Contents

MSDP commands

cache-sa-enable

Use **cache-sa-enable** to enable the SA message cache mechanism to cache the (S, G) entries contained in SA messages.

Use **undo cache-sa-enable** to disable the SA message cache mechanism.

Syntax

cache-sa-enable

undo cache-sa-enable

Default

The SA message cache mechanism is enabled. The device caches the (S, G) entries contained in received SA messages.

Views

MSDP view

Predefined user roles

network-admin

Examples

# Enable the SA message cache mechanism on the public network, so that the device caches the (S, G) entries contained in the received SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] cache-sa-enable
```

Related commands

- **display msdp sa-cache**
- **display msdp sa-count**

display msdp brief

Use **display msdp brief** to display brief information about MSDP peers.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **brief** [**state** { **connect** | **disabled** | **established** | **listen** | **shutdown** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays brief information about MSDP peers on the public network.

state: Specifies a state. If you do not specify this keyword, the command displays brief information about MSDP peers in all states.

connect: Specifies the connecting state.

disabled: Specifies the connection failure state.

established: Specifies the session state.

listen: Specifies the listening state.

shutdown: Specifies the shutdown state.

Examples

# Display brief information about MSDP peers in all states on the public network.

```
<Sysname> display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
1            1            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
20.20.20.20     Established 00:00:13        100        0          0
```

Table 1 Command output

Field	Description
Configured	Number of MSDP peers that have been configured.
Established	Number of MSDP peers in established state.
Listen	Number of MSDP peers in listening state.
Connect	Number of MSDP peers in connecting state.
Shutdown	Number of MSDP peers in shutdown state.
Disabled	Number of MSDP peers in disabled state.
Peer address	MSDP peer address.
State	MSDP peer status: • **Established**—A session has been established and the MSDP peer is in session. • **Listen**—A session has been established and the local device acts as the server in listening state. • **Connect**—A session is not established and the local device acts as a client in connecting state. • **Shutdown**—The session has been torn down. • **Down**—The connection failed.
Up/Down time	Length of time since the MSDP peering connection was established or torn down.
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
SA count	Number of (S, G) entries.
Reset count	MSDP peering connection reset times.

display msdp peer-status

Use **display msdp peer-status** to display detailed status of MSDP peers.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **peer-status** [*peer-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this commands displays detailed status of the MSDP peers on the public network.

peer-address: Specifies an MSDP peer by its address. If you do not specify an MSDP peer, this command displays the detailed status of all MSDP peers.

Examples

# Display the detailed status of MSDP peer 20.20.20.20 on the public network.

```
<Sysname> display msdp peer-status 20.20.20.20
MSDP peer 20.20.20.20; AS 100
 Description:
 Information about connection status:
   State: Disabled
   Up/down time: 14:41:08
   Resets: 0
   Connection interface: LoopBack0 (20.20.20.30)
   Received/sent messages: 867/867
   Discarded input messages: 0
   Discarded output messages: 0
   Elapsed time since last connection or counters clear: 14:42:40
   Mesh group peer joined: momo
   Last disconnect reason: Hold timer expired with truncated message
   Truncated packet: 5 bytes in buffer, type: 1, length: 20, without packet time: 75s
 Information about (Source, Group)-based SA filtering policy:
   Import policy: None
   Export policy: None
 Information about SA-Requests:
   Policy to accept SA-Requests: None
   Sending SA-Requests status: Disable
 Minimum TTL to forward SA with encapsulated data: 0
 SAs learned from this peer: 0, SA cache maximum for the peer: 4294967295
 Input queue size: 0, Output queue size: 0
 Counters for MSDP messages:
   RPF check failure: 0
   Incoming/outgoing SA: 0/0
```

```
Incoming/outgoing SA-Request: 0/0
Incoming/outgoing SA-Response: 0/0
Incoming/outgoing Keepalive: 867/867
Incoming/outgoing Notification: 0/0
Incoming/outgoing Traceroutes in progress: 0/0
Incoming/outgoing Traceroute reply: 0/0
Incoming/outgoing Unknown: 0/0
Incoming/outgoing data packet: 0/0
```

Table 2 Command output

Field	Description
MSDP peer	MSDP peer address.
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
State	MSDP peer status: • **Established**—A session has been established and the MSDP peer is in session. • **Listen**—A session has been established and the local device acts as the server in listening state. • **Connect**—A session is not established and the local device acts as a client in connecting state. • **Shutdown**—The session has been torn down. • **Disabled**—The connection failed.
Up/Down time	Length of time since the MSDP peering connection was established or torn down.
Resets	MSDP peering connection reset times.
Connection interface	Interface and IP address used for setting up a TCP connection with the remote MSDP peer.
Received/sent messages	Number of SA messages sent and received through this connection.
Discarded input messages	Number of discarded incoming messages.
Discarded output messages	Number of discarded outgoing messages.
Elapsed time since last connection or counters clear	Elapsed time since the MSDP peer information was last cleared.
Mesh group peer joined	Mesh group that the MSDP peer has joined. This field is not displayed if the MSDP peer does not join a mesh group.
Last disconnect reason	Reason why last MSDP peering connection was torn down. If the connection is not terminated, this field is not displayed. • **Hold timer expired without message**—Hold timer expires and the receiving cache has no messages. • **Hold timer expired with truncated message**—Hold timer expires and messages in the receiving cache are not intact. ○ **bytes in buffer**—Size of data in the receiving cache when the connection was terminated. ○ **type**—Type of packets in the receiving cache when the connection was terminated. ○ **length**—Length of packets in the receiving cache when the connection was terminated. If the packet is too small in size, this field cannot be resolved and is not displayed. ○ **without packet time**—Length of time since packets were

Field	Description
	last processed. - **Remote peer has been closed**—The MSDP peering connection has been torn down. - **TCP ERROR/HUP event received**—Error/hup event received by the TCP socket when the MSDP peer sent messages. - **Illegal message received**—The MSDP peer received illegal messages. - **Notification received**—The MSDP peer received notification messages. - **Reset command executed**—The user executed the **reset msdp peer** command. - **Shutdown command executed**—The user executed the **shutdown** command. - **Interface downed**—The MSDP peer received the interface down event when connecting to the remote MSDP peer.
Information about (Source, Group)-based SA filtering policy	SA message filtering list information: - **Import policy**—Filter list for receiving SA messages from the specified MSDP peer. - **Export policy**—Filter list for forwarding SA messages from the specified MSDP peer.
Information about SA-Requests	SA request information: - **Policy to accept SA request messages**—Filtering rule for receiving or forwarding SA request messages from the specified MSDP peer. If SA request messages are not filtered, this field displays **None**. - **Sending SA requests status**—Whether the MSDP peer is enabled to send an SA request message to the designated MSDP peer after receiving a new join message.
Minimum TTL to forward SA with encapsulated data	Minimum TTL value for the multicast packets encapsulated in SA messages.
SAs learned from this peer	Number of cached (S, G) entries learned from the specified MSDP peer.
SA-cache maximum for the peer	Maximum number of (S, G) entries learned from the specified MSDP peer that the device can cache.
Input queue size	Data size cached in the input queue.
Output queue size	Data size cached in the output queue.

Field	Description
Counters for MSDP message	MSDP peer statistics: • **RPF check failure**—Number of SA messages discarded because of RPF check failure. • **Incoming/outgoing SA**—Number of received and sent SA messages. • **Incoming/outgoing SA-Request**—Number of received and sent SA requests. • **Incoming/outgoing SA-Response**—Number of received and sent SA responses. • **Incoming/outgoing Keepalive**—Number of received and sent keepalive messages. • **Incoming/outgoing Notification**—Number of received and sent notification messages. • **Incoming/outgoing Traceroutes in progress**—Number of received and sent traceroute-in-progress messages. • **Incoming/outgoing Traceroute reply**—Number of received and sent traceroute replies. • **Incoming/outgoing Unknown**—Number of received and sent unknown messages. • **Incoming/outgoing data packet**—Number of received and sent SA messages encapsulated with multicast data.

display msdp sa-cache

Use **display msdp sa-cache** to display (S, G) entries in the SA cache.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **sa-cache** [*group-address* | *source-address* | *as-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays (S, G) entries in the SA cache on the public network.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays (S, G) entries for all multicast groups.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command displays (S, G) entries for all sources.

as-number: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, this command displays (S, G) entries for all ASs.

Usage guidelines

You must execute the **cache-sa-enable** command before you execute this command. Otherwise, this command does not give any output.

Examples

# Display information about the (S, G) entries in the SA cache on the public network.

```
<Sysname> display msdp sa-cache
Total Source-Active Cache - 5 entries
Matched 5 entries

Source          Group           Origin RP       Pro  AS         Uptime   Expires
10.10.1.2       225.0.0.1       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.2       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.3       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.4       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.5       10.10.10.10     BGP  100        00:00:11 00:05:49
```

Table 3 Command output

Field	Description
Total Source-Active Cache	Total number of multicast sources in the SA cache.
Matched	Total number of (S, G) entries that match a multicast source.
Source	Multicast source address.
Group	Multicast group address.
Origin RP	Address of the RP that generated the (S, G) entry.
Pro	Type of protocol from which the AS number of the origin RP originates. If the system could not obtain the AS number, this field displays a question mark (?).
AS	AS number of the origin RP. If the system could not obtain the AS number, this field displays a question mark (?).
Uptime	Length of time for which the cached (S, G) entry has existed.
Expires	Length of time in which the cached (S, G) entry will expire.

Related commands

cache-sa-enable

display msdp sa-count

Use **display msdp sa-count** to display the number of (S, G) entries in the SA cache.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **sa-count** [*as-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the number of (S, G) entries in the SA cache on the public network.

as-number: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, this command displays the number of (S, G) entries in the SA cache of all ASs.

Usage guidelines

You must execute the **cache-sa-enable** command before you execute this command. Otherwise, this command does not give any output.

Examples

# Display the number of (S, G) entries in the SA cache on the public network.

```
<Sysname> display msdp sa-count
(S, G) entries statistics, counted by peer
  Peer address       SA count
  10.10.10.10        5

(S, G) entries statistics, counted by AS
  AS          Source count        Group count
  ?           3                   3

5 (S, G) entries in total
```

Table 4 Command output

Field	Description
(S, G) entries statistics, counted by peer	Number of (S, G) entries on an MSDP peer basis.
Peer address	Address of the MSDP peer that sent SA messages.
SA count	Number of (S, G) entries from this MSDP peer.
(S, G) entries statistics, counted by AS	Number of cached (S, G) entries on an AS basis.
AS	AS number. If the system could not obtain the AS number, this field displays a question mark (?).
Source count	Number of multicast sources from this AS.
Group count	Number of multicast groups from this AS.
(S, G) entries in total	Total number of (S, G) entries.

Related commands

cache-sa-enable

encap-data-enable

Use **encap-data-enable** to enable multicast data encapsulation in SA messages.

Use **undo encap-data-enable** to restore the default.

Syntax

encap-data-enable

undo encap-data-enable

Default

An SA message contains only (S, G) entries. No multicast data is encapsulated in an SA message.

Views

MSDP view

Predefined user roles

network-admin

Examples

# Enable multicast data encapsulation in SA messages on the public network.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

import-source

Use **import-source** to configure an SA message creation policy.

Use **undo import-source** to remove the configured SA message creation policy.

Syntax

import-source [**acl** *acl-number*]

undo import-source

Default

When an SA message is created, all the (S, G) entries within the domain are advertised in the SA message.

Views

MSDP view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999. If you specify an ACL, this command advertises only the (S, G) entries that the ACL permits. This command does not advertise any (S, G) entries when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

During ACL matching, the protocol ID in the ACL rule is not verified.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

This command controls the creation of SA messages. You can also use the **peer sa-policy** command to configure a filtering rule to control forwarding and acceptance of SA messages.

Examples

# On the public network, configure an SA creation policy to advertise only the (10.10.0.0/16, 225.1.0.0/16) entries when an SA message is created.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

Related commands

peer sa-policy

msdp

Use **msdp** to enable MSDP and enter MSDP view.

Use **undo msdp** to disable MSDP and remove the configurations in MSDP view to release the resources occupied by MSDP.

Syntax

msdp [**vpn-instance** *vpn-instance-name*]

undo msdp [**vpn-instance** *vpn-instance-name*]

Default

MSDP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command applies to the public network.

Usage guidelines

This command takes effect only when IP multicast routing is enabled.

Examples

# Enable IP multicast routing on the public network, and enable MSDP on the public network and enter public network MSDP view.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] msdp
[Sysname-msdp]
```

Related commands

multicast routing

originating-rp

Use **originating-rp** to configure an interface address as the RP address of SA messages.

Use **undo originating-rp** to remove the configuration.

Syntax

originating-rp *interface-type interface-number*

undo originating-rp

Default

The PIM RP address is used as the RP address of SA messages.

Views

MSDP view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

# On the public network, specify the IP address of VLAN-interface 100 as the RP address of SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] originating-rp vlan-interface 100
```

peer connect-interface

Use **peer connect-interface** to create an MSDP peering connection.

Use **undo peer connect-interface** to remove an MSDP peering connection.

Syntax

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

Default

MSDP peering connection is not created.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

interface-type interface-number: Specifies an interface by its type and number. The local device uses the primary IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

Usage guidelines

You must execute this command before you use any other **peer** command. Otherwise, the system notifies you that the MSDP peer does not exist.

Examples

# On the public network, configure the router with IP address 125.10.7.6 as the MSDP peer of the local router, and configure VLAN-interface 100 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
```

peer description

Use **peer description** to configure the description for an MSDP peer.

Use **undo peer description** to delete the description for an MSDP peer.

Syntax

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

Default

No description is configured for an MSDP peer.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

text: Specifies a description, a case-sensitive string of 1 to 80 characters, including spaces.

Examples

# On the public network, configure a description of **CustomerA** for the device at 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description CustomerA
```

peer mesh-group

Use **peer mesh-group** to configure an MSDP peer as a mesh group member.

Use **undo peer mesh-group** to remove an MSDP peer from the mesh group.

Syntax

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

Default

An MSDP peer does not belong to any mesh group.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

name: Specifies a mesh group, a case-sensitive string of 1 to 32 characters. A mesh group name must not contain any spaces.

Examples

# On the public network, configure MSDP peer 125.10.7.6 as a member of mesh group **Group1**.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 mesh-group Group1
```

peer minimum-ttl

Use **peer minimum-ttl** to configure the lower TTL threshold for multicast data packets encapsulated in SA messages.

Use **undo peer minimum-ttl** to restore the default.

Syntax

peer *peer-address* **minimum-ttl** *ttl-value*

undo peer *peer-address* **minimum-ttl**

Default

The lower TTL threshold for a multicast packet to be encapsulated in an SA message is 0.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

ttl-value: Specifies the lower TTL threshold in the range of 0 to 255.

Examples

# On the public network, set the lower TTL threshold for multicast packets to be encapsulated in SA messages to 10. Only multicast data packets whose TTL value is larger than or equal to 10 can be encapsulated in SA messages and forwarded to MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

peer password

Use **peer password** to configure an MD5 authentication key used by both MSDP peers to establish a TCP connection.

Use **undo peer password** to restore the default.

Syntax

peer *peer-address* **password** { **cipher | simple** } *password*

undo peer *peer-address* **password**

Default

MSDP peers do not perform MD5 authentication to establish TCP connections.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

cipher: Specifies a ciphertext MD5 authentication key.

simple: Specifies a plaintext MD5 authentication key.

password: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 80 characters. If **cipher** is specified, it must be a ciphertext string of 33 to 137 characters.

Usage guidelines

The MSDP peers involved in MD5 authentication must be configured with the same authentication method and key. Otherwise, the authentication fails and the TCP connection cannot be established.

For security purposes, all keys, including keys configured in plain text, are saved in cipher text.

Examples

# On the public network, configure an MD5 authentication key in plaintext as **aabbcc** for the TCP connections between the local end and MSDP peer 10.1.100.1. The configuration on the remote peer is similar.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 10.1.100.1 password simple aabbcc
```

peer request-sa-enable

Use **peer request-sa-enable** to enable the device to send an SA request message to an MSDP peer after receiving a new join message.

Use **undo peer request-sa-enable** to disable the device from sending an SA request message to the specified MSDP peer.

Syntax

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

Default

After receiving a new join message, the device does not send an SA request message to any MSDP peer. Instead, it waits for the next SA message to come.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

Usage guidelines

You must disable SA message cache mechanism before you execute this command. Otherwise, the device does not send out SA request messages.

Examples

# On the public network, disable the SA message cache mechanism. Enable the device to send an SA request message to MSDP peer 125.10.7.6 after it receives a new join message.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

Related commands

- **cache-sa-enable**
- **display msdp peer-status**

peer sa-cache-maximum

Use **peer sa-cache-maximum** to configure the maximum number of cached (S, G) entries learned from an MSDP peer.

Use **undo peer sa-cache-maximum** to restore the default.

Syntax

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

Default

The device can cache a maximum of 4294967295 (S, G) entries learned from any MSDP peer.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

sa-limit: Specifies the maximum number of (S, G) entries that the device can cache, in the range of 1 to 4294967295.

Examples

# On the public network, enable the device to cache up to 100 (S, G) entries learned from its MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

Related commands

- **display msdp brief**
- **display msdp peer-status**
- **display msdp sa-count**

peer sa-policy

Use **peer sa-policy** to configure an SA incoming or outgoing policy.

Use **undo peer sa-policy** to remove the configured SA incoming or outgoing policy.

Syntax

peer *peer-address* **sa-policy** { **export** | **import** } [**acl** *acl-number*]

undo peer *peer-address* **sa-policy** { **export** | **import** }

Default

All SA messages are accepted or forwarded.

Views

MSDP view

Predefined user roles

network-admin

Parameters

export: Specifies the outgoing direction.

import: Specifies the incoming direction.

peer-address: Specifies an MSDP peer by its IP address.

acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999. If you specify an ACL, the device accepts and forwards only SA messages that the ACL permits. If you do not specify an ACL, the device discards all SA messages when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

When you configure a rule in the IPv4 advanced ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast source address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

This command controls the acceptance and forwarding of SA messages. You can also use the **import-source** command to configure a filtering rule to control the creation of SA messages.

Examples

# On the public network, configure an SA outgoing policy to forward only SA messages that ACL 3100 permits to MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

Related commands

- **display msdp peer-status**
- **import-source**

peer sa-request-policy

Use **peer sa-request-policy** to configure an SA request policy.

Use **undo peer sa-request-policy** to remove the configured SA request policy.

Syntax

peer *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

Default

SA request messages are not filtered.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the switch accepts only SA requests that the ACL permits. All SA requests are filtered out when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.

- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

# On the public network, configure an SA request policy to process SA requests originated from the MSDP peer 175.58.6.5 with multicast groups in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Use **reset msdp peer** to reset the TCP connection with an MSDP peer and clear statistics for the MSDP peer.

Syntax

reset msdp [**vpn-instance vpn-instance**-*name*] **peer** [*peer-address*]

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command resets the TCP connection with the specified MSDP peer and clears statistics for the MSDP peer on the public network.

peer-address: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, this command resets the TCP connections with all MSDP peers.

Examples

# On the public network, reset the TCP connection with MSDP peer 125.10.7.6, and clear all statistics for this MSDP peer.

```
<Sysname> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Use **reset msdp sa-cache** to clear (S, G) entries from the SA cache.

Syntax

reset msdp [**vpn-instance vpn-instance**-*name*] **sa-cache** [*group-address*]

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears (S, G) entries from the SA cache on the public network.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command clears the cached (S, G) entries for all multicast groups from the SA cache.

Examples

# Clear the (S, G) entries for multicast group 225.5.4.3 from the SA cache on the public network.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

Related commands

- **cache-sa-enable**
- **display msdp sa-cache**

reset msdp statistics

Use **reset msdp statistics** to clear statistics for the specified MSDP peer without resetting the TCP connection with the MSDP peer.

Syntax

reset msdp [**vpn-instance vpn-instance**-*name*] **statistics** [*peer-address*]

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears statistics for the specified MSDP peer without resetting the TCP connection with the MSDP peer on the public network.

peer-address: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, this command clears statistics for all MSDP peers.

Examples

# Clear statistics for MSDP peer 125.10.7.6 on the public network.

```
<Sysname> reset msdp statistics 125.10.7.6
```

shutdown (MSDP view)

Use **shutdown** to tear down the connection with an MSDP peer.

Use **undo shutdown** to re-establish the connection with an MSDP peer.

Syntax

shutdown *peer-address*

undo shutdown *peer-address*

Default

The connection with any MSDP peer is active.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

Examples

# Tear down the connection with MSDP peer 125.10.7.6 on the public network.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6
```

Related commands

- **display msdp brief**
- **display msdp peer-status**

static-rpf-peer

Use **static-rpf-peer** to configure a static RPF peer.

Use **undo static-rpf-peer** to remove a static RPF peer.

Syntax

static-rpf-peer *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

Default

No static RPF peer is configured.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on the RP addresses in SA messages. The *ip-prefix-name* argument is the filtering policy name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

When you configure multiple static RPF peers at the same time, observe the following rules:

- If the **rp-policy** keyword is specified for all the static RPF peers, SA messages from the active static RPF peers are filtered according to the configured filtering policy. The router receives only SA messages that have passed the filtering.
- If the **rp-policy** keyword is not specified for the static RPF peers, the router receives all SA messages from the active static RPF peers.

Examples

# Configure a static RPF peer on the public network.

```
<Sysname> system-view
[Sysname] ip prefix-list list1 permit 130.10.0.0 16 greater-equal 16 less-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

Related commands

- **display msdp peer-status**
- **ip prefix-list**

timer retry

Use **timer retry** to configure the interval between MSDP peering connection attempts.

Use **undo timer retry** to restore the default.

Syntax

timer retry *interval*

undo timer retry

Default

The interval between MSDP peering connection attempts is 30 seconds.

Views

MSDP view

Predefined user roles

network-admin

Parameters

interval: Specifies an interval between MSDP peering connection attempts, in the range of 1 to 60 seconds.

Examples

# Set the MSDP peering connection attempt interval to 60 seconds on the public network.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] timer retry 60
```