Configuring Dynamic Neighbors

Last Updated: April 10, 2012

When neighbors are not adjacent, normal Cisco SAF peering mechanisms cannot be used to exchange SAF information over the networking cloud. The neighbors are often multiple hops away, and separated by dark nets (routers not running SAF).

To support this type of network, SAF provides the **neighbor** command, which allows remote neighbors to be configured and sessions established though unicast packet transmission. However, as the number of Forwarders needing to exchange SAF information over the networking cloud increases, unicast SAF neighbor definitions may become cumbersome to manage. Each neighbor has to be manually configured, resulting in increased operational costs.

To better accommodate deployment of these topologies, ease configuration management, and reduce operational costs, the Dynamic Neighbors feature provides support for the dynamic discovery of remote unicast and multicast neighbors (referred to as “remote neighbors”). Remote neighbor support allows Cisco SAF peering to one or more remote neighbors, which may not be known at the time the router is configured, thus reducing configuration management.

This section contains the following major topics:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Dynamic Neighbors

Before configuring SAF dynamic neighbors, ensure that when using:

- Unicast-listen mode--IP connectivity (reachability) exists between routers that need to do dynamic peering.
- Multicast-group mode--Multicast is running on the network.
- The **allow-list**

  keyword--The configured Access Control List that will specify the remote IP addresses from which EIGRP neighbor connections may be accepted.

Restrictions for Dynamic Neighbors

- The **remote-neighbors** command requires a loopback as a source interface.
- Only named ACLs (Access Control Lists) are permitted with the **allow-list** keyword. Numbered ACLs that are configured are not permitted.

Within a service-family, the following restrictions apply:

- Only one **remote-neighbors unicast-listen** command and one **remote-neighbors multicast-group** command may be configured per interface. For example, you cannot configure **remote-neighbors source Loopback1 multicast-group 224.1.1.1** and **remote-neighbors source Loopback1 multicast-group 224.1.1.2**. If you want to configure multiple different multicast-group addresses in the same service-family, you need to use multiple source interfaces.
- A multicast-group address may only be associated to a single source interface. For example, you cannot configure **remote-neighbors source Loopback1 multicast-group 224.1.1.1** and **remote-neighbors source Loopback2 multicast-group 224.1.1.1**.

Information About Dynamic Neighbors

When neighbors are not adjacent, normal Cisco SAF peering mechanisms cannot be used to exchange SAF information over the networking cloud. The neighbors are often multiple hops away, and separated by dark nets (routers not running SAF).

To support this type of network, SAF provides the **neighbor** command, which allows remote neighbors to be configured and sessions established though unicast packet transmission. However, as the number of Forwarders needing to exchange SAF information over the networking cloud increases, unicast SAF neighbor definitions may become cumbersome to manage. Each neighbor has to be manually configured, resulting in increased operational costs.

To better accommodate deployment of these topologies, ease configuration management, and reduce operational costs, the Dynamic Neighbors feature provides support for the dynamic discovery of remote unicast and multicast neighbors (referred to as “remote neighbors”). Remote neighbor support allows Cisco SAF peering to one or more remote neighbors, which may not be known at the time the router is configured, thus reducing configuration management.

Remote Neighbor Session Policy

When using remote unicast-listen or remote multicast-group neighbor configurations, SAF neighbor IP addresses are not pre-defined, and neighbors may be many hops away. A router with this configuration could peer with any router that sends a valid HELLO packet. Because of security considerations, this open aspect requires policy capabilities to limit peering to valid routers and to restrict the number of neighbors to limit resource consumption. This capability is accomplished using the following manually configured parameters, and takes effect immediately.

Neighbor Filter List

The optional **allow-list** keyword, available in the **remote-neighbors** command, enables you to use an access list (Access Control List) to specify the remote IP addresses from which Cisco SAF neighbor connections may be accepted. If you do not use the **allow-list** keyword, then all IP addresses (permit any) will be accepted.

The Access Control List (ACL) defines a range of IPv4 or IPv6 IP addresses with the following conditions:

- Any neighbor that has a source IP address that matches an IP address in the access-list will be allowed (or denied) based on the user configuration.
- If the **allow-list** keyword is not specified, any IP address will be permitted (permit any).
- The **allow-list** keyword is supported only for remote multicast-group and unicast-listen neighbors. It is not available for static, remote static, or local neighbors.
- Incoming Cisco SAF packets that do not match the specified access list will be rejected.

Maximum Remote Neighbors

The optional **max-neighbors**keyword, available in the **remote-neighbors** command, enables you to specify a maximum number of remote neighbors that Cisco SAF can create using the remote neighbor configurations. When the maximum number of remote neighbors has been created for a configuration, Cisco SAF rejects all subsequent connection attempts for that configuration. This option helps to protect against denial-of-service attacks that attempt to create many remote neighbors in an attempt to overwhelm router resources.

The **max-neighbors** configuration option has the following conditions:

- This option is supported only for remote multicast-group or unicast-listen neighbors. It is not available for local, static, or remote static neighbors.
- There is no default maximum. If you do not specify a maximum number of remote neighbors, the number of remote neighbors is limited only by available memory and bandwidth.
- Reducing the maximum number of remote neighbors to a number less than the current sessions will result in the neighbors (in no specific order) being dropped until the count reaches the new limit.

Configuration Changes for Neighbor Filter List and Maximum Remote Neighbors

When the **allow-list** or **max-neighbors** configurations are changed, any existing remote Cisco SAF sessions that are no longer allowed by the new configuration will be removed automatically and immediately. Pre-existing neighbors that are still allowed by the new configuration will not be affected.

Neighbor Types

The following terms are used when describing neighbor types:

- Local Neighbor--A neighbor that is adjacent on a shared subnet (or common subnet) and uses a link-local multicast address for packet exchange. This is the default type of neighbor in Cisco SAF.
- Static Neighbor--Any neighbor that uses unicast to communicate, is one hop away, is on a common subnet, and whose IP address has been specified using the **neighbor***ip-address* command.
- Remote Neighbor--Any neighbor that is multiple hops away, including Remote Static Neighbors.
- Remote Static Neighbor--Any neighbor that uses unicast to communicate, is multiple hops away, and whose IP address has been specified using the **neighbor***ip-address* command.
- Remote Multicast-Group--Any neighbor that is multiple hops away, but does not have its IP address manually configured using the **neighbor***ip-address* command, and uses a configured multicast group address for packet exchange.
- Remote Unicast-listen (or simply Unicast-listen)--Any neighbor that uses unicast to communicate, is multiple hops away, and whose IP address has not been configured using the **neighbor***ip-address* command.

Remote Unicast-Listen (Point-to-Point) Neighbors

For configurations in which multiple remote neighbors peer with a single hub (point-to-point), the hub can be configured for remote unicast-listen peering using the **remote-neighbors** command to allow the remote neighbors to peer with the hub without having to manually configure the remote neighbor IP addresses on the hub.

When configured with this command, the hub router:

- Uses its interface IP address as the source IP address for any unicast transmissions. This IP address must be routable.
- Requires neighbors peering with the hub to be configured using the **neighbor***ip-address* **loopback** *loopback-interface-number* **remote***maximum-hops* command where *ip-address* is the unicast address of the local router interface IP address.
- Listens for unicast HELLO packets on the interface specified in the **remote-neighbor** command.
- Accepts a unicast HELLO packet if it is in the IP address range configured using the **allow-list** keyword, or any unicast HELLO packet if an allow list is not defined.
- Rejects multicast HELLO packets from any neighbor that is also sending unicast HELLO packets and is permitted by the unicast allow-list (or all neighbors if an allow-list is not defined).
- Begins normal neighbor establishment using the IP addresses of the remote neighbors for packet transmission once the neighbor relationship is established.

Remote Multicast-Group (Multipoint-to-Multipoint) Neighbors

Multicast can be used to provide an efficient transport between multiple Cisco SAF neighbors. A single multicast-group address can be used for multiple Cisco SAF neighbors to exchange information within the

same multicast-group. To configure multipoint-to-multipoint configurations, use the **multicast-group** keyword available in the **remote neighbors** command.

When configured with this command, the router:

- Uses the interface IP address as the source IP address for any unicast transmissions. This IP address must be routable.
- Uses the configured multicast-group address for all multicast packets sent and received.
- Requires all forwarders and routers, which form the multipoint-to-multipoint neighbor relationships, to be configured using the same multicast-group IP address.
- Requires multicast forwarding for the defined multicast-group address to be configured and functional for packet delivery.

Inheritance and Precedence of the Remote Neighbor Configurations

Static neighbors configured with the **neighbor***ip-address* or the **neighbor***ip address***remote** commands take precedence over the remote neighbors that are created as a result of the **remote-neighbors** command. If the remote IP address of an incoming unicast Cisco SAF connection matches both a static neighbor and the remote unicast-listen neighbor access list, the static neighbor is used and no remote unicast-listen neighbor is created. If you configure a new static neighbor while a remote neighbor for the same remote IP address already exists, Cisco SAF automatically removes the remote unicast-listen neighbor.

Remote unicast-listen neighbors take precedence over remote multicast-group neighbors. If Cisco SAF is receiving both unicast and multicast HELLOs from the same remote IP address targeted at the same local interface, the neighbor will be treated as unicast (unicast-listen) rather than multicast (multicast-group) for packet exchange.

How to Configure Dynamic Neighbors

To configure Cisco SAF dynamic neighbors, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. **service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **remote-neighbors source** *interface* {**unicast-listen** | **multicast-group** *group-address* } [**allow-list** *access-list-name*] [**max-neighbors** *max-remote-peers*]
6. **exit-service-family**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**remote-neighbors source** *interface* {**unicast-listen** | **multicast-group** *group-address* } [**allow-list** *access-list-name*] [**max-neighbors** *max-remote-peers*] **Example:** `Router(config-router-sf)# remote-neighbors source Loopback1 unicast-listen allow-list myNeighborList`	Configures a SAF process that enables remote neighbors to accept inbound connections from any remote IP address. Use the: • **allow-list** keyword to use an access list (Access Control List) to specify the remote IP addresses from which Cisco SAF neighbor connections may be accepted. If you do not use the allow-list keyword, then all IP addresses (permit any) will be accepted. • **max-neighbors** keyword to specify the maximum number of remote neighbors. If you do not specify a number, the maximum number of remote neighbors is limited only by available memory and bandwidth.
Step 6	**exit-service-family** **Example:** `Router(config-router-sf)# exit-service-family`	Exits service-family configuration mode.

Configuration Examples for Dynamic Neighbors

Examples: Configuring Cisco SAF Dynamic Neighbors

The following examples show how to configure both routers involved in the neighbor relationship.

This example uses the **unicast-listen** keyword to configure remote neighbors to accept inbound connections from IP addresses that match the access list myNeighborList.

```
Router1(config)# interface Loopback1
Router1(config-if)# ip address 10.1.1.1 255.255.255.255
Router1(config-if)# exit
Router1(config)# ip access-list standard myNeighborList
Router1(config-std-nacl)# permit 10.0.0.0 0.255.255.255
Router1(config-std-nacl)# exit
Router1(config)# router eigrp virtual-name
Router1(config-router)# service-family ipv4 autonomous-system 4453
Router1(config-router-sf)# remote-neighbors source Loopback1 unicast-listen allow-list
myNeighborList
Router2(config)# interface Loopback2
Router2(config-if)# ip address 10.2.2.2 255.255.255.255
Router2(config-if)# exit
Router2(config)# router eigrp virtual-name
Router2(config-router)# service-family ipv4 autonomous-system 4453
Router2(config-router-sf)# neighbor 10.1.1.1 Loopback2 remote 20
```

This example uses the **multicast-group** keyword to use IP multicast to discover remote neighbors and form remote neighbor relationships. It also specifies 30 as the maximum number of inbound connections from remote neighbors that a member of the multicast group may accept.

```
Router1(config)# interface Loopback1
Router1(config-if)# ip address 10.1.1.1 255.255.255.255
Router1(config-if)# ip pim sparse-mode
Router1(config-if)# exit
Router1(config)# router eigrp virtual-name
Router1(config-router)# service-family ipv4 autonomous-system 4453
Router1(config-router-sf)# remote-neighbors source Loopback1 multicast-group 224.44.56.1
max-neighbors 30
Router2(config)# interface Loopback2
Router2(config-if)# ip address 10.2.2.2 255.255.255.255
Router2(config-if)# ip pim sparse-mode
Router2(config-if)# exit
Router2(config)# router eigrp virtual-name
Router2(config-router)# service-family ipv4 autonomous-system 4453
Router2(config-router-sf)# remote-neighbors source Loopback2 multicast-group 224.44.56.1
max-neighbors 30
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Service Advertisement Framework commands	Cisco IOS Service Advertisement Framework Technology Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Dynamic Neighbors

Table 1 Feature Information for Dynamic Neighbors

Feature Name	Releases	Feature Information
Dynamic Neighbors	15.1(2)S, 15.2(3)T, 15.2(2)S, 15.1(1)SG Cisco IOS XE Release 3.6S, Cisco IOS XE Release 3.3SG	The Dynamic Neighbors feature provides support for the dynamic discovery of remote unicast and multicast neighbors (referred to as “remote neighbors”). Remote neighbor support allows Cisco SAF peering to one or more remote neighbors. The following commands were introduced or modified: • **authentication mode** • **remote-neighbors source** • **show eigrp service-family external-client**