Cisco IOS Service Advertisement Framework Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **SAF Commands: A through bandwidth-percent** 1

accept-lifetime 2

allow-list 5

authentication key-chain (EIGRP) 7

authentication mode (EIGRP) 9

bandwidth-percent 12

CHAPTER 2 **SAF Commands: clear eigrp service-family through default external-client** 15

clear eigrp service-family 16

clear service-routing capabilities-manager 19

clear service-routing xmcp client 20

client (XMCP) 22

client unauthenticated (XMCP) 24

dampening-change 26

dampening-interval 28

debug eigrp service-family 30

default (SAF) 34

default external-client 35

domain 36

CHAPTER 3 **SAF Commands: eigrp log-neighbor-changes through hold-time** 39

eigrp log-neighbor-changes 40

eigrp log-neighbor-warnings 42

eigrp router-id 44

eigrp stub (service-family) 46

exit-service-family 48

exit-sf-interface 49

exit-sf-topology 51

external-client 53
hello-interval 56
hold-time 58

CHAPTER 4 SAF Commands keepalive SAF through remote-neighbors SAF 61

keepalive (SAF) 62
keepalive (XMCP) 64
key 66
key chain 69
key-string (authentication) 72
max-clients 75
maximum-service (EIGRP) 77
metric weights (EIGRP) 80
neighbor (service-family) 83
nonce 87
password (SAF) 89
remote-neighbors source 91

CHAPTER 5 SAF Commands send-lifetime through username SAF 93

send-lifetime 94
service-family 97
service-family external-client listen 99
service-routing xmcp listen 101
sf-interface 103
show eigrp plugins 105
show eigrp protocols 108
show eigrp service-family external-client 111
show eigrp service-family ipv4 topology 114
show eigrp service-family ipv6 topology 118
show eigrp tech-support 122
show service-routing capabilities-manager 125
show service-routing capabilities-manager internal 128
show service-routing plugins capman 130
show service-routing xmcp clients 132
show service-routing xmcp server 135

split-horizon (EIGRP) **137**

timers graceful-restart purge-time **139**

topology **142**

username (SAF) **144**

SAF Commands: A through bandwidth-percent

- accept-lifetime, page 2
- allow-list, page 5
- authentication key-chain (EIGRP), page 7
- authentication mode (EIGRP), page 9
- bandwidth-percent, page 12

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime**command inkey chain key configuration mode. To revert to the default value, use the **no** form of this command.

accept-lifetime commandaccept-lifetime *start-time* {**infinite**| *end-time*| **duration** *seconds*}

no accept-lifetime [*start-time* {**infinite**| *end-time*| **duration** *seconds*}]

Syntax Description

start-time	Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following: *hh* **:** *mm* **:** *ss Month date year* *hh* **:** *mm* **:** *ss date Month year* • *hh* --hours • *mm* --minutes • *ss*-- s econds • *Month*-- first three letters of the month • *date*-- date (1-31) • *year*-- y ear (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be received from the *start-time* value on.
end-time	Key is valid to be received from the *start-time* value until the *end-time*value. The syntax is the same as that for the *start-time*value. The *end-time* value must be after the *start-time*value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Command Default

The authentication key on a key chain is received as valid forever (the starting time is January 1, 1993, and the ending time is infinite).

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you assign a lifetime to a key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and will be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and will be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain)# key-string key2
Router(config-keychain)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for

migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router
 eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

allow-list

To restrict the IP addresses that are permitted to connect as an XMCP (Extensible Messaging Client Protocol) client, use the **allow-list** command in XMCP configuration mode. To remove this restriction, use the **no** form of this command.

allow-list {**ipv4**| **ipv6**} {*acl-name*}

no allow-list {**ipv4**| **ipv6**}

Syntax Description

ipv4	Restricts IPv4 client IP addresses. Only one allow list may be configured at a time.
ipv6	Restricts IPv6 client IP addresses. Only one allow list may be configured at a time.
acl-name	Access control list to use to restrict client IP addresses.

Command Default

No ACL is configured, which allows all source IP addresses to connect as XMCP clients.

Command Modes

XMCP configuration (config-xmcp)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS 15.2(2)T.

Usage Guidelines

The **allow-list** command is used to restrict the IP addresses that are permitted to connect as clients. After an allow list is configured, a client attempting to register will be permitted only if its IP address is permitted by the access list specified.

After an allow list is added or modified, any currently connected clients that would no longer be permitted by the new allow list will have their sessions terminated.

Only one IPv4 and one IPv6 allow list may be configured at a time.

Examples

The following example show how to restrict access for IPv4 clients to connect only from source IP addresses permitted by the access list client_acl and restricts access for IPv6 clients to connect only from source IP addresses permitted by the access list acl_ipv6:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# allow-list ipv4 client_acl
Router(config-xmcp)# allow-list ipv6 acl_ipv6
Router(config-xmcp)# end
```

Related Commands

Command	Description
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

authentication key-chain (EIGRP)

To specify an authentication key chain for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **authentication key-chain** (EIGRP) command in address-family interface configuration mode or service-family interface configuration mode. To remove the authentication key-chain, use the **no** form of this command.

authentication key-chain *name-of-chain*

no authentication key-chain *name-of-chain*

Syntax Description

name-of-chain	Group of keys that are valid.

Command Default

No key chains are specified for EIGRP.

Command Modes

Address-family interface configuration (router-config-af-interface) Service-family interface configuration (router-config-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The **key-chain** command has no effect until the **authentication mode md5**command is configured.

Only one authentication key chain is applied to EIGRP at one time. That is, if you configure a second **authentication key-chain** command, the first is overridden.

Examples

The following example configures EIGRP to apply authentication to address-family autonomous system 1 and identifies a key chain named SITE1:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain SITE1
Router(config-router-af-interface)# authentication mode md5
```

The following example configures EIGRP to apply authentication to service-family autonomous system 1 and identifies a key chain named SITE1:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 1
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain SITE1
Router(config-router-sf-interface)# authentication mode md5
```

Related Commands

Command	Description
authentication mode (EIGRP)	Specifies the type of authentication used in EIGRP address-family packets for the EIGRP instance.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
router eigrp	Configures the EIGRP address-family process.

authentication mode (EIGRP)

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) address-family or service-family packets for an EIGRP instance, use the **authentication mode** command in address family interface configuration mode or service family interface configuration mode. To disable a configured authentication type, use the **no** form of this command.

authentication mode {**hmac-sha-256** {**0**| **7**} *password*| **md5**}

no authentication mode

Syntax Description

hmac-sha-256	Specifies the Hashed Message Authentication Code (HMAC)-Secure Hash Algorithm (SHA)-256 authentication.
0	Indicates that there is no password encryption. 0 is the default.
7	Indicates that there is an explicit password encryption.
password	Password string to be used with SHA authentication. The string can contain 1 to 32 characters including white spaces; however, the first character cannot be a number.
md5	Specifies message digest algorithm 5 (MD5) authentication.

Command Default

No authentication mode is provided for EIGRP packets.

Command Modes

Address family interface configuration (config-router-af-interface)

Service family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Release	Modification
15.1(2)S	This command was modified. The **hmac-sha-256** keyword and the *encryption-type* and *password* arguments were added.
Cisco IOS XE Release 3.3S	This command was modified. The **hmac-sha-256** keyword and the *encryption-type* and *password* arguments were added.
15.2(1)T	This command was modified. The **hmac-sha-256** keyword and the *encryption-type* and *password* arguments were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can configure authentication to prevent unapproved sources from introducing unauthorized or false service messages.

When the **authentication mode**(EIGRP)command is used in conjunction with the **authentication key-chain** command, an MD5 keyed digest is added to each EIGRP packet.

To configure basic HMAC-SHA-256 authentication, use the **authentication mode hmac-sha-256** command on each interface of each router that should use authentication.

Examples

The following example shows how to configure the interface to use MD5 authentication in address-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain TEST1
Router(config-router-af-interface)# authentication mode md5
```

The following example shows how to configure the interface to use MD5 authentication in service-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 1
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain TEST1
Router(config-router-sf-interface)# authentication mode md5
```

The following example shows how to configure the interface to use basic HMAC SHA authentication with password password1 in address-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv6 autonomous-system 4453
Router(config-router-af)# af-interface ethernet 0
Router(config-router-af-interface)# authentication mode hmac-sha-256 7 password1
```

The following example shows how to configure an interface to use basic HMAC SHA authentication with password password1 in service-family packets:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 6473
Router(config-router-sf)# sf-interface ethernet 0
Router(config-router-sf-interface)# authentication mode hmac-sha-256 7 password1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address family interface configuration mode to configure interface-specific EIGRP commands.
authentication key-chain	Specifies the type of authentication used in EIGRP address-family or service-family packets for the EIGRP instance.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
router eigrp	Configures an EIGRP routing process.

bandwidth-percent

To configure the percentage of bandwidth that may be used by an Enhanced Interior Gateway Routing Protocol (EIGRP) address family or service family on an interface, use the **bandwidth-percent**command in address-family interface configuration mode or service-family interface configuration mode. To restore the default value, use the **no** form of this command.

bandwidth-percent *maximum-bandwidth-percentage*

no bandwidth-percent

Syntax Description

maximum-bandwidth- percentage	Percent of configured bandwidth that EIGRP may use to send packets. Valid range is 1 to 999999. The default is 50 percent.

Command Default

EIGRP limits bandwidth usage to 50 percent of the configured interface bandwidth.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **bandwidth-percent** command to configure a different percentage of bandwidth for use by EIGRP than specified for the link by using the **bandwidth interface**command. Values greater than 100 percent may be configured. This option might be useful if the link bandwidth is set artificially low for other reasons. The default bandwidth percent uses 50 percent of the configured bandwidth of the link.

Examples

The following example uses up to 75 percent (42 kbps) of a 56-kbps serial link for address-family autonomous system 4453:

```
Router(config)# router eigrp virtual-name
```

```
Router(config-router)# address-family ipv4 autonomous-system 4453

Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# bandwidth-percent 75
```

The following example uses up to 75 percent (42 kbps) of a 56-kbps serial link for service-family autonomous system 4533:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface serial 0
Router(config-router-sf-interface)# bandwidth-percent 75
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
router eigrp	Configures the EIGRP address-family process.
service-family	Configures VRF metrics for an EIGRP service-family.
sf-interface	Configures interface-specific commands for an EIGRP service-family.

SAF Commands: clear eigrp service-family through default external-client

- clear eigrp service-family, page 16
- clear service-routing capabilities-manager, page 19
- clear service-routing xmcp client, page 20
- client (XMCP), page 22
- client unauthenticated (XMCP), page 24
- dampening-change, page 26
- dampening-interval, page 28
- debug eigrp service-family, page 30
- default (SAF), page 34
- default external-client, page 35
- domain, page 36

clear eigrp service-family

To clear information for a Cisco SAF service family, use the **clear eigrp service-family**command in privileged EXEC mode.

clear eigrp service-family {**external-client** *name*| {**ipv4| ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **neighbors** [*neighbor-address*| *interface-type interface-number*] **[soft]**}

Syntax Description

external-client	Deletes a specified external client.
name	Specifies the name of the external client.
ipv4	Deletes neighbors formed using the IPv4 protocol family.
ipv6	Deletes neighbors formed using the IPv6 protocol family.
vrf	(Optional) Specifies all virtual routing forwarding (VRF) instance tables or a specific VRF table for an IP address.
vrf-name	(Optional) Names a specific VRF table for the specified IP address.
autonomous- system-number	Specifies the autonomous system number.
neighbors	Deletes neighbors formed using the IP protocol family.
neighbor-address	(Optional) IP address of neighbor.
interface-type	(Optional) Deletes from the neighbor table the interface type and number that all entries learned through this interface.
interface-number	(Optional) Specifies the interface number for the *interface-type* argument.
soft	(Optional) Resyncs with peer without an adjacency reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the clear service-routing xmcp client command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the clear service-routing xmcp client command.
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the clear service-routing xmcp client command.

Usage Guidelines

Use the **clear eigrp service-family**command in privileged EXEC mode to remove information related to Cisco SAF service-family neighbors and external clients.

Note Using the **clear eigrp service-family ipv6** commands requires an IPv6-enabled SAF client, which currently does not exist.

Examples

The following example clears an EIGRP service-family External Client named “example_2” from Cisco SAF:

```
Router> enable
Router# show eigrp service-family external-client
External SAF Connected Clients
Client Label     Client No.     Client API Handle   File Descriptor
example_1      1                   1           1
example_2      2     2      2
Router# clear eigrp service-family external-client example_2
Router# show eigrp service-family external-client
External SAF Connected Clients
Client Label     Client No.     Client API Handle   File Descriptor
example_1      1                   1           1
```

Related Commands

Command	Description
show eigrp service-family	Displays information about the EIGRP IPv4 or IPv6 service families.
show eigrp service-family external-client	Displays information about the EIGRP service-family External Clients.

clear service-routing capabilities-manager

To clear current capabilities information, use the **clear service-routing capabilities-manager** command in user EXEC or privileged EXEC mode.

clear service-routing capabilities-manager

Syntax Description

This command has no keywords or arguments.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

Use the **clear service-routing capabilities-manager** command in user or privileged EXEC mode to remove current capabilities information. Capabilities Manager will automatically rediscover new capabilities.

Examples

The following example shows how to clear registered capabilities information:

```
Router# clear service-routing capabilities-manager
Router# clear service-routing capabilities-manager
%SR-CAPMAN: Restarting Capabilities Manager
```

Related Commands

Command	Description
show service-routing capabilities-manager	Displays information about registered capabilities.
show service-routing capabilities-manager internal	Displays information about Capabilities Manager.
show service-routing plugins capman	Displays Capabilities Manager plugin information.

clear service-routing xmcp client

To forcibly disconnect a connected XMCP (Extensible Messaging Client Protocol) client, use the **clear service-routing xmcp client** command in privileged EXEC mode.

clear service-routing xmcp client{ *ip-address* | *handle*}

Syntax Description

ip-address	IPv4 or IPv6 IP address of a single client to disconnect.
handle	Handle of a single client to disconnect. A handle is a number assigned dynamically by XMCP. The number range is 1 to 1023, and is displayed in the Handle field of the display.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS 15.2(2)T.

Usage Guidelines

Use the **clear service-routing xmcp client** command in privileged EXEC mode to disconnect a connected XMCP client. The client will be sent a RegisterRevoke packet informing it that its connection has been revoked.

To ensure you are disconnecting the correct XMCP client, use the **show service-routing xmcp clients detail** command to display client information before entering the **clear** command.

Examples

The following example displays information for the service-routing XMCP clients and then uses the **clear service-routing xmcp clients** command to disconnect the client using the client IP address (10.1.1.1).

```
Router# show service-routing xmcp clients

XMCP Clients
Codes: A - Authenticated, T - TCP

    Handle Address                                  Port  Keepalive
AT  1      10.1.1.1                                 47519    24/30
    Client name: UCM/CM_ccmbeijing/NodeId=1/8.5.1.10000-26
 23     2001:0DB8:E123:1000:3615:9EFF:FE0B:AFA4   3478  3120/3600
    Client name: CapMan Viewer/glmatthe-mac.example.com/Mac OS X 10.6.6 (10J567)

Router# clear service-routing xmcp client 10.1.1.1
%RegisterRevoke sent to client 1 (10.1.1.1:47519)
```

The following example disconnects the client using the client handle (23).

```
Router# clear service-routing xmcp client 23
%RegisterRevoke sent to client 23 ([2001:0DB8:E123:1000:3615:9EFF:FE0B:AFA4]:3478)
```

Related Commands

Command	Description
show service-routing xmcp	Displays currently connected XMCP clients.

client (XMCP)

To configure a username and password that will be accepted for XMCP (Extensible Messaging Client Protocol) client connections, use the **client** command in XMCP configuration mode. To remove this username and password, use the **no** form of this command.

client username *username* {[**0**] **password** *password* | *encryption-type* *encryption-password* }

no client username *username*

Syntax Description

username *username*	Specifies the username for client authentication. The username must be unique across all user names defined for this port. A username can be 1 to 64 characters in length.
0	(Optional) Specifies no password encryption (clear-text). This is the default encryption type.
password *password*	Specifies an unencrypted clear-text password. An XMCP password is defined as follows: • Must contain from 11 to 64 ASCII characters • Must not begin with a digit • Must not contain spaces or control characters
encryption-type	Cisco proprietary algorithm used to encrypt a password. Valid encryption types are 0 (clear text by default) or 6. When you specify type 6 encryption, the next value you supply must be an encrypted password.
encrypted-password	Encrypted password, which is copied from another router configuration. An encrypted password is a password that is already encrypted by a Cisco router.

Command Default

No username or password is defined. The default encryption type for passwords is 0 (that is, clear-text) unless password encryption has been enabled, in which case all passwords (even those entered as clear-text) will be converted to use type 6 encryption.

Command Modes

XMCP configuration (config-xmcp)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **client** command is used to define which clients are permitted to connect to the configured XMCP port. Unauthenticated clients, if permitted, provide limited functionality to subscribe and query some services, but are unable to access restricted services and are prevented from publishing services of their own. Authenticated clients use a specific username and password as authentication credentials and have full access to the service-routing network.

A maximum of five unauthenticated connections from a single source IP address are allowed.

Once a username and password are defined, the password associated with this username can only be changed by using the **no client username** command.

When configuring authenticated clients, you typically do not enter an encryption type. You enter an encryption type only if you copy and paste this command from another Cisco router configuration command.

You can enable password encryption with the **password encryption aes** command. After you enter this command, all existing clear-text client passwords are converted to use type 6 encryption. Once a password is encrypted, it will remain encrypted even after you configure the **no password encryption aes** command.

Examples

The following commands configure XMCP and permit unauthenticated clients and authenticated clients using username username1 and password examplePASSWORD123:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# client unauthenticated
Router(config-xmcp-client)# client username username1 password examplePASSWORD123
Router(config-xmcp-client)# end
```

Related Commands

Command	Description
external-client (SAF)	Configures a Cisco Service Advertisement Framework (Cisco SAF) External Client. This command is deprecated and replaced by the **client** command.
key config-key password-encryption	Stores a type 6 encryption key in private NVRAM.
password encryption aes	Enables a type 6 encrypted preshared key.
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

client unauthenticated (XMCP)

To permit clients to connect without authentication credentials, use the **client unauthenticated** command in XMCP configuration mode. To prevent clients without authentication credentials from connecting, use the **no** form of this command.

client unauthenticated

no client unauthenticated

Syntax Description

unauthenticated	Permit clients to connect without authentication credentials. Unauthenticated clients can subscribe and query for some services, but cannot publish services.

Command Default

Unauthenticated clients are not permitted.

Command Modes

XMCP configuration (config-xmcp)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **client** command is used to define which clients are permitted to connect to the configured XMCP port. Unauthenticated clients, if permitted, provide limited functionality to subscribe and query some services, but are unable to access restricted services and are prevented from publishing services of their own. Authenticated clients use a specific username and password as authentication credentials and have full access to the service-routing network. Use the **client** command in XMCP mode to assign a username and pasword.

A maximum of five unauthenticated connections from a single source IP address are allowed.

Examples

The following commands configure XMCP and permits unauthenticated clients as well as authenticated clients using username username1 and password examplePASSWORD123:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# client unauthenticated
Router(config-xmcp-client)# client username username1 password examplePASSWORD123
Router(config-xmcp-client)#  end
```

Related Commands

Command	Description
client username password	Configures a username and password that will be accepted for XMCP client connections.
external-client (SAF)	Configures a Cisco Service Advertisement Framework (Cisco SAF) External Client. This command is deprecated and replaced by the client command.
key config-key password-encryption	Stores a type 6 encryption key in private NVRAM.
password encryption aes	Enables a type 6 encrypted preshared key.
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

dampening-change

To set a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an Enhanced Interior Gateway Routing Protocol (EIGRP) address family or service family, use the **dampening-change** command in address-family interface configuration mode or service-family interface configuration mode. To restore the default value, use the **no** form of this command.

dampening-change [*change-percentage*]

no dampening-change

Syntax Description

change-percentage	(Optional) The percentage a metric must change before the value is stored for future decisions on advertisements. Value range is 1 to 100. If a *change-percentage* value is not specified, the default is 50 percent of the computed metric.

Command Default

No threshold percentage is configured.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The **dampening-change** command is supported only for Mobile Ad Hoc Networking (MANET) router-to-radio links.

When a peer metric changes on an interface that is configured with the **dampening-change** command, EIGRP multiplies the dampening-change percentage with the old peer metric and compares the result (the threshold) to the difference between the old and new metrics. If the metric difference is greater than the calculated

threshold, then the new metric is applied and routes learned from that peer are updated and advertised to other peers. If the metric difference is less than the threshold, the new metric is discarded.

There are exceptions that will result in an immediate update regardless of the dampening-change setting:

- An interface is down.
- A route is down.
- A change in metric which results in the router selecting a new next hop.

Peer metric changes that do not exceed a configured change percentage and that do not result in a routing change do not result in an update being sent to other adjacencies. Peer metric changes are based on the stored last-update of the peer. Peer metric changes that exceed the threshold value are stored and used for future comparisons.

Examples

The following example configures an EIGRP address family to accept a peer metric change if the change is greater than 75 percent of the last updated value:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 5400
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# dampening-change 75
```

The following example configures an EIGRP service family to accept a peer metric change if the change is greater than 75 percent of the last updated value:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface serial 0
Router(config-router-sf-interface)# dampening-change 75
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
dampening-interval	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
router eigrp	Configures the EIGRP address-family process.
service-family	Specifies service-family configuration mode.
sf-interface	Configures interface-specific commands under a service family.

dampening-interval

To set a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in an Enhanced Interior Gateway Routing Protocol (EIGRP) address family or service family, use the **dampening-interval** command in address-family interface configuration mode or service-family interface configuration mode. To restore to the default value, use the **no** form of this command.

dampening-interval [*interval*]

no dampening-interval [*interval*]

Syntax Description

interval	(Optional) Time interval, in seconds, that must elapse before a route change will cause an update to occur. Value range is 1 to 65535. If an *interval*value is not specified, the default is 30 seconds.

Command Default

A dampening interval is not enabled.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The **dampening-interval** command is supported only in Mobile Ad Hoc Networking (MANET) Router-to-Radio links.

When a peer metric changes on an interface that is configured with a dampening interval, EIGRP will apply the metric change only if the time difference since the last metric changed exceeds the specified interval. If the time difference is less than the specified interval, the update is discarded.

There are exceptions that result in an immediate update regardless of the dampening interval settings:

- An interface is down.

- A route is down.
- A change in metric that results in the router selecting a new next hop.

Examples

The following example configures EIGRP address-family Ethernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Router(config)# router eigrp virtual-name

Router(config-router)# address-family ipv4 autonomous-system 5400
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# dampening-interval 45
```

The following example configures EIGRP service-family Serial interface 0 to limit the metric change frequency to no more than one change in a 30 second interval:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface serial0
Router(config-router-sf-interface)# dampening-interval 30
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
dampening-change	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
router eigrp	Configures the EIGRP address-family process.
service-family	Specifies service-family configuration mode.
sf-interface	Configures interface-specific commands under a service family.
shutdown	Disables service family on the interface.

debug eigrp service-family

To troubleshoot an Enhanced Interior Gateway Routing Protocol (EIGRP) service-family external client, client, neighbor, notification, topology, or a VRF instance, use the **debug eigrp service-family**command in privileged EXEC mode.

{**debug eigrp service-family** [**external-client** {**client** *client-label*| **messages** [*client-label*]| **protocol** [*client-label*]}]| {**ipv4**| **ipv6**} [[**vrf** *vrf-name*| *autonomous-system-number*| *service-instance-number*]| **client** *client-label*| **neighbor** *neighbor-ip-address*| **notifications topology** *service-instance-number*]}

Syntax Description

external-client	(Optional) Displays information for a Cisco SAF External Client.
client	Displays information for managing clients and TCP connections.
messages	(Optional) Reliability metric. The range is 0 to 255, entered in increments of 2.5 where 255 is 100-percent reliable.
protocol	(Optional) Displays information on an external-client protocol.
client-label	(Optional) Displays a **client**, **message**, or **protocol** debug for the specified Cisco SAF External Client.
ipv4	Specifies the IP Version 4 address family for this debug.
ipv6	Specifies the IP Version 6 address family for this debug.
vrf	(Optional) Specifies all virtual routing forwarding (VRF) instance tables or a specific VRF table for an IP address.
vrf-name	(Optional) Specifies a VRF table for an IP address.
autonomous-system-number	The Autonomous system number.
service-instance- number	(Optional) Service-instance number between 1 and 65535. Service instance numbers display as: service:subservice:instance.instance.instance.instance.
client	(Optional) Displays EIGRP client information.
client-label	(Optional) A specific client.

neighbors	(Optional) Displays EIGRP neighbor debugging information.
neighbor-ip- address	(Optional) The IP address of the neighbor.
notifications	(Optional) Displays EIGRP notification debugging information.
topology	(Optional) Specifies a service topology.
service-instance- number	(Optional) Service-instance number between 1 and 65535. Topology service instance numbers display as: service:subservice:instance.instance.instance.instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the debug service-routing xmcp command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the debug service-routing xmcp command.
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the debug service-routing xmcp command.

Usage Guidelines

Use the **debug eigrp service-family external-client client**command to display information to help manage clients and TCP connections. Use the **debug eigrp service-family external-client messages**command to display message content and decoded messages. Use the **debug eigrp service-family external-client protocol**command to display encode and decode information to help manage the interaction with the Cisco SAF internal API.

Note Using the **debug eigrp service-family ipv6** commands requires an IPv6-enabled SAF client, which currently does not exist.

Examples

```
The following is sample output of a Cisco SAF External-Client debugging message:
Router# debug eigrp service-family external-client messages

*Jun 11 14:25:10.051: 2 found c1 c1
*Jun 11 14:25:10.051: SAF-EC: 100 byte message from c1
*Jun 11 14:25:10.051: 0001 0050 7F5A 9BC7 D285 A1D8 3C54 552F 37AE 655B 0014 0005 2253 4146
 2200
*Jun 11 14:25:10.051: 0000 0006 0005 756E 616D 6500 0000 1005 0002 6331 0000 1003 0004 0001
 0000
*Jun 11 14:25:10.051: 1001 0002 6331 0000 1004 0004 0000 0005 0008 0014 45F4 57A9 42CF 0556
 4077
*Jun 11 14:25:10.051: 7AA3 B94A 703F 1BA3 ACA7
*Jun 11 14:25:10.051:
*Jun 11 14:25:10.051:
Class: Success Response Method: Register
*Jun 11 14:25:10.051: Packet Length: 52 Not including 20 byte Saf Header
*Jun 11 14:25:10.051: Magic Cookie: 7F5A9BC7 Transaction ID: D285A1D83C54552F37AE65
Router#5B
*Jun 11 14:25:10.051: Realm: 014: Length: 5: "SAF"
*Jun 11 14:25:10.051: Keep Alive: 1006: Length: 4: 360000
*Jun 11 14:25:10.051: Client Handle: 1002: Length: 4: 2
*Jun 11 14:25:10.051: Message Integrity: 008: Length: 20:
86839D4C64E36476D743AAF26112D28C32E3DF99
*Jun 11 14:25:10.051: 0101 0034 7F5A 9BC7 D285 A1D8 3C54 552F 37AE 655B 0014 0005 2253 4146
 2200
*Jun 11 14:25:10.051: 0000 1006 0004 0005 7E40 1002 0004 0000 0002 0008 0014 8683 9D4C 64E3
 6476
*Jun 11 14:25:10.051: D743 AAF2 6112 D28C 32E3 DF99
*Jun 11 14:25:10.055:
*Jun 11 14:25:10.055: SAF-EC: kicked timer 360000
The following is sample output of a Cisco SAF External-Client debugging protocol message:
Router# debug eigrp service-family external-client protocol

*Jun 11 14:27:11.467: SAF-EC: attribute found, type: 1005
*Jun 11 14:27:11.467: No error
*Jun 11 14:27:11.467:
Class: Request Method: Register
*Jun 11 14:27:11.467: Packet Length: 80 bytes Not including 20 byte Saf Header
*Jun 11 14:27:11.467: Magic Cookie: 7F5A9BC7 Transaction ID: 8F1F3F36EE43784D0DFABEA6
*Jun 11 14:27:11.467: Realm: 014: Length: 5: "SAF"
*Jun 11 14:27:11.467: Username: 006: Length: 5: uname
*Jun 11 14:27:11.467: Client Label: 1005: Length: 2: c1
*Jun 11 14:27:11.467: Protocol Version: 1003: Length: 4: 10000
*Jun 11 14:27:11.467: Client Name: 1001: Length: 2: c1
*Jun 11 14:27:11.467: Page Size: 1004: Length: 4: 5
Router#
*Jun 11 14:27:11.467: Message Integrity: 008: Length: 20:
AB3D7C39E4E0673B1539750D6E21A79ACFCE51F8
*Jun 11 14:27:11.467: SAF-EC: request start.
*Jun 11 14:27:11.467: SAF-EC: client successfully registered. client_handle 3
Router#
```

Related Commands

Command	Description
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP process.

Command	Description
service-family	Specifies service-family configuration mode.

default (SAF)

To reset an Enhanced Interior Gateway Routing Protocol (EIGRP) service-family external clients to their default values, use the **default** command in external-client configuration mode.

default{**exit**| **keepalive**| **password***password* | **username** *username*}

Syntax Description

client-name	Specifies a client name, entered up to 64 characters.

Command Default

The external-client options are set at their configured values.

Command Modes

External-client configuration (config-external-client-mode)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Examples

The following example sets an external-client named example to its keepalive default value:

```
Router(config)# service-family external-client listen ipv4 4533
Router(config-external-client)# external-client example
Router(config-external-client-mode)# default keepalive
```

Related Commands

Command	Description
external-client	Configures a Cisco SAF External-Client.
service-family external-client listen	Configure a Cisco SAF Forwarder listen TCP port for the Cisco SAF Forward to listen on,

default external-client

To reset Enhanced Interior Gateway Routing Protocol (EIGRP) service-family External Clients to their default values, use the **default external-client**command in external-client configuration mode.

default external-client *client-name*

Syntax Description

client-name	A Client name, up to 64 characters.

Command Default

The external-client options are set to their configured values.

Command Modes

External-client configuration (config-external-client)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Examples

The following example sets an External Client to its default values:

```
Router(config)# service-family external-client listen ipv4 4533
Router(config-external-client)# default external-client example
```

Related Commands

Command	Description
external-client	Configures a Cisco SAF External Client.
service-family external-client listen	Configure a TCP port for a Cisco External Client which interfaces to a Cisco SAF Forwarder.

domain

To define the service-routing domain associated with a specific client, use the **domain** command in XMCP client configuration mode. To remove this association, use the **no** form of this command.

domain *domain-number* {**default** | **only**}

no domain

Syntax Description

domain-number	The domain number to which the client is assigned.
default	Clients are assigned to domain 7177 by default, but may request a different domain.
only	Clients are not permitted to request a different domain.

Command Default

All clients are assigned to domain 7177 by default, but may request a different domain.

Command Modes

XMCP client configuration (config-xmcp-client)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **domain** command is used to define the default service-routing domain a client will register against. Clients may request a different domain to override this value unless the **only** keyword is configured.

When this command is configured or modified while clients are connected using this client configuration, all clients will be disconnected and must reconnect.

Examples

The following example restricts unauthenticated clients to domain 1228:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# client unauthenticated
Router(config-xmcp-client)# domain 1228 only
Router(config-xmcp-client)# end
```

The following example assigns clients connecting with username user1 to domain 47 by default, but permits them to request any other domain as an alternative:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# client username user1 password examplePASSWORD456
Router(config-xmcp-client)# domain 47 default
Router(config-xmcp-client)# end
```

Related Commands

Command	Description
client (XMCP)	Defines the properties of XMCP clients.
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

SAF Commands: eigrp log-neighbor-changes through hold-time

- eigrp log-neighbor-changes, page 40
- eigrp log-neighbor-warnings, page 42
- eigrp router-id, page 44
- eigrp stub (service-family), page 46
- exit-service-family, page 48
- exit-sf-interface, page 49
- exit-sf-topology, page 51
- external-client, page 53
- hello-interval, page 56
- hold-time, page 58

eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **eigrp log-neighbor-changes** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of changes in EIGRP neighbor adjacencies, use the **no**form of thiscommand.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af) Service-family configuration (config-router-sf)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the **no** form of this command.

To enable the logging of changes for EIGRP address-family neighbor adjacencies, use the **eigrp log-neighbor-changes**command in address-family configuration mode.

To enable the logging of changes for EIGRP service-family neighbor adjacencies, use the **eigrp log-neighbor-changes**command in service-family configuration mode.

Examples

The following configuration disables logging of neighbor changes for EIGRP process 209:

```
Router(config)# router eigrp 209
Router(config-router)# no eigrp log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 209:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp log-neighbor-changes
```

The following example shows how to disable logging of neighbor changes for EIGRP address-family with autonomous-system 4453:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# no eigrp log-neighbor-changes
Router(config-router-af)# exit-address-family
```

The following configuration enables logging of neighbor changes for EIGRP service-family process 209:

```
Router(config)# router eigrp 209
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp log-neighbor-changes
Router(config-router-sf)# exit-service-family
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no**form of thiscommand.

eigrp log-neighbor-warnings commandeigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range is from 1 to 65535. The default is 10.

Command Default

Neighbor warning messages are logged at 10-second intervals.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af) Service-family configuration (config-router-sf)

Command History

Release	Modification
12.0(5)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family and service-family configuration modes were added.
12.2(33)SRE	This command was modified. Address-family and service-family configuration modes were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With this command, you can disable and enable neighbor warning messages, and you can configure the interval between repeated neighbor warning messages.

To enable the logging of warning messages for an EIGRP address family, use the **eigrp log-neighbor-warnings** command in address-family configuration mode.

To enable the logging of warning messages for an EIGRP service family, use the **eigrp log-neighbor-warnings** command in service-family configuration mode.

Examples

The following command will log neighbor warning messages for EIGRP process 209 and repeat the warning messages in 5-minute (300 seconds) intervals:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the service family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the address family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp router-id

To set the router ID used by Enhanced Interior Gateway Routing Protocol (EIGRP) when communicating with its neighbors, use the **eigrp router-id**command in router configuration mode, address-family configuration mode, or service-family configuration mode. To remove the configured router ID, use the **no**form of thiscommand.

eigrp router-id *router-id*

no eigrp router-id [*router-id*]

Syntax Description

router-id	EIGRP router ID in IP address format.

Command Default

EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest local IP address is selected and loopback interfaces are preferred. The router ID is not changed unless the EIGRP process is removed with the **no router eigrp** command or if the router ID is manually configured with the **eigrp router-id** command.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af) Service-family configuration (config-router-sf)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. The router ID can be configured with any IP address with two exceptions; 0.0.0.0 and 255.255.255.255 are not legal values and cannot be entered. A unique value should be configured for each router.

In EIGRP named IPv4, named IPv6, and Cisco Service Advertisement Framework (SAF) configurations, the *router-id* is also included for identifying internal routes and loop detection.

Examples

The following example configures 172.16.1.3 as a fixed router ID:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp router-id 172.16.1.3
```

The following example configures 172.16.1.3 as a fixed router ID for service-family autonomous-system 4533:

```
Router(config)# router eigrp 209
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp router-id 172.16.1.3
```

The following example configures 172.16.1.3 as a fixed router ID for address-family autonomous-system 4533:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp stub (service-family)

To configure a router as an Enhanced Interior Gateway Routing Protocol (EIGRP) stub, use the **eigrp stub** command in service-family configuration mode. To disable the EIGRP stub routing feature, use the **no** form of this command.

eigrp stub [**receive-only**| **connected**]

no eigrp stub

Syntax Description

receive-only	(Optional) Sets the router as a receive-only neighbor.
connected	(Optional) Advertises connected routes.

Command Default

Stub routing is not enabled.

Command Modes

Service-family configuration (config-router-sf)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **eigrp stub command to configure a router as a stub that does not advertise all of its services to other routers.**

The **eigrp stub** command can be modified with several options. The **receive-only** keyword will restrict the router from sharing any of its services with any other router in that EIGRP autonomous system.

The **connected** keyword permits the EIGRP stub routing feature to send only connected services.

If no keywords are used with the **eigrp stub** command, the **eigrp stub connected** is configured, by default.

Note Multi-access interfaces, such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25, are supported by the EIGRP Stub Routing feature only when all routers on that interface, except the hub, are configured as stub routers.

Examples

The following example configures a router as a receive-only stub that advertises no services:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# eigrp stub receive-only
```

The following example configures a router as a stub that advertises only connected services:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# eigrp stub connected
```

The following example also configues a router as a stub that advertises only connected services:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# eigrp stub
```

Related Commands

Command	Description
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

exit-service-family

To exit Enhanced Interior Gateway Routing Protocol (EIGRP) service-family configuration mode, use the **exit-service-family**command in service-family configuration mode.

exit-service-family

Syntax Description

This command has no arguments or keywords.

Command Modes

Service-family configuration (config-router-sf)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **exit-service-family** command to exit service-family configuration mode and return to router configuration mode.

Examples

The following example exits service-family configuration mode:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# exit-service-family
Router(config-router)#
```

Related Commands

Command	Description
router eigrp	Configures the EIGRP process.
service-family	Specifies service-family configuration mode.

exit-sf-interface

To exit Enhanced Interior Gateway Routing Protocol (EIGRP) service-family interface configuration mode, use the **exit-sf-interface**command in service-family interface configuration mode.

exit-sf-interface

Syntax Description

This command has no arguments or keywords.

Command Modes

Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **exit-sf-interface** command to exit service-family interface configuration mode and return to service-family configuration mode.

Examples

The following example exits service-family interface configuration mode:

```
Router(config)# router eigrp virtual-name
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)# exit-sf-interface
Router(config-router-sf)#
```

Related Commands

Command	Description
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP process.
service-family	Specifies service-family configuration mode.

Command	Description
sf-interface	Configures interface-specific commands under a service family.
shutdown	Disables a service family on the interface.

exit-sf-topology

To exit Enhanced Interior Gateway Routing Protocol (EIGRP) service-family topology configuration mode, use the **exit-sf-topology**command in service-family topology configuration mode.

exit-sf-topology

Syntax Description

This command has no arguments or keywords.

Command Modes

Service-family topology configuration (config-router-sf-topology)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **exit-sf-topology** command to exit service-family topology configuration mode and return to service-family configuration mode.

Examples

The following example exits service-family topology configuration mode:

```
Router(config)# router eigrp virtual-name
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)#
```

Related Commands

Command	Description
exit-service-family	Exits service-family configuration mode.
exit-sf-interface	Exits service-family interface configuration mode.
router eigrp	Configures the EIGRP process.

Command	Description
service-family	Specifies service-family configuration mode.
sf-interface	Configures interface-specific commands undera service family.
topology	Enables topology configuration mode.

external-client

To configure a Cisco Service Advertisement Framework (Cisco SAF) External Client, use the **external-client** command in external-client configuration mode. To configure a Cisco SAF External Client to a topology, use the **external-client** command in service-family topology configuration mode. To remove the associated external-client configuration, use the **no** form of this command.

The **basename** keyword is only available in external-client configuration mode.

external-client *client-label* **basename**

no external-client

Syntax Description

client-label	A client label. The client label can be a maximum of 64 characters.
basename	Available only in external-client configuration mode. Specify the **basename** keyword in external-client configuration mode to allow SAF external clients to use a naming convention based on the client-label. The naming convention takes the form of *client-label*@[1-1024]. 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*).

Command Default

No service-family external-client configurations exist.

Command Modes

External-client configuration (config-external-client) Service-family topology (config-router-sf-topology)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Release	Modification
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.1(3)S	The maximum number of external clients was increased from 50 to 1024 in Cisco IOS Release 15.1(3)S.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the client (XMCP) command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the client (XMCP) command.
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the client (XMCP) command.

Usage Guidelines

Use the **external-client** command in service-family topology configuration mode to share the configuration with multiple clients. The **no** form of this command in service-family topology configuration mode removes a client in that topology. The **no** form of this command in external-client configuration mode removes the TCP connection from the clients to the forwarder.

Use the **service-family external-client listen** command in router configuration mode to configure a Cisco SAF External-Client listen port to which the external client can connect.

Note Using the **service-family external-client listen ipv6** commands requires an IPv6-enabled SAF client, which currently does not exist.

Examples

The following example assigns a Cisco SAF External Client with the username “example” to the topology base:

```
Router(config)# router eigrp virtual-name
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)# exit sf-interface
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# external-client example
```

Related Commands

Command	Description
service-family external-client listen	Configures a Cisco SAF Forwarder listen TCP port.
service-family	Specifies service-family configuration mode.
sf-interface	Configures interface-specific commands under a service family.

Command	Description
shutdown	Disables a specific routing instance without removing any existing configuration parameters for a service family.
topology	Configures service topology-specific commands for a service family.

hello-interval

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) address-family or service-family configurations, use the **hello-interval** command in address-family interface configuration mode or service-family interface configuration mode. To configure the default hello interval, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description

seconds	Hello interval in seconds. The range is 1 to 65535. The default is 60 for low-speed nonbroadcast multiaccess (NBMA) networks, and 5 for all other networks.

Command Default

The EIGRP hello interval is 60 seconds for low-speed NBMA networks and 5 seconds for all other networks.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The 60-second default applies only to low-speed, NBMA media. Low speed is considered a rate of T1 or slower, as specified by the **bandwidth** command in interface configuration mode.

For the purposes of EIGRP, Frame Relay and Switched Multimegabit Data Service (SMDS) networks are considered to be NBMA if the interface has not been configured to use physical multicasting. Otherwise, Frame Relay and SMDS networks are not considered to be NBMA.

Examples

The following example configures a 10-second hello interval for address-family Ethernet interface 0/0:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453

Router(config-router-af-interface)# af-interface ethernet0/0
Router(config-router-af-interface)# hello-interval 10
```

The following example sets a 10 second hello-interval for service-family Ethernet interface 0/0:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface Ethernet 0/0
Router(config-router-sf-interface)# hello-interval 10
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
hold-time	Configures the hold time for EIGRP address-family or service-family configurations.
router eigrp	Configures the EIGRP address-family process.
service-family	Specifies service-family configuration mode.
sf-interface	Configures interface-specific commands under a service family.

hold-time

To configure the hold time for Enhanced Interior Gateway Routing Protocol (EIGRP) address-family or service-family configurations, use the **hold-time** command in address-family interface configuration mode or service-family interface configuration mode. To configure the default hold time, use the **no** form of this command.

hold-time *seconds*

no hold-time

Syntax Description

seconds	Interval, in seconds, before a neighbor is considered down. Valid range is 1 to 65535 seconds (approximately 18 hours). The default is 180 seconds for low-speed nonbroadcast multiaccess (NBMA) networks and 15 seconds for all other networks.

Command Default

The EIGRP hold time is 180 seconds for NBMA networks and 15 seconds for all other networks.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

On very congested and large networks, the default hold time may not be sufficient for all routers and access servers to receive hello packets from neighbors. In this case, increase the hold time duration. The hold time should be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, services through this router are considered unavailable. Increasing the hold time will delay route convergence across the network.

Examples

The following example sets a 50-second hold time for address-family Ethernet interface 0/0:

```
Router(config)# router eigrp virtual-name

Router(config-router)# address-family ipv4 autonomous-system 4453

Router(config-router-af-interface)# af-interface ethernet0/0
Router(config-router-af-interface)# hold-time 50
```

The following example sets a 40-second hold time for service-family Ethernet interface 0/0:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface Ethernet 0/0
Router(config-router-sf-interface)# hold-time 40
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
router eigrp	Configures the EIGRP routing process.
hello-interval	Configures the hello interval for EIGRP address-family or service-family configurations.
router eigrp	Configures the EIGRP address-family process.
service-family	Specifies service-family configuration mode.
sf-interface	Configures interface-specific commands under service-family.

SAF Commands keepalive SAF through remote-neighbors SAF

- keepalive (SAF), page 62
- keepalive (XMCP), page 64
- key, page 66
- key chain, page 69
- key-string (authentication), page 72
- max-clients, page 75
- maximum-service (EIGRP), page 77
- metric weights (EIGRP), page 80
- neighbor (service-family), page 83
- nonce, page 87
- password (SAF), page 89
- remote-neighbors source, page 91

keepalive (SAF)

To specify a time interval for sending keepalives messages for a Cisco SAF External Clients, use the **keepalive** command in external-client configuration mode. To reset the keepalive to its default value, use the **no** form of this command.

keepalive *interval_in_milliseconds*

no keepalive

Syntax Description

interval_in_ milliseconds	The keepalive time interval in milliseconds, between 5000 and 3600000.

Command Default

7900 milliseconds.

Command Modes

External-client configuration (config-external-client-mode)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the keepalive (xmcp) command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the keepalive (xmcp) command.
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the keepalive (xmcp) command.

Usage Guidelines

Examples

The following example configures a keepalive of 8000 milliseconds for a Cisco SAF External Client named example.

```
Router(config)# service-family external-client listen ipv4 2444
Router(config-external-client)# external-client
 example
Router(config-external-client-mode)# keepalive
 8000
```

Related Commands

Command	Description
external-client	Configures a Cisco SAF External-Clients.
service-family external-client listen	Configures a Cisco SAF External-client listen TCP port.

keepalive (XMCP)

To define the keepalive interval associated with a specific client, use the **keepalive** command in XMCP client configuration mode. To reset the keepalive to its default value, use the **no** form of this command.

keepalive *seconds*

no keepalive

Syntax Description

seconds	Time, in seconds, after which a client will be assumed to be lost if no packets are received from the client during this interval. The valid range is 5 to 3600 seconds.

Command Default

The default is 8 seconds.

Command Modes

XMCP client configuration (config-xmcp-client)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **keepalive** command is used to define the length of time a client session will remain alive after receiving no further communication from the client. After the router receives any packet from the client, and the keepalive interval elapses with no further communication, the router will assume that the client has been lost and will terminate the connection.

Changes to this command will be applied to new client sessions but existing client sessions will continue to use the keepalive interval under which they were initially established.

Examples

The following example defines a keepalive interval of 30 seconds for unauthenticated clients:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# client unauthenticated
Router(config-xmcp-client)# keepalive 30
Router(config-xmcp-client)# end
```

Related Commands

Command	Description
client (XMCP)	Defines the properties of XMCP clients.
keepalive (SAF)	Specifies a time interval for sending keepalive messages for a Cisco SAF External Clients. This command is deprecated and replaced by the **keepalive (xmcp)** command.
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key commandkey *key-id*

no key *key-id*

Syntax Description

key-id	Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.

Command Default

No key exists on the key chain.

Command Modes

Key-chain configuration (config-keychain)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router
eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named chain1 for EIGRP service-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# network 10.0.0.0
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# authentication key-chain trees
```

```
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

key chain commandkey chain *name-of-chain*

no key chain *name-of-chain*

Syntax Description

name-of-chain	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.

Command Default

No key chain exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from

2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following named configuration example configures a key chain named trees for service-family. The key named chestnut will be accepted from 1:30 pm to 3:30 pm and be sent from 2:00 pm to 3:00 pm. The key birch will be accepted from 2:30 pm to 4:30 pm and be sent from 3:00 pm to 4:00 pm. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# sf-interface ethernet
Router(config-router-sf-interface)# authentication key chain trees
Router(config-router-sf-interface)# authentication mode md5
Router(config-router-sf-interface)# exit
Router(config-router-sf)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string chestnut
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
```

```
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string birch
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string**(authentication) command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

key-string commandkey-string *text*

no key-string *text*

Syntax Description

text	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.

Command Default

No authentication string for a key exists.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains. Each key can have only one key string.

If password encryption is configured (with the **service password-encryption** command), the software saves the key string as encrypted text. When you write to the terminal with the **more system:running-config** command, the software displays key-string 7 encrypted text.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from

2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.

Command	Description
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
service password-encryption	Encrypts passwords.
show key chain	Displays authentication key information.

max-clients

To limit the number of simultaneous client connections permitted, use the **max-clients** command in XMCP configuration mode. To remove this restriction, use the **no** form of this command.

max-clients {**unauthenticated** *number* [**total** *number*]| **total** *number* [**unauthenticated** *number*]}

Syntax Description

unauthenticated *number*	Maximum number of unauthenticated clients. The range is 1 to 1024.
total *number*	Maximum number of connected clients of any type. The range is 1 to 1024.

Command Default

Clients are limited only by available bandwidth and memory by default.

Command Modes

XMCP configuration (config-xmcp)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **max-clients** command is used to limit the number of simultaneous XMCP client connections. The limit can be applied to unauthenticated clients specifically and to all XMCP clients.

When the **max-clients** command is applied or modified while XMCP clients are connected, and the number of connected clients exceeds any of the new limits, the sessions of some existing clients (in no defined order) will be terminated until the total number falls within the new limits.

Examples

The following example permits a maximum of 10 unauthenticated clients at a time and no more than 20 clients total:

```
Router(config)# service-routing xmcp listen ipv4
Router(config-xmcp)# max-clients unauthenticated 10 total 20
Router(config-xmcp)# end
```

Related Commands

Command	Description
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

maximum-service (EIGRP)

To specify the maximum number of services that are permitted in a Cisco SAF service family, use the **maximum-service**command in service-family configuration mode. To disable this service, use the **no** form on this command.

maximum-service *number* [*threshold-value*] **dampened [default]** [*interface-type interface-number*]

no maximum-service

Syntax Description

number	Limit of maximum services, entered by a number from 1 to 4294967295.
threshold-value	(Optional) Threshold value (%) that enables a warning message, entered by a number between 1 and 100. The default is 75 percent.
dampened	(Optional) Exponentially increases the restart time interval.
reset-time	(Optional) Specifies the duration after which the restart history is cleared.
interval	(Optional) Specifies the reset-time interval, in minutes, entered using a number between 1 and 65535.
restart	(Optional) Automatically reestablishes a peering session that was disabled because the maximum-service limit had been exceeded.
interval	(Optional) Specifies the restart interval, in minutes, entered using a number between 1 and 65535.
restart-count	(Optional) Specifies the number of times a peer is auto-restarted.
count	(Optional) Specifies the number of times to restart, entered using a number between 1 and 65535.
warning-only	(Optional) Generates a warning-only message when the limit is exceeded.

Command Default

Command Modes

Service-family configuration (config-router-sf)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. The address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The address-family configuration mode was added.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

To specify how much memory is consumed from services received, use the **maximum-service**command in service-family configuration mode. To disable this function, use the **no** form on this command.

When the amount of memory exceeds the maximum amount configured, the router disables the peering session (by default):

- If the **restart** keyword is configured, the router automatically reestablishes the peering session at the configured time interval. If the restart interval is not configured, a disabled session stays down by default after the maximum-service limit is exceeded.
- If the **warning-only** keyword is configured, the router only sends a log message, but continues peering with the sender. If the neighbor is terminated, the neighbor remains down until the **clear eigrp service-family** command is configured.

Use the **show eigrp service-family ipv4** command with the **neighbor** keyword to verify neighbor configurations.

Examples

The following example sets the restart interval to 30 minutes, retries the restart 5 times, and clears the restart history after 60 minutes for service-family IPv4 autonomous-system 4533:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# maximum-service 1000 restart 30 restart-count 5 dampened
reset-time 60
```

The following example sets the maximum memory services to 1000 kilobytes, that are allowed from service-family IPv4 autonomous-system 4533:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# maximum-service 1000
```

The following example sets the maximum memory services to 500 kilobytes that are allowed from service-family IPv4 autonomous-system 4533 and configures a warning to display when the maximum-service limit has been exceeded.

```
Router(config)# router eigrp virtual-name
```

```
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# maximum-service 500 warning-only
```

Related Commands

Command	Description
clear eigrp service-family	Clears information for a Cisco SAF service family.
router eigrp	Configures the EIGRP process.
service-family	Configures commands under service-family mode.
sf-interface	Configures interface-specific commands under a service family.
show eigrp service-family	Displays information for a Cisco SAF service family.

metric weights (EIGRP)

To tune Enhanced Interior Gateway Routing Protocol (EIGRP) metric calculations, use the **metric weights** command in router configuration mode or address family configuration mode. To reset the values to their defaults, use the **no** form of this command.

metic weights *tos k1 k2 k3 k4 k5*

no metric weights

Syntax Description

tos	Type of service. This value must always be zero.
k1 k2 k3 k4 k5	Constants that convert an EIGRP metric vector into a scalar quantity. Valid values are 0 to 255. Default values are: • *tos:* 0 • *k1:* 1 • *k2:* 0 • *k3:* 1 • *k4:* 0 • *k5:* 0

Command Default

EIGRP metric K values are set to their default values.

Command Modes

Router configuration (config-router) Address family configuration (config-router-af)

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
15.0(1)M	This command was modified. The address-family configuration mode was added.
12.2(33)SRE	This command was modified. The address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The address-family configuration mode was added.

Usage Guidelines

Use this command to alter the default behavior of EIGRP routing and metric computation and allow the tuning of the EIGRP metric calculation for a particular type of service (ToS).

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

metric = [k1 * bandwidth + (k2 * bandwidth)/(256 - load) + k3 * delay]

If k5 does not equal zero, an additional operation is performed:

metric = metric * [k5/(reliability + k4)]

Bandwidth is inverse minimum bandwidth of the path in bps scaled by a factor of 2.56 * 1012. The range is from a 1200-bps line to 10 terabits per second.

Delay is in units of 10 microseconds. The range of delay is from 10 microseconds to 168 seconds. A delay of all ones indicates that the network is unreachable.

The delay parameter is stored in a 32-bit field, in increments of 39.1 nanoseconds. The range of delay is from 1 (39.1 nanoseconds) to hexadecimal FFFFFFFF (decimal 4,294,967,040 nanoseconds). A delay of all ones (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable.

The table below lists the default values used for several common media.

Table 1: Bandwidth Values by Media Type

Media Type	Delay	Bandwidth
Satellite	51,200,000 (2 seconds)	5120 (500 megabits)
Ethernet	25600 (1 millisecond [ms])	256,000 (10 megabits)
1.544 Mbps	51,200,000 (20 ms)	1,657,856 bits
64 kbps	51,200,000 (20 ms)	40,000,000 bits
56 kbps	51,200,000 (20 ms)	45,714,176 bits
10 kbps	51,20,000 (20 ms)	256,000,000 bits
1 kbps	51,200,000 (20 ms)	2,560,000,000 bits

Reliability is given as a fraction of 255. That is, 255 is 100 percent reliability or a perfectly stable link.

Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

Examples

The following example sets the metric weights to slightly different values than the defaults:

```
Router(config)# router eigrp 109
Router(config-router)#
network 192.168.0.0
Router(config-router)# metric weights 0 2 0 2 0 0
```

The following example configures an address-family metric weight to tos: 0; K1: 2; K2: 0; K3: 2; K4: 0; K5: 0.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4533
Router(config-router-af)# metric weights 0 2 0 2 0 0
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
bandwidth (interface)	Sets a bandwidth value for an interface.
delay (interface)	Sets a delay value for an interface.
ipv6 router eigrp	Configures the EIGRP for IPv6 routing process.
metric holddown	Keeps new EIGRP routing information from being used for a certain period of time.
metric maximum-hops	Causes the IP routing software advertise as unreachable routes with a hop count higher than is specified by the command (EIGRP only).
router eigrp	Configures the EIGRP address-family process.

neighbor (service-family)

To configure properties of an Enhanced Interior Gateway Routing Protocol (EIGRP) service-family neighbor, use the **neighbor**command in service-family configuration mode. To remove the properties of the neighbor, use the **no** form of this command.

neighbor *ip-address* {*interface-type interface-number*| **loopback** *loopback-interface-number* [**remote** *maximum-hops*]| **description** *description-string* **maximum-service** *maximum-service-limit* [*threshold-value*] **[warning-only]**| **dampened** [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*]}

no neighbor *ip-address* {*interface-type interface-number*| **loopback** *loopback-interface-number*| **description** *description-string*| **maximum-service**}

Syntax Description

ip-address	IP address of the service-family neighbor, in A.B.C.D. format.
interface-type	Specifies the interface type.
interface-number	Specifies the interface number.
loopback	Specifies the loopback interface.
loopback-interface- number	Specifies the loopback interface number.
remote	(Optional) Specifies that the neighbor is remote.
maximum-hops	(Optional) Specifies the maximum number of hops, entered using a number from 3 to 100.
description	(Optional) Specifies a description for the neighbor.
description-string	Specifies the description string for the neighbor.
maximum-service	(Optional) Configures the maximum number of services acceptable from all neighbors.
maximum-service- limit	Specifies the limit of maximum services, entered by a number from 1 to 4294967295.
threshold-value	(Optional) Threshold value (%) that enables a warning message, entered by a number between 1 and 100. The default is 75 percent.
warning-only	(Optional) Generates a warning-only message when the configured limit is exceeded.
dampened	(Optional) Exponentially increases the restart-time interval.

reset-time	(Optional) Specifies the duration after which the system clears the restart history.
minutes	(Optional) Specifies the reset-time interval, in minutes, entered using a number between 1 and 65535.
restart	(Optional) Automatically reestablishes a peering session that was disabled because the maximum-service limit had been exceeded.
minutes	(Optional) Specifies the restart interval, in minutes, entered using a number between 1 and 65535.
restart-count	(Optional) Specifies the number of times that a peer is auto-restarted.
number	(Optional) Specifies the restart-count interval in minutes, entered using a number between 1 and 65535.

Command Default

No neighbor establishments are configured.

Command Modes

Service-family configuration (config-router-sf)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

To configure a neighbor router with which to exchange routing information, use the **neighbor**command in service-family configuration mode. This command permits the point-to-point (non-broadcast) exchange of routing information. You can repeat this command to configure multiple neighbors.

Use the **neighbor** *ip-address* **loopback** *interface-number* **remote** *maximum-hops*command to configure neighbors that are multiple hops away and are not on the same subnet as the router. This command can be used only with loopback interfaces.

To configure the amount of memory used to store services from all EIGRP service-family neighbors, use the **neighbor maximum-service**command in service-family configuration mode. To disable this function, use the **no** form on this command.

When the amount of memory exceeds the maximum amount configured, the router disables the peering session (by default):

- If the **restart** keyword is configured, the router automatically reestablishes the peering session at the configured time interval. If the restart-interval is not configured, a disabled session stays down by default after the maximum-service limit is exceeded.
- If the **warning-only** keyword is configured, the router sends only a log message, but continues peering with the sender. If the neighbor is terminated, the neighbor remains down until the **clear eigrp service-family** command is configured.

Use the **show eigrp service-family ipv4** command with the **neighbor** keyword to verify neighbor configurations.

Examples

The following example sets the maximum hops to three for the remote neighbor 10.1.10.2 on Ethernet interface 0/0:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# neighbor 10.1.10.2
Router(config-router-sf)# Ethernet 0/0
Router(config-router-sf)# remote 3
```

The following example sets the restart interval to 30 minutes, retries the restart five times, and clears the restart history after 60 minutes for neighbor 10.1.10.1:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# neighbor 10.1.10.1
Router(config-router-sf)# reset-time 60
```

The following example set the maximum memory services to 1000 kilobytes that are allowed from neighbor 10.1.10.1:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# neighbor 10.1.10.1
Router(config-router-sf)# maximum-service 1000
```

The following example set the maximum memory services to 500 kilobytes that are allowed from neighbor 10.1.10.1 and configures a warning to display when the maximum-service limit has been exceeded:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# neighbor 10.1.10.1
Router(config-router-sf)# maximum-service 500 warning-only
```

Related Commands

Command	Description
clear eigrp service-family	Clears information for a Cisco SAF service family.
neighbor peer-group	Configures an EIGRP service-family neighbor to a peer group.

Command	Description
router eigrp	Configures the EIGRP process.
service-family	Configures commands under service-family mode.
sf-interface	Configures interface-specific commands under service-family.

nonce

To define the lifetime of the authentication nonces provide to a client, use the **nonce lifetime** command in XMCP client configuration mode. To disable nonces, use the **nonce none** command. To restore the default nonce lifetime, use the **no** form of this command.

nonce {**lifetime** *seconds*| **none**}

no nonce

Syntax Description

lifetime *seconds*	Duration, in seconds, for which each issued nonce will remain valid. Valid range is 5 to 3600.
none	Disables nonces.

Command Default

The default nonce lifetime is 800 seconds.

Command Modes

XMCP client configuration (config-xmcp-client)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **nonce** command is used to define how long each authentication nonce remains valid after first being issued to an XMCP (Extensible Messaging Client Protocol) client. When the nonce lifetime expires, the nonce is invalidated, and Cisco IOS software will issue a new nonce to the client after receiving (and rejecting) a request using the previous expired nonce. Configuring a shorter nonce lifetime provides greater security against packet replay attacks but at the cost of more processing and communication overhead on the client and the Cisco IOS router.

Nonces are not used with unauthenticated clients. Therefore this command may be configured only in conjunction with the **client username** command.

In security engineering, nonce is an abbreviation of a number used once. It is often a random or pseudorandom number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. For example, nonces are used in HTTP digest access authentication to calculate an MD5 (Message Digest-5) digest of the password. The nonces are different each time the 401 authentication challenge response code is presented, thus making replay attacks virtually impossible.

Examples

The following example defines a nonce lifetime of 100 seconds for clients using username user1:

```
Router(config)# service-routing XMCP listen
Router(config-xmcp)# client username user1 password exampleexample111
Router(config-xmcp-client)# nonce lifetime 100
Router(config-xmcp-client)# end
```

Related Commands

Command	Description
client (XMCP)	Defines the properties of XMCP clients.
client username	Defines the properties of XMCP clients.
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

password (SAF)

To configure a password for a Cisco SAF External Client, use the **password**command in external-client label configuration mode. To reset the password, use the **no** form on this command.

password *password-name*

no password *password-name*

Syntax Description

password-name	Specifies the name of the password for a Cisco SAF External-Client, entered using 11 to 64 characters.

Command Default

No passwords are configured.

Command Modes

External-client label configuration (config-external-client-mode)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the client (xmcp) command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the client (xmcp) command.
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the client (xmcp) command.

Usage Guidelines

Use the **password** command to set a password for a Cisco SAF External Client.

Examples

The following example configures a password named example for a Cisco SAF External Client:

```
Router(config)# service-family external-client listen ipv4 2444
Router(config-external-client)# external-client
 example
Router(config-external-client-mode)# password
 example
```

Related Commands

Command	Description
external-client	Configures Cisco SAF External-Clients.
service-family external-client listen	Configures Cisco SAF External-client listen TCP ports.

remote-neighbors source

To configure a Service Advertisement Framework (SAF) process that enables remote neighbors to accept inbound connections from any remote IP address, use the **remote-neighbors source** command in service-family configuration mode. To remove the configuration, use the no form of this command.

remote-neighbors source *interface* {**unicast-listen** | **multicast-group** *group-address*} [**allow-list** *access-list-name*] [**max-neighbors** *max-remote-peers*]

no remote-neighbors source

Syntax Description

Interface	Specifies the loopback interface to use as the source for packets that are sent to remote neighbors. Only loopback interfaces are permitted.
unicast-listen	Accepts connections initiated by remote neighbors and forms remote neighbor relationships without having to manually configure the remote neighbor IP address.
multicast-group	Uses IP multicast to discover remote neighbors and form remote neighbor relationships.
group-address	Multicast address that EIGRP will use to discover remote neighbors and exchange information. Only routers using the same group address will discover one another as neighbors.
allow-list (Optional)	Uses an access list (Access Control List) to specify the remote IP addresses from which EIGRP neighbor connections may be accepted. If you do not use the **allow-list** keyword, then all IP addresses (permit any) will be accepted.
access-list-name (Optional)	Name of the access list to use with the **allow-list** keyword.
max-neighbors (Optional)	Uses a maximum number of remote neighbors. If you do not use this keyword, the maximum number of remote neighbors is limited only by available memory and bandwidth.
max-remote-peers (Optional)	Maximum number of remote neighbors that a member of the multicast group may accept. The range is from 1 to 65535.

Command Default No remote neighbors are specified.

Command Modes Service-family configuration (config-router-sf)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T

Usage Guidelines Configure the **allow-list** keyword for enhanced security. This keyword allows only specific IP addresses to connect to the remote neighbor.

Examples The following example shows how to use unicast to configure remote neighbors to accept inbound connections from IP addresses that match an access list:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf-interface)# remote-neighbors source Loopback1 unicast-listen
allow-list myNeighborList
```

The following example shows how to use multicast to discover similarly configured routers as remote neighbors, with no restriction on neighbor IP addresses (no allow-list specified), and a maximum of 30 neighbors:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf-interface)# remote-neighbors source Loopback2 multicast-group
224.44.56.1 max-neighbors 30
```

Related Commands

Command	Description
service-family (SAF)	Enters service-family configuration mode.
neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information on a router that is running Enhanced Interior Gateway Routing Protocol (EIGRP).

SAF Commands send-lifetime through username SAF

- send-lifetime, page 94
- service-family, page 97
- service-family external-client listen, page 99
- service-routing xmcp listen, page 101
- sf-interface, page 103
- show eigrp plugins, page 105
- show eigrp protocols, page 108
- show eigrp service-family external-client, page 111
- show eigrp service-family ipv4 topology, page 114
- show eigrp service-family ipv6 topology, page 118
- show eigrp tech-support, page 122
- show service-routing capabilities-manager, page 125
- show service-routing capabilities-manager internal, page 128
- show service-routing plugins capman, page 130
- show service-routing xmcp clients, page 132
- show service-routing xmcp server, page 135
- split-horizon (EIGRP), page 137
- timers graceful-restart purge-time, page 139
- topology, page 142
- username (SAF), page 144

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

send-lifetime *start-time* {**infinite**| *end-time*| **duration** *seconds*}

no send-lifetime *start-time* {**infinite**| *end-time*| **duration** *seconds*}

Syntax Description

start-time	Beginning time that the key specified by the **key** command is valid to be sent. The syntax can be either of the following: *hh* **:** *mm* **:** *ss* *Month date year* *hh* **:** *mm* **:** *ss* *date Month year* • *hh* --hours • *mm* --minutes • *ss* -- seconds • *Month* -- first three letters of the month • *date* -- date (1-31) • *year*-- year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be sent from the *start-time* value on.
end-time	Key is valid to be sent from the *start-time* value until the *end-time*value. The syntax is the same as that for the *start-time*value.The *end-time* value must be after the *start-time*value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be sent.

Command Default

Forever (the starting time is January 1, 1993, and the ending time is infinite)

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you intend to set lifetimes on keys.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# af-interface ethernet0/0
```

```
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
show key chain	Displays authentication key information.

service-family

To configure virtual routing and forwarding (VRF) metrics for a Cisco SAF service-family, use the **service-family** command in router configuration mode. To disable the service-family configuration, use the **no** form of this command.

service-family {**ipv4 | ipv6**}[**vrf** *vrfname*]**autonomous-system** *autonomous-system number*

no service-family {**ipv4 | ipv6**}[**vrf** *vrfname*]**autonomous-system** *autonomous-system number*

Syntax Description

ipv4	Specifies the IP Version 4 address family and enters service-family configuration mode.
ipv6	Specifies the IP Version 6 address family and enters service-family configuration mode.
vrf	(Optional) Specifies all virtual routing forwarding (VRF) instance tables or a specific VRF table for an IP address.
vrf-name	(Optional) Names a specific VRF table for an IPv4 address.
autonomous- system	Specifies the autonomous system.
autonomous-system-number	Specifies the autonomous system number.

Command Default

No service family configurations exist.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. The address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The address-family configuration mode was added.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **service-family** command to enter service-family configuration mode.

Note Using the **service-family ipv6** commands requires an IPv6-enabled SAF client, which currently does not exist.

Examples

The following example configures a service-family autonomous-system number 4533:

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

Related Commands

Command	Description
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP process.

service-family external-client listen

To configure a Cisco SAF External-Client TCP port, use the **service-family external-client listen**command in global configuration mode. To remove the associated external-client configuration, use the **no** form on this command.

service-family external-client listen {**ipv4**| **ipv6**} *tcp-port-number vrf-name*

no service-family external-client listen

Syntax Description

ipv4	Specifies the IP Version 4 address family.
ipv6	Specifies the IP Version 6 address family.
tcp-port-number	The TCP port number to listen on. Port numbers range between 1024 and 65536.
vrf-name	VRF name to listen on. Default is base.

Command Default

No external-client configurations exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. The address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The address-family configuration mode was added.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the service-routing xmcp listen command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the service-routing xmcp listen command.

Release	Modification
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the service-routing xmcp listen command.

Usage Guidelines

Use the **service-family external-client listen**command to configure a TCP port on which the Cisco SAF Forwarder is to listen. The **no** form of this command removes all clients from the Cisco SAF network, the External-Client database, tears down all sockets, and removes the TCP listen socket.

Note Using the **service-family external-client listen ipv6** commands requires an IPv6-enabled SAF client, which currently does not exist.

Use the **show eigrp service-family external-client** command to verify information on EIGRP external clients.

Examples

The following example configures an external-client TCP port number 4355 for the Cisco SAF Forwarder to listen on:

```
Router(config)# service-family external-client listen ipv4 4355
```

Related Commands

Command	Description
show eigrp service-family external-client	Displays information on Cisco SAF External Clients.

service-routing xmcp listen

To enable XMCP (Extensible Messaging Client Protocol) on a port and to configure parameters for accepting client connections, use the **service-routing xmcp listen** command in global configuration mode. To disable XMCP on a port, use the **no** form of this command.

service-routing xmcp listen [**ipv4**| **ipv6**] [**transport tcp**] [**port** *port-number*][**vrf** *vrf-name*]

Syntax Description

ipv4	(Optional) Allows connections from IPv4 clients only.
ipv6	(Optional) Allows connections from IPv6 clients only.
transport tcp	(Optional) Allows connections over TCP only. Specifying this keyword restricts clients to TCP only because UDP is unsupported; however, this configuration is implied even if it is not specified.
port *port-number*	(Optional) Specifies a TCP or UDP port number. The range is 1024 to 65536. If the **port** keyword is not specified, the port number defaults to 4788.
vrf *vrf-name*	(Optional) Allows connections within a specific VRF (virtual routing and forwarding) instance. If the **vrf** keyword is not specified, clients may connect only using the default IP routing table.

Command Default

XMCP is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **service-routing xmcp listen** command is used to configure a router to listen for XMCP client connections, optionally under a specific transport protocol.

If neither the **ipv4** nor the **ipv6** keyword is specified, clients are permitted to connect over either protocol.

Only a single **service-routing xmcp listen** command can be configured on a router. Once configured, you can only change this command by configuring the **no service-routing xmcp listen** command.

Examples

The following example configures XMCP with its default behavior, which is to accept IPv4 and IPv6 connections over TCP on port 4788:

```
Router(config)# service-routing xmcp listen
Router(config-xmcp)# end
```

The following example configures XMCP to accept only client connections using TCP over IPv6 on port 2100:

```
Router(config)# service-routing xmcp listen ipv6 transport tcp port 2100
Router(config-xmcp)# end
```

Related Commands

Command	Description
client (XMCP)	Defines properties for XMCP clients.
service-family external-client	Configures a Cisco SAF External-Client TCP port. This command is deprecated. It is replaced by the **routing xmcp listen** command.

sf-interface

To configure interface-specific commands for a Cisco SAF service family, use the **sf-interface** command in service-family configuration mode. To disable the service-family mode, use the **no** form on this command.

sf-interface {*interface-type interface-number*| **default**}

no sf-interface {*interface-type interface-number*| **default**}

Syntax Description

interface-type	Specifies the interface type.
interface-number	Specifies the interface number.
default	Specifies the service-family default interface configuration.

Command Modes

Service-family configuration (config-router-sf)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was modified. The address-family configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The address-family configuration mode was added.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **sf-interface default**command to set the Cisco SAF default configuration for all interfaces on the router.

Use the **sf-interface** *interface-type interface-number*command to apply a Cisco SAF configuration to a specific interface. Any configuration using this command overrides the default configuration.

Examples

The following example places a router in service-family configuration mode and enables Ethernet interface 0/0, while disabling all other interfaces:

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

```
Router(config-router-sf)# sf-interface default
Router(config-router-sf-interface)# shutdown
Router(config-router-sf-interface)# Ethernet 0/0
Router(config-router-sf-interface)# no shutdown
```

Related Commands

Command	Description
exit-service-family	Exits service-family configuration mode.
exit sf-interface	Exits service-family interface configuration mode.
router eigrp	Configures the EIGRP process.
service-family	Configures commands under service-family mode.
shutdown	Disables a service family on the interface.

show eigrp plugins

To display general information including the versions of the Enhanced Interior Gateway Routing Protocol (EIGRP) protocol features that are currently running, use the **show eigrp plugins** command in user EXEC or privileged EXEC mode.

show eigrp [**vrf** *name*] [*as-number*] **plugins** [*pluginname*] **[detailed]**

Syntax Description

vrf *-name*	(Obsolete) (Optional) Specifies a particular VPN routing and forwarding (VRF) instance name. **Note** This keyword and argument are obsolete and configuring them has no effect on the output displayed.
as-number	(Obsolete) (Optional) Autonomous system number. **Note** This argument is obsolete and configuring it has no effect on the output displayed.
plugin-name	(Optional) Name of an EIGRP plugin to display.
detailed	(Optional) Displays detailed information about EIGRP features.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.0(1)M	This command was modified. The **vrf** keyword, the *name*, and the *as-number*arguments were removed.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use the **show eigrp plugins** command in user EXEC or privileged EXEC mode to determine if a particular EIGRP feature is available in your Cisco IOS image. This command displays a summary of information about EIGRP service families and address families.

This command is useful when contacting Cisco technical support.

Examples

The following example shows how to display EIGRP plugin information:

```
Router# show eigrp plugins
EIGRP feature plugins:::
    eigrp-release      :   5.00.00 : Portable EIGRP Release
                       :  19.00.00 : Source Component Release(rel5)
    igrp2              :   3.00.00 : Reliable Transport/Dual Database
    bfd                :   1.01.00 : BFD Platform Support
    mtr                :   1.00.01 : Multi-Topology Routing(MTR)
    eigrp-pfr          :   1.00.01 : Performance Routing Support
    ipv4-af            :   2.01.01 : Routing Protocol Support
    ipv4-sf            :   1.01.00 : Service Distribution Support
    external-client    :   1.02.00 : Service Distribution Client Support
    ipv6-af            :   2.01.01 : Routing Protocol Support
    ipv6-sf            :   1.01.00 : Service Distribution Support
    snmp-agent         :   1.01.01 : SNMP/SNMPv2 Agent Support
```

The table below describes the significant fields shown in the display.

Table 2: show eigrp plugins Field Descriptions

Field	Description
eigrp release	Displays the portable EIGRP release version.
igrp2	Displays the reliable transport and dual database version.
bfd	Displays the EIGRP-BFD feature version.
mtr	Displays the EIGRP multitopology routing (MTR) version.
eigrp-pfr	Displays the EIGRP performance routing feature version.
ipv4-af	Displays the EIGRP IPv4 routing protocol feature version.
ipv4-sf	Displays the EIGRP IPv4 service distribution feature version.
external-client	Displays the EIGRP service distribution client support feature version.
ipv6-af	Displays the EIGRP IPv6 routing protocol feature version.

Field	Description
ipv6-sf	Displays the EIGRP IPv6 service distribution feature version.
snmp-agent	Displays the EIGRP SNMP and SNMPv2 Agent Support version.

Related Commands

Command	Description
clear eigrp service-family	Clears entries from the EIGRP neighbor table.
show eigrp service-family external-client	Displays information about the EIGRP service-family external clients.
show eigrp service-family ipv4 topology	Displays information from the EIGRP IPv4 service-family topology table.
show eigrp service-family ipv6 topology	Displays information from the EIGRP IPv6 service-family topology table.
show eigrp tech-support	Generates a report of all EIGRP-related information.

show eigrp protocols

To display general information about Enhanced Interior Gateway Routing Protocol (EIGRP) protocols that are currently running, use the **show eigrp protocols** command in user EXEC or privileged EXEC mode.

show eigrp protocols [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about the specified VRF.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **show eigrp protocols**command in user EXEC or privileged EXEC mode to see a summary of information on EIGRP IPv4 service families or address families.

Examples

The following example shows how to display general EIGRP information:

```
Router# show eigrp protocols
EIGRP-IPv4 Protocol for AS(10)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 1.1.1.1
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
EIGRP-IPv4 Protocol for AS(5) VRF(red)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 1.1.1.1
Topology : 0 (base)
Active Timer: 3 min
```

```
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
Total Prefix Count: 0
Total Redist Count: 0
```

The following example shows how to display general EIGRP information for VRF1:

```
Router# show eigrp protocols vrf vrf1
EIGRP-IPv4 Protocol for AS(5) VRF(vrf1)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 1.1.1.1
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
Total Prefix Count: 0
Total Redist Count: 0
```

The table below describes the significant fields shown in the display.

Table 3: show eigrp protocols Field Descriptions

Field	Description
EIGRP-IPv4 Protocol for AS(10)	EIGRP instance and AS number.
Metric weight	EIGRP metric calculations.
NSF-aware route hold timer	Route-hold timer value for an NSF-aware router.
Router-ID	Router ID.
Topology	Number of entries in the EIGRP topology table.
Active Timer	EIGRP routing active time limit.
Distance	Internal and external administrative distance.
Maximum path	Maximum number of parallel routes that EIGRP can support.
Maximum hop count	Maximum hop count (in decimal).
Maximum metric variance	Metric variance used to find feasible paths for a route.
EIGRP-IPv4 Protocol	EIGRP instance and AS number for VRF Red.
Total Prefix Count	The aggregate sum of the prefixes in an EIGRP instance topology table. It includes prefixes learned from all neighbors or from redistribution.
Total Redist Count	The number of prefixes redistributed into an EIGRP process.

Related Commands

Command	Description
clear eigrp service-family	Clears entries from the EIGRP neighbor table.
show eigrp service-family external-client	Displays information about the EIGRP service-family external clients.
show eigrp service-family ipv4 topology	Displays information from the EIGRP IPv4 service-family topology table.
show eigrp service-family ipv6 topology	Displays information from the EIGRP IPv6 service-family topology table.
show tech-support	Generates a report of all EIGRP-related information.

show eigrp service-family external-client

To display information about Cisco Service Advertisement Framework (Cisco SAF) external clients, use the **show eigrp service-family external-client**command in user EXEC or privileged EXEC mode.

show eigrp service-family external-client[*client-label*]

Syntax Description

client-label	(Optional) Displays detailed client information for the specified client label.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.1(2)S	The command was modified. The output was revised to include additional information about the clients, such as basename and socket ID.
Cisco IOS XE Release 3.3S	The command was modified. The output was revised to include additional information about the clients, such as basename and socket ID.
15.1(3)S	The command was modified. The output was revised to remove the PID (Process ID) column.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the show service-routing xmcp clients command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the show service-routing xmcp clients command.
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the show service-routing xmcp clients command.

Usage Guidelines

Use the **show eigrp service-family external-client**command in user or privileged EXEC mode to see a summary of the information about Cisco SAF external clients that are currently registered with the Cisco SAF system.

Examples

The following is sample output from the **show eigrp service-family external-client**command if any clients are registered:

```
Router# show eigrp service-family external-client
SAF External Clients
example-using-basename (basename)
  Client  Socket   Keep  Address                                    Port  Tag
  Handle  FD       (ms)
  1       1     3268319  10.1.1.1                                  47519  @12
  2       2     3268347  192.168.100.101                           36997  @1
example-configured-but-no-clients-connected
  No connected clients
example-client-without-basename
  Client  Socket   Keep  Address                                    Port  Tag
  Handle  FD       (ms)
  3       3      208373  10.1.1.2                                  51294  --
```

The table below describes the significant fields shown in the display.

Table 4: show eigrp service-family external-client Field Descriptions

Field	Description
Client Handle	Specifies the Cisco SAF internal client handle.
Socket FD (File Descriptor)	Specifies the socket API file descriptor for this Cisco SAF External Client.
Keep (ms)	Specifies the remaining keepalive time (in milliseconds) before the client will be disconnected if no further communications are received from the client.
Address	Specifies the IP address of the selected external client.
Port	Specifies the TCP port number of the selected external client.
Tag	Specifies the identifying tag provided by the client if the *client-label* argument was configured using the **basename** keyword. The **basename** keyword allows SAF external clients to uniquely identify themselves using the naming convention in the form of *client-label@tag* (where tag is a number from 1 to 50).

The following is sample output from the **show eigrp service-family external-client** *client-label*command if the specified client is registered:

```
Router# show eigrp service-family external-client example-using-basename@12
SAF External Client "example-using-basename" (basename)
  Listening on port 1024, keepalive time 3600000 ms
  VR(saf) SFv4 AS(1) Topology(base)
  Client  Socket   Keep  Address                                    Port  Tag
  Handle  FD       (ms)
  1       1     3322871  10.1.1.1                                  47519  @12
    Client name "thisistheclientnameweprovided"
    Page size 1, currently allowed to send 1
    Protocol version 1.0
    2 subscriptions
```

The table below describes the significant fields shown in the display.

Table 5: show eigrp service-family external-client client-label Field Descriptions

Field	Description
Client name	Specifies the descriptive name provided by the client to identify itself.
Page size	Specifies the page size provided by the client and specifies the number of additional requests allowed to be sent at the time the **show** command is issued (between 0 and the number specified for Page size).
Protocol version	Specifies the version of the SAF External Client protocol being used by the client to communicate with the SAF forwarder.
subscriptions	Specifies the number of SAF subscriptions owned by the client. When the number of subscriptions is 0, this field displays “No subscriptions”.

Related Commands

Command	Description
clear eigrp service-family	Clears entries from the EIGRP neighbor table.
show eigrp service-family	Displays EIGRP IPv4 service-family information.
show eigrp service-family ipv4 topology	Displays information in the EIGRP IPv4 service-family topology table.
show eigrp service-family ipv6 topology	Displays information in the EIGRP IPv6 service-family topology table.
external-client	Configures a Cisco SAF Service Advertisement Framework (Cisco SAF) External Client.

show eigrp service-family ipv4 topology

To display topology information for an Enhanced Interior Gateway Routing Protocol (EIGRP) IPv4 service family, use the **show eigrp service-family ipv4 topology**command in user EXEC or privileged EXEC mode.

show eigrp service-family ipv4 [**vrf** *vrf-name*] *autonomous-system-number* **topology** [*service-instance-number*| **active**| **all-links**| **detail-links**| **pending service-type** [**connected**| **external**| **internal**| **local**| **redistributed**| **summary**]| **summary**| **zero-successors**]

Syntax Description

vrf	(Optional) Specifies all virtual routing forwarding (VRF) instance tables or a specific VRF table for an IP address.
vrf-name	(Optional) Names a specific VRF table for an IPv4 address.
autonomous-system-number	Specifies the autonomous-system number.
service-instance- number	(Optional) Displays detailed information about the specified service-instance number. Service-instance numbers display as service:subservice:instance.instance.instance.instance. Service-instance numbers can range from 1:1:0.0.0.1 to 65534:65534:FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFE.
active	(Optional) Displays only active entries in the topology table.
all-links	(Optional) Displays all service sources (including non-feasible sources) in the topology table.
detail-links	(Optional) Specifies all links in the topology table.
pending	(Optional) Displays all active entries in the topology table that are waiting either for an update or reply from a neighbor.
service-type	(Optional) Specifies the service with the given type in the topology table.
connected	(Optional) Displays only connected services.
external	(Optional) Displays all external services.
internal	(Optional) Displays all internal services.
local	(Optional) Display all locally originated services.

redistributed	(Optional) Displays all redistributed services.
summary	(Optional) Displays all summary services.
summary	(Optional) Specifies a summary of the topology table.
zero-successors	(Optional) Displays only services in the topology table that have zero successors.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **show eigrp service-family ipv4 topology**command in user EXEC or privileged EXEC mode to see a summary of information on EIGRP IPv4 service-families services.

Examples

The following is sample output from the **show eigrp service-family ipv4 topology** command:

```
Router> enable
Router# show
 eigrp service-family ipv4 4453 topology
EIGRP-SFv4 Topology Table for process 4453
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status
P 1:2:0.0.0.3, 2 successors, FD is 0
 via 10.16.80.28 (46251776/46226176), Ethernet0
 via 10.16.81.28 (46251776/46226176), Ethernet1
 via 10.16.80.31 (46277376/46251776), Serial0
P 4:5:0.0.0.6, 1 successors, FD is 37200
 via Connected, Ethernet1
 via 10.16.81.28 (307200/281600), Ethernet1S
 via 10.16.80.28 (307200/281600), Ethernet0
 via 10.16.80.31 (332800/307200), Serial0
```

The following is sample output from the **show eigrp service-family ipv4 topology** command for a specified service:

```
Router> enable
Router# show
 eigrp service-family ipv4 4453 topology 1:2:0.0.0.3
EIGRP-SFv4 VR(example) Topology Table entry for AS(4453)/ID(10.1.1.1)1:2:0.0.0.3
```

```
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
Service Description Blocks:
1:2:3.0.0.0.3 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
Composite metric is (409600/128256), Route is External
Vector metric:
 Minimum bandwidth is 10000 Kbit
 Total delay is 6000 microseconds
 Reliability is 255/255
 Load is 1/255
 Minimum MTU is 1500
 Hop count is 1
External data:
 Originating router is 10.89.245.1
 AS number of route is 0
 External protocol is Connected, external metric is 0
 Administrator tag is 0 (0x00000000)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status
P 1:2:0.0.0.3, 2 successors, FD is 0
 via 10.16.80.28 (46251776/46226176), Ethernet0
 via 10.16.81.28 (46251776/46226176), Ethernet1
 via 10.16.80.31 (46277376/46251776), Serial0
P 4:5:0.0.0.6, 1 successors, FD is 37200
 via Connected, Ethernet1
 via 10.16.81.28 (307200/281600), Ethernet1S
 via 10.16.80.28 (307200/281600), Ethernet0
 via 10.16.80.31 (332800/307200), Serial0
```

The table below describes the significant fields shown in the **show eigrp service-family ipv4 topology**command output.

Table 6: show eigrp service-family ipv4 topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P	Passive--No EIGRP computations are being performed for this destination.
A	Active--EIGRP computations are being performed for this destination.
U	Update--Indicates that an update packet was sent to this destination.
Q	Query--Indicates that an query packet was sent to this destination.
R	Reply--Indicates that an reply packet was sent to this destination.
r	Reply status--A flag set after the service has sent a query and is waiting for a reply.
1:2.0.0.0.3	Service number.

Field	Description
successors	Number of successors. Corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state.
FD	Flexible distance--The best metric to reach the destination or the best metric that was known when the service went active.
via	IP address of the peer that told the service about this destination. The first n of these entries, where n is the number of successors, is the current successors. The remaining entries in the list are feasible successors. If “all-links” or “detailed-links” is specified, the feasible successors are followed by sources that are neither successors nor feasible successors.
(46251776/46226176)	Two EIGRP metric numbers. The first number represents the cost to the destination; the second number is the metric that this peer advertised.
Ethernet0	Indicates the interface from which this information was learned.

Related Commands

Command	Description
clear eigrp service-family	Clears entries from the EIGRP neighbor table.
show eigrp service-family	Displays information about Cisco SAF service-family Clients, External Clients, and subscriptions.
show eigrp service-family external-client	Displays information about the Cisco SAF service-family External Clients.
show eigrp service-family ipv6 topology	Displays information from the Cisco SAF IPv6 service-family topology table.

show eigrp service-family ipv6 topology

To display topology information for an Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 service family, use the **show eigrp service-family ipv6 topology**command in user EXEC or privileged EXEC mode.

show eigrp service-family ipv6 [**vrf** *vrf-name*] *autonomous-system-number* **topology** [*service-instance-number*| **active**| **all-links**| **detail-links**| **pending service-type** [**connected**| **external**| **internal**| **local**| **redistributed**| **summary**]| **summary**| **zero-successors**]

Syntax Description

vrf	(Optional) Specifies all virtual routing forwarding (VRF) instance tables or a specific VRF table for an IP address.
vrf-name	(Optional) Names a specific VRF table for an IPv6 address.
autonomous-system-number	Specifies the autonomous-system number.
service-instance- number	(Optional) Displays detailed information about the specified service-instance number. Service-instance numbers display as service:subservice:instance.instance.instance.instance. Service-instance numbers can range from 1:1:0.0.0.1 to 65534:65534:FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFE.
active	(Optional) Displays only active entries in the topology table.
all-links	(Optional) Displays all service sources (including non-feasible sources) in the topology table.
detail-links	(Optional) Specifies all links in the topology table.
pending	(Optional) Displays all active entries in the topology table that are waiting for an update or reply from a neighbor.
service-type	(Optional) Specifies the service with the given type in the topology table.
connected	(Optional) Displays only connected services.
external	(Optional) Displays all external services.
internal	(Optional) Displays all internal services.
local	(Optional) Display all locally originated services.

redistributed	(Optional) Displays all redistributed services.
summary	(Optional) Displays all summary services.
summary	(Optional) Specifies a summary of the topology table.
zero-successors	(Optional) Displays only services in the topology table that have zero successors.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **show eigrp service-family ipv6 topology**command in user EXEC or privileged EXEC mode to see a summary of information on EIGRP IPv6 service-family topology services.

Note Using the **show eigrp service-family ipv6 topology**commands requires an IPv6-enabled SAF client, which currently does not exist.

Examples

The following is sample output from the **show eigrp service-family ipv6 topology** command:

```
Router> enable
Router# show
 eigrp service-family ipv6 4453 topology
EIGRP-SFv4 Topology Table for process 4453
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status
P 1:2:0.0.0.3, 2 successors, FD is 0
 via 10.16.80.28 (46251776/46226176), Ethernet0
 via 10.16.81.28 (46251776/46226176), Ethernet1
 via 10.16.80.31 (46277376/46251776), Serial0
P 4:5:0.0.0.6, 1 successors, FD is 37200
 via Connected, Ethernet1
 via 10.16.81.28 (307200/281600), Ethernet1S
 via 10.16.80.28 (307200/281600), Ethernet0
 via 10.16.80.31 (332800/307200), Serial0
```

The following is sample output from the **show eigrp service-family ipv6 topology** command for a specified service:

```
Router> enable
Router# show
 eigrp service-family ipv6 4453 topology 1:2:0.0.0.3
EIGRP-SFv4 VR(example) Topology Table entry for AS(4453)
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
Service Description Blocks:
1:2:3.0.0.0.3 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
Composite metric is (409600/128256), Route is External
Vector metric:
 Minimum bandwidth is 10000 Kbit
 Total delay is 6000 microseconds
 Reliability is 255/255
 Load is 1/255
 Minimum MTU is 1500
 Hop count is 1
External data:
 Originating router is 10.89.245.1
 AS number of route is 0
 External protocol is Connected, external metric is 0
 Administrator tag is 0 (0x00000000)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status
P 1:2:0.0.0.3, 2 successors, FD is 0
 via 10.16.80.28 (46251776/46226176), Ethernet0
 via 10.16.81.28 (46251776/46226176), Ethernet1
 via 10.16.80.31 (46277376/46251776), Serial0
P 4:5:0.0.0.6, 1 successors, FD is 37200
 via Connected, Ethernet1
 via 10.16.81.28 (307200/281600), Ethernet1S
 via 10.16.80.28 (307200/281600), Ethernet0
 via 10.16.80.31 (332800/307200), Serial0
```

The table below describes the significant fields shown in the **show eigrp service-family ipv6 topology**command output.

Table 7: show eigrp service-family ipv6 topology Field Descriptions

Field	Description
Codes:	State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P	Passive--No EIGRP computations are being performed for this destination.
A	Active--EIGRP computations are being performed for this destination.
U	Update--Indicates that an update packet was sent to this destination.
Q	Query--Indicates that an query packet was sent to this destination.
R	Reply--Indicates that an reply packet was sent to this destination.

Field	Description
r	Reply status--A flag set after the service has sent a query and is waiting for a reply.
1:2.0.0.0.3	Service number.
successors	Number of successors. Corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state.
FD	Flexible distance--The best metric to reach the destination or the best metric that was known when the service went active.
via	IP address of the peer that told the service about this destination. The first n of these entries, where n is the number of successors, is the current successors. The remaining entries in the list are feasible successors. If “all-links” or “detailed-links” is specified, the feasible successors are followed by sources that are neither successors nor feasible successors.
(46251776/46226176)	Two EIGRP metric numbers. The first number represents the cost to the destination; the second number is the metric that this peer advertised.
Ethernet0	Indicates the interface from which this information was learned.

Related Commands

Command	Description
clear eigrp service-family	Clears entries from the EIGRP neighbor table.
show eigrp service-family	Displays information about Cisco SAF IPv4 service-family Clients, External Clients, and subscriptions.
show eigrp service-family external-client	Displays information about Cisco SAF service-family External Clients.
show eigrp service-family ipv4 topology	Displays information from Cisco SAF IPv4 service-family topology table.

show eigrp tech-support

To generate a report of the Enhanced Interior Gateway Routing Protocol (EIGRP) internal state information, use the **show eigrp tech-support** command in privileged EXEC mode.

show eigrp tech-support [detailed]

Syntax Description

detailed	(Optional) Displays detailed output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.1(3)S	This command was modified. The command output was modified to display relevant wide metric information.
Cisco IOS XE Release 3.4S	This command was modified. The command output was modified to display relevant wide metric information.
15.1(1)SY	This command was modified. The command output was modified to display relevant wide metric information.

Usage Guidelines

Use the **show eigrp tech-support** command in privileged EXEC mode to display various internal EIGRP states.

Note This command is useful for debugging and troubleshooting by Cisco technical support, but it is not intended for normal EIGRP administration tasks. This command should not be used without guidance from Cisco technical support.

Examples

The following is sample output from the **show eigrp tech-support detailed** command:

```
Device# show eigrp tech-support detailed

EIGRP feature plugins:::
    eigrp-release      :   8.00.00 : Portable EIGRP Release
                       :   3.00.21 : Source Component Release(dev8)
                                     + HMAC-SHA-256 Authentication
    parser             :   2.02.00 : EIGRP Parser Support
    igrp2              :   2.00.00 : Reliable Transport/Dual Database
                                     + Wide Metrics
    eigrp-nsf          :   2.00.00 : Platform Support
    bfd                :   1.01.00 : BFD Platform Support
    mtr                :   1.00.01 : Multi-Topology Routing(MTR)
    eigrp-pfr          :   1.00.01 : Performance Routing Support
                                     + IPv4 PFR
    EVN/vNets          :   1.00.00 : Easy Virtual Network (EVN/vNets)
                                     + IPv4 EVN/vNets
    ipv4-af            :   2.01.01 : Routing Protocol Support
    ipv4-sf            :   1.02.00 : Service Distribution Support
                                     + Dynamic Remote Neighbors
    ipv6-af            :   2.01.01 : Routing Protocol Support
                                     + IPv6 VRF
    ipv6-sf            :   2.01.00 : Service Distribution Support
                                     + Dynamic Remote Neighbors
                                     + IPv6 VRF
    vNets-parse        :   1.00.00 : EIGRP vNets Parse Support
    snmp-agent         :   1.01.01 : SNMP/SNMPv2 Agent Support
EIGRP Internal Process States

 procinfoQ:
   1: 0x1FC6EB4C vrid:0 afi:1 as:46    tableid:0 vrfid:0 tid:0 name:virtual-name
       topo_ddbQ(1) 0x1FCC478C tableid:0 name:base
       topo_ddbQ.count: 1
   procinfoQ.count: 1

     deadQ:

      ddbQ:
       1: 0x1FCC478C name:base
      ddbQ.count: 1
 ------------------------------------------------------------

EIGRP Memory Usage:

  EIGRP Memory                 In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  EIGRP IP pdb            :      8216      8216/8268          1  8216   --/--
  EIGRP-Core: DDB         :      2440      2440/2492          1  2440   --/--
  EIGRP-Core: Dual Events :     30000     30000/30052         1 30000   --/--
  EIGRP-Core: IIDB        :       928       928/980           1   928   --/--
  EIGRP-Core: IIDB Scratc :        24        24/76            1    24   --/--
  EIGRP-Core: Peer Handle :        76        76/180           2    38   --/--
  EIGRP-Core: Peer Sub-To :        32        32/84            1    32   --/--
  EIGRP-Core: Topology II :       104       104/156           1   104   --/--
  EIGRP-IPv4: Proto Priva :        24        24/76            1    24   --/--
  EIGRP-IPv4: Protocol In :      3464      3464/3516          1  3464   --/--
  EIGRP-IPv4: VR-Router   :        32        32/84            1    32   --/--
  EIGRP-Parser: dBase Hdr :      1740      1740/2052          6   290   --/--
  EIGRP-v4: Work Entry    :        --      4260/4728         --    60   50/71
  EIGRP: Anchor entries   :        --      7404/10052        --    12  500/617
  EIGRP: Dummy thread ent :        --      8892/10052        --    36  200/247
  EIGRP: ExtData          :        --      1320/1708         --    24   50/55
  EIGRP: Input packet hea :        --      2304/3052         --    16  100/144
  EIGRP: Large packet buf :        --     57512/65588        --  8216  100/7
  EIGRP: List Large       :        --      1332/1552         --   148    5/9
  EIGRP: List Medium      :        --      1296/1604         --    72   10/18
  EIGRP: Max packet buffe :        --     49224/65588        -- 16408    5/3
  EIGRP: Medium packet bu :        --     64856/65588        --   536  100/121
```

```
  EIGRP: Packet descripto :        --      4260/4728         --    60   50/71
  EIGRP: Queue elements   :        --     11788/13640        --    28  200/421
  EIGRP: Small Pool       :        32       624/956           2    16   32/39
  EIGRP: Small packet buf :        --      4444/5052         --    44  100/101
  EIGRP: cmd handles      :        56        56/160           2    28   --/--
  EIGRP: mgd_timer        :      1600      1600/2640         20    80   --/--
  Total                   :     48768    268252/304704       42    --   --/--

  Total allocated: 0.290 Mb, 297 Kb, 304704 bytes
-------------------------------------------------------------

EIGRP-IPv4 VR(virtual-name) Address-Family Protocol for AS(46)
 {vrid:0 afi:1 as:46 mode:3 tableid:0 vrfid:0 tid:0 name:virtual-name }

          PIDs: Hello: (no process)  PDM: (no process)
     Router-ID: 10.4.9.87
       Threads: procinfo: 0x1FC72E58   ddb: 0x1FC73050
         workQ:
         iidbQ:
 passive_iidbQ:
         peerQ:
 unicast_peerQ:
      suspendQ:
      networkQ:
 RedistStructs: src:(0)default  distflag:0x4  ipdb->pdb->mask:0x4
                count: 1
      summaryQ:
  Socket Queue: %EIGRP(ERROR): invalid socket
   Input Queue: 0/2000/0/0 (current/max/highest/drops)
       GRS/NSF: enabled    hold-timer: 240
  Active Timer: 3 min
      Distance: internal 90 external 170
      Max Path: 4
  Max Hopcount: 100
      Variance: 1
     Rib-scale: 1
    Metric Ver: 32bit
 ---------------------------------------------------------------------
```

Related Commands

Command	Description
show eigrp plugins	Displays general information including the versions of the EIGRP protocol features currently running.

show service-routing capabilities-manager

To display information about registered capabilities, use the **show service-routing capabilities-manager** command in user EXEC or privileged EXEC mode.

show service-routing capabilities-manager

Syntax Description

group *value*	(Optional) Specifies a group type; 1 (Hardware) or 2 (Software).
local	(Optional) Provides registered capabilities information for only the local router.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Examples

The following example shows how to display information about all registered capabilities and groups 1 (Hardware) and 2 (Software):

```
Router# show service-routing capabilities-manager

Router# show service-routing capabilities-manager

Service-Routing Capabilities Manager
====================================
Registered Capabilities
=======================
Group/ID: HARDWARE/1
Service: 100:1:31343134.34333137.32000000.0
Originator: 1.1.1.1
Capability Data:
<Capabilities>
<Group Name="HARDWARE">
  <Capability Name="HostName">
    <Value>R100</Value>
  </Capability>
  <Capability Name="Platform">
    <Value>Solaris Unix (Sparc) processor</Value>
  </Capability>
  <Capability Name="MainMemorySize">
    <Value>63682Kbytes</Value>
  </Capability>
</Group>
</Capabilities>
```

```
Group/ID: SOFTWARE/2
Service: 100:2:31343134.34333137.32000000.0
Originator: 1.1.1.1
Capability Data:
<Capabilities>
<Group Name="SOFTWARE">
  <Capability Name="HostName">
    <Value>R100</Value>
  </Capability>
  <Capability Name="Software">
    <Value>Cisco IOS Software</Value>
  </Capability>
  <Capability Name="Image">
    <Value> Solaris Software (UNIX-ADVENTERPRISE-M)</Value>
  </Capability>
  <Capability Name="Version">
    <Value> Experimental Version 15.1(20110404:193816) </Value>
  </Capability>
  <Capability Name="ipmulticast">
    <Value>Subsystem Loaded</Value>
</Capability>
  <Capability Name="eigrp_ipv4">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="eigrp_ipv6">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="ospf">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="ospfv3">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="isis">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="isis_ipv6">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="bgp_ipv4">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="bgp_ipv6">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="fh_fd_ipsla">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="service_routing">
    <Value>Subsystem Loaded</Value>
  </Capability>
</Group>
</Capabilities>
```

The following example shows how to display information for only the local router and for only group 1 (Hardware):

```
Router# show service-routing capabilities-manager group 1 local

Service-Routing Capabilities Manager
====================================

Registered Capabilities
=======================

Group/ID: HARDWARE/1
Service: 100:1:31343134.34333137.32000000.0
Originator: 1.1.1.1
Capability Data:
<Capabilities>
<Group Name="HARDWARE">
```

```
  <Capability Name="HostName">
    <Value>R100</Value>
  </Capability>
  <Capability Name="Platform">
    <Value>Solaris Unix (Sparc) processor</Value>
  </Capability>
  <Capability Name="MainMemorySize">
    <Value>63682Kbytes</Value>
  </Capability>
</Group>
</Capabilities>
```

The table below describes the significant fields shown in the display.

Table 8: show service-routing capabilities-manager Field Descriptions

Field	Description
Group/ID	Specifies either group 1 (Hardware) or 2 (Software).
Service	Specifies the Capabilities Manager service identifier.
Originator	Specifies the originator of the service.
Capability Name	Specifies the name of the capability.

Related Commands

Command	Description
show service-routing plugins capman	Displays Capabilities Manager plugin information.
show service-routing capabilities-manager internal	Displays information about Capabilities Manager.

show service-routing capabilities-manager internal

To display information about Capabilities Manager, use the **show service-routing capabilities-manager internal** command in user EXEC or privileged EXEC mode.

show service-routing capabilities-manager internal

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

Use the **show service-routing capabilities-manager internal** command in user or privileged EXEC mode to see a summary of the information about Cisco SAF external clients that are currently registered with the Cisco SAF system.

Examples

The following is sample output from the **show service-routing capabilities-manager internal** command.

```
Router# show service-routing capabilities-manager internal
Service-Routing Capabilities Manager
====================================
Major Version: 1  Minor Version: 0  Edit Version: 0
Reachability: 2.2.2.2:0
Local Instance GUID: 31343134-3433-3137-3200-000000000000
```

The table below describes the significant fields shown in the display.

Table 9: show service-routing capabilities-manager internal Field Descriptions

Field	Description
Major Version	Specifies the Capabilities Manager major version.
Minor Version	Specifies the Capabilities Manager minor version.
Reachability	Specifies the Capabilities Manager reachability information.

Field	Description
Local Instance GUID	Specifies the instance number used by local Capabilities Manager services.

Related Commands

Command	Description
show service-routing plugins capman	Displays Capabilities Manager plugin information.
show service-routing capabilities-manager	Displays information about registered capabilities.

show service-routing plugins capman

To display Capabilities Manager plugin information, use the **show service-routing plugins capman** command in user EXEC or privileged EXEC mode.

show service-routing plugins capman [**detail**]

Syntax Description

detail	Not implemented. This keyword will be implemented in a future release.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

Use the **show service-routing plugins capman** command in user or privileged EXEC mode to determine if SAF and Capabilities Manager are available. When Capabilities Manager is available, the version is also displayed.

Examples

The following example shows how to display Capabilities Manager plugin information:

```
Router# show service-routing plugins capman
Service-Routing feature plugins:::
   capman      :   1.00.00 : Cisco Capabilities Manager
```

The table below describes the significant fields shown in the display.

Table 10: show service-routing plugins capman Field Descriptions

Field	Description
capman	Specifies the Capabilities Manager version.
Cisco Capabilities Manager	Specifies when Capabilities Manager is available on the router.

Related Commands

Command	Description
show service-routing capabilities-manager internal	Displays information about Capabilities Manager.
show service-routing capabilities-manager	Displays information about registered capabilities.

show service-routing xmcp clients

To display information about connected XMCP (Extensible Messaging Client Protocol) clients, use the **show service-routing xmcp clients** command in user EXEC or privileged EXEC mode.

show service-routing xmcp clients [*ip-address*| *handle*] [**detail**]

Syntax Description

ip-address	(Optional) IPv4 or IPv6 IP address of a single client to display.
handle	(Optional) Handle of a single client to display. A handle is a number assigned dynamically by XMCP. The number range is 1 to 1023, and is displayed in the Handle field of the display.
detail	(Optional) Displays additional information about XMCP clients.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **show service-routing xmcp clients** command is used to display detailed information about currently connected XMCP clients. Include an IP address to show a single client. Include the **detail** keyword to display additional information.

Examples

The following is sample output from the **show service-routing xmcp clients** command:

```
Router# show service-routing xmcp clients

XMCP Clients
Codes: A - Authenticated, T - TCP

    Handle Address                                  Port  Keepalive
AT  1      10.1.1.1                                 47519    24/30
    Client name: UCM/CM_ccmbeijing/NodeId=1/8.5.1.10000-26
```

```
 23     2001:0DB8:E123:1000:3615:9EFF:FE0B:AFA4   3478  3120/3600
    Client name: CapMan Viewer/glmatthe-mac.example.com/Mac OS X 10.6.6 (10J567)
```

The following is sample output from the **show service-routing xmcp clients detail** command:

```
Router# show service-routing xmcp clients detail

XMCP Clients
Codes: A - Authenticated, T - TCP

    Handle Address                                    Port  Keepalive
AT  1      10.1.1.2                                   47532    22/30
    Client name: UCM/CM_ccmbeijing/NodeId=1/8.5.1.10000-26
 XMCP version: 1.0
 Page-size: 5 (11/5 requests enqueued/awaiting response)
    Username: CUCM_CLIENT
    Socket FD: 1
    Domain: 100
    Nonce: lifetime 51/800 seconds
 23     2001:0DB8:E123:1000:3615:9EFF:FE0B:AFA4   3478  3120/3600
    Client name: CapMan Viewer/glmatthe-mac.example.com/Mac OS X 10.6.6 (10J567)
 XMCP version: 2.0
    Page-size: 3 (0/2 requests enqueued/awaiting response)
    Socket FD: 2
    Domain: 123
    Nonce: none
```

The table below describes the significant fields shown in the display.

Table 11: show service-routing xmcp clients Field Descriptions

Field	Description
Codes	Indicates properties of the client. Valid codes are: • A, indicates that the client is authenticated • T, indicates that the client is connected over TCP
Handle	The service-routing client handle associated with this client.
Address	The IPv4 or IPv6 IP address from which the client has connected.
Port	The port number from which the client has connected.
Keepalive	Shows the current and maximum value of the keepalive timer associated with this client session. The timer is reset to its maximum value each time a packet is received from the client. If the keepalive reaches zero, the client session will be terminated.
Client name	Descriptive string provided by the client to identify itself.
XMCP version	Version of the XMCP protocol being used by the client.

Field	Description
Page-size	Maximum number of simultaneous requests that can be sent and are awaiting a response from the client.
requests enqueued/awaiting	Number of requests currently waiting to be sent and number of requests that have been sent to the client but are awaiting a response.
Username	Username in use for client authentication.
Socket FD	Internal file descriptor used to identify the socket associated with this session.
Domain	Service-routing domain with which this client is associated.
Nonce	Whether nonces are enabled for this session, and if so, the current and maximum duration (lifetime in seconds) for which a given nonce will remain valid.

Related Commands

Command	Description
service-routing xmcp listen	Defines a port on which XMCP clients can connect.

show service-routing xmcp server

To display information about the XMCP (Extensible Messaging Client Protocol) server status, use the **show service-routing xmcp server** command in user EXEC or privileged EXEC mode.

show service-routing xmcp server

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **show service-routing xmcp server** command displays an overview of the XMCP server configuration and status. For more detailed information about individual XMCP client sessions, use the **show service-routing xmcp clients** command.

Examples

The following is sample output from the **show service-routing xmcp server** command:

```
Router# show service-routing xmcp server

XMCP Server listening on port 4788
  Socket descriptors: 0 (TCP/IPv4), 1 (TCP/IPv6)
  Connected clients: 1 unauthenticated, 2 total
  Maximum clients: 5 unauthenticated, 10 total
  Allow-lists: "v4nacl" (IPv4), "naclv6" (IPv6)
  Clients configured:
    Username "a", 1 client(s) connected
    Unauthenticated, 1 client(s) connected
```

The table below describes the significant fields shown in the display.

Table 12: show service-routing xmcp server Field Descriptions

Field	Description
XMCP Server listening on port 4758	Indicates that the XMCP server is enabled, and displays the port number and name of the VRF (virtual routing and forwarding) instance (if any) with which the server is associated.
Socket descriptors	Internal socket descriptor numbers for the listen ports associated with the XMCP server.
Connected clients	Number of current unauthenticated client sessions and total number of all current client sessions.
Maximum clients	Client limits as defined by the **max-clients** command.
Allow-lists	Access-lists restricting clients, as defined by the **allow-list** command.
Clients configured	List of configured client authentication options as defined by the client username and client unauthenticated commands, and the number of current client sessions using each authentication.

Related Commands

Command	Description
client (XMCP)	Defines the properties of XMCP clients.
max-clients	Limits the number of concurrent XMCP client sessions.
service-routing xmcp listen	Defines a port on which XMCP clients can connect.
show service-routing xmcp clients	Displays currently connected XMCP clients.

split-horizon (EIGRP)

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) split-horizon, use the **split-horizon** command in address-family interface configuration mode or service-family interface configuration mode. To disable EIGRP split-horizon, use the **no** form of this command.

split-horizon

no split-horizon

Syntax Description

This command has no arguments or keywords.

Command Default

EIGRP split-horizon is enabled by default. However, for ATM interfaces and subinterfaces **split-horizon** is disabled by default.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The split-horizon rule prohibits a router from advertising a route through an interface that the router itself uses to reach the destination. The following are general rules for EIGRP split-horizon:

- Split-horizon behavior is turned on by default.
- When you change the EIGRP split-horizon setting on an interface, all adjacencies with EIGRP neighbors reachable over that interface are reset.
- Split-horizon should typically be disabled only on non-broadcast multi-access interfaces.
- The EIGRP split-horizon behavior is not controlled or influenced by the **ip split-horizon** command.

To configure split-horizon for an EIGRP address family, use the **split-horizon**command in address-family interface configuration mode.

To configure split-horizon for an EIGRP service family, use the **split-horizon**command in service-family interface configuration mode.

Examples

The following example disables EIGRP split-horizon for serial interface 3/0 in address-family 5400:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 5400
Router(config-router-af)# af-interface serial3/0
Router(config-router-af-interface)# no split-horizon
```

The following example disables EIGRP split-horizon for serial interface 3/0 in service-family 5400:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 5400
Router(config-router-sf)# sf-interface serial3/0
Router(config-router-sf-interface)# no split-horizon
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
router eigrp	Configures the EIGRP address-family process.
service-family ipv4	Configures commands under service-family configuration mode.
sf-interface	Configures interface-specific commands under service-family configuration mode.

timers graceful-restart purge-time

To set the graceful-restart purge-time timer to determine how long a nonstop forwarding (NSF)-aware router that is running the Enhanced Interior Gateway Routing Protocol (EIGRP) must hold routes for an inactive peer, use the **timers graceful-restart purge-time** command in router configuration, address family configuration, or service-family configuration mode. To return the graceful-restart purge-time timer to the default value, use the **no** form of this command.

timers graceful-restart purge-time *seconds*

no timers graceful-restart purge-time

Syntax Description

seconds	Time, in seconds, for which EIGRP must hold routes for an inactive peer. The range is from 20 to 300. The default is 240.

Command Default

The default graceful-restart purge-time timer is 240 seconds.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Service-family configuration (config-router-sf)

Command History

Release	Modification
15.0(1)M	This command was introduced. This command replaces the **timers nsf route-hold** command.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.6S	This command was modified. Support for IPv6 and IPv6 VPN Routing and Forwarding (VRF) was added.
15.2(2)S	This command was modified. Support for IPv6 and IPv6 VRF was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The graceful-restart purge-time timer sets the maximum period of time for which the NSF-aware router must hold known routes for an NSF-capable neighbor during a switchover operation or a well-known failure condition. The graceful-restart purge-time timer is configurable so that you can tune network performance and avoid undesired effects, such as "black holing" routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

Note The **timers nsf signal** command is supported only on platforms that support High Availability.

Examples

The following example shows how to set the graceful-restart purge-time timer to 60 seconds for an NSF-aware IPv4 address family:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# timers graceful-restart purge-time 60
```

The following example shows how to set the graceful-restart purge-time timer to 300 seconds for an NSF-aware-service family configuration:

```
Device(config)# router eigrp virtual-name
Device(config-router)# service-family ipv4 autonomous-system 4533
Device(config-router-sf)# timers graceful-restart purge-time 300
```

The following example shows how to set the graceful-restart purge-time timer to 200 seconds for an NSF-aware IPv6 address family configuration:

```
Device(config)# router eigrp e1
Device(config-router)# address-family ipv6 autonomous-system 4
Device(config-router-af)# timers graceful-restart purge-time 300
```

Related Commands

Command	Description
debug eigrp address-family ipv6 notifications	Displays information about EIGRP address family IPv6 event notifications.
debug eigrp nsf	Displays notifications and information about NSF events for an EIGRP routing process.
debug ip eigrp notifications	Displays EIGRP events and notifications in the console of the router.
nsf (EIGRP)	Enables EIGRP NSF or EIGRP IPv6 NSF on an NSF-capable router.
show eigrp neighbors	Displays the neighbors discovered by EIGRP.
show ip protocols	Displays the parameters and the current state of the active routing protocol process.

Command	Description
show ipv6 protocols	Displays the parameters and the current state of the active IPv6 routing protocol process.
timers nsf converge	Sets the maximum time that the restarting router must wait for the end-of-table notification from an NSF-capable or NSF-aware peer.
timers nsf signal	Sets the maximum time for the initial restart period.

topology

To configure topology-specific commands for an Enhanced Interior Gateway Routing Protocol (EIGRP) service family, use the **topology**command in service-family interface configuration mode. To disable the service-family topology configuration mode, use the **no** form of this command.

topology base

no topology base

Syntax Description

base	Configures the base topology.

Command Modes

Service-family configuration (config-router-sf)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **topology**command to configure Cisco SAF for multitopology networks.

Note In Cisco IOS Release 15.0(1)M, only the base topology is supported.

Use the **show eigrp service-family ipv4 topology**command to verify the topology base configuration.

Examples

The following example configures the base topology:

```
Router(config)# router eigrp virtual-name
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)# exit
-sf-interface
Router(config-router-sf)# topology base
```

Related Commands

Command	Description
exit-service-family	Exits service-family configuration mode.
exit sf-interface	Exits service-family interface configuration mode.
router eigrp	Configures the EIGRP process.
sf-interface	Configures interface-specific commands under the service-family interface configuration mode.
show eigrp service-family ipv4 topology	Displays information on EIGRP service-family IPv4 topologies.
shutdown	Disables service family on the interface.

username (SAF)

To configure username for a Cisco SAF External-Client, use the **username**command in external-client label configuration mode. To negate the username, use the **no** form of this command.

username *name*

no username *name*

Syntax Description

name	Specifies the name for the external client between 1 and 64 characters.

Command Modes

External-client label configuration (config-external-client-mode)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(1)S	This command was deprecated in Cisco IOS Release 15.2(1)S and replaced by the client (xmcp) command.
Cisco IOS XE Release 3.5S	This command was deprecated in Cisco IOS XE Release 3.5S and replaced by the client (xmcp) command.
15.2(2)T	This command was deprecated in Cisco IOS Release 15.2(2)T and replaced by the client (xmcp) command.

Usage Guidelines

Use the **username**command to configure Cisco SAF External Clients. Entering a new username value overwrites the old value, but the new value will only take affect after the Cisco SAF External Client re-registers.

Use the **show eigrp service-family ipv4 external-client**command to verify the Cisco SAF External Client configuration.

Examples

The following example configures a Cisco SAF External Client named example:

```
Router(config)# service-family external-client listen ipv4 2444
Router(config-external-client)# external-client
 example
Router(config-external-client-mode)# username
 example
```

Related Commands

Command	Description
external-client	Configures Cisco SAF External Clients.
service-family external-client listen	Configures Cisco SAF External Client listen TCP ports.
show eigrp service-family ipv4 external-client	Displays information on Cisco SAF External Clients.