Configuring SAF

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.

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 IP routing is configured between each Cisco SAF Forwarder.

Restriction for Cisco SAF

• Cisco SAF works independently of Cisco EIGRP routing.

Information About Cisco SAF

Cisco SAF Overview

Cisco 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, as applications advertise and discover services on networks. Service information distributes though 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.

These 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 --Services are advertised and can be discovered

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

This section provides the following information:

Cisco SAF Forwarder Overview

A Cisco SAF Forwarder receives services advertised by Cisco SAF Clients, distributes the services reliably through the network, and make services available for Cisco SAF Clients to use. 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 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) you want blocked to other interfaces attempting to discover their services.

The Cisco SAF Forwarder can send service metadata to its SAF neighbor 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 environments until such time that the version of EIGRP/SAF is upgraded.

You can configure a Cisco SAF Forwarder across a non-SAF node to automatically allow dynamic discovery of services. For example, Cisco SAF Forwarders 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.

Cisco SAF Client Overview

A Cisco SAF Client is a producer (advertises to the network) or 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) to, or request (subscribe), services. The figure below shows a typical Cisco SAF network.
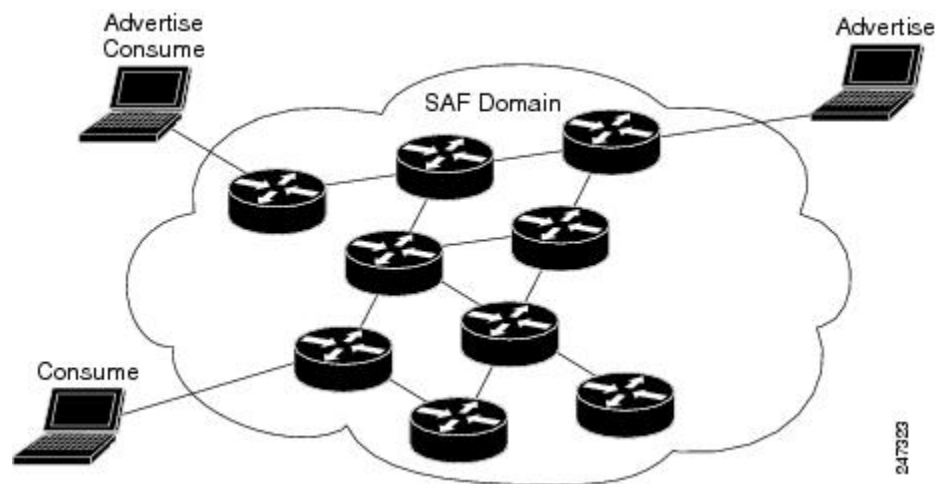
When advertising a service, a Cisco SAF Client publishes (sends) advertisements to the Cisco SAF Forwarder that contain information about the service it offers. Services are identified by a unique service ID, sub-service ID, and instance ID, and are described by service data. For more information on service identifiers, see "Cisco SAF Service Identifier Number Formats". 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 computes its own message-integrity value for the request. If the computations match, then 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 will be 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 liveliness of the Cisco SAF Client to advertise its services into the Cisco SAF network. In XMCP, this is accomplished by exchanging a liveliness timer between the client and 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 an external Cisco SAF Client failed if it has not seen an XMCP request from the client in a time period equal to the liveliness 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 liveliness 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, that 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 requiring 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 Role of Domains in a Network

As the variety and number of network services grows, 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 increases. Protocols responsible for the service advertisement need to scale to handle this increased load. These protocols also need to react to rapid changes efficiently 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 sub-domains.

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 (AD); 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 only require a single domain to use for advertising all services. However, due to 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 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 my 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 administrative domain (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, which operate independently. The addition of a Virtual Router ID (VRID) to the base Cisco EIGRP packet encoding allows for multiple instances.

As each virtual router 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 routers 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 requiring a traditional configuration methodology.
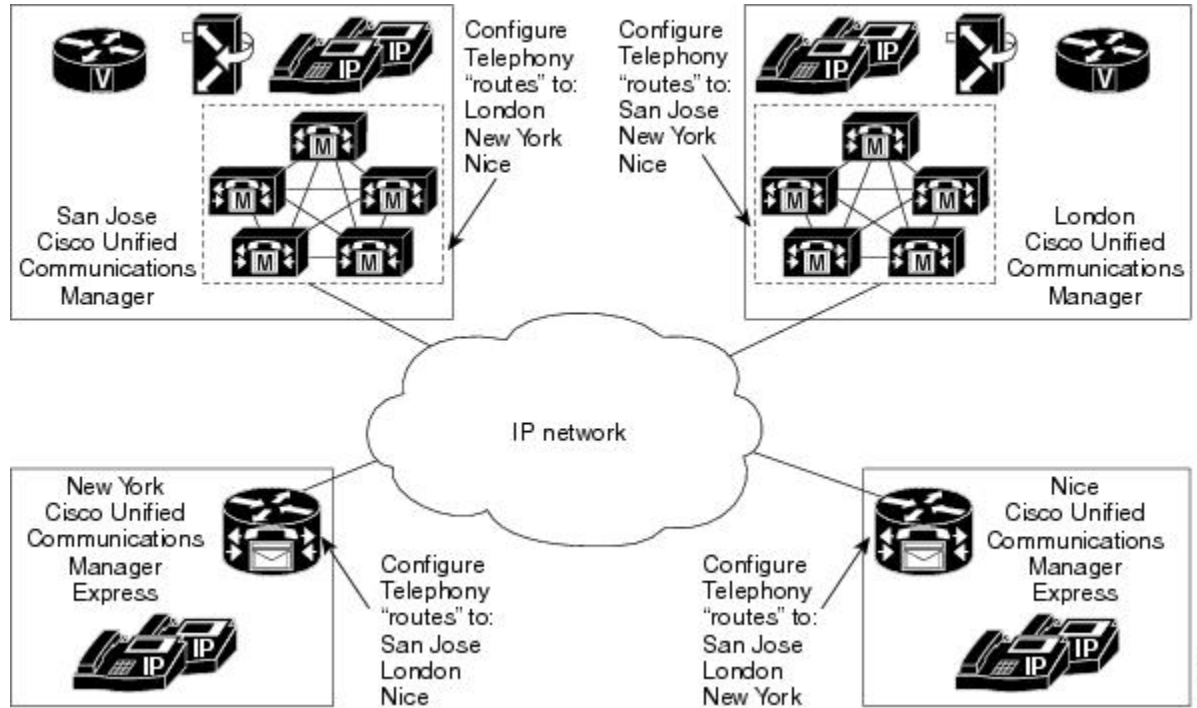
Cisco SAF provides a framework that allows networking applications to automatically discover the existence, location, and configuration of networked services within networks. This automated discovery of services replaces the manual entry of complex configurations such as dial plans, that often require 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 using Cisco SAF.
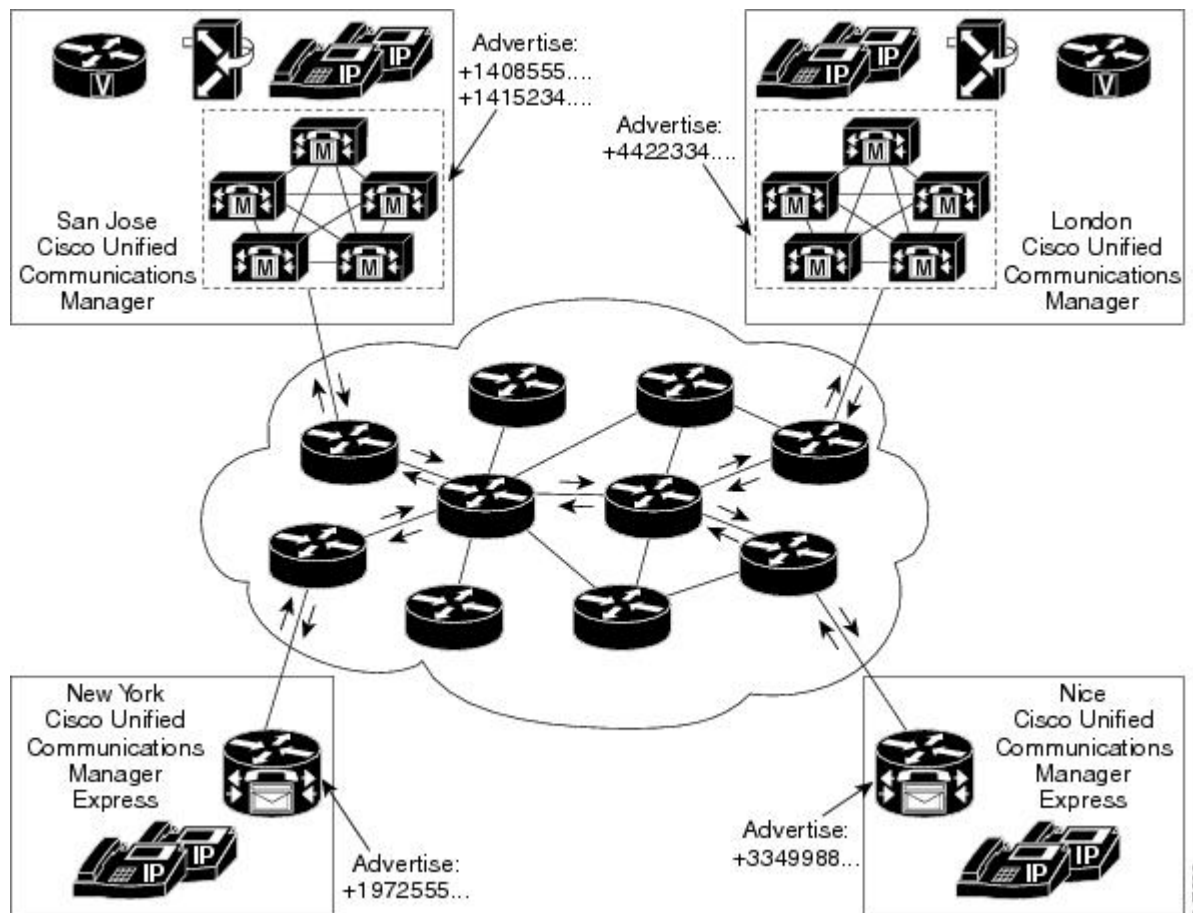
You can configure a Cisco SAF Client either on the same router as the Cisco SAF Forwarder or on an external router.

How to Configure a Cisco SAF Forwarder

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:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** Router(config)# router eigrp saf	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** Router(config-router)# service-family ipv4 autonomous-system 4453	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**exit-service-family** **Example:** Router(config-router-sf)# exit-service-family	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 sf-interface configuration mode have priority over specific sf-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-name interface-number*
6. **sf-interface**
7. **exit-sf-interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4**	**ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Creates a Cisco SAF service family for the specified autonomous system on the router, which is enabled by default.
Step 5	**sf-interface** *interface-name interface-number* **Example:** `Router(config-router-sf)# sf-interface ethernet 0/0`	Enables service-family interface configuration mode for the specified interface on the router.

	Command or Action	Purpose

Step 6	**sf-interface**
	
	Example:
	
	`Router(config-router-sf-interface)# sf-interface`
	`hello-interval 10`
		Enter the appropriate **interface** commands required for your configuration.

Step 7	**exit-sf-interface**
	
	Example:
	
	`Router(config-router-sf-interface)#`
	`exit-sf-interface`
		Exits service-family interface configuration mode.

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.

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	**Purpose**
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified Autonomous system on the router.
Step 5	**topology base** **Example:** `Router(config-router-sf)# topology base`	Enables service-family interface topology configuration mode and creates a topology base for the specified interface on the router.
Step 6	**exit-sf-topology** **Example:** `Router(config-router-sf-topology)# exit-sf-topology`	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	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** Router(config)# router eigrp saf	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4**	**ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** Router(config-router)# service-family ipv4 autonomous-system 4453	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**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**]} **Example:** Router(config-router-sf)# neighbor 10.10.10.1 Ethernet 0/0	Enables a Cisco SAF neighbor relationship for the specified interface on the router.

	Command or Action	Purpose
Step 6	**exit-service-family** **Example:** Router(config-router-sf)# exit-service-family	Exits service-family configuration mode.

Configuring Stub Routing for Cisco SAF

You can configure a Cisco SAF Forwarder as a stub router. For complete information on Cisco EIGRP stub routing, refer to the Configuring EIGRP module in the *Cisco IOS IP Routing: EIGRP Configuration Guide* .

To create an Cisco SAF stub router, 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
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** Router(config)# router eigrp saf	Enables an EIGRP virtual instance in global configuration mode.

	Command or Action	Purpose
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**eigrp stub** [**receive-only** | **connected**] **Example:** `Router(config-router-sf)# eigrp stub connected`	Configures a stub router for Cisco SAF.
Step 6	**exit-service-family** **Example:** `Router(config-router-sf)# exit-service-family`	Exits service-family configuration mode.

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-name 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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4**	**ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified autonomous system on the router.

	Command or Action	Purpose
Step 5	**sf-interface** *interface-name interface-number* **Example:** `Router(config-router-sf)# sf-interface ethernet 0/0`	Enables IPv4 service-family interface configuration mode for the specified interface on the router.
Step 6	**authentication key-chain** *name-of-chain* **Example:** `Router(config-router-sf-interface)# authentication key-chain example`	Specifies an authentication key chain for EIGRP.
Step 7	**authentication mode** {**hmac-sha-256** {**0** | **7**} *password* | **md5**} **Example:** `Router(config-router-sf-interface)# authentication mode md5`	Enables IPv4 service-family authentication mode HMAC-SHA-256 or MD5 for the specified interface on the router.
Step 8	**exit-sf-interface** **Example:** `Router(config-router-sf-interface)# exit-sf-interface`	Exits service-family interface configuration mode.
Step 9	**exit-service-family** **Example:** `Router(config-router-sf)# exit-service-family`	Exits service-family configuration mode.
Step 10	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode.
Step 11	**key-chain** *name-of-chain* **Example:** `Router(config)# key-chain example`	Defines an authentication key chain needed to enable authentication for routing protocols and enters key-chain configuration mode.
Step 12	**key** *key-id* **Example:** `Router(config-keychain)# key example`	Identifies an authentication string for a key.

	Command or Action	**Purpose**
Step 13	**key-string** *text* **Example:** Router(config-keychain-key)# key-string example	Specifies the authentication string for a key.
Step 14	**accept-lifetime** *start-time* [**local** {**duration** *seconds* | **end-time** | **infinite**}] **Example:** Router(config-router-sf-interface)# accept-lifetime example	Set the time period during that the authentication key in a key chain is received as valid.
Step 15	**send-lifetime** *start-time* [**local** {**duration** *seconds* | **end-time** | **infinite**}] **Example:** Router(config-router-sf-interface)# send-lifetime example	Configures a time period during that an authentication key on a key chain is valid to be sent.
Step 16	**exit** **Example:** Router(config-router-sf-interface)# exit	Exits service-family interface configuration mode.

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 reenable 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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**eigrp log-neighbor-changes** **Example:** `Router(config-router-sf)# eigrp log-neighbor-changes`	Enables the logging of changes in EIGRP service-family neighbor adjacencies.
Step 6	**eigrp log-neighbor-warnings** *seconds* **Example:** `Router(config-router-sf)# eigrp log-neighbor-warnings 60`	Enables the logging of changes in service-family warning messages.
Step 7	**exit-service-family** **Example:** `Router(config-router)# exit-service-family`	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-name interface-number*
6. **bandwidth-percent** *maximum-bandwidth-percentage*
7. **exit-sf-interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4**	**ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified autonomous system on the router.

	Command or Action	Purpose
Step 5	**sf-interface** *interface-name interface-number* **Example:** `Router(config-router-sf)# sf-interface ethernet0/0`	Enables service-family interface configuration mode for the specified interface on the router.

Step 6	**bandwidth-percent** *maximum-bandwidth-percentage*
	
	Example:
	
	`Router(config-router-sf-interface)#`
	`bandwidth-percent 75`
		Configures the maximum percentage of bandwidth used by the link for Cisco SAF.

Step 7	**exit-sf-interface**
	
	Example:
	
	`Router(config-router-sf-interface)#`
	`exit-sf-interface`
		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 though 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 any change in a metric that results in the router selecting a new nexthop or a down interface or router.

Dampening the metric changes 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

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4**	**ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**sf-interface** *interface-name interface-number* **Example:** `Router(config-router-sf)# sf-interface ethernet0/0`	Enables service-family interface configuration mode for the specified interface on the router.

	Command or Action	**Purpose**

Step 6	**dampening-change** [*change-percentage*]
	
	Example:
	
	`Router(config-router-sf-interface)#`
	`dampening-change 50`
		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.

Step 7	**exit-sf-interface**
	
	Example:
	
	`Router(config-router-sf-interface)#`
	`exit-sf-interface`
		Exits service-family interface configuration mode.

Interval-based Dampening Configuration

Use the following commands to configure the interval-based dampening for Cisco SAF interfaces. The value 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**
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router eigrp** *virtual-instance-name* **Example:** Router(config)# router eigrp saf	Enables an EIGRP virtual instance in global configuration mode.
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** Router(config-router)# service-family ipv4 autonomous-system 4453	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**sf-interface** *interface-name interface-number* **Example:** Router(config-router-sf)# sf-interface ethernet0/0	Enables service-family interface configuration mode for the specified interface on the router.
Step 6	**dampening-interval** *[interval]* **Example:** Router(config-router-sf-interface)# dampening-interval 30	Sets the EIGRP interval-based dampening interval.
Step 7	**exit-sf-interface** **Example:** Router(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 routers 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 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 routers 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 the 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 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-name interface-number*
6. **hello-interval** *seconds*
7. **hold-time** *seconds*
8. **exit-sf-interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.

Step 4	**service-family** {**ipv4**	**ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
		
		Example:
		
		`Router(config-router)# service-family ipv4`
		`autonomous-system 4453`
			Enables a Cisco SAF service family for the specified autonomous system on the router.

	Command or Action	**Purpose**
Step 5	**sf-interface** *interface-name interface-number* **Example:** Router(config-router-sf)# sf-interface ethernet0/0	Enables service-family interface configuration mode for the specified interface on the router.
Step 6	**hello-interval** *seconds* **Example:** Router(config-router-sf-interface)# hello-interval 50	Configures a time period for an EIGRP service-family process.
Step 7	**hold-time** *seconds* **Example:** Router(config-router-sf-interface)# hello-interval 50	Configures a time period for an EIGRP service-family routing process designated by an autonomous system number.
Step 8	**exit-sf-interface** **Example:** Router(config-router-sf-interface)# exit-sf-interface	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 router 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-name interface-number*
6. **no split-horizon**
7. **exit-sf-interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.

Step 4	**service-family** {**ipv4**	**ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
		
		Example:
		
		`Router(config-router)# service-family ipv4`
		`autonomous-system 4453`
			Enables a Cisco SAF service family for the specified autonomous system on the router.

Step 5	**sf-interface** *interface-name interface-number* **Example:** `Router(config-router-sf)# sf-interface ethernet0/0`	Enables service-family interface configuration mode for the specified interface on the router.
Step 6	**no split-horizon** **Example:** `Router(config-router-sf-interface)# no split-horizon`	Disables split-horizon.

	Command or Action	Purpose

Step 7	**exit-sf-interface**
	
	Example:
	
	`Router(config-router-sf-interface)#`
	`exit-sf-interface`
		Exits service-family interface configuration mode.

Setting Metric Maximum Hops

Maximum 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-name interface-number*
6. **metric maximum-hops**
7. **exit-sf-interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp saf`	Enables an EIGRP virtual instance in global configuration mode.

	Command or Action	Purpose
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# service-family ipv4 autonomous-system 4453`	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**sf-interface** *interface-name interface-number* **Example:** `Router(config-router-sf)# sf-interface ethernet 0/0`	Enables service-family interface configuration mode for the specified interface on the router.
Step 6	**metric maximum-hops** **Example:** `Router(config-router-sf-interface)# metric maximum-hops 5`	Specifies a hop count to have the IP routing software advertise as unreachable routes.
Step 7	**exit-sf-interface** **Example:** `Router(config-router-sf-interface)# exit-sf-interface`	Exits service-family interface configuration mode.

How to Configure a Cisco SAF External Client

This section describes the tasks to configure a Cisco SAF External Client.

Cisco SAF Clients connect to the Cisco SAF network in one of two ways:

- Reside on the same router as a Cisco SAF Forwarder, in which case the Cisco SAF Client uses an internal API to connect to a Cisco SAF Forwarder. See the "Configuring Capabilities Manager" section for more information.

- Is external to a Cisco SAF Forwarder. In this configuration, the SAF Client is referred to as a Cisco SAF External Client, and it requires a protocol interface for connecting to the Cisco SAF Forwarder.

Prerequisites

Before configuring:

- Cisco SAF Clients, you should understand the concepts in the Cisco SAF Client Overview.

• Neighbor relationships for Cisco SAF External Clients located on separate LANs, ensure that you have IP routing configured between each Cisco External Client.

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. **exit**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** Router(config)# router eigrp saf	Enables an EIGRP virtual instance in global configuration mode.

	Command or Action	Purpose
Step 4	**service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** Router(config-router)# service-family ipv4 autonomous-system 4453	Enables a Cisco SAF service family for the specified autonomous system on the router.
Step 5	**topology base** **Example:** Router(config-router-sf)# topology base	Enables service-family interface topology configuration mode for the specified interface on the router.
Step 6	**external-client** *client-label* **Example:** Router(config-router-topology)# external-client example	Configures a Cisco SAF External Client with the specified Client label.
Step 7	**exit-sf-topology** **Example:** Router(config-router-sf-topology)# exit-sf-topology	Exits service-family topology configuration mode.
Step 8	**exit-service-family** **Example:** Router(config-router-sf)# exit-service-family	Exits service-family configuration mode.
Step 9	**exit** **Example:** Router(config-router)# exit	Exits router configuration mode.
Step 10	**service-family external-client listen** {**ipv4** | **ipv6**} tcp_port_number **Example:** Router(config)# service-family external-client listen ipv4 5050	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.

	Command or Action	Purpose
Step 11	**external-client** *client-label* **basename** **Example:** `Router(config-external-client)# external-client example basename`	Configures a Cisco SAF External Client with the specified client label and optionally, a basename. 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 *client-label* @[1-1024] where you can specify a maximum of 1024 SAF external clients. For example, if the **external-client** command specifies a client label of *example* , then the basename for a SAF external client would be *example@1*. Another SAF external client would be *example@2* , and so on up to a maximum of 1024 basenames (*@1024*).
Step 12	**username** *user-name* **Example:** `Router(config-external-client)# username example`	Enables external-client label configuration mode and configures a Cisco SAF External Client with the specified username.
Step 13	**password** *password-name* **Example:** `Router(config-external-client-mode)# password examplepass`	Configures a password for a Cisco SAF External Client. The minimum password length is 11 characters.
Step 14	**keepalive** *number* **Example:** `Router(config-external-client-mode)# keepalive 360000`	(Optional) Specifies the keepalive timer for the Cisco SAF External Client. The keepalive value is in milliseconds (msecs). The default is 9600 msecs.
Step 15	**exit** **Example:** `Router(config-external-client-mode)# exit`	Exits external-client label configuration mode.

How to Display 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** [*ip_address*	*handle*] [**detail**] **Example:** `Router> show service-routing clients detail`	Displays information about connected XMCP clients.

	Command or Action	Purpose
Step 2	**show service-routing xmcp server** **Example:** `Router> show service-routing xmcp server`	Displays information about clients, external clients, or subscriptions configured for Cisco SAF.
Step 3	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **accounting** **Example:** `Router# show eigrp service-family ipv4 4453 accounting`	Displays accounting information about Cisco SAF.
Step 4	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **clients** [**detail**] **Example:** `Router# show eigrp service-family ipv4 4453 clients`	Displays information about Cisco SAF Clients.
Step 5	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **events** [*starting-event-number ending-event-number*] **Example:** `Router# show eigrp service-family ipv4 4453 events`	Displays information about Cisco SAF events.
Step 6	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **interfaces** [*interface-type interface-number*] [**detail**] **Example:** `Router# show eigrp service-family ipv4 4453 interfaces`	Displays information about Cisco SAF interfaces.
Step 7	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **subscriptions** **Example:** `Router# show eigrp service-family ipv4 4453 subscriptions`	Displays information about Cisco SAF subscriptions.
Step 8	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **timers** **Example:** `Router# show eigrp service-family ipv4 4453 timers`	Displays information about Cisco SAF timers.

	Command or Action	Purpose
Step 9	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **summary** **Example:** `Router# show eigrp service-family ipv4 4453 summary`	Displays summary information about Cisco SAF.
Step 10	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **zero successors** **Example:** `Router# show eigrp service-family ipv4 4453 zero successors`	Displays information about Cisco SAF zero successors.
Step 11	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** **Example:** `Router# show eigrp service-family ipv4 4453 topology`	Displays information about the Cisco SAF topology table.
Step 12	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology active** **Example:** `Router# show eigrp service-family ipv4 4453 topology active`	Displays only active entries for a Cisco SAF topology table.
Step 13	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology all-links** **Example:** `Router# show eigrp service-family ipv4 4453 topology all-links`	Displays all active link entries for a Cisco SAF topology table.
Step 14	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology base** *service-instance-number* | **clients** [**detail**] **Example:** `Router# show eigrp service-family ipv4 4453 topology base clients`	Displays all active link entries for a Cisco SAF topology base.
Step 15	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** [**detail-links**] **Example:** `Router# show eigrp service-family ipv4 4453 topology detail-links`	Displays information about Cisco SAF.

	Command or Action	Purpose
Step 16	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology events** [*starting-event-number ending-event-number*] **Example:** `Router# show eigrp service-family ipv4 4453 topology`	Displays information about Cisco SAF.
Step 17	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology pending** **Example:** `Router# show eigrp service-family ipv4 4453 topology pending`	Displays information about Cisco SAF.
Step 18	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** [**service-type connected** | **external** | **internal** | **local** | **redistributed** | **summary**] **Example:** `Router# show eigrp service-family ipv4 4453 topology service-type connected`	Displays information about the specified service type for a Cisco SAF topology table.
Step 19	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology sia-events** *starting-event-number ending-event-number* **Example:** `Router# show eigrp service-family ipv4 4453 topology sia-events`	Displays logged Stuck in Active (SIA) events in the Cisco SAF topology table.
Step 20	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology sia-statistics** [*ip-address*] **Example:** `Router# show eigrp service-family ipv4 4453 topology sia-statistics 10.10.10.1`	Displays Stuck in Active (SIA) events for a Cisco SAF topology table.
Step 21	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology summary** **Example:** `Router# show eigrp service-family ipv4 4453 topology summary`	Displays a summary of a Cisco SAF topology table.

	Command or Action	Purpose

Step 22	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology zero-successors**
	
	Example:
	
	`Router# show eigrp service-family ipv4 4453 topology`
	`zero-successors`
		Displays information about available services that have zero successors in a Cisco SAF topology table.

How to Delete 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** {*address* \| *handle*}
2. **clear eigrp service-family** {**ipv4** \| **ipv6**} **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

Step 1	**clear service-family xmcp client** {*address* | *handle*}
	
	Example:
	
	`Router> clear service-family xmcp client`
	`1.1.1.1`
		Disconnects a connected XMCP client.

Step 2	**clear eigrp service-family** {**ipv4** | **ipv6**} **ipv6** [**vrf** *vrf-name*] *autonomous-system-number* **Example:** `Router# clear eigrp service-family ipv4 4453`	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. **Note** — Using the **clear eigrp service-family ipv6** command requires an IPv6-enabled SAF client, which currently does not exist.

Step 3	**clear eigrp service-family neighbors** *neighbor-address* | *interface-type interface-number*
	
	Example:
	
	`Router> clear eigrp service-family neighbors`
	` Ethernet 0/0`
		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.

Configuration Examples for Cisco SAF

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.

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

Example: Configuring Cisco SAF Interfaces

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

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

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

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

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

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

The following example places the router in service-family configuration mode and enables SAF on the Ethernet2/0 and Ethernet2/1 interfaces and disables all other interfaces.

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

Example: Configuring Cisco SAF Topology

The following examples configures a Cisco SAF topology base.

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

Example: Configuring Cisco SAF Stub Routing

The following examples configures a Cisco SAF Forwarder as a stub router.

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

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

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# exit-sf-topology
Router(config-router-sf)# exit service-family
Router(config-router)# router ospf 787
Router(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.

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

```
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(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 examples configures two Cisco SAF Forwarders located on separate LANs.

> **Note** Use loopback mode to configure remote neighbors.

Cisco SAF Forwarder 1:

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

Cisco SAF Forwarder 2:

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

> **Note** This example assumes IP routing is configured between the two routers and the routers can ping both loopbacks.

Configuring a Centralized Cisco SAF Forwarder Example

The following example configures a centralized Cisco SAF Forwarder from which all service advertisements will send to neighbors on IP addresses 10.4.15.5 and 10.4.15.1.

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface loopback0
Router(config-router-sf-interface)# no split-horizon
Router(config-router-sf-interface)# exit-sf-interface
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# exit-sf-topology
Router(config-router-sf)# neighbor 10.4.15.5 Loopback0 remote 20
Router(config-router-sf)# neighbor 10.4.15.1 Loopback0 remote 20
Router(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 360000 seconds.

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

The following example configures eight 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 360000 seconds.

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# external-client example1
Router(config-router-sf-topology)# external-client example2
Router(config-router-sf-topology)# external-client example3
Router(config-router-sf-topology)# external-client example4
Router(config-router-sf-topology)# external-client example5
Router(config-router-sf-topology)# exit-sf-topology
Router(config-router-sf)# exit-service-family
Router(config-router)# exit
Router(config)# service-family external-client listen ipv4 3444
Router(config-external-client)# external-client example1
Router(config-external-client-mode)# username
 username_example1
Router(config-external-client-mode)# password
 password_example1
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example2
Router(config-external-client-mode)# username
 username_example2
Router(config-external-client-mode)# password
 password_example2
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example3
Router(config-external-client-mode)# username
 username_example3
Router(config-external-client-mode)# password
 password_example3
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example4
Router(config-external-client-mode)# username
 username_example4
Router(config-external-client-mode)# password
 password_example4
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example5
```

```
Router(config-external-client-mode)# username
 username_example5
Router(config-external-client-mode)# password
 password_example5
Router(config-external-client-mode)# keepalive
 360000
```

Additional References

Related Documents

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

Technical Assistance

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

Feature Information for Cisco SAF

Table 1: Feature Information for Cisco Service Advertisement Framework

Feature Name	Software Releases	Feature Configuration Information
Cisco Service Advertisement Framework	15.0M, 12.2(33)SRE, 12.2(33)XNE, 15.1T, 12.2(33)SXI4, 15.0(1)S, 15.1(2)S, 12.2(50)SY, 15.2(1)T, 15.2(3)T, 15.2(2)S, 15.1(1)SG Cisco IOS XE 2.5, Cisco IOS XE 3S, Cisco IOS XE 3.3SG	

Feature Name	Software Releases	Feature Configuration Information
		This feature allows applications to discover the existence, location, and configuration of networked resources within networks, and provides a timely and reliable awareness of the services within networks, as applications advertise and discover services on networks.
		This feature was introduced in Cisco IOS Release 15.0M.
		In Cisco IOS XE 2.5, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
		In Cisco IOS XE 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches.
		The following commands were introduced in this feature: **authentication (service-family)** **bandwidth-percent** **clear eigrp service-family** **dampening-change** **dampening-interval** **default external-client** **default (SAF)** **debug eigrp service-family** **default-metric (EIGRP)** **eigrp stub (service-family)** **exit-service-family** **exit-sf-interface** **exit-sf-topology** **external-client** **keepalive (SAF)** **maximum-service (EIGRP)** **neighbors (service-family)**

Feature Name	Software Releases	Feature Configuration Information
		• **password (SAF)**
		• **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**
		• **topology**
		• **username (SAF)**
Cisco Service Advertisement Framework	15.0M, 12.2(33)SRE, 12.2(33)XNE, 15.0(1)S, 15.1(2)S, 15.2(3)T, 15.2(2)S Cisco IOS XE Release 2.5, Cisco IOS XE Release 3S, Cisco IOS XE Release 3.4S, Cisco IOS XE Release 3.6S	The following commands were modified in this feature: • **accept-lifetime** • **eigrp log-neighbor-changes** • **eigrp-log-neighbor-warnings** • **eigrp router-id** • **hello-interval** • **hold-time** • **key** • **key chain** • **key-string (authentication)** • **metric weights (EIGRP)** • **next-hop-self** • **send-lifetime** • **split-horizon** • **timers**

Feature Name	Software Releases	Feature Configuration Information
Dynamic Neighbor	15.1(2)S, 15.2(3)T, 15.2(2)S, XE 3.6S	The following commands were introduced or modified: • **authentication mode** • **remote-neighbors source** • **show eigrp service-family external-client**
Capabilities Manager	15.0(1)SY, 15.2(3)T, 15.2(2)S, XE 3.6S	The following commands were introduced or modified: • **clear service-routing capabilities-manager** • **service-routing capabilities-manager** • **show service-routing plugins capman** • **show service-routing capabilities-manager internal** • **show service-routingcapabilities-manager group**
XMCP (Extensible Messaging Client Protocol)	15.2(2)T, 15.2(1)S, 15.2(3)T, 15.2(2)S, XE 3.6S	The following commands were introduced or modified: • **allow-list** • **clear service-routing xmcp client** • **client (XMCP)** • **domain** • **keepalive (XMCP)** • **max-clients** • **nonce** • **service-routingxmcp clients** • **service-routingxmcp server**