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

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.

Release	Modification
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)
```

clear service-routing xmcp client

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.

Command	Description
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-nameautonomous-system-numberservice-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.
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.

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

domain