

debug ip urd [<hostname> | <ip-address>]
Logs received and processed intercepted TCP connections to the URD port 659.
The <hostname> / <ip-address> options are currently ignored. [12.1(5)T, 12.2, 12.0(15)S]

debug ip cgmp
Logs CGMP packet/event activity. [11.1]

debug ip dvmrp [detail [<acl>] [in|out]] [pruning]
Logs DVMRP packets received and transmitted. Keyword "detail" will log packet contents. If <acl> is specified, only routes associated with the access-list are logged. Keywords "in" and "out" can be used to look at routes received in DVMRP reports or routes transmitted in DVMRP reports, respectively. If "pruning" is specified, only DVMRP pruning and grafting events are logged. [10.2]

debug ip pim [<group-name-or-address>]
Logs PIM packet received and transmitted as well as PIM related events. An optional group address is allowed to monitor a single group's PIM activity. [10.2]

debug ip pim hello
Logs PIM Hello messages. Introduced with sub-second convergence support. See "ip pim query-interval <time> msec". [CSCdv33013, 12.0(22)S, 12.1(11b)E, 12.2(15)T, 12.2(11)S]

debug ip pim auto-rp
Displays Auto-RP packet activity. [11.1]

Use this command to also display information about auto-rp messages filteered by the "filter-autorp" option to the "ip multicast boundary" command. [12.0(22)S, 12.2(8)]

debug ip pim atm
Logs PIM ATM signalling activity. [11.3]

debug ip mrouting [<group-name-or-address>]
Logs transaction events to and from the IP multicast routing table. An optional group address is allowed to monitor a single group's routing table activity. [10.2]

debug ip mcache
Enables debug logging for IP multicast fast-switching events. [11.0]

```
  debug ip sdr
      Enables logging of received sd and sdr announcements. [11.1]

  debug ip mds ipc [event | packet]
      Logs MDS IPC related activity. This command is used both on the RP
      and line-card consoles. [11.1(20)CC]

  debug ip mds process
      Logs MDS RP and line card events. This command is used both on the
      RP and line-card consoles. [11.1(20)CC]

  debug ip mds mevent
      Logs multicast FIB related events on the line card. Used to debug
      MFIB route creation, deletion, and update events. [11.1(20)CC]

  debug ip mds mpacket
      Logs MDS switching events. Used to debug packet drops, interface
      drops, and switching failures. [11.1(20)CC]

  debug ip mbgp updates
      Logs MBGP related information passed in BGP Update messages.
      [11.1(20)CC]

  debug ip mbgp dampening [<acl>]
      Logs route flap dampening activity. If <acl> is specified, logging
      occurs for the routes specified in the access-list only. [11.1(20)CC]

-----------------------------------------------------------------------

Show commands:

  show ip igmp interface [<interface-unit>]
      Displays learned groups for given interface. [10.2]

  show ip igmp groups [<group-name> | <group-address>] | [<interface-unit>]
                      [detail]
      Displays directly connected groups learn via IGMP. [10.2]

    If the "detail" option is given, the router will output information
      about SSM sources [12.1(5)T, 12.0(15)S, 12.2(1)]

  show ip igmp ssm-mapping [ <group> ]
      Use this exec level command to determine the sources that SSM mapping
      is or would use for a partigular group <group>. If there is no
      SSM mapping currently known for <group>, then this command
      will also initiate DNS based SSM mapping for this group
      if enabled (eg: will send out a DNS query). If no <group> argument
      is specified, the output will instead show the configured state of the
      SSM mapping feature.

      See also ftp://ftpeng.cisco.com/ipmulticast/config-notes/ssm-map.txt
      for more information. [CSCdx32173, 12.3(1)T].



  show ip pim neighbor [<interface-unit>]
      Displays PIM neighbors discovered. [10.2]
```

```
show ip pim rp [<group-name> | <group-address>] [mapping]
   Displays active RPs that are cached with associated multicast routing
   entries. If "mapping" is supplied, displays all group-to-RP mappings
   that are configured and/or learned from Auto-RP. [10.2]

show ip pim interface [<interface-unit>] count
    Displays PIM interface information. [10.2]

show ip pim interface [<interface-unit>] detail
    Displays detail PIM interface information. [12.1(3)T]

show ip pim vc [<group-or-name>] [<interface>]
    Displays ATM VC status information for multipoint VCs opened by PIM.
    When <group-or-name> is specified, only the single group is displayed.
    When <interface> is specified, only the single ATM interface is
    displayed. [11.3]

show ip pim bsr
    Displays the bootstrap router (BSR) information, including the
    elected BSR's IP address, priority, hash mask length etc.
    Information is shown if the local router is a candidate bootstrap
    router (BSR) but not an elected BSR. This commands also displays
    information about locally configured candidate RP advertisement.
    [11.3T]

show ip pim rp-hash <group>,
    shows which RP is being selected for the <group>. It also shows
    whether this RP was learned via Auto-RP or v2 bootstrap mechanism.
    [11.3T]

show ip pim joiners <interface> <group-or-source> [<group-or-source>]
    Sends a PIM Joiner-ID Request on interface <interface>. If two
    addresses are supplied, then the request is made for a (S,G). If
    just one address is supplied and it is a group address, a request is
    made for (*,G). Routers supporting Joiner-ID will respond indicating
    whether or not they are sending joins to the querying router for the
    specified multicast route. They will include their outgoing interface
    lists and several flags.
    [CSCdm77243, 12.0(6)S]

show ip pim pruners <interface> <group-or-source> [<group-or-source>]
    Sends a PIM Pruner-ID Request on interface <interface>. If two
    addresses are supplied, then the request is made for a (S,G). If
    just one address is supplied and it is a group address, a request is
    made for (*,G). Routers supporting Pruner-ID will respond indicating
    whether or not they are sending prunes to the querying router. They
    will include their outgoing intreface lists (if applicable), and
    flags indicating the type of Prune being sent (RP-bit).
    [CSCdm77243, 12.0(6)S]

show ip mroute [[<group-name> | <group-address>] [<source-address>]]
               [summary]
    Displays the IP multicast routing table. When "summary" is specified,
    a one line abbreviated display is provided. When "count" is
    specified, group count, source count, and packet count statistics
    are provided. [10.2]
```

```
show ip mroute [[<group-name-or-address>] [<source-name-or-address>]] count
    Displays packet count per (S,G) multicast routing table entry. Also
    includes average packet size and data rate in kilobits per second.
    [10.2]

show ip mroute [<group-name-or-address>] active [<kbps>]
    This command shows you the rate active sources are sending to multicast
    groups. You can display for all groups or specify a single <group>.
    <kbps> will only display sources that are sending >= <kbps>. The
    default setting shows all sources sending at a rate greater than or
    equal to 1 kilobit/second. If sd is running on the router, the sd
    session name is displayed. [11.0]

show ip mroute [<group-name-or-address>] [<source-name-or-address>] pruned
    Displays (S,G) entries that have been pruned. [11.3]

show ip mroute [<group-name-or-address>] [<source-name-or-address>]
               [<interface>]
    Display the multicast routing table entries that have <interface> in
    the outgoing interface list. [11.3]

show ip mroute [<group-name-or-address>] active [<kbps>] [<interface>]"
    Display the active multicast routing table entries that have
    <interface> in the outgoing interface list. [11.3]

show ip mroute static
    Displays staticly configured multicast static routes. [11.2]

show ip mpacket [detail]
show ip mpacket <source-address-or-name> [detail]
show ip mpacket <group-address> [detail]
show ip mpacket <source-address-or-name> <group-address> [detail]
show ip mpacket [read-only]
    Displays the contents of the circular cache-header buffer. Each time
    this command is entered, a new buffer is allocated. The summary
    display shows IP packet ident, ttl, source and destination IP
    addresses plus a local timestamp when the packet was received.  The
    detail display shows the rest of the IP header fields on an additional
    line plus the first 8 bytes after the IP header (usually the UDP port
    numbers). This command is only applicable when the "ip multicast
    cache-headers" command is in effect. [11.1]

    When keyword "read-only" is specified, a new buffer is not allocated.
    The old buffer contineus to accumulate packet entries. Useful for
    repeating the display with more or less detail the second time.
    [11.1(22)CC, 12.0S]

show ip mpacket <group-address> [<source-address-or-name>] quality
    Displays RTP loss statistics for each given source sending to
    group <group-address> or the single source specified in <source-
    address-or-name>. Packets received, packets lost, packets misordered,
    average loss gap, and loss percentage is provided. [11.1(20)CC]

show ip dvmrp route [<name-or-address> | <interface>]
    Displays the DVMRP routing table. The DVMRP routing table contains
    unicast destinations only when any DVMRP is running on an interface or
```

tunnel. If <name-or-address> is specified, a longest match lookup is performed and the entry that matches is displayed. If <interface> is specified, all routes with a next-hop interface of <interface> is displayed. [10.2]

show ip dvmrp route [<name-or-address>] poison
Display interfaces where a DVMRP report with a poisoned-reversed metric has been received for the route. [11.3]

show ip mcache [<group> [<source>]]
Displays the IP fast-switching cache. If <group> is specified, the fastswitching cache for the single group is displayed. <group> can be either a Class D IP address or a DNS name. If <source> is specified with <group>, a single multicast cache entry is displayed. <source> can be either a unicast IP address or a DNS name. [11.0]

Displays "mds" if MDS is being used instead of the fastswiching. Displays the "last used time" if the fastswitching is being used. Displays "never" if the fastswitching entry is not used (process level switched). Note that if MDS is not enabled on an incoming interface which is capable of doing MDS, incoming packets wont be distributed fastswitched and will be fastswitched at the RP. Also, if the incoming interface is not MDS capable, the packet will get fastswitched or process-level switched at the RP. If the incoming interface is enabled for MDS but at least one of the outgoing interfaces is not fastswitch capable, packets will be process-level switched. So it is a good idea not to disable fastswitching on any interface when MDS is enabled. [11.1(20)CC]

show ip sdr [<group> | "<session-name>" | detail]
Displays the sdr cache. If the router is configured to be a member of 224.2.127.254 (the default sd group), it will cache sdr announcements. If no parameters are used, a sorted list of session names are displayed. If <group> is specified, the session(s) defining the multicast group will be displayed in detail format. If "<session-name>" is specified, the single session is displayed in detail format. If the keyword "detail" is specified, all sessions are display detail format. [11.1]

show ip rpf <source-address-or-name>
Displays how IP multicast routing does Reverse Path Forwarding. Since the cisco can RPF from multiple routing tables (i.e. unicast routing table, DVMRP routing table, or static mroutes), this command tells you where the information is retreived from. [11.0]

show tech-support ipmulticast
Provides output for a set of IP multicast related show commands. This is useful for a customer to use a single type-in to provide the necessary information so cisco can debug an IP multicast related problem. [11.2]

show ip mds stats [switching | linecard]
Displays distributed fastswitching stats and linecard stats. [11.1(20)CC]

show ip mds interface
Displays MDS related interface information. [11.1(20)CC]

```
  show ip mds forwarding [<group>] [<source>]
      Displays the MFIB table on the line-card. Displays forwarding
      information and related flags and counts for MDS. This command is
      used on the line cards via the line-card console. [11.1(20)CC]

  show ip mds summary
      Displays MDS summary information on the line-card. This command is
      used on the line cards via the line-card console. [11.1(20)CC]

  show ip mbgp <command>
      <command> can be any of the existing BGP commands supported by
      "show ip bgp <command>". The MBGP variants show multicast RIB related
      information. Use this command in conjunction with "show ip rpf"
      to determine if IP multicast routing is using MBGP routes.
      [11.1(20)CC]

-------------------------------------------------------------------------

Clear commands:

  clear ip mroute [<group-name> | <group-address> [<source-address>]] | [*]
      Deletes entries from the IP multicast routing table. [10.2]

  clear ip igmp group [<group-name> | <group-address>] | [<interface-unit>]
      Deletes entries from the IGMP cache. [10.2]

  clear ip cgmp [<interface>]
      Sends a CGMP Leave message with a group address of 0000.0000.0000 and
      a unicast address of 0000.0000.0000. This instructs the switches to
      clear all group entries they have cached. If <interface> is specified,
      the Leave is sent only on <interface>. Otherwise, it is sent on all
      CGMP enabled interfaces. [11.1]

  clear ip dvmrp route * | <route>
      Deletes routes from the DVMRP routing table. When "*" is used, all
      routes are deleted. When <route> is used, the longest match route
      will be deleted. [10.2]

  clear ip sdr [<group-address> | "<session-name>"]
      Deletes an sdr cache entry. No parameters delete the entire sdr cache.
      If <group-address> is supplied, all sessions associated with the IP
      group address are deleted. If "<session-name>" is specified, only
      the sdr cache entry with the supplied name is deleted. [11.1]

  clear ip pim interface [<interface>] count
      Clears the multicast packet counters for interface <interface>. Or
      clears for all interfaces when <interface> is not specified. [11.2]

  clear ip pim auto-rp <rp-address>
      Clears the Auto-RP cache. When <rp-address> is specified, only the
      entries related to RP <rp-address> are cleared. Otherwise, the entire
      Auto-RP cache is cleared. [11.2]

  clear ip mds forwarding *
      Clears this linecards MFIB table and resync with the RP. This command
      is used on the line cards via the line-card console. [11.1(20)CC]
```

Exec commands:

  mrinfo [<hostname-or-address>] [<source-address-or-interface>]
      mrinfo is the MBONE's original tool to determine what neighboring multicast routers are peering with a multicast router. cisco has supported responding to mrinfo requests since release 10.2. Now you can query a multicast router using the mrinfo exec command. If <hostname-or-address> is not used, the router queries itself. Otherwise, the DNS name or IP address of the multicast router is queried. The output format is identical to the mrouted version. If <source-address-or-interface> is specified, that is the source address used on mrinfo requests. When it is omitted, the source address is based on the outbound interface for the destination. [11.0]

  mtrace <source> [<destination>] [<group>]
      mtrace is a multicast traceroute. It allows you to trace the path from a source to a destination branch for a multicast distribution tree for a given group. The trace traverses in the reverse direction from destination to source. This allows you to isolate multicast routing failures. When <group> is not specified, 224.2.0.1 is used. This is the group used for "MBone Audio". When <destination> is not specified, the mtrace starts from the system that the command is typed from. <source> is required and can be a DNS name or the IP address of a multicast capable source. <destination> and <group> can also take DNS names. When no parameters are entered, the router will interactively ask you for the parameters. [11.0]

  mstat <source> [<destination>] [<group>]
      The form of Unix mtrace that reports packet rate/loss information. Takes the same input as mtrace. [11.0]

  ping <group-address-or-name>
      You can send ICMP Echo Requests to a multicast group address. When you supply <group-address-or-name>, a single Echo Request packet is sent. When you type ping with no arguments, you will be prompted. [10.2]

MBGP Router subcommands: [All in 11.1(20)CC]

  [no] neighbor <addresss> remote-as <asn> [nlri unicast | multicast]
      Configures a BGP peer and associated AS number. If the "multicast" keyword only is supplied, only multicast NLRI will be sent to the neighbor. Counterwise, if the "unicast" keyword only is supplied, only unicast NLRI will be sent to the neighbor. Both keywords may be supplied which indicates the neighbor will be sent both types of routes. Unicast NLRI will be sent in the conventional encoding and the multicast NLRI will be send in the MP_REACH and MP_UNREACH path attribute. The default is to send unicast NLRI only. This version of BGP will negotiate NLRI in the Capabilities Option of the Open message. Therefore, both sides of a BGP connection must be configured consistently with respect to NLRI or the TCP connection will not be established.

[no] neighbor <tag> peer-group [nlri unicast | multicast]
Configures the peer-group to support either unicast NLRI, multicast NLRI or both. Supplying the both keywords "unicast" and "multicast" indicates both NLRI are sent. The default value is unicast only.

[no] neighbor <address-or-tag> description <user-supplied>
Configures a user supplied description string for the neighbor.

[no] neighbor <address-or-tag> dont-capability-negotiate
This hidden command configures whether Capability Parameter negotiation in BGP Open messages are used. By default, capability negotiation is performed. This command is used to interoperate with older MBGP implementations in which no Capability Parameters are used in Open messages between multicast peers. This command is not applicable when peering between two unicast-only BGP neighbors. This command will eventually go away.

[no] distance mbgp <dist1> <dist2> <dist3>
For configuring adminstrative distance for MBGP routes. <dist1> is the distance for external routes, <dist2> is the distance for internal routes, and <dist3> is the distance for local routes. The default values are the same as for BGP.

[no] network <address> [mask <mask>] [nlri unicast | multicast]
Determines if network in the AS should be injected into the BGP unicast RIB or the MBGP multicast RIB. If both keywords "unicast" and "multicast" are specified, it is injected in both RIBs. If "multicast" is specified, it is injected in the multicast RIB only. The default is unicast only.

[no] aggregate-address <address> <mask> [nlri unicast | multicast]
This command, used with the keyword "multicast" indicates if the aggregate should be applied to the multicast RIB. If the keyword is not supplied, then it applies to the unicast RIB. If you want it to apply to both RIBs, enter the both keywords "unicast" and "multicast".

[no] redistribute dvmrp [route-map <map-name>]
Configures redistribution of DVMRP routes into MBGP. If you supply a route-map, you can specify various BGP attribute settings.

MBGP route-map subcommands: [All in 11.1(20)CC]

[no] match nlri unicast | multicast
The route-map criteria can be based on the unicast or multicast RIB (or both). If the multicast RIB entry is being processed for a route-map with a "match nlri multicast", then the route-map condition will yield true, likewise for the unicast corrolary. If both keywords "unicast" and "multicast" are specified, then either RIB entry being processed will yield TRUE. The default value is both.

This command can be used in conjunction with the "neighbor <address> route-map <map> in" command so you can use one route-map reference to describe filtering policies for different NLRI types.

[no] set nlri unicast | multicast

If the route-map match criteria is met, decide if the route should be injected into the unicast or multicast RIB. If both keywords "unicast" and "multicast" are specified, the route is injected into both RIBs and advertised as separate NLRI in a BGP Update message. If "multicast" is specified, the route is injected only into the multicast RIB. The default value is unicast only in all cases accept when this route-map is referenced by a "neighbor <foo> route-map <foo> out" command. This route-map subcommand is used when referencing a route-map by various router subcommands (i.e. like "redistribute", "aggregate-address", and neighbor outbound route-map references).

This command can be used in conjunction with the "neighbor <address> default-originate route-map <map>". If the "set nlri" is supplied in the route-map referenced by the neighbor command, the multicast default route can be generated independent of the unicast default route.

MSDP commands: Unless otherwise noted, MSDP command were introduced in Cisco IOS 12.0S and Cisco IOS 12.1

Global Commands:

[no] ip msdp peer <ip-address-or-name> [connect-source <interface>] [remote-as <asn>]

Configures an MSDP peer. If you are also BGP peering with with this MSDP peer, you should use the same IP address for MSDP as you do for BGP. However, you are not required to run BGP/MBGP with the MSDP peer as long as there is a BGP/MBGP path between the MSDP peers. If there is not, you are required to use "ip msdp default-peer" command. The keyword "connect-source" is used to supply a source IP address for the TCP connection. The primary address configured on <interface> is used.

When the "remote-as" keyword is used, you can specify the AS number of the MSDP peer. This is only used for display purposes. There are cases where a peer may appear to be in another AS (other than the one it really resides in) when you MSDP peer but don't BGP peer with it. In this case, if the prefix of the peer is injected by another AS, it is displayed as the peer's AS number (and is misleading).

[no] ip msdp description <peer-name-or-address> <text>

This command adds a descriptive text string <text> to the configuration for the peer <peer-name-or-address>. You can see this description when doing NV command generation or via the "show ip msdp peer" command.

[no] ip msdp shutdown <peer-name-or-address>

This command adminstratively shuts down a configured peer. This command is used when you want to configure many MSDP commands for the same peer and don't want the peer to go active. This command could also be used if a MSDP session needs to be shut down for a period of time without

losing configuration information for the peer.

[no] ip msdp sa-filter out <ip-address-or-name>
[list <acl>] [route-map <map>]
[rp-list <acl> | rp-route-map <map>]

Configures outgoing filter list for Source-Active messages sent to MSDP peer <ip-address>. The default setting is all SA messages received are forwarded to the peer. <acl> is an extended access-list that can describe source/group pairs to pass through the filter. If route-map <map> is specified, you can filter based on match criteria in <map>. If all match criteria is true, a permit from the route-map will pass routes through the filter. A deny will filter routes. If both keywords are used, all conditions must be true to pass/filter any (S,G) in outgoing SA messages. If neither are specified, all source/group pairs are filtered. [12.0S, 1.0T]

With the rp-list and rp-route-map arguments it is possible to filter SA messages based on the announcing RP address contained in the SA message. This allows to filter messages based on their origin even after they may have already transited one or more other MSDP speakers. [12.0(11)S, 12.1(2)T, 12.1(2)E, CSCdp44032]

[no] ip msdp sa-filter in <ip-address-or-name>
[list <acl>] [route-map <map>]
[rp-list <acl> | rp-route-map <map>]

Configures incoming filter list for Source-Active messages received from MSDP peer <ip-address>. The default setting is all SA messages are received. <acl> is an extended access-list that can describe source/group pairs to pass through the filter. If route-map <map> is specified, you can filter based on match criteria in <map>. If all match criteria is true, a permit from the route-map will pass routes through the filter. A deny will filter routes. If both keywords are used, all conditions must be true to pass/filter any (S,G) in incoming SA messages. If neither are specified, all source/group pairs are filtered. [12.0S, 1.0T]

With the rp-list and rp-route-map arguments it is possible to filter SA messages based on the announcing RP address contained in the SA message. This allows to filter messages based on their origin even after they may have already transited one or more other MSDP speakers. [12.0(11)S, 12.1(2)T, 12.1(2)E, CSCdp44032]

[no] ip msdp sa-limit <peer-address-or-name> <limit>

Configure this command to limit the overall number of SA messages the router will accept from MSDP peer <peer-address-or-name>. The router keeps a per-peer count of MSDP SA messages in his SA cache and will ignore new messages from a peer if the configured limit for that peer is reached. If the router receives SA messages in excess of the configured limit from an MSDP peer, it generates a rate-limited (once a minute) syslog message:

%MSDP-4-SA_LIMIT: SA from peer 172.12.0.1, RP 172.1.0.1 for
(1 72.1.0.45, 234.1.1.1) exceeded sa-limit of 40

The "ip msdp sa-limit" command was introduced as a mean of protection against (distributed) denial of service attacks (DoS-attacks). It is recommended to configure "ip msdp sa-limit" on all peerings. An appropriately low SA limit should be configured on peerings with a stub MSDP region (eg: a peer that may have some further downstream peers but that will not transit SA messages from the rest of the Internet). A high SA limit should be configured with all transit MSDP peerings.

The commands "show ip msdp summary" and "show ip msdp count" have been enhanced to show the number of SA learned from each peer, "show ip msdp peer" has been enhanced to show the count and the limit if configured [12.0(15)S, 12.1(7), 12.2(2)T, 12.2(3), 12.2S, CSCdt19258].

[no] ip msdp sa-request <ip-address-or-name>

This informs the router to request SA messages from the peer when a new joiner for the group becomes active. The default setting if this command is not used, is to not send any SA-Request messages.

[no] ip msdp filter-sa-request <ip-address-or-name> [list <acl>]

Configures if the router should honor SA request messages from the peer for groups described by simple access-list <acl>. The defalut setting if this command is not used, is that all SA-Request messages from peer <ip-address> are honored. If <acl> is not specified, all SA-Request messges are ignored.

[no] ip msdp ttl-threshold <ip-address-or-name> <ttl>

Configures what multicast data packets are sent in data-encapsulated SA messages. When <ttl> is configured, only multicast packets with IP header TTL greater than or equal to <ttl> are sent to the peer <ip-address-or-name>. The default value is 0.

[no] ip msdp redistribute [list <acl>] [asn <aspath-acl>] [route-map <map>]

Configures what (S,G) entries from the multicast routing table are advertised in SA messages to MSDP peers. By default only local sources are advertised provided they send to groups this system is RP for or for all groups if "ip msdp border" command is used.

If "list <acl>" is used, you can further filter what local sources are advertised (and to what groups they send to) by using the extended access-list <acl> where you can supply a source address, source mask, group address and group mask.

If "asn <aspath-acl>" is used alone, you can advertise all sources sending to any group which match the <aspath-acl> reference to a "ip as-path access-list <aspath-acl>" command. If "asn 0" is used, sources from all ASes are advertised. This is useful when connecting dense-mode domains to a sparse-mode domain running MSDP. Or when you use MSDP in a router that isn't configured with BGP (and therefore you don't know if a source is local or not).

If "route-map <map>" is used, you advertise all sources that satisfy

the match criteria from route-map <map>.

When all keywords are used, all conditions must be true before any multicast source is advertised in an SA message.

When you specify "ip msdp redistribute", no multicast sources are advertised. This command is used for SA message origination and not for SA message forwarding. If you want to filter what SA messages are forwarded from one peer to another, use the "ip msdp sa-filter" command.

[no] ip msdp cache-rejected-sa <num-entries>

Enable this global configuration command to have the router MSDP SA messages received from MSDP peers but rejected. By default, this command is not enabled. If enabled, the router will keep a ring-buffer of the last <num-entries> number of rejected MSDP entries. Each entry requires approximately 30 bytes of memory on the router. Enabling this command is purely for troubleshooting MSDP. It has no effect on the protocol operation. See "show ip msdp sa-cache" on how to see rejected SA messages during troubleshooting [CSCdv13858, 12.0(22)S].

[no] ip msdp cache-sa-state [list <acl> rp-list <extended-acl> rp-route-map <route-map>]

This command is obsolete. In all current and recommended IOS images, caching of MSDP SA messages is mandatory and can not be manually enabled or disabled. "ip msdp cache-sa-state" will automatically be NVgened if at least one MSDP peer is configured. It can not be unconfigured but will be removed automatically when the last MSDP peer is removed from the configuration [12.0(14)ST, 12.0(15)S, 12.1(7), 12.2, CSCdr93446].

If you need to run an older version of IOS and can not immediately upgrade, enable "ip msdp cache-sa-state" without further arguments to achieve best operations and interoperability of MSDP.

[no] ip msdp default-peer <ip-address-or-name> [prefix-list <list>]

Defines a previously configured peer from which MSDP SA messages may come from. This command is used when you are not MBGP/BGP peering with an MSDP peer. If "prefix-list <list>" is not specified, all SA messages received from the configured default-peer are accepted. If "prefix-list <list>" is specified, SA messages originated from RPs covered by prefix-list <list> will be accepted from the configured default-peer. If <list> is specified, and there is no prefix-list configured, the default-peer will be used for all prefixes. You can enter multiple commands with the either the "prefix-list" keyword or without the "prefix-list" keyword, however, all commands must either have the keyword or all must not have the keyword.

When you use multiple "ip msdp default-peer" commands without the "prefix-list" keyword, you use a single active peer to accept all SA messages. If that peer goes down, then you move to the next configured default-peer to accept all SA messages. This is typically used at a stub site.

When you use multiple "ip msdp default-peer" commands with the "prefix-list" keyword, you use all the default-peers at the same time for different RP prefixes. This is typically used inside at a service provider cloud which connects stub site clouds.

When you have a single peer configured, you don't need to use a default-peer command since there is only a single place to accept SA messages from (and you can't cause an SA forwarding loop).

[no] ip msdp border sa-address <interface>
Configures a MSDP border function which is used in a router that borders a sparse-mode region with a dense-mode region. If you want the router to send SA messages for sources active in the dense-mode region, use this command. The IP address on <interface> is used as RP address in SA messages so MSDP peers can forward SA messages away from this border.

[no] ip msdp originator-id <interface>
Allows a MSDP speaker, which originates an SA message, to use the IP address associated with <interface> as the RP address in the SA message. If this command is used with the "ip msdp border" command, the originator-id address will be used.

[no] ip msdp mesh-group <name> <ip-address-or-name>
Configures an MSDP peer <ip-address-or-name> to be a member of a mesh-group. A mesh group is a group of MSDP speakers which have fully meshed MSDP connectivity between one another. Any SA messages received from a peer in a mesh-group are not forwarded to other peers in the same mesh-group. Mesh groups are useful in two scenarios, 1) to reduce SA message flooding, and 2) to simplify peer-RPF flooding (no need to run MBGP/BGP amoung MSDP peers).

Debug Commands:

[un]debug ip msdp [<peer-address-name>] [detail] [routes]
Enables debugging MSDP protocol activity. If <peer-address> is specified, debug events for that peer only are logged. When keyword "detail" is specified, more detail debugging is enabled. When keyword "routes" is specified, SA message contents are displayed.

[un]debug ip msdp resets
Enables debugging of MSDP peer reset reasons. This cannot be used with other forms of "debug ip msdp" parameters described above.

Show Commands:

show ip msdp summary
Displays MSDP peer status. A "*" in front of the peer address column indicates a default peer.

Example output:

```
sjck-rp1>sh ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
```

```
                                   Downtime Count Count
    192.135.250.116  109   Up      1d10h    9     111   rtp5-rp1
    *144.228.240.253 1239  Up      14:24:00 5     4010  sl-rp-stk
    172.17.253.19    109   Up      12:36:17 5     10    shinjuku-rp1
    172.17.170.110   109   Up      1d11h    9     12    ams-rp1
```

The "SA Count" column was introduced in IOS images supporting the "ip msdp sa-limit" command [12.0(15)S, 12.1(7), 12.2(2)T, 12.2(3), 12.2S, CSCdt19258].

show ip msdp peer [<peer-address-name>]

Displays detail information about the MSDP peer. If <peer-address-name> is not supplied, all peers are displayed.

In images supporting the "ip msdp sa-limit" command, the output will also display the number of SA messages learned from each peer and, if configured, the sa-limit for that peer [12.0(15)S, 12.1(7), 12.2(2)T, 12.2(3), 12.2S, CSCdt19258].

Example output:

```
sjck-rp1>sh ip msdp peer
MSDP Peer 192.135.250.116 (rtp5-rp1.cisco.com), AS 109 (configured AS)
Description:
  Connection status:
    State: Up, Resets: 9, Connection source: Loopback2 (204.69.199.17)
    Uptime(Downtime): 1d10h, Messages sent/received: 436765/429062
    Output messages discarded: 0
    Connection and counters cleared 1w2d     ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
    Sending SA-Requests to peer: disabled
  Peer ttl threshold: 0
  SAs learned from this peer: 32, SAs limit: 500
  Input queue size: 0, Output queue size: 0
```

show ip msdp sa-cache [<group-or-source>] [<group-or-source>] [<asn>] [rejected-sa [detail] [read-only]]

Displays (S,G) state learned from MSDP peers. State is cached only when "ip msdp cache-sa-state" is configured. When <asn> is specified, only state originated by AS number <asn> is displayed. When two addresses (or names) are specified, an (S,G) entry corresponding to those addresses is displayed. Otherwise, a single group address can be specified to display all sources for that group [12.0S 12.1].

To display SA messages that were not cached, but rejected, enable the global configuration command "ip msdp cache-rejected-sa", then use "show ip msdp sache-cache ... rejected-sa [detail] [read-only]" to display the last received and rejected MSDP SA messages. If "read-only" is NOT specified, the router will display the rejected MSDP SA messages out of the active cache of rejected MSDDP SA messages.

```
    This may result in unexpected inconsistencies during display when older
    rejected SA messages are being overwritten with currently received and
    rejected SA messages while output for the command is happening.
    To avoid this, use the "read-only" option, which will make the router
    checkpoint the rejected-sa cache - this requires a second copy of the
    rejected-sa cache, so if the router is low on memory, "read-only"
    may fail due to lack of memory. Note also that checkpointing will clear
    the actively used cache of MSDP messages - calling "show ip msdp
    sa-cache rejected-sa ... read-only" twice in a rows will thus produce
    an empty of small list of SA messages. If the "detail" keyword is
    specified, the output will also contain the sending peer and reject
    reason for each SA entry [CSCdv13858, 12.0(22)S].

  Reasons for rejecting MSDP SA entries:
     "no-memory" - the router ran out of memory allocating storage
                for the MSDP SA message. This should not happen
     "sa-limit-exceeded - The SA message was not stored because the
                configured "ip msdp sa-limit" was already exhausted
                when the message was received.
   "ssm-range" - The message was rejected because it indicated a group
                in the SSM range.
   "autorp-group" - The message was rejected because it indicated on
                of the two AutoRP groups 224.0.1.39/224.0.1.40.
   "rp-filter" - The message was rejected because it was filtered by
                    a configured "ip msdp sa-filter in ... [rp-list <acl>
                                          | rp-route-map <map>]"
   "rpf-fail" -  The message was rejected because it failed the MSDP
                RPF check.
   "in-filter" - The message was rejected because it was filtered by
                a configured "ip msdp sa-filter in ...  [list <acl>]
                                        [route-map <map>]"
    Example output:
      router#show ip msdp sa-cache rejected detail read-only
      MSDP Rejected SA Cache
      35 rejected SAs received over 02:50:01, cache size: 50 entries
      Timestamp (source, group)
      2832.248, (52.52.52.4, 227.7.7.12), RP: 52.52.52.4, Peer: 52.52.52.4,
        Reason: sa-limit-exceeded
      2915.232, (50.50.50.2, 224.1.1.1), RP: 11.11.11.1, Peer: 50.50.50.2,
        Reason: in-filter
      3509.584, (50.50.50.2, 225.5.5.5), RP: 52.52.52.2, Peer: 50.50.50.2,
        Reason: rpf-fail
    ... (the timestamp is the uptime of the router in <sec>.<msec>)


show ip msdp count [<asn>]
    When SA caching is enabled, this command displays the number of
    sources and groups originated in SA messages from each AS.

  In images supporting the "ip msdp sa-limit" command, the output
  will also display the number of SA messages learned from each
  peer [12.0(15)S, 12.1(7), 12.2(2)T, 12.2(3), 12.2S, CSCdt19258].

  Example output:

    sjck-rp1>show ip msdp count
    SA State per Peer Counters, <Peer>: <# SA learned>
```

```
          192.135.250.116: 24
          144.228.240.253: 3964
          172.17.253.19: 10
          172.17.170.110: 11

      SA State per ASN Counters, <asn>: <# sources>/<# groups>
          Total entries: 4009
          ?: 198/98, 9: 1/1, 14: 107/57, 17: 7/5
          18: 4/3, 25: 23/17, 26: 39/27, 27: 2/2
          32: 19/7, 38: 2/1, 52: 4/4, 57: 1/1
          68: 4/4, 73: 12/8, 81: 19/1, 87: 9/6
          ...

Clear Commands:

  clear ip msdp peer <peer-address-or-name>
      Clears TCP connection for peer <peer-address-or-name>. Also resets
      message counters.

  clear ip msdp sa-cache [<group-name-or-address>]
      Clears SA cache entry (if SA caching is enabled) for 1) all entries,
      2) all sources for a specific group, or 3) all a specific source/group
      pair.

 clear ip msdp statistics [<peer-address-or-name>]
     Clears statistics counters of one or all MSDP peers without reseting
     the sessions.  The counters cleared include the reset count and the
     input/output packet count.

--------------------------------------------------------------------------
```