



Configuring Cisco SAF

Last Updated: September 27, 2012

Cisco Service Advertisement Framework (SAF) provides a framework that allows applications to discover the existence, location, and configuration of networked resources within networks. Cisco SAF allows a timely and reliable awareness of the services within networks, while applications advertise and discover services on networks. Service information distributes through a network of Cisco SAF cooperative nodes that assume specific functions to efficiently distribute knowledge of services and facilitate their discovery.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Cisco SAF, page 1](#)
- [Restriction for Cisco SAF, page 2](#)
- [Information About Cisco SAF, page 2](#)
- [How to Configure a Cisco SAF Forwarder, page 8](#)
- [Configuration Examples for Cisco SAF, page 39](#)
- [Additional References, page 43](#)
- [Feature Information for Cisco SAF, page 43](#)

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. An account on Cisco.com is not required.

Prerequisites for Cisco SAF

- Before configuring Cisco SAF, you should understand the concepts in this guide.
- Before configuring neighbor relationships for Cisco SAF Forwarders located on separate LANs, ensure that IP routing is configured between each Cisco SAF Forwarder.



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

Restriction for Cisco SAF

- Cisco SAF works independently of Cisco EIGRP routing.

Information About Cisco SAF

- [Cisco SAF Overview](#), page 2
- [Cisco SAF Service Identifier Number Formats](#), page 5
- [Cisco SAF and the Role of Domains in a Network](#), page 5
- [Cisco SAF Virtual Routers](#), page 6
- [Cisco SAF Neighbor Relationships](#), page 6
- [Benefits of Cisco SAF](#), page 6

Cisco SAF Overview

Cisco Service Advertisement Framework (SAF) provides a framework that allows applications to discover the existence, location, and configuration of networked resources within networks. Cisco SAF allows a timely and reliable awareness of the services within networks, while applications advertise and discover services on networks. Service information distributes through a network of Cisco SAF cooperative nodes that assume specific functions to efficiently distribute knowledge of services and facilitate their discovery.

A non-SAF node is any node in a network that does not understand SAF. Non-SAF nodes are called “dark nets” and are required to traverse ISPs. Cisco SAF messages are IP-based and therefore are unaffected by dark nets.

Cisco SAF cooperative network nodes are grouped into two major functional responsibilities:

- Cisco SAF forwarder—Distributes service information through the network and makes these services discoverable by clients in the network.
- Cisco SAF client—Advertises and discovers services.

An effective Cisco SAF network requires both roles to be configured.

- [Cisco SAF Forwarder Overview](#), page 2
- [Cisco SAF Client Overview](#), page 3
- [External Cisco SAF Client Using XMCP Overview](#), page 4

Cisco SAF Forwarder Overview

A Cisco SAF forwarder receives services advertised by Cisco SAF Clients, distributes the services reliably through the network, and makes services available for Cisco SAF clients. A Cisco SAF forwarder:

- Ensures reliable delivery of service advertisements.
- Maintains knowledge of path redundancy.
- Is scalable.
- Minimizes the use of network bandwidth by using targeted multicast and unicast messages.

The Cisco SAF forwarder can propagate service advertisements to other Cisco SAF forwarders and can propagate across a LAN, campus network, WAN, or ISP.

A basic Cisco SAF forwarder provides the relationship between Cisco SAF clients and the framework. A Cisco SAF forwarder is normally located at the edges or boundaries of a network. The Cisco SAF forwarder receives service advertisements and stores a copy before forwarding the advertisement to its neighbor SAF nodes. The client and forwarder relationship is to maintain the advertisement. If a client removes a service or disconnects from the forwarder node, the node will inform the framework about the services that are no longer available. When the forwarder node receives advertisements from other forwarder nodes, it will keep a copy of the entire advertisement (header and opaque data) and forward it to other SAF peers.

You can configure a Cisco SAF forwarder on a LAN to automatically allow dynamic discovery of services to all enabled interfaces and, at the same time, specify interfaces (static configuration) that you want blocked to other interfaces attempting to discover their services.

You can configure a Cisco SAF forwarder across a non-SAF node to automatically allow dynamic discovery of services. For example, Cisco SAF forwarders can join a common peer group. You can also create static configurations (unicast) between pairs of Cisco SAF forwarders.

**Note**

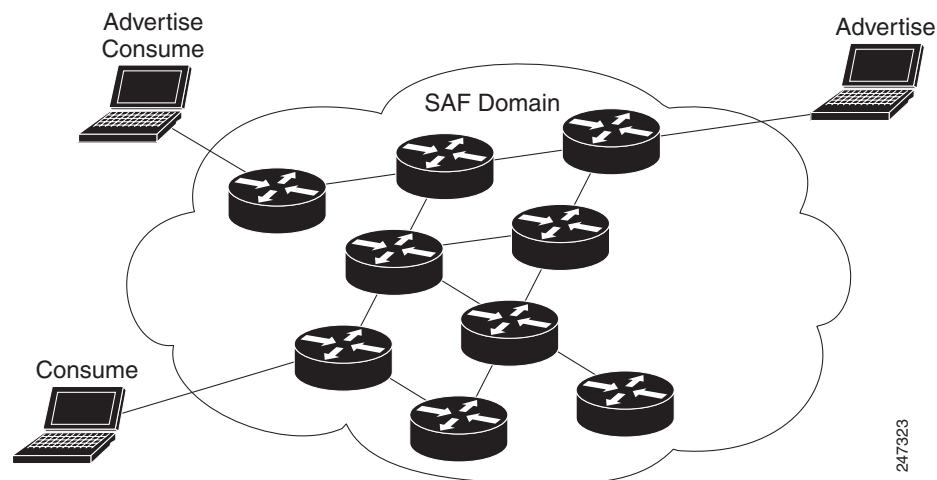
Multicast routing is required to allow dynamic discovery of services.

**Note**

With CSCts55778 and CSCtq71851, the Cisco SAF forwarder can send service metadata to its neighbor SAF nodes. Metadata is XML information, and service data is information that a server communicates to a client about itself. The service metadata does not propagate in mixed software release environments until such time that the version of EIGRP and SAF is upgraded.

Cisco SAF Client Overview

A Cisco SAF client is a producer (advertises to the network) or a consumer of services (requests a service from the network), or both. When a Cisco SAF client sends a register message to a Cisco SAF forwarder, it establishes a relationship with the Cisco SAF forwarder. The Cisco SAF forwarder uses this register message to obtain a unique handle that distinctly identifies this Cisco SAF client from others connected to the same forwarder. Only after a Cisco SAF client registers is it able to advertise (publish) or request (subscribe to) services. The figure below shows a typical Cisco SAF network.



When advertising a service, a Cisco SAF client publishes (sends) advertisements, to the Cisco SAF forwarder, that contain information about the service it offers. Services are identified by a unique service ID, sub-service ID, and instance ID and are described by service data. For more information on service identifiers, see [Cisco SAF Service Identifier Number Formats](#), page 5. The Cisco SAF client can send multiple publish requests, each advertising a distinct service. The Cisco SAF forwarder advertises all services published by the Cisco SAF client. The Cisco SAF client can update an existing service advertisement by sending a new publish request for the same service. The client can also generate an unpublish request, which removes one of its existing service advertisements.

When requesting a service, the Cisco SAF client sends a request notification of services using a subscribe request. The subscribe request contains a filter that describes the set of services in which the Cisco SAF client is interested. In response to this request, the Cisco SAF forwarder sends the current set of services that match the filter to the Cisco SAF client in a series of notify requests. As with a publish request, the Cisco SAF client can generate multiple subscribe requests, each with a different filter. The Cisco SAF client can also generate an unsubscribe request, which removes one of its existing subscriptions.

Cisco SAF clients can be internal (existing within a Cisco SAF forwarder) or external (existing on a separate device and communicating with a Cisco SAF forwarder using the XMCP protocol). Internal Cisco SAF clients include Capabilities Manager (see [Configuring Capabilities Manager](#)) and Cisco Unified Communications Manager Express (Cisco Unified CME). External Cisco SAF clients using XMCP include Cisco Unified Communications Manager.

External Cisco SAF Client Using XMCP Overview

An external Cisco SAF client initiates a TCP connection to a Cisco SAF forwarder that has been configured as an XMCP server. Once the TCP connection is established, the client begins an XMCP session over this connection by sending an XMCP register message to the Cisco SAF forwarder.

An XMCP session uses a username and password for security.

- The username is included in requests from the XMCP client (Cisco SAF client) to the XMCP server (Cisco SAF forwarder).
- The password is a shared secret that is not sent in requests, but is used by the client to compute a message-integrity value that is appended to the request.

When an XMCP server receives a request, it locates the username attribute in that request and uses it to access its local copy of the password, and then it computes its own message-integrity value for the request. If the computations match, the passwords must match and the request is authenticated, permitting the XMCP client to act as a Cisco SAF client. If they do not match, the password is incorrect and the request will be rejected.

Once the XMCP session has been established successfully, the XMCP client may send XMCP publish, unpublish, subscribe, and unsubscribe requests. When the server receives and successfully authenticates these requests, it translates the requests into the equivalent Cisco SAF client requests and sends them to the Cisco SAF forwarder. Similarly, Cisco SAF client notify requests from the forwarder are translated into XMCP notify requests and sent to the XMCP client.

Because an external Cisco SAF client may lose connectivity to the Cisco SAF network in the event of a network outage, a Cisco SAF forwarder requires periodic verification regarding the liveness of the Cisco SAF client to advertise its services to the Cisco SAF network. In XMCP, this is accomplished by exchanging a liveness timer between the client and the server at the time of registration. The XMCP client is responsible for ensuring that the interval between requests never exceeds this value. An XMCP client has no data (publish or subscribe) to send, so it generates a small keepalive message to refresh the timer on the server.

A Cisco SAF forwarder considers that an external Cisco SAF client has failed if it has not seen an XMCP request from the client in a time period equal to the liveness timer. When a Cisco SAF forwarder detects

that the Cisco SAF client has failed, it withdraws the services advertised on behalf of that Cisco SAF client from the network and removes any subscriptions that the Cisco SAF client had established. As an alternative to waiting for the liveness timer to expire, a Cisco SAF client can be manually unregistered (sending an unregister request to terminate the XMCP session) to gracefully cause a Cisco SAF forwarder to withdraw all services and subscriptions.

Cisco SAF Service Identifier Number Formats

A service is any information that a Cisco SAF client application wishes to advertise, which can then be used by other Cisco SAF client applications. A service advertisement consists of service data. Service advertisements are propagated between forwarders using header data. Cisco SAF clients that are interested in a service receive, and may inspect, service header and service data.

A service identifier number uniquely identifies the service on a network. The following example shows the format of a service identifier number:

```
service:sub-service:instance.instance.instance.instance
```

The service identifier is a 16-bit decimal identifier for the major service being advertised. A major service refers to a specific technology area, such as Cisco Unified Communications (UC). Service identifiers are assigned by Cisco to various customers who require an SAF client.

The following example shows the service ID values for IP Everywhere and Cisco Unified Communications:

```
Cisco Defined Numbers
SAF_SERVICE_ID_IPE           = 100      ! IP Everywhere
SAF_SERVICE_ID_UC           = 101      ! Unified Communications
```

The sub-service identifier is a 16-bit decimal identifier for the minor service being advertised. A sub-service (also referred to as a minor service) refers to the type of service within a technology. For example, within UC:

- Sub-service 1 is TDM gateway.
- Sub-service 2 is hosted-DN.
- Instance identifies a specific service advertisement for this kind of service.

For example, service identifier 101:1:abcd.1234.ef.678 could be an advertisement of a UC (service 101) TDM gateway (sub-service 1) announced by the Communications Manager cluster in a certain location (instance abcd.1234.ef.678). The instance identifier is a unique 128-bit number that identifies the specific service advertised.

Client teams define the use of sub-service and instance values for their applications. Clients must ensure instance uniqueness within a Cisco SAF domain.

Cisco SAF and the Role of Domains in a Network

As the variety and number of network services grow, providing timely and reliable awareness of these services starts to play a more significant role in increasing productivity and efficiency. One of the biggest challenges in propagating service availability awareness over a WAN is one of scalability. As networks grow, the services offered by the devices on these networks increase. Protocols responsible for the service advertisement need to scale to handle this increased load. These protocols also need to react efficiently to rapid changes and propagate the new information in a timely manner.

Cisco SAF is designed to be a scalable solution for enterprise service locations and is capable of spanning LAN and WAN Internet segments. As an enterprise solution, you can configure Cisco SAF to use domains to scale for very large networks. Just as Cisco Enhanced Interior Gateway Routing Protocol (EIGRP)

defines the concept of an autonomous system in which routes can be searched for in a hierarchical manner, Cisco SAF employs the similar concept of a domain and subdomains.

Cisco SAF provides a dynamic peer discovery and service advertisement propagation technique known as IP multicast. IP multicast requires the cooperation of IP Cisco SAF forwarders (the devices that connect IP subnets together to form intranets). IP multicasting, however, may not be completely implemented across some intranets. In the absence of IP multicasting, Cisco SAF operates within the configured subnet or within the groups of subnets over which IP multicast is supported.

Cisco SAF forwarders offer two primary types of administrative domains (ADs); a domain and a subdomain. A domain and a subdomain function the same with one notable exception; subdomains do not form unique neighbor relationships, but instead rely on a single peering.

Ideally, a network would require only a single domain for advertising all services. However, because of scaling and policy issues, some networks require the creation of multiple domains. The recommendation is to use a single domain. Consider using multiple domains when:

- More than 30,000 services are registered in a single domain.
- Logical grouping of services is needed to restrict propagation of services.

Closed groups are needed to prevent users from browsing services that they are not allowed to access.

Service redistribution allows different domains to exchange service information. Services may need to be bound to specific areas of the network, or the number of services in a given network may need to be limited. If you cannot use a single domain, service advertisement redistribution might be the solution.

Each domain on a network is separated into an AD. All Cisco SAF forwarders in the same AD (running the same domain) have complete knowledge of the entire AS. A Cisco forwarder that connects two (or more) administrative domains is known as a border forwarder. A border forwarder advertises service information from one AS to another AS. Proper design should also be considered if multiple border forwarders are used to avoid loops (information learned from one AD being sent back to the same AD).

Cisco SAF Virtual Routers

Cisco EIGRP service-family support extends the named configuration to allow configuration of multiple instances that operate independently. The addition of a Virtual Router ID (VRID) to the base Cisco EIGRP packet encoding allows for multiple instances.

As each virtual device is created, a VRID is assigned to the top-level router and shared with the address families and service families that are configured under it.

Cisco SAF Neighbor Relationships

Cisco SAF forwarders can operate in networks that do not have devices that support the Cisco SAF forwarder protocol. These networks are referred to as “dark nets.” There are two methods for configuring Cisco SAF forwarders over IP networks that do not support Cisco SAF (IP clouds); unicast Cisco SAF neighbors and multicast Cisco SAF neighbors.

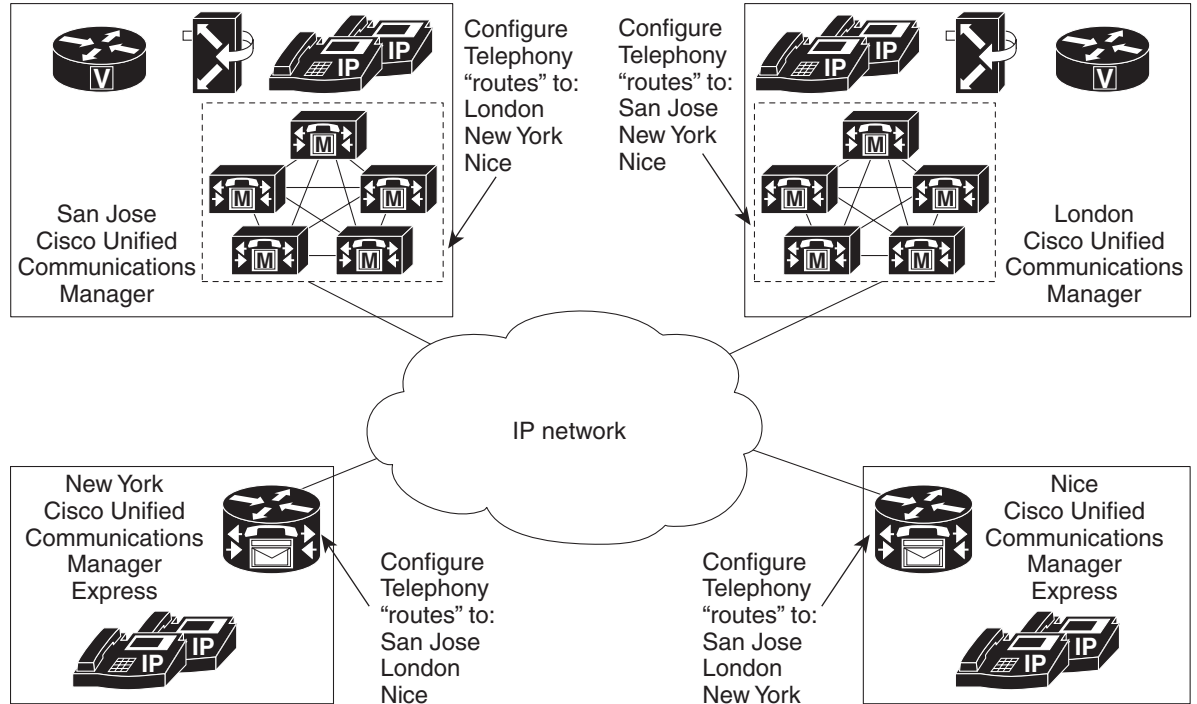
You can use a unicast configuration to provide a reliable point-to-point adjacency with neighbors. As the number of Cisco SAF forwarders increases, you can use multicast to provide an efficient transport between multiple Cisco SAF neighbors. A single IP multicast group address can be used for multiple Cisco SAF neighbors to exchange SAF information in a peer-group.

Benefits of Cisco SAF

Traditionally, to locate services on a network, network applications must be configured with the hostname and the network address of the desired service or must use an overlay mechanism such as DNS. Existing

protocols that support service advertisement provide periodic-based announcements of resource utilization. These network services are typically LAN-based.

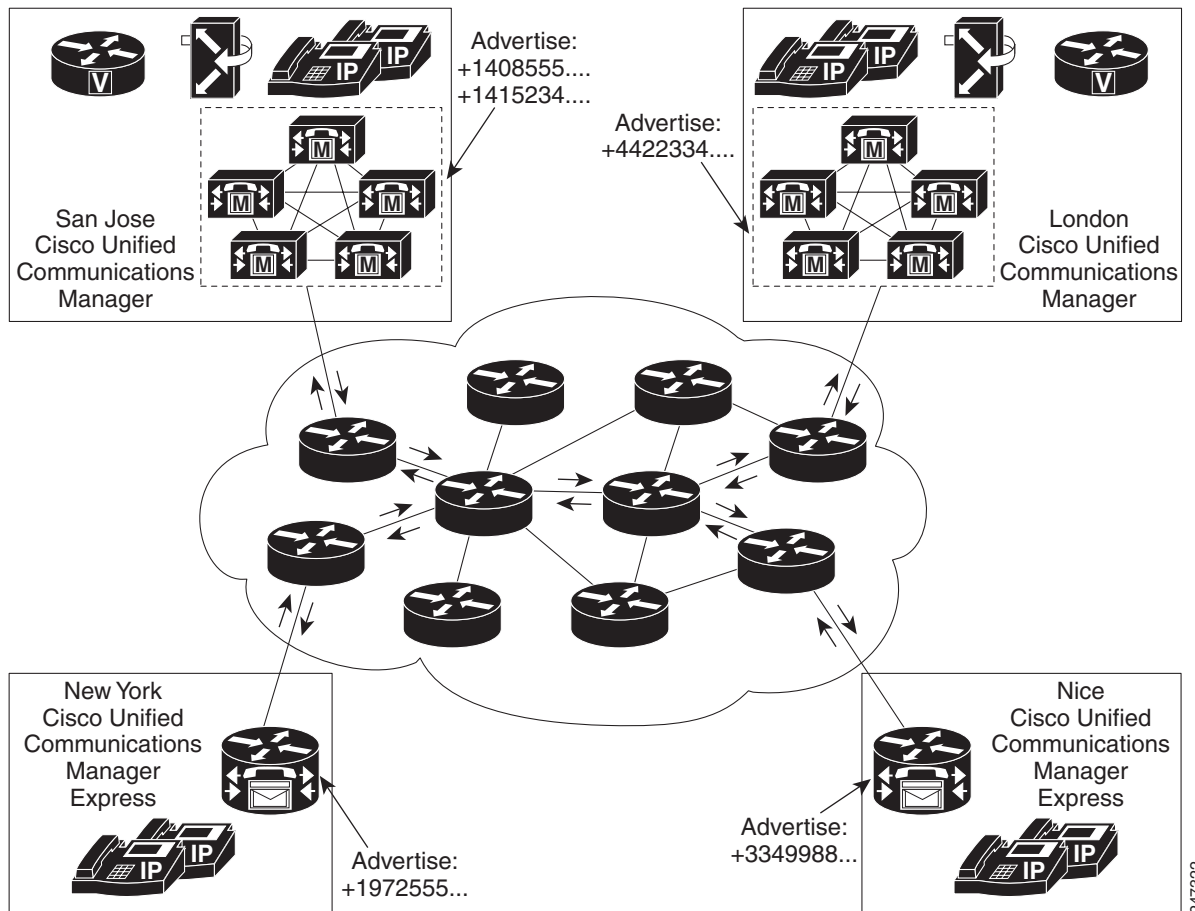
The figure below shows a Cisco Unified Communications Manager network that requires a traditional configuration methodology.



Cisco SAF provides a framework that allows networking applications to automatically discover the existence, location, and configuration of networked services within networks. This automated discovery of services replaces the manual entry of complex configurations such as dial plans that often require repetitive configuration changes. Cisco SAF also allows applications to advertise and discover their services. Cisco SAF allows you to create a configuration once and then have it propagate to all devices that require the information.

The figure below shows a Cisco Unified Communications Manager network that uses Cisco SAF.

247686



You can configure a Cisco SAF client either on the same device as the Cisco SAF forwarder or on an external device.

How to Configure a Cisco SAF Forwarder

- [Enabling Cisco SAF, page 9](#)
- [Configuring Interface-Specific Commands for Cisco SAF, page 10](#)
- [Configuring Cisco SAF for Multi-Topology Networks, page 11](#)
- [Configuring Static Neighbor Relationships for Cisco SAF, page 13](#)
- [Configuring Stub Routing for Cisco SAF, page 14](#)
- [Configuring Route Authentication for Cisco SAF, page 15](#)
- [Configuring Logs for Neighbor Changes and Warnings, page 18](#)
- [Configuring the Percentage of Link Bandwidth Used for Cisco SAF, page 20](#)
- [Setting Metric Dampening Intervals for Cisco SAF Interfaces, page 21](#)
- [Adjusting the Interval Between Hello Packets and the Hold Time, page 25](#)
- [Disabling Split Horizon, page 27](#)
- [Setting Metric Maximum Hops, page 28](#)
- [Configuring a Cisco SAF External Client, page 30](#)

- [Displaying Cisco SAF Statistics, page 33](#)
- [Deleting Information from a Cisco SAF Configuration, page 38](#)

Enabling Cisco SAF

To enable Cisco SAF and create a Cisco SAF service-discovery process, 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. **exit-service-family**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 router eigrp <i>virtual-instance-name</i> Example: Device(config)# router eigrp saf	Enables an EIGRP virtual instance.
Step 4 service-family { ipv4 ipv6 } [vrf vrf-name] autonomous-system <i>autonomous-system-number</i> Example: Device(config-router)# service-family ipv4 autonomous-system 4453	Enters service-family configuration mode and enables Cisco SAF service family for the specified autonomous system.

Command or Action	Purpose
Step 5 <code>exit-service-family</code> Example: Device(config-router-sf)# <code>exit-service-family</code>	Exits service-family configuration mode.

Configuring Interface-Specific Commands for Cisco SAF

Cisco SAF provides an inheritance precedence for interface-specific commands. Configurations made in service-family interface configuration mode have priority over specific service-family interface and factory default configurations. To configure interface-specific commands under the service family for Cisco SAF, 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. `sf-interface` *interface-type interface-number*
6. `sf-interface`
7. `exit-sf-interface`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3 <code>router eigrp</code> <i>virtual-instance-name</i> Example: Device(config)# <code>router eigrp saf</code>	Enables an EIGRP virtual instance.

Command or Action	Purpose
<p>Step 4 <code>service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system autonomous-system-number</code></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	<p>Enters service-family configuration mode and creates a Cisco SAF service family for the specified autonomous system on the device, which is enabled by default.</p>
<p>Step 5 <code>sf-interface interface-type interface-number</code></p> <p>Example:</p> <pre>Device(config-router-sf)# sf-interface ethernet 0/0</pre>	<p>Enters service-family configuration mode and enables service-family interface configuration mode for the specified interface.</p>
<p>Step 6 <code>sf-interface</code></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# sf-interface hello-interval 10</pre>	<p>Enter the appropriate interface commands required for your configuration.</p>
<p>Step 7 <code>exit-sf-interface</code></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# exit-sf-interface</pre>	<p>Exits service-family interface configuration mode.</p>

Configuring Cisco SAF for Multi-Topology Networks

Use the following configuration to register clients and publish or subscribe services into a named topology. If you configure a second topology using an existing topology name, but with a different ID, it will replace the existing topology, rather than create two IDs for the same topology.



Note

With CSCts55778 and CSCtq71851, the Cisco SAF forwarder can send service metadata to its neighbor SAF nodes. Metadata is XML information, and service data is information that a server communicates to a client about itself. The service metadata does not propagate in mixed software release environments until such time that the version of EIGRP and SAF is upgraded.

To configure Cisco SAF for multi-topology networks, 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. **topology base**
6. **exit-sf-topology**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 router eigrp <i>virtual-instance-name</i> Example: Device(config)# router eigrp saf	Enables an EIGRP virtual instance.
Step 4 service-family { ipv4 ipv6 } [vrf <i>vrf-name</i>] autonomous-system <i>autonomous-system-number</i> Example: Device(config-router)# service-family ipv4 autonomous-system 4453	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.
Step 5 topology base Example: Device(config-router-sf)# topology base	Enables service-family interface topology configuration mode and creates a topology base for the specified service-family interface.

Command or Action	Purpose
Step 6 <code>exit-sf-topology</code> Example: Device(config-router-sf-topology)# <code>exit-sf-topology</code>	Exits service-family interface topology configuration mode.

Configuring Static Neighbor Relationships for Cisco SAF

Use the following commands to configure static neighbor adjacencies between Cisco SAF forwarders.

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. `neighbor {ip-address interface-type interface-number | description word | maximum-service | maximum-service number threshold-value [dampened | reset-time | restart interval | restart-count | warning-only]}`
6. `exit-service-family`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3 <code>router eigrp virtual-instance-name</code> Example: Device(config)# <code>router eigrp saf</code>	Enables an EIGRP virtual instance in global configuration mode.

Command or Action	Purpose
<p>Step 4 service-family {ipv4 ipv6} [vrf <i>vrf-name</i>] autonomous-system <i>autonomous-system-number</i></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.
<p>Step 5 neighbor {<i>ip-address interface-type interface-number</i> description <i>word</i> maximum-service maximum-service <i>number threshold-value</i> dampened reset-time restart <i>interval</i> restart-count warning-only}}</p> <p>Example:</p> <pre>Device(config-router-sf)# neighbor 10.10.10.1 Ethernet 0/0</pre>	Enables a Cisco SAF neighbor relationship for the specified interface.
<p>Step 6 exit-service-family</p> <p>Example:</p> <pre>Device(config-router-sf)# exit-service-family</pre>	Exits service-family configuration mode.

Configuring Stub Routing for Cisco SAF

You can configure a Cisco SAF forwarder as a stub device. For complete information on Cisco EIGRP stub routing, see the “Configuring EIGRP” module in the *IP Routing: EIGRP Configuration Guide*.

To create an Cisco SAF stub device, 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** *number*
5. **eigrp stub** [**receive-only** | **connected**]
6. **exit-service-family**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>router eigrp virtual-instance-name</code></p> <p>Example:</p> <pre>Device(config)# router eigrp saf</pre>	<p>Enables an EIGRP virtual instance.</p>
<p>Step 4 <code>service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system number</code></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	<p>Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.</p>
<p>Step 5 <code>eigrp stub [receive-only connected]</code></p> <p>Example:</p> <pre>Device(config-router-sf)# eigrp stub connected</pre>	<p>Configures a stub device for Cisco SAF.</p>
<p>Step 6 <code>exit-service-family</code></p> <p>Example:</p> <pre>Device(config-router-sf)# exit-service-family</pre>	<p>Exits service-family configuration mode.</p>

Configuring Route Authentication for Cisco SAF

Cisco SAF route authentication provides Message Digest 5 (MD5) authentication of routing updates from the routing protocol. The MD5 keyed digest in each packet prevents the introduction of unauthorized or false routing messages from unapproved sources. To configure route authentication for Cisco SAF, 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. **sf-interface** *interface-type interface-number*
6. **authentication key-chain** *name-of-chain*
7. **authentication mode** { **hmac-sha-256** { **0** | **7** } *password* | **md5** }
8. **exit-sf-interface**
9. **exit-service-family**
10. **exit**
11. **key-chain** *name-of-chain*
12. **key** *key-id*
13. **key-string** *text*
14. **accept-lifetime** *start-time* [**local** { **duration** *seconds* | **end-time** | **infinite** }]
15. **send-lifetime** *start-time* [**local** { **duration** *seconds* | **end-time** | **infinite** }]
16. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router eigrp <i>virtual-instance-name</i> Example: Device(config)# router eigrp saf	Enables an EIGRP virtual instance.

	Command or Action	Purpose
Step 4	<p>service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system <i>autonomous-system-number</i></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.
Step 5	<p>sf-interface <i>interface-type interface-number</i></p> <p>Example:</p> <pre>Device(config-router-sf)# sf-interface ethernet 0/0</pre>	Enters service-family configuration mode and enables IPv4 service-family interface configuration mode for the specified interface.
Step 6	<p>authentication key-chain <i>name-of-chain</i></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# authentication key-chain example</pre>	Specifies an authentication key chain for EIGRP.
Step 7	<p>authentication mode {hmac-sha-256 {0 7} <i>password</i> md5}</p> <p>Example:</p> <pre>Device(config-router-sf-interface)# authentication mode md5</pre>	Enables IPv4 service-family authentication mode HMAC-SHA-256 or MD5 for the specified interface.
Step 8	<p>exit-sf-interface</p> <p>Example:</p> <pre>Device(config-router-sf-interface)# exit-sf-interface</pre>	Exits service-family interface configuration mode.
Step 9	<p>exit-service-family</p> <p>Example:</p> <pre>Device(config-router-sf)# exit-service-family</pre>	Exits service-family configuration mode.
Step 10	<p>exit</p> <p>Example:</p> <pre>Device(config-router)# exit</pre>	Exits router configuration mode.

Command or Action	Purpose
<p>Step 11 <code>key-chain</code> <i>name-of-chain</i></p> <p>Example:</p> <pre>Device(config)# key-chain example</pre>	<p>Defines an authentication key chain needed to enable authentication for routing protocols and enters key-chain configuration mode.</p>
<p>Step 12 <code>key</code> <i>key-id</i></p> <p>Example:</p> <pre>Device(config-keychain)# key example</pre>	<p>Enters key configuration mode and identifies an authentication string for a key.</p>
<p>Step 13 <code>key-string</code> <i>text</i></p> <p>Example:</p> <pre>Device(config-keychain-key)# key-string example</pre>	<p>Specifies the authentication string for a key.</p>
<p>Step 14 <code>accept-lifetime</code> <i>start-time</i> [<code>local</code> { <code>duration</code> <i>seconds</i> <code>end-time</code> <code>infinite</code> }]</p> <p>Example:</p> <pre>Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200</pre>	<p>Enters service-family configuration mode and sets the time period during which the authentication key in a key chain is received as valid.</p>
<p>Step 15 <code>send-lifetime</code> <i>start-time</i> [<code>local</code> { <code>duration</code> <i>seconds</i> <code>end-time</code> <code>infinite</code> }]</p> <p>Example:</p> <pre>Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600</pre>	<p>Configures a time period during which an authentication key on a key chain is valid to be sent.</p>
<p>Step 16 <code>exit</code></p> <p>Example:</p> <pre>Device(config-keychain-key)# end</pre>	<p>Exits service-family interface configuration mode.</p>

Configuring Logs for Neighbor Changes and Warnings

By default, the system logs neighbor adjacency changes to help you monitor the stability of the routing system and detect problems. If you disabled logging of such changes and want to re-enable logging, 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. **eigrp log-neighbor-changes**
6. **eigrp log-neighbor-warnings** *seconds*
7. **exit-service-family**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 router eigrp <i>virtual-instance-name</i> Example: Device(config)# router eigrp saf	Enables an EIGRP virtual instance.
Step 4 service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system <i>autonomous-system-number</i> Example: Device(config-router)# service-family ipv4 autonomous-system 4453	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.
Step 5 eigrp log-neighbor-changes Example: Device(config-router-sf)# eigrp log-neighbor-changes	Enables the logging of changes in EIGRP service-family neighbor adjacencies.

Command or Action	Purpose
Step 6 <code>eigrp log-neighbor-warnings seconds</code> Example: <pre>Router(config-router-sf)# eigrp log-neighbor-warnings 60</pre>	Enables the logging of changes in service-family warning messages.
Step 7 <code>exit-service-family</code> Example: <pre>Device(config-router-sf)# exit-service-family</pre>	Exits service-family configuration mode.

Configuring the Percentage of Link Bandwidth Used for Cisco SAF

By default, packets consume a maximum of 50 percent of the link bandwidth, as configured with the **bandwidth interface** configuration command. You may want to change the value if a different level of link utilization is required or if the configured bandwidth does not match the actual link bandwidth (it may have been configured to influence route metric calculations). Use the following commands to configure the percentage of link bandwidth used for Cisco SAF.

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. `sf-interface interface-type interface-number`
6. `bandwidth-percent maximum-bandwidth-percentage`
7. `exit-sf-interface`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 <code>configure terminal</code> Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>router eigrp virtual-instance-name</code> Example: <pre>Device(config)# router eigrp saf</pre>	Enables an EIGRP virtual instance.
Step 4 <code>service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system autonomous-system-number</code> Example: <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system on the device.
Step 5 <code>sf-interface interface-type interface-number</code> Example: <pre>Device(config-router-sf)# sf-interface ethernet0/0</pre>	Enables service-family interface configuration mode for the specified interface.
Step 6 <code>bandwidth-percent maximum-bandwidth-percentage</code> Example: <pre>Device(config-router-sf-interface)# bandwidth-percent 75</pre>	Configures the maximum percentage of bandwidth used by the link for Cisco SAF.
Step 7 <code>exit-sf-interface</code> Example: <pre>Device(config-router-sf-interface)# exit-sf-interface</pre>	Exits service-family interface configuration mode.

Setting Metric Dampening Intervals for Cisco SAF Interfaces

Because metric components can be changed rapidly, the frequency of the changes can have an impact on the network. Frequent changes require that prefixes learned through the SAF interface be updated and sent to all adjacencies. This update can result in further updates and, in a worst-case scenario, cause network-wide churn. To prevent such effects, metrics can be dampened or thresholds set so that any change that does not exceed the dampening threshold is ignored.

Network changes that cause an immediate update include when a device selects a new nexthop or a down interface or device.

Thresholds can be configured based on a change or on a time interval. If the dampening method is:

- Change-based, changes in routes learned though a specific interface or in the metrics for a specific interface will not be advertised to adjacencies until the *computed* metric changes from the last advertised value are significant enough to cause an update to be sent.
- Interval-based, changes in routes learned though a specific interface or in the metrics for a specific interface will not be advertised to adjacencies until the *specified* interval is met or unless the change results in a new route path selection. When the timer expires, routes that have outstanding changes to report are sent. If a route changes and the final metric of the route matches the last updated metric, no updated routes are sent.

Refer to the following sections for information on configuring change-based and interval-based metric dampening parameters.

- [Change-based Dampening Configuration, page 22](#)
- [Interval-based Dampening Configuration, page 23](#)

Change-based Dampening Configuration

Use the following commands to set the maximum change-based dampening percentage for Cisco SAF interfaces.

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. **sf-interface** *interface-type interface-number*
6. **dampening-change** [*change-percentage*]
7. **exit-sf-interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
<p>Step 3 <code>router eigrp</code> <i>virtual-instance-name</i></p> <p>Example:</p> <pre>Device(config)# router eigrp saf</pre>	Enables an EIGRP virtual instance.
<p>Step 4 <code>service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system</code> <i>autonomous-system-number</i></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.
<p>Step 5 <code>sf-interface</code> <i>interface-type interface-number</i></p> <p>Example:</p> <pre>Device(config-router-sf)# sf-interface ethernet0/0</pre>	Enables service-family interface configuration mode for the specified interface on the device.
<p>Step 6 <code>dampening-change</code> [<i>change-percentage</i>]</p> <p>Example:</p> <pre>Device(config-router-sf-interface)# dampening-change 50</pre>	Configures the percentage of change in a route learned through an EIGRP service-family interface that causes an update to be advertised to adjacent peers.
<p>Step 7 <code>exit-sf-interface</code></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# exit-sf-interface</pre>	Exits service-family interface configuration mode.

Interval-based Dampening Configuration

Use the following commands to configure interval-based dampening for Cisco SAF interfaces. The value that you configure sets the interval when updates occur for topology changes that affect Cisco SAF interfaces and peers.

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. **sf-interface** *interface-name interface-number*
6. **dampening-interval** [*interval*]
7. **exit-sf-interface**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 router eigrp <i>virtual-instance-name</i></p> <p>Example:</p> <pre>Device(config)# router eigrp saf</pre>	<p>Enables an EIGRP virtual instance.</p>
<p>Step 4 service-family {ipv4 ipv6} [vrf <i>vrf-name</i>] autonomous-system <i>autonomous-system-number</i></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	<p>Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.</p>
<p>Step 5 sf-interface <i>interface-name interface-number</i></p> <p>Example:</p> <pre>Device(config-router-sf)# sf-interface ethernet0/0</pre>	<p>Enables service-family interface configuration mode for the specified interface.</p>

Command or Action	Purpose
Step 6 <code>dampening-interval</code> [<i>interval</i>] Example: Device(config-router-sf-interface)# dampening-interval 30	Sets the EIGRP interval-based dampening interval (in seconds).
Step 7 <code>exit-sf-interface</code> Example: Device(config-router-sf-interface)# exit-sf-interface	Exits service-family interface configuration mode.

Adjusting the Interval Between Hello Packets and the Hold Time

Routing devices periodically send hello packets to each other to dynamically learn of other devices on their directly attached networks. This information is used to discover neighbors and to learn when neighbors become unreachable or inoperative.

By default, hello packets are sent every 5 seconds. The exception is on low-speed, nonbroadcast multiaccess (NBMA) media on which the default hello interval is 60 seconds. Low speed is considered to be a rate of T1 or slower as specified in the **bandwidth interface** configuration command. The default hello interval remains at 5 seconds for high-speed NBMA networks. Note that for the purposes of Frame Relay and Switched Multimegabit Data Service (SMDS), networks may or may not be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise they are not considered NBMA.

The hold time is advertised in hello packets and indicates to neighbors the length of time for which they should consider the sender valid. The default hold time is three times the hello interval, or 15 seconds. For slow-speed NBMA networks, the default hold time is 180 seconds. On congested and large networks, the default hold time might not be sufficient time for all devices to receive hello packets from their neighbors. In this case, you may want to increase the hold time. Do not adjust the hold time without advising your technical support personnel. To change the hold time on a specific interface for a particular routing process designated by an autonomous system number, use the **hold time** command.

You can adjust the interval between hello packets and the hold time. To change the interval between hello packets and the hold time, 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. **sf-interface** *interface-type interface-number*
6. **hello-interval** *seconds*
7. **hold-time** *seconds*
8. **exit-sf-interface**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>router eigrp virtual-instance-name</code></p> <p>Example:</p> <pre>Device(config)# router eigrp saf</pre>	<p>Enables an EIGRP virtual instance.</p>
<p>Step 4 <code>service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system autonomous-system-number</code></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	<p>Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.</p>
<p>Step 5 <code>sf-interface interface-type interface-number</code></p> <p>Example:</p> <pre>Device(config-router-sf)# sf-interface ethernet0/0</pre>	<p>Enables service-family interface configuration mode for the specified interface.</p>
<p>Step 6 <code>hello-interval seconds</code></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# hello-interval 50</pre>	<p>Configures the time period for an EIGRP service-family process.</p>
<p>Step 7 <code>hold-time seconds</code></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# hold-time 50</pre>	<p>Configures the time period for an EIGRP service-family routing process designated by an autonomous system number.</p>

Command or Action	Purpose
Step 8 <code>exit-sf-interface</code> Example: <pre>Device(config-router-sf-interface)# exit-sf-interface</pre>	Exits service-family interface configuration mode.

Disabling Split Horizon

When split horizon is enabled on an interface, it blocks route information (such as update and query packets) from being advertised by a device out of any interface from which that information originates. Controlling update and query packets in this manner reduces the possibility of routing loops.

This behavior usually optimizes communications among multiple routing devices, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and SMDS), situations can arise for which this behavior is less than ideal. For these situations, including networks in which you have Cisco SAF configured, you may want to disable split horizon.

By default, split horizon is enabled on all interfaces. To disable split horizon, use the **no split-horizon** command in interface configuration mode.

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. **sf-interface** *interface-type interface-number*
6. **no split-horizon**
7. **exit-sf-interface**

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.

Command or Action	Purpose
<p>Step 3 <code>router eigrp</code> <i>virtual-instance-name</i></p> <p>Example:</p> <pre>Device(config)# router eigrp saf</pre>	Enables an EIGRP virtual instance.
<p>Step 4 <code>service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system</code> <i>autonomous-system-number</i></p> <p>Example:</p> <pre>Device(config-router)# service-family ipv4 autonomous-system 4453</pre>	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.
<p>Step 5 <code>sf-interface</code> <i>interface-type interface-number</i></p> <p>Example:</p> <pre>Device(config-router-sf)# sf-interface ethernet0/0</pre>	Enables service-family interface configuration mode for the specified interface.
<p>Step 6 <code>no split-horizon</code></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# no split-horizon</pre>	Disables split horizon.
<p>Step 7 <code>exit-sf-interface</code></p> <p>Example:</p> <pre>Device(config-router-sf-interface)# exit-sf-interface</pre>	Exits service-family interface configuration mode.

Setting Metric Maximum Hops

The maximum number of hops limits the number of hops a service can propagate to advertise its service. The default number of maximum hops is 100.

To limit the number of hops used to advertise a service, 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. **sf-interface** *interface-type interface-number*
6. **metric maximum-hops** *hop-count*
7. **exit-sf-interface**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 router eigrp <i>virtual-instance-name</i> Example: Device(config)# router eigrp saf	Enables an EIGRP virtual instance.
Step 4 service-family { ipv4 ipv6 } [vrf vrf-name] autonomous-system <i>autonomous-system-number</i> Example: Device(config-router)# service-family ipv4 autonomous-system 4453	Enables a Cisco SAF service family for the specified autonomous system.
Step 5 sf-interface <i>interface-type interface-number</i> Example: Device(config-router-sf)# sf-interface ethernet 0/0	Enables service-family interface configuration mode for the specified interface on the device.

Command or Action	Purpose
Step 6 <code>metric maximum-hops</code> <i>hop-count</i> Example: Device(config-router-sf-interface)# <code>metric maximum-hops 5</code>	Specifies a hop count for the routes that the IP routing software advertises as unreachable.
Step 7 <code>exit-sf-interface</code> Example: Device(config-router-sf-interface)# <code>exit-sf-interface</code>	Exits service-family interface configuration mode.

Configuring a Cisco SAF External Client

To configure a Cisco SAF external client, 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. `topology base`
6. `external-client` *client-label*
7. `exit-sf-topology`
8. `exit-service-family`
9. `exit`
10. `service-family external-client listen` {`ipv4` | `ipv6`} *tcp-port-number*
11. `external-client` *client-label* `basename`
12. `username` *user-name*
13. `password` *password-name*
14. `keepalive` *number*
15. `end`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router eigrp <i>virtual-instance-name</i> Example: Device(config)# router eigrp saf	Enables an EIGRP virtual instance.
Step 4	service-family { ipv4 ipv6 } [vrf <i>vrf-name</i>] autonomous-system <i>autonomous-system-number</i> Example: Device(config-router)# service-family ipv4 autonomous-system 4453	Enters service-family configuration mode and enables a Cisco SAF service family for the specified autonomous system.
Step 5	topology base Example: Device(config-router-sf)# topology base	Enables service-family interface topology configuration mode.
Step 6	external-client <i>client-label</i> Example: Device(config-router-topology)# external-client example	Configures a Cisco SAF external client with the specified client label.
Step 7	exit-sf-topology Example: Device(config-router-sf-topology)# exit-sf-topology	Exits service-family interface topology configuration mode.
Step 8	exit-service-family Example: Device(config-router-sf)# exit-service-family	Exits service-family configuration mode.

Command or Action	Purpose
<p>Step 9 <code>exit</code></p> <p>Example:</p> <pre>Device(config-router)# exit</pre>	<p>Exits router configuration mode.</p>
<p>Step 10 <code>service-family external-client listen {ipv4 ipv6} tcp-port-number</code></p> <p>Example:</p> <pre>Device(config)# service-family external-client listen ipv4 5050</pre>	<p>Configures a Cisco SAF external client TCP port to use to communicate with a Cisco SAF forwarder. The valid port range is 1024 to 65536.</p>
<p>Step 11 <code>external-client client-label basename</code></p> <p>Example:</p> <pre>Device(config-external-client)# external-client example basename</pre>	<p>Configures a Cisco SAF external client with the specified client label and a basename.</p> <p>Specifying the basename keyword allows SAF external clients to use a naming convention based on the client label. The naming convention takes the form of <i>client-label @[1-1024]</i> where you can specify a maximum of 1024 SAF external clients. For example, if the external-client command specifies a client label of <i>example</i>, then the basename for a SAF external client would be <i>example@1</i>. Another SAF external client would be <i>example@2</i>, and so on up to a maximum of 1024 basenames (<i>@1024</i>).</p>
<p>Step 12 <code>username user-name</code></p> <p>Example:</p> <pre>Device(config-external-client)# username example</pre>	<p>Enables external-client label configuration mode and configures a Cisco SAF external client with the specified username.</p>
<p>Step 13 <code>password password-name</code></p> <p>Example:</p> <pre>Device(config-external-client-mode)# password examplepass</pre>	<p>Configures a password for a Cisco SAF external client. The minimum password length is 11 characters.</p>
<p>Step 14 <code>keepalive number</code></p> <p>Example:</p> <pre>Device(config-external-client-mode)# keepalive 360000</pre>	<p>(Optional) Specifies the keepalive timer for the Cisco SAF external client. The keepalive value is in milliseconds. The default is 9600 ms.</p>

Command or Action	Purpose
Step 15 end Example: Device(config-external-client-mode)# end	Exits external-client label configuration mode.

Displaying Cisco SAF Statistics

To display Cisco SAF statistics, use the following commands in privileged EXEC mode.

SUMMARY STEPS

1. **show service-routing xmcp clients** [*ip-address* | *handle*] [**detail**]
2. **show service-routing xmcp server**
3. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **accounting**
4. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **clients** [**detail**]
5. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **events** [*starting-event-number ending-event-number*]
6. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **interfaces** [*interface-type interface-number*] [**detail**]
7. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **subscriptions**
8. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **timers**
9. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **summary**
10. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **zero successors**
11. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology**
12. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology active**
13. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology all-links**
14. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology base** *service-instance-number* **clients** [**detail**]
15. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology** [**detail-links**]
16. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology events** [*starting-event-number ending-event-number*]
17. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology pending**
18. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology** [*service-type connected* | *external* | *internal* | *local* | *redistributed* | **summary**]
19. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology sia-events** [*starting-event-number ending-event-number*]
20. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology sia-statistics** [*ip-address*]
21. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology summary**
22. **show eigrp service-family** {*ipv4* | *ipv6*} [*vrf vrf-name*] *autonomous-system-number* **topology zero-successors**

DETAILED STEPS

	Command or Action	Purpose
Step 1	show service-routing xmcp clients [<i>ip-address</i> <i>handle</i>] [detail]	Displays information about connected XMCP clients.
	Example:	
	Device# show service-routing xmcp clients detail	

	Command or Action	Purpose
Step 2	<p>show service-routing xmcp server</p> <p>Example:</p> <pre>Device# show service-routing xmcp server</pre>	Displays information about clients, external clients, or subscriptions configured for Cisco SAF.
Step 3	<p>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number accounting</p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 accounting</pre>	Displays accounting information about Cisco SAF.
Step 4	<p>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number clients [detail]</p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 clients</pre>	Displays information about Cisco SAF Clients.
Step 5	<p>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number events [starting-event-number ending-event-number]</p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 events</pre>	Displays information about Cisco SAF events.
Step 6	<p>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number interfaces [interface-type interface-number] [detail]</p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 interfaces</pre>	Displays information about Cisco SAF interfaces.
Step 7	<p>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number subscriptions</p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 subscriptions</pre>	Displays information about Cisco SAF subscriptions.

Command or Action	Purpose
<p>Step 8 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number timers</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 timers</pre>	Displays information about Cisco SAF timers.
<p>Step 9 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number summary</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 summary</pre>	Displays summary information about Cisco SAF.
<p>Step 10 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number zero successors</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 zero successors</pre>	Displays information about Cisco SAF zero successors.
<p>Step 11 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology</pre>	Displays information about the Cisco SAF topology table.
<p>Step 12 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology active</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology active</pre>	Displays only active entries for a Cisco SAF topology table.
<p>Step 13 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology all-links</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology all-links</pre>	Displays all active link entries for a Cisco SAF topology table.

Command or Action	Purpose
<p>Step 14 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology base service-instance-number clients [detail]</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology base clients detail</pre>	<p>Displays all active link entries for a Cisco SAF topology base.</p>
<p>Step 15 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology [detail-links]</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology detail-links</pre>	<p>Specifies all links in the topology table.</p>
<p>Step 16 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology events [starting-event-number ending-event-number]</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology events</pre>	<p>Specifies all events in the topology table.</p>
<p>Step 17 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology pending</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology pending</pre>	<p>Displays all active entries in the topology table that are waiting either for an update or reply from a neighbor.</p>
<p>Step 18 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology [service-type connected external internal local redistributed summary]</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology service-type connected</pre>	<p>Displays information about the specified service type for a Cisco SAF topology table.</p>
<p>Step 19 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology sia-events[starting-event-number ending-event-number]</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology sia-events</pre>	<p>Displays logged Stuck in Active (SIA) events in the Cisco SAF topology table.</p>

Command or Action	Purpose
<p>Step 20 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology sia-statistics [ip-address]</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology sia-statistics 10.10.10.1</pre>	Displays Stuck in Active (SIA) events for a Cisco SAF topology table.
<p>Step 21 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology summary</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology summary</pre>	Displays a summary of a Cisco SAF topology table.
<p>Step 22 <code>show eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number topology zero-successors</code></p> <p>Example:</p> <pre>Device# show eigrp service-family ipv4 4453 topology zero-successors</pre>	Displays information about available services that have zero successors in a Cisco SAF topology table.

Deleting Information from a Cisco SAF Configuration

To delete service-family information from a Cisco SAF configuration, use the following commands in EXEC mode.

SUMMARY STEPS

1. `clear service-family xmcp client {ip-address | handle}`
2. `clear eigrp service-family {ipv4 | ipv6} [vrf vrf-name] autonomous-system-number`
3. `clear eigrp service-family neighbors neighbor-address | interface-type interface-number`

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>clear service-family xmcp client {ip-address handle}</code></p> <p>Example:</p> <pre>Device# clear service-family xmcp client 1.1.1.1</pre>	Disconnects a connected XMCP client.

Command or Action	Purpose
<p>Step 2 <code>clear eigrp service-family {ipv4 ipv6} [vrf vrf-name] autonomous-system-number</code></p> <p>Example:</p> <pre>Device# clear eigrp service-family ipv4 4453</pre>	<p>Deletes neighbors formed using the IPv4 or IPv6 protocol family for the specified autonomous system. Optionally, you can delete all virtual routing forwarding (VRF) instance tables or a specific VRF table for an IP address.</p> <p>Note Using the <code>clear eigrp service-family ipv6</code> command requires an IPv6-enabled SAF client, which currently does not exist.</p>
<p>Step 3 <code>clear eigrp service-family neighbors neighbor-address interface-type interface-number</code></p> <p>Example:</p> <pre>Device# clear eigrp service-family neighbors Ethernet 0/0</pre>	<p>Deletes neighbors formed using the IPv4 protocol family from the neighbor table. Optionally, you can resynchronize with a peer without an adjacency reset (soft). Optionally, you can delete the interface type and number from the neighbor table that contains all entries learned through this interface.</p>

Configuration Examples for Cisco SAF

- [Example: Enabling Cisco SAF, page 39](#)
- [Examples: Configuring Cisco SAF Interfaces, page 39](#)
- [Example: Configuring Cisco SAF Topology, page 40](#)
- [Example: Configuring Cisco SAF Stub Routing, page 40](#)
- [Example: Configuring Cisco SAF with IP-RIP, page 40](#)
- [Example: Configuring Cisco SAF with OSPF, page 41](#)
- [Example: Configuring Cisco SAF with EIGRP, page 41](#)
- [Example: Configuring Cisco SAF Forwarders Located on Separate LANs, page 41](#)
- [Example: Configuring a Centralized Cisco SAF Forwarder, page 42](#)
- [Examples: Configuring a Cisco SAF Client, page 42](#)

Example: Enabling Cisco SAF

The following example enters router configuration mode, configures a Cisco SAF forwarder, enables the service-family forwarder process, and configures an autonomous system named 4533.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
```

Examples: Configuring Cisco SAF Interfaces

The following example places the device in service-family configuration mode and enables all interfaces.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# sf-interface default
Device(config-router-sf-interface)# no shutdown
```

The following example places the device in service-family configuration mode and enables Ethernet interface 0/0.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# sf-interface ethernet0/0
```

The following example places the device in service-family configuration mode and enables SAF on all interfaces, except Ethernet0/0 interface.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 3
Device(config-router-sf)# interface default
Device(config-router-sf)# sf-interface ethernet0/0
Device(config-router-sf-interface)# shutdown
Device(config-router-sf-interface)# end
```

The following example places the device in service-family configuration mode, enables SAF on Ethernet interfaces 2/0 and 2/1, and disables SAF on all other interfaces.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 2
Device(config-router-sf)# sf-interface default
Device(config-router-sf-interface)# shutdown
Device(config-router-sf-interface)# sf-interface ethernet2/0
Device(config-router-sf-interface)# no shutdown
Device(config-router-sf-interface)# sf-interface ethernet2/1
Device(config-router-sf-interface)# no shutdown
Device(config-router-sf-interface)# end
```

Example: Configuring Cisco SAF Topology

The following examples configures a Cisco SAF topology base.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# sf-interface default
Device(config-router-sf-interface)# no shutdown
Device(config-router-sf-interface)# topology base
```

Example: Configuring Cisco SAF Stub Routing

The following examples configures a Cisco SAF forwarder as a stub device.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# eigrp stub connected
```

Example: Configuring Cisco SAF with IP-RIP

The following configuration example enables Cisco SAF with IP RIP routing on network 10.0.0.0.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# topology base
Device(config-router-sf-topology)# exit-sf-topology
Device(config-router-sf)# exit-service-family
Device(config-router)# router rip
Device(config-router)# network 10.0.0.0
```


Example: Configuring Cisco SAF with OSPF

The following configuration example enables Cisco SAF with OSPF routing on network 10.0.0.0, area 0.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# topology base
Device(config-router-sf-topology)# exit-sf-topology
Device(config-router-sf)# exit-service-family
Device(config-router)# router ospf 787
Device(config-router)# network 10.0.0.0 0.0.0.255 area 0
```

Example: Configuring Cisco SAF with EIGRP

The following configuration example enables Cisco SAF with EIGRP routing on network 10.0.0.0.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 6476
Device(config-router-sf)# network 10.0.0.0 0.0.0.255
Device(config-router-sf)# topology base
Device(config-router-sf-topology)# exit-sf-topology
Device(config-router-sf)# exit-service-family
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# topology base
```



Note

There is no requirement to run routing over the same interfaces or networks in which services are distributed; however this could lead to services being distributed to areas where reachability is not guaranteed.

Example: Configuring Cisco SAF Forwarders Located on Separate LANs

The following example configures two Cisco SAF forwarders located on separate LANs.



Note

Use loopback mode to configure remote neighbors.

Cisco SAF Forwarder 1

```
Device(config)# interface loopback1
Device(config-if)# ip address 10.1.1.1 255.255.255.255
Device(config-if)# exit
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 1
Device(config-router-sf)# neighbor 10.2.2.2 loopback1 remote 10
```

Cisco SAF Forwarder 2

```
Device(config)# interface loopback1
Device(config-if)# ip address 10.2.2.2 255.255.255.255
Device(config-if)# exit
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 1
Device(config-router-sf)# neighbor 10.1.1.1 loopback1 remote 10
```

**Note**

This example assumes that IP routing is configured between the two devices and that the devices can ping both loopbacks.

Example: Configuring a Centralized Cisco SAF Forwarder

The following example configures a centralized Cisco SAF forwarder that sends all service advertisements to neighbors on IP addresses 10.4.15.5 and 10.4.15.1.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# sf-interface loopback0
Device(config-router-sf-interface)# no split-horizon
Device(config-router-sf-interface)# exit-sf-interface
Device(config-router-sf)# topology base
Device(config-router-sf-topology)# exit-sf-topology
Device(config-router-sf)# neighbor 10.4.15.5 Loopback0 remote 20
Device(config-router-sf)# neighbor 10.4.15.1 Loopback0 remote 20
Device(config-router-sf)# exit-service-family
```

Examples: Configuring a Cisco SAF Client

The following example configures a Cisco SAF external client named *example*, with a username of *username_example*, a password of *password_example*, and a keepalive setting of 360,000 seconds.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# topology base
Device(config-router-sf-topology)# external-client example
Device(config-router-sf-topology)# exit-sf-topology
Device(config-router-sf)# exit-service-family
Device(config-router)# exit
Device(config)# service-family external-client listen ipv4 3444
Device(config-external-client)# external-client example
Device(config-external-client-mode)# username username_example
Device(config-external-client-mode)# password password_example
Device(config-external-client-mode)# keepalive 360000
```

The following example configures five Cisco SAF external clients named *example1* through *example5*, with usernames of *username_example1* through *username_example5*, passwords of *password_example1* through *password_example5*, and keepalive settings of 360,000 seconds.

```
Device(config)# router eigrp saf
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# topology base
Device(config-router-sf-topology)# external-client example1
Device(config-router-sf-topology)# external-client example2
Device(config-router-sf-topology)# external-client example3
Device(config-router-sf-topology)# external-client example4
Device(config-router-sf-topology)# external-client example5
Device(config-router-sf-topology)# exit-sf-topology
Device(config-router-sf)# exit-service-family
Device(config-router)# exit
Device(config)# service-family external-client listen ipv4 3444
Device(config-external-client)# external-client example1
Device(config-external-client-mode)# username username_example1
Device(config-external-client-mode)# password password_example1
Device(config-external-client-mode)# keepalive 360000
Device(config-external-client-mode)# external-client example2
Device(config-external-client-mode)# username username_example2
Device(config-external-client-mode)# password password_example2
Device(config-external-client-mode)# keepalive 360000
```

```

Device(config-external-client-mode)# external-client example3
Device(config-external-client-mode)# username username_example3
Device(config-external-client-mode)# password password_example3
Device(config-external-client-mode)# keepalive 360000
Device(config-external-client-mode)# external-client example4
Device(config-external-client-mode)# username username_example4
Device(config-external-client-mode)# password password_example4
Device(config-external-client-mode)# keepalive 360000
Device(config-external-client-mode)# external-client example5
Device(config-external-client-mode)# username username_example5
Device(config-external-client-mode)# password password_example5
Device(config-external-client-mode)# keepalive 360000

```

Additional References

Related Documents

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

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 Cisco SAF

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. An account on Cisco.com is not required.

Table 1 *Feature Information for Cisco Service Advertisement Framework*

Feature Name	Software Releases	Feature Configuration Information
Cisco Service Advertisement Framework	12.2(33)SRE	<p>This feature allows applications to discover the existence, location, and configuration of networked resources within networks, and it provides a timely and reliable awareness of the services within networks, as applications advertise and discover services on networks.</p> <p>This feature was introduced in Cisco IOS Release 15.0M.</p> <p>In Cisco IOS XE Release 2.5, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced in this feature:</p> <ul style="list-style-type: none"> • accept-lifetime • authentication (service-family) • bandwidth-percent • clear eigrp service-family • dampening-change • dampening-interval • debug eigrp service-family • default external-client • default (SAF) • default-metric (EIGRP) • eigrp log-neighbor-changes • eigrp-log-neighbor-warnings • eigrp router-id • eigrp stub (service-family) • exit-service-family • exit-sf-interface • exit-sf-topology • external-client • hello-interval • hold-time • keepalive (SAF) • key • key chain
	12.2(33)SXI4	
	12.2(33)XNE	
	12.2(50)SY	
	15.0M	
	15.0(1)S	
	15.1(1)SG	
	15.1(2)S	
	15.1T	
	15.2(1)T	
	15.2(2)S	
	15.2(3)T	
	Cisco IOS XE Release 2.5	
Cisco IOS XE Release 3S,		
Cisco IOS XE Release 3.3SG		
Cisco IOS XE Release 3.4S		
Cisco IOS XE Release 3.6S		

Feature Name	Software Releases	Feature Configuration Information
		<ul style="list-style-type: none"> • key-string (authentication) • maximum-service (EIGRP) • metric weights (EIGRP) • neighbors (service-family) • next-hop-self • password (SAF) • send-lifetime • service-family • service-family external-client listen • sf-interface • show eigrp service-family • show eigrp service-family ipv4 topology • show eigrp service-family ipv6 topology • show eigrp tech-support • shutdown • split-horizon • timers • topology • username (SAF)

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. 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.