



# Configuring Dynamic Neighbors

---

**Last Updated: October 15, 2012**

When neighbors are not adjacent, normal Cisco Service Advertisement Framework (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 through 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 must 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 device is configured, thus reducing configuration management.

This section contains the following major topics:

- [Finding Feature Information, page 1](#)
- [Prerequisites for Dynamic Neighbors, page 2](#)
- [Restrictions for Dynamic Neighbors, page 2](#)
- [Information About Dynamic Neighbors, page 2](#)
- [How to Configure Dynamic Neighbors, page 5](#)
- [Configuration Examples for Dynamic Neighbors, page 7](#)
- [Additional References, page 8](#)
- [Feature Information for Dynamic Neighbors, page 9](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.



---

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

## Prerequisites for Dynamic Neighbors

Before configuring SAF dynamic neighbors, ensure that when using:

- Unicast-listen mode—IP connectivity (reachability) exists between devices that need to do dynamic peering.
- Multicast-group mode—Multicast is running on the network.

## Restrictions for Dynamic Neighbors

- The **remote-neighbors** command requires a loopback as a source interface.
- Only named access control lists (ACLs) are permitted with the **allow-list** keyword. Numbered ACLs 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 must use multiple source interfaces.
- A multicast-group address may 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

- [Dynamic Neighbors Overview, page 2](#)
- [Remote Neighbor Session Policy, page 3](#)
- [Neighbor Types, page 4](#)
- [Remote Unicast-Listen \(Point-to-Point\) Neighbors, page 4](#)
- [Remote Multicast-Group \(Multipoint-to-Multipoint\) Neighbors, page 4](#)
- [Inheritance and Precedence of the Remote Neighbor Configurations, page 5](#)

## Dynamic Neighbors Overview

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 (devices not running SAF).

To support this type of network, SAF provides the **neighbor** command, which allows remote neighbors to be configured and sessions established through 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 must 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 device 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 predefined, and neighbors may be many hops away. A device with this configuration could peer with any device that sends a valid HELLO packet. Because of security considerations, this open aspect requires policy capabilities to limit peering to valid devices and to restrict the number of neighbors in order to limit resource consumption. This capability is accomplished using the following manually configured parameters, and takes effect immediately.

- [Neighbor Filter List, page 3](#)
- [Maximum Remote Neighbors, page 3](#)
- [Configuration Changes for the Neighbor Filter List and Maximum Number of Remote Neighbors, page 4](#)

### 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 device 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 less than the current number of sessions will result in the neighbors (in no specific order) being dropped until the count reaches the new limit.

## Configuration Changes for the Neighbor Filter List and Maximum Number of 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 device:

- Uses its interface IP address as the source IP address for any unicast transmissions. This IP address must be routable.
- Requires neighbors that peer 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 device interface.
- 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 device:

- 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

- [Configuring Dynamic Neighbors, page 5](#)

### Configuring 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
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <code>router eigrp virtual-instance-name</code></p> <p><b>Example:</b></p> <pre>Device(config)# router eigrp saf</pre>	<p>Enables an EIGRP virtual instance.</p>
<p><b>Step 4</b> <code>service-family {ipv4   ipv6} [vrf vrf-name] autonomous-system autonomous-system-number</code></p> <p><b>Example:</b></p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	<p>Enables a Cisco SAF service family for the specified autonomous system.</p>
<p><b>Step 5</b> <code>remote-neighbors source interface {unicast-listen   multicast-group group-address} [allow-list access-list-name] [max-neighbors max-remote-peers]</code></p> <p><b>Example:</b></p> <pre>Device(config-router-sf)# remote-neighbors source Loopback1 unicast-listen allow-list myNeighborList</pre>	<p>Configures a SAF process that enables remote neighbors to accept inbound connections from any remote IP address.</p> <ul style="list-style-type: none"> <li>• <b>allow-list</b> 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, all IP addresses will be accepted.</li> <li>• <b>max-neighbors</b> 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.</li> </ul>
<p><b>Step 6</b> <code>exit-service-family</code></p> <p><b>Example:</b></p> <pre>Device(config-router-sf)# exit-service-family</pre>	<p>Exits service-family configuration mode.</p>

# Configuration Examples for Dynamic Neighbors

- [Examples: Configuring Cisco SAF Dynamic Neighbors, page 7](#)
- [Example: Enhancements to the show neighbor detail Command, page 7](#)

## Examples: Configuring Cisco SAF Dynamic Neighbors

The following examples show how to configure both devices 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.

```
Device1(config)# interface Loopback1
Device1(config-if)# ip address 10.1.1.1 255.255.255.255
Device1(config-if)# exit
Device1(config)# ip access-list standard myNeighborList
Device1(config-std-nacl)# permit 10.0.0.0 0.255.255.255
Device1(config-std-nacl)# exit
Device1(config)# router eigrp virtual-name
Device1(config-router)# service-family ipv4 autonomous-system 4453
Device1(config-router-sf)# remote-neighbors source Loopback1 unicast-listen allow-list
myNeighborList
```

```
Device2(config)# interface Loopback2
Device2(config-if)# ip address 10.2.2.2 255.255.255.255
Device2(config-if)# exit
Device2(config)# router eigrp virtual-name
Device2(config-router)# service-family ipv4 autonomous-system 4453
Device2(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.

```
Device1(config)# interface Loopback1
Device1(config-if)# ip address 10.1.1.1 255.255.255.255
Device1(config-if)# ip pim sparse-mode
Device1(config-if)# exit
Device1(config)# router eigrp virtual-name
Device1(config-router)# service-family ipv4 autonomous-system 4453

Device1(config-router-sf)# remote-neighbors source Loopback1 multicast-group 224.44.56.1
max-neighbors 30
Device2(config)# interface Loopback2
Device2(config-if)# ip address 10.2.2.2 255.255.255.255
Device2(config-if)# ip pim sparse-mode
Device2(config-if)# exit
Device2(config)# router eigrp virtual-name
Device2(config-router)# service-family ipv4 autonomous-system 4453
Device2(config-router-sf)# remote-neighbors source Loopback2 multicast-group 224.44.56.1
max-neighbors 30
```

## Example: Enhancements to the show neighbor detail Command

The existing detail option of the show neighbor command will be extended to show the information as to how the neighbor was configured. If the neighbor is:

- Configured as static single hop. It is listed as a static neighbor.
- Configured as static multi-hop. It is listed as a remote static neighbor (static multi-hop).
- Configured as remote unicast-listen. It is listed as a remote neighbor (unicast-listen).

- Configured as remote multicast-group. It is listed as a group neighbor (multicast-group <ip addr>.)
- Not manually configured. It has no special listing here.

For example:

```
Device# show eigrp ipv4 neighbor detail

EIGRP-SFv4 VR(test) Service-Family Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num

1 10.1.2.1 Lo0 12 00:02:20 3 100 0 3
Static neighbor
Version 8.0/4.0, Retrans: 0, Retries: 0
Topology-ids from peer - 0

1 1.1.2.1 Lo0 12 00:02:20 3 100 0 3
Remote Static neighbor (static multihop)
Version 8.0/4.0, Retrans: 0, Retries: 0
Topology-ids from peer - 0

1 10.1.1.4 Lo0 12 00:02:01 3 100 0 1
Remote neighbor (unicast-listen)
Version 8.0/4.0, Retrans: 0, Retries: 0
Topology-ids from peer - 0

1 10.1.1.5 Lo0 14 00:04:07 1552 5000 0 3
Group neighbor (multicast-group 224.1.1.1)
Version 8.0/4.0, Retrans: 0, Retries: 0
Topology-ids from peer - 0

0 3.1.2.3 Et1/0 12 00:02:20 1999 5000 0 1
Version 8.0/4.0, Retrans: 0, Retries: 0
Topology-ids from peer - 0
```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Service Advertisement Framework commands	<a href="#">Cisco IOS Service Advertisement Framework Technology Command Reference</a>
Cisco EIGRP stub routing	<a href="#">Configuring EIGRP</a>

## 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for Dynamic Neighbors

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1** Feature Information for Dynamic Neighbors

Feature Name	Releases	Feature Information
Dynamic Neighbors	15.1(2)S	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.
	15.2(2)S	
	15.1(1)SG	
	15.1(1)SY	
	15.2(3)T	
	Cisco IOS XE Release 3.6S	
	Cisco IOS XE Release 3.3SG	The following commands were introduced or modified:
		<ul style="list-style-type: none"> <li>• <b>authentication mode</b></li> <li>• <b>remote-neighbors source</b></li> <li>• <b>show eigrp service-family external-client</b></li> </ul>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks).

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2012 Cisco Systems, Inc. All rights reserved.