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.

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.

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 *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.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0M.
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

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)# router 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.
authentication key-chain	Specifies an authentication key chain EIGRP.
authentication mode (EIGRP)	Specifies the type of authentication used in EIGRP packets for the EIGRP instance.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
network	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP process.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
service-family	Configures VRF metrics for a Cisco SAF service-family.
sf-interface	Configure interface-specific commands for a Cisco SAF service family.
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 *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.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0M.
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

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 *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, except that the first character cannot be a number.

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.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0M.
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

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
```

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 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.
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.

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** | **reset-time** *interval* | **restart** *interval* | **restart-count** *count* | **warning-only**]

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.

metric 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.
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 $2.56 * 10^{12}$. 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.

Table 1 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.
router eigrp	Configures the EIGRP process.
service-family	Configures commands under service-family mode.
sf-interface	Configures interface-specific commands under service-family.

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.

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

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

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.

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).