

h225 address

To configure the sourceAddress and destinationAddress fields of an H.225 message in the H.323 adjacency, use the **h225 address** command in the H.323 adjacency configuration mode. To return to the default value, use the **no** form of this command.

h225 address {block | usage {e164 | h323id}}

no h225 address {block | usage}

Syntax Description		
block		Specifies that the sourceAddress and destinationAddress in a H.225 message are not passed through.
usage		Specifies the interpretation of the H.225 sourceAddress and destinationAddress fields in an adjacency when Q.931 callingPartyNumber or calledPartyNumber is not present.
e164		Specifies the e164 format for the addresses. All the other formats are ignored.
h323id		If the field begins with a numeric prefix, such as [0123456789*,] of 6 or greater characters, it is used as either the calling party number or the called party number, and the rest of the ID is ignored.

Command Default By default, the sourceAddress and destinationAddress in a H.225 message are not blocked. The H.225 sourceAddress and destinationAddress fields are interpreted in the *H.323-ID* format.

Command Modes Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how to configure the SBC to block the sourceAddress and destinationAddress fields in H.225 messages received on the adjacency by using the **h225 address block** command in the H.323 adjacency configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# h225 address block
```

The following example shows how to configure the H.225 sourceAddress and destinationAddress fields so that they are interpreted in the e164 format:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# h225 address usage e164
```

Related Commands

Command	Description
h225 timeout	Configures the H.225 timeout interval.

h225 address (session border controller)

To configure the sourceAddress and destinationAddress of H.225 message in the H.323 adjacency, use the **h225 address** command in the H.323 adjacency configuration mode. To return to the default value, use the **no** form of this command.

```
h225 address {block | usage {e164 | h323id}}
```

```
no h225 address {block | usage}
```

Syntax Description		
block		Specifies that the sourceAddress and destinationAddress in a H.225 message are not passed through.
usage		Specifies the interpretation of the H.225 sourceAddress and destinationAddress fields in an adjacency when Q.931 callingPartyNumber or calledPartyNumber is not present.
e164		Specifies the e164 format for the addresses. All the other formats are ignored.
h323id		If the field begins with a numeric prefix, such as [0123456789*,] of 6 or greater characters, it is used as either the calling party number or the called party number, and the rest of the ID is ignored.

Command Default *By default, the sourceAddress and destinationAddress in a H.225 message are not blocked. The H.225 sourceAddress and destinationAddress fields are interpreted in the H.323-ID format.*

Command Modes Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how to configure the SBC to block the sourceAddress and destinationAddress fields in H.225 messages received on the adjacency by using the **h225 address block** command in the H.323 adjacency configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# h225 address block
```

The following example shows how to configure the H.225 sourceAddress and destinationAddress fields so that they are interpreted in the e164 format:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# h225 address usage e164
```

Related Commands

Command	Description
h225 timeout	Configures the H.225 timeout interval.

h225 timeout

To configure the H.225 timeout interval, use the **h225 timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

h225 timeout { **setup** | **proceeding** | **establishment** } *value*

no h225 timeout { **setup** | **proceeding** | **establishment** } *value*

Syntax Description	setup	Specifies the setup state. Default value for this state is 4 seconds.
	proceeding	Specifies the proceeding state. Default value for this state is 10 seconds.
	establishment	Specifies the establishment state. Default value for this state is 180 seconds.
	<i>value</i>	Specifies the timeout period in seconds. For setup and proceeding timeout periods, valid values are from 1 to 30. For establishment timeout, valid values are from 30 to 300.

Command Default *No default behavior or values are available.*

Command Modes Adjacency H.323 configuration (config-sbc-sbe-adj-h323)
H.323 configuration (config-sbc-sbe-h323)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how the **h225 timeout** command configures an H.225 timeout interval in adjacency H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# h225 timeout setup 30
Router(config-sbc-sbe-adj-h323)# h225 timeout proceeding 30
Router(config-sbc-sbe-adj-h323)# h225 timeout establishment 30
```

The following example shows how the **h225 timeout** command configures an H.225 timeout interval in H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# h225 timeout setup 30
Router(config-sbc-sbe-h323)# h225 timeout proceeding 30
Router(config-sbc-sbe-h323)# h225 timeout establishment 30
```

h245-address-pass

To specify when an H.245 address is passed to the caller when the caller does not support tunneling, use the **h245-address-pass** command in the adjacency H.323 configuration mode. The **no** form of this command shows default behavior, where H.323 supplies the H.245 address on a Q.931 call proceeding, and all subsequent messages to the caller until the H.245 connection is opened.

h245-address-pass wait-connect

no h245-address-pass wait-connect

Syntax Description	wait-connect	Pass H.245 address to caller until call is connected. H.323 supplies only the H.245 address on the Q.931 connect
--------------------	--------------	--

Command Default	Default value is the no form of the command.
-----------------	--

Command Modes	Adjacency H.323 configuration (config-sbc-sbe-adj-h323)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	Updated the command for the wait-connect option.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to configure the H.323 adjacency to allow delay passing the H.245 address to caller:
----------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 2651XM-5
Router(config-sbc-sbe-adj-h323)# h245-address-pass wait-connect
Router(config-sbc-sbe-adj-h323)# exit
```

Related Commands	Command	Description
	h245-tunnel disable	Disables H.245 tunneling on a per-adjacency basis.

h245-tunnel disable

To disable H.245 tunneling on a per-adjacency basis, use the **h245-tunnel disable** command in adjacency H.323 configuration mode. To enable tunneling, use the **no** form of this command.

h245-tunnel disable

no h245-tunnel disable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	<i>No default behavior or values are available.</i>
------------------------	---

Command Modes	Adjacency H.323 configuration (config-sbc-sbe-adj-h323)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how the h245-tunnel disable command disables H.245 tunneling on an H.323 adjacency named H323ToIsp42:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 H323ToIsp42
Router(config-sbc-sbe-adj-h323)# h245-tunnel disable
```

h248-profile-version

To configure the vDBE H.248 profile version to interoperate with media gateway controller (SBE), use the **h248-profile-version** command in the vDBE H.248 profile configuration mode. To return to the default value, use the **no** form of this command.

h248-profile-version {*profile-version*}

no h248-profile-version

Syntax Description	<i>profile-version</i>	Version number of the H.248 profile. The values are from 1 to 3. The value of 3 stands for gate control. The value of 1 stands for etsi-bgf.
---------------------------	------------------------	--

Command Default	Default value is 3.
------------------------	---------------------

Command Modes	vDBE H.248 profile configuration (config-sbc-dbe-vdbe-h248-profile)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. To use this command, you must be in the correct configuration mode and submode. The “Examples” section shows the hierarchy of modes and submodes required to run the command. Use the h248-profile-version command after you have defined the name of the profile using the h248-profile command.
-------------------------	--

Examples	The following example shows how to configure the vDBE H.248 profile version to interoperate with the media gateway controller (SBE):
-----------------	---

```
Router# configure terminal
Router(config-sbc) # sbc mysbc dbe
Router(config-sbc-dbe) # vdbe
Router(config-sbc-dbe-vdbe) # h248-profile etsi-bgf
Router(config-sbc-dbe-vdbe-h248-profile) # h248-profile-version 1
```

Related Commands	Command	Description
	h248-profile	Configures the vDBE H.248 profile name to interoperate with the media gateway controller (SBE).

Command	Description
show sbc dbe h248-profile	Displays the information on the specified profile, including transport, H.248 version, and active packages.
vdbe	Enters Virtual Data Border Element (vDBE) configuration mode.

h248-profile

To configure a Virtual Data Border Element (VDBE) H.248 profile name to interoperate with the data border element (DBE), use the **h248-profile** command in the vDBE configuration mode. To return to the default value, use the **no** form of this command.

h248-profile {etsi-bgf | gate-ctrl} version *version-number*

no h248-profile

Syntax Description	etsi-bgf	Configures the Ia profile for ETSI_BGF.
	gate-ctrl	Configures the Cisco profile for SBC_GateControl.
	version	Configures the profile version.
	<i>version-number</i>	The profile's version number. The default version number for etsi-bgf is 2 and gate-ctrl is 3.

Command Default Default value is gatecontrol.

Command Modes VDBE configuration (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.1S	The version keyword and the <i>version-number</i> argument were added to configure the profile version.

Usage Guidelines To use this command, you must be in a user group that is associated with a task group that includes the proper task IDs. To use this command, you must also be in the correct configuration mode and submode. The Examples section that follows shows the hierarchy of the modes and submodes required to run the command.

After the DBE is configured to use the H.248 profile name, the applicable profile name is advertised with the Service Change messages.

Examples The following example shows how to configure the vDBE H.248 Ia profile to interoperate with the DBE:

```
Router# configure terminal
Router(config-sbc) # sbc mysbc dbe
Router(config-sbc-dbe) # vdbe
Router(config-sbc-dbe-vdbe) # h248-profile etsi-bgf version 2
```

Related Commands

Command	Description
h248-version	Defines the version of an H.248 protocol that the DBE uses when it forms associations with an H.248 controller.
bandwidth-fields mandatory	Sets the bandwidth description of SDP as mandatory.
vdbe	Enters VDBE configuration mode.

h248-version (session border controller)

To define the version of an H.248 protocol that the data border element (DBE) uses when it forms associations with an H.248 controller, use the **h248-version** command in VDBE configuration mode. To leave the default as version 2 of the H.248 protocol, use the **no** form of this command.

h248-version *version-number*

no h248-version *version-number*

Syntax Description

version-number	Specifies the version number. The DBE can accept H.248.1 version 2 or version 3. The default is H.248.1 version 2.
----------------	--

Command Default

H.248.1 version 2 is used.

Command Modes

VDBE configuration mode (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for distributed SBC.

Usage Guidelines

This command configures the DBE to support H.248.1v3, thus allowing the DBE to interoperate with an SBE or media gateway controller (MGC) which requires H.248.1 version 3. The DBE can accept H.248.1 version 2 or version 3.

The DBE rejects attempts to negotiate with the MGC to a lower version once the DBE is configured to support version 3.

Examples

The following example creates a DBE service on an SBC called “mySbc” and configures the DBE to use version 3 of the H.248.1 protocol, for a distributed SBC:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
h248-napt-package	Defines which H.248 package, either IP NAT Traversal package (ipnapt) or NAT Traversal package (ntr), the DBE uses for signaling Network Address Translation (NAT) features.

h248 allow-all-mg

To configure the H.248 signaling stack to allow connections from all Media Gateways, use the **h248 allow-all-mg** command in the SBE configuration mode. Use the **no** form of this command to deconfigure the H.248 signaling stack from allowing connections from all media gateways.

h248 allow-all-mg

no h-248 allow-all-mg

Syntax Description This command has no arguments or keywords.

Command Default Default is the **no** form of this command

Command Modes SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following command configures the H.248 signaling stack to allow any Media Gateway to connect to the SBE:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h248 allow-all-mg
Router(config-sbc-sbe)#
```

h323 (session border controller)

To enter the H.323 configuration mode, use the **h323** command in SBE configuration mode.

h323

Syntax Description This command has no arguments or keywords.

Command Default *No default behavior or values are available.*

Command Modes SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was not supported in Cisco IOS XE Release 2.4 on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how to enter the H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)#
```

Related Commands	Command	Description
	hunting-trigger	Configures failure return codes to trigger hunting.
	ras retry	Configures an H.323 Registration, Admission, and Status (RAS) retry count for an RAS transaction type.
	ras rrq	Configures the registration request (RRQ).
	ras timeout	Configures an H.323 RAS timeout interval.
	adjacency timeout	Configures the adjacency retry timeout interval.

header-editor

To set a specified header editor for inbound and outbound signaling on the signaling border element (SBE) session initiation protocol (SIP) adjacency, use the **header-editor** command in the Adjacency SIP configuration mode. To remove a header editor, use the **no** form of this command.

header-editor {inbound | outbound} {editor-name | default}

no header-editor {inbound | outbound} {editor-name | default}

Syntax Description

inbound	Sets the inbound SIP header editor.
outbound	Sets the outbound SIP header editor.
<i>editor-name</i>	Name of the header editor to be set for inbound or outbound signaling on the adjacency. The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
default	Sets the header editor to the default settings.

Command Default

No default behavior or values are available.

Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

The following example shows how the **header-editor** command sets header editors for inbound and outbound signaling on the SIPP SBE SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# header-editor inbound editor1
Router(config-sbc-sbe-adj-sip)# header-editor outbound default
Router(config-sbc-sbe-adj-sip)#
```

Related Commands

Command	Description
sip header-editor	Configures a header editor.

header-editor (method)

To add a header editor to act on a method, use the **header-editor** command in the signaling border element (SBE) SIP method element configuration mode. To remove a header editor, use the **no** form of this command.

header-editor *editor-name*

no header-editor

Syntax Description	<i>editor-name</i> Name of the header editor. It can be upto 30 characters.
--------------------	---

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	SBE SIP Method Element configuration (config-sbc-sbe-mep-mth-ele)
---------------	---

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE Release 3.3S</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr></table>	Release	Modification	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
------------------	--

Examples	The following example shows how the header-editor command adds a header editor to act on a method:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPPP
Router(config-sbc-sbe-adj-sip)# sip method-editor MethodEditor1
Router(config-sbc-sbe-mep-mth)# method Method2
Router(config-sbc-sbe-mep-mth-ele)# header-editor HeaderEditor1
```

Command	Description
sip header-editor	Configures a header editor.
sip method-editor	Configures a method editor.

header-name

To configure various headers, use the **header-name** command in the adjacency SIP configuration mode. To deconfigure the headers, use the **no** form of this command.

```
header-name {contact {add [tls-param] | contact-param {passthrough | strip}} | expires
suppress | from {passthrough} | p-asserted-id {assert | header-value {word}} | record-route
{passthrough} | route {destination-address {word} | port port number} | supported
{header-value {timer {insert}}} | to {passthrough} |
via {passthrough {inbound | outbound}}}
```

```
no header-name {contact {add [tls-param] | contact-param {passthrough | strip}} | expires
suppress | from {passthrough} | p-asserted-id {assert | header-value {word}} | record-route
{passthrough} | route {destination-address {word} | port port number} | supported
{header-value {timer {insert}}} | to {passthrough} |
via {passthrough {inbound | outbound}}}
```

Syntax Description

contact	Configures settings affecting the Contact: header in non-REGISTER requests.
add	Adds a specific parameter to the header.
tls-param	Specifies a 'transport=tls' parameter to SBC-originated Contact and Record-Route headers when using Transport Layer Security (TLS). This is only relevant for a trusted-encrypted or untrusted-encrypted adjacency.
contact-param	Configures settings affecting the contact header parameters.
passthrough	Passthrough header parameters from contact headers. This is the default value.
strip	Specifies strip header parameters from contact headers.
expires suppress	Specifies whether to include Expires header in the outgoing INVITE requests.
from	Configures settings affecting the From: header in non-REGISTER requests.
passthrough	Passthrough header in non-REGISTER requests.
p-asserted-id	Configures settings affecting the P-Asserted-Identity: header.
assert	Determines whether the SBC must assert a registered subscriber's identity on any outbound signal from this adjacency, by converting a P-Preferred-Identity header to a P-Asserted-Identity header on an outbound INVITE request or an OOD request. This field can be used to override the inherit profile.
header-value	Specifies the value of the P-Asserted-Identity header on the outgoing SIP message, for the messages received on this adjacency.
word	Specifies the header value.
record-route	Specifies type of SIP header to configure.
passthrough	Passthrough header in non-REGISTER requests.
route	Configures settings affecting the Route: header.
destination-address	Configures the route header destination, which is either the IP address or the domain name.
word	Specifies the IP address or the domain name.
port	Configures the route header port.
<i>port-number</i>	Specifies the port of the route header port.
supported	Configures settings affecting the Supported: header.

header-value	Configures settings affecting the Supported header-value:header.
timer	Configures settings affecting the Supported timer: header.
insert	Inserts a Supported: timer header.
to	Configures settings affecting the To: header in non-REGISTER requests.
passthrough	Passthrough header in non-REGISTER requests.
via	Configures settings affecting the Via: header.
passthrough	Allows the Via header passthrough.
inbound	Allows the Inbound Via Header passthrough.
outbound	Allows the Outbound Via Header passthrough.

Command Default No default behavior or values are available.

Command Modes Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	The keyword expires suppress was added.
	Cisco IOS XE Release 3.2	This command was modified. The contact-param keyword was added.
	Cisco IOS XE Release 3.6	This command was modified. The Via keyword was added.

Usage Guidelines This command is used in configuring Aggregate Registration.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how the **header-name** command is used to configure the passthrough header for non-REGISTER requests:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# header-name from passthrough
Router(config-sbe-adj-sip)# header-name to passthrough
```

The following example shows how the **header-name** command is used to suppress the expires header in the outgoing INVITE messages:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip mySIP
Router(config-sbe-adj-sip)# header-name expires suppress
```

Related Commands

Command	Description
request-line request-uri rewrite	Requests the SBC to rewrite the Request-URI to a different user and hostname before sending a request to a registered subscriber.

header-name p-asserted-id

To specify the value for the P-Asserted-Identity on the outgoing SIP message, use the **header-name p-asserted-id** command in SBC SBE Adjacency SIP mode. Use the **no** form of this command to remove the P-Asserted-Identity.

header-name p-asserted-id [*header-value* [*header-value*] | **assert**]

no header-name p-asserted-id [*header-value* [*header-value*] | **assert**]

Syntax Description

<i>header-value</i>	A value for the P-Asserted-Identity header as defined by RFC 3325.
assert	Enable the P-Asserted-Identity on the outgoing SIP messages.

Command Default

No default behavior or values are available.

Command Modes

SBC SBE Adjacency SIP (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The header is added to all requests and responses except ACK, CANCEL, INFO, PRACK, REGISTER and UPDATE.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following example shows how to specify the header value for the P-Asserted-Identity for adjacency CORE. In the following example, sip:1234@cisco.com is specified as the header-value:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip CORE
Router(config-sbc-sbe-adj-sip)# header-name p-asserted-id header-value sip:1234@cisco.com
Router(config-sbc-sbe-adj-sip)# header-name p-asserted-id assert
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# exit
Router(config-sbc)# exit
Router(config)# exit
```

The following show command output provides details of the above configuration:

```
Router# show sbc test sbe adjacencies CORE detail
SBC Service "test"
Adjacency CORE (SIP)
  Status: Detached
  Signaling address: 44.33.107.8:default
  Signaling-peer: :5060 (Default)
  Force next hop: No
  Account:
  Group: None
  In header profile: Default
  Out header profile: Default
  In method profile: Default
  Out method profile: Default
  In body profile: None
  Out body profile: None
  In UA option prof: Default
  Out UA option prof: Default
  In proxy opt prof: Default
  Out proxy opt prof: Default
  Priority set name: None
  Local-id: None
  Rewrite REGISTER: Off
  Register contact username: Rewrite
  Target address: None
  NAT Status: Auto Detect
  Reg-min-expiry: 3000 seconds
  Fast-register: Enabled
  Fast-register-int: 30 seconds
  Register aggregate: Disabled
  Registration Required: Enabled
  Register Out Interval: 0 seconds
  Parse username params: Disabled
  Supported timer insert: Disabled
  Suppress Expires: Disabled
p-asserted-id header-value: sip:1234@cisco.com
p-assert-id assert: Enabled
  Authenticated mode: None
  Authenticated realm: None
  Auth. nonce life time: 300 seconds
  IMS visited NetID: None
  Inherit profile: Default
  Force next hop: No
  Home network Id: None
  UnEncrypt key data: None
  SIPI passthrough: No
  Passthrough headers:
  Media passthrough: No
  Incoming 100rel strip: No
  Incoming 100rel supp: No
  Out 100rel supp add: No
  Out 100rel req add: No
  Parse TGID parms: No
  IP-FQDN inbound:
  IP-FQDN outbound:
  FQDN-IP inbound:
  FQDN-IP outbound:
  Outbound Flood Rate: None
  Hunting Triggers: Global Triggers
  Add transport=tls param: Disabled
  Redirect mode: Pass-through
  Security: Untrusted-Unencrypted
  TLS mutual authentication: No
```

```
Ping: Disabled
Ping Interval: 32 seconds
Ping Life Time: 32 seconds
Ping Peer Fail Count: 3
Ping Trap sending: Enabled
Ping Peer Status: Not Tested
Rewrite Request-uri: Disabled
Registration Monitor: Disabled
DTMF SIP NOTIFY Relay: Enabled
DTMF SIP NOTIFY Interval: 2000
DTMF SIP default duration: 200
DTMF Preferred Method: SIP NOTIFY
Realm : None
Statistics setting: Summary
```

Router#

header-name supported header-value timer insert

To insert a “Supported:timer” header, use the *header-name supported header-value timer insert* command in SBC SBE Adjacency SIP mode. Use the **no** form of this command to disable inserting the header.

header-name supported header-value timer insert

no header-name supported header-value timer insert

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values are available.

Command Modes SBC SBE Adjacency SIP (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how to configure the SIP adjacency CORE to insert a supported timer header:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip CORE
Router(config-sbc-sbe-adj-sip)# header-name supported header-value timer insert
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# exit
Router(config-sbc)# exit
Router(config)# exit
```

The following show command output provides details on the above configuration. Note the value of the supported timer insert field:

```
Router# show sbc test sbe adjacencies CORE detail
SBC Service "test"
Adjacency CORE (SIP)
  Status: Detached
  Signaling address: 44.33.107.8:default
  Signaling-peer: :5060 (Default)
  Force next hop: No
```

```

Account:
Group:                None
In header profile:    Default
Out header profile:   Default
In method profile:    Default
Out method profile:   Default
In body profile:      None
Out body profile:     None
In UA option prof:    Default
Out UA option prof:   Default
In proxy opt prof:    Default
Out proxy opt prof:   Default
Priority set name:    None
Local-id:             None
Rewrite REGISTER:     Off
Register contact username: Rewrite
Target address:       None
NAT Status:           Auto Detect
Reg-min-expiry:       3000 seconds
Fast-register:        Enabled
Fast-register-int:    30 seconds
Register aggregate:   Disabled
Registration Required: Enabled
Register Out Interval: 0 seconds
Parse username params: Disabled
Supported timer insert: Enabled
Suppress Expires:     Disabled
p-asserted-id header-value: sip:1234@cisco.com
p-assert-id assert:   Enabled
Authenticated mode:   None
Authenticated realm:  None
Auth. nonce life time: 300 seconds
IMS visited NetID:    None
Inherit profile:      Default
Force next hop:       No
Home network Id:      None
UnEncrypt key data:   None
SIPi passthrough:     No
Passthrough headers:
Media passthrough:    No
Incoming 100rel strip: No
Incoming 100rel supp: No
Out 100rel supp add:  No
Out 100rel req add:   No
Parse TGID parms:     No
IP-FQDN inbound:
IP-FQDN outbound:
FQDN-IP inbound:
FQDN-IP outbound:
Outbound Flood Rate:  None
Hunting Triggers:     Global Triggers
Add transport=tls param: Disabled
Redirect mode:         Pass-through
Security:              Untrusted-Unencrypted
TLS mutual authentication: No
Ping:                  Disabled
Ping Interval:         32 seconds
Ping Life Time:        32 seconds
Ping Peer Fail Count:  3
Ping Trap sending:     Enabled
Ping Peer Status:      Not Tested
Rewrite Request-uri:   Disabled
Registration Monitor:  Disabled
DTMF SIP NOTIFY Relay: Enabled

```

```
DTMF SIP NOTIFY Interval: 2000
DTMF SIP default duration: 200
DTMF Preferred Method: SIP NOTIFY
Realm : None
Statistics setting: Summary
```

header-name via passthrough

To configure the session border controller (SBC) to allow the Via headers on inbound requests or outbound requests for a specified adjacency to pass through, use the **header-name via passthrough** command in the adjacency SIP configuration mode. To disable passthrough of Via headers on inbound requests or outbound requests, use the **no** form of this command.

header-name via passthrough {inbound | outbound}

no header-name via passthrough {inbound | outbound}

Syntax Description	inbound	Specifies that the Via headers on inbound requests for a specified adjacency must be allowed to pass through.
	outbound	Specifies that the Via headers on outbound requests for a specified adjacency must be allowed to pass through.

Command Default	The SBC removes the existing Via headers and adds its own Via header.
-----------------	---

Command Modes	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
---------------	--

Command History	Release	Modification
	3.6S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to use the header-name via passthrough command to allow the Via headers on inbound requests and outbound requests for a specified adjacency to pass through:
----------	---

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe) # adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# header-name via passthrough inbound
Router(config-sbc-sbe-adj-sip)# header-name via passthrough outbound
```

Related Commands

Command	Description
header-name	Configures the contact header and passthrough header in non-REGISTER requests.
header-name p-asserted-id	Specifies the value for the P-Asserted-Identity header on outgoing SIP messages.
header-name supported header-value timer insert	Inserts the Supported:timer header in SIP messages.

header-prio header-name

To configure the priority of a header that is used to derive a source, destination, or diverted-by address, use the **header-prio header-name** command in the appropriate SIP header address configuration mode. To remove the priority from a header, use the **no** form of this command.

header-prio *priority-level* **header-name** *header-name* [**request-uri**]

no header-prio *priority-level* **header-name** *header-name* [**request-uri**]

Syntax Description

<i>priority-level</i>	Specifies the priority number to assign to the header. Priority levels are 1 to 10.
<i>header-name</i>	Name of the existing header, that is used to derive the source, destination, or diverted-by address, to which the <i>priority-level</i> is assigned.
request-uri	(Optional) Specifies that the Request URI is to be used for extraction of the destination address. (Available only in destination address mode.)

Command Default

No default behavior or values are available.

Command Modes

SIP header destination address configuration (config-sbc-sbe-sip-hdr-dst)
SIP header source address configuration (config-sbc-sbe-sip-hdr-src)
SIP header diverted-by address configuration (config-sbc-sbe-sip-hdr-div)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of modes required to run the command.

This command can be used multiple times to set the priorities of multiple headers.

Examples

The following example shows how to configure the priority of a header that uses the Request URI to derive a destination address:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile HP1
Router(config-sbc-sbe-sip-hdr) dst-address
Router(config-sbc-sbe-sip-hdr-dst)# header-prio 1 header-name request-uri
Router(config-sbc-sbe-sip-hdr-dst)#
```

The following example shows how to configure a list of headers to derive a destination address:

```

ASR-1002# configure terminal
ASR-1002(config)# sbc mySBC
ASR-1002(config-sbc)# sbe
ASR-1002(config-sbc-sbe)# sip header-profile Hprof1
ASR-1002(config-sbc-sbe-sip-hdr)# dst-address
ASR-1002(config-sbc-sbe-sip-hdr-dst)# header-prio 1 header-name P-Called-ID
ASR-1002(config-sbc-sbe-sip-hdr-dst)# header-prio 2 header-name To
ASR-1002(config-sbc-sbe-sip-hdr-dst)# header-prio 2 header-name Request-uri
ASR-1002(config-sbc-sbe-sip-hdr-dst)# end

```

The following example shows how to configure a list of headers to derive a source address:

```

ASR-1002# configure terminal
ASR-1002(config)# sbc mySBC
ASR-1002(config-sbc)# sbe
ASR-1002(config-sbc-sbe)# sip header-profile Hprof1
ASR-1002(config-sbc-sbe-sip-hdr)# src-address
ASR-1002(config-sbc-sbe-sip-hdr-src)# header-prio 1 header-name Remote-Party-ID
ASR-1002(config-sbc-sbe-sip-hdr-src)# header-prio 2 header-name P-Preferred-Identity
ASR-1002(config-sbc-sbe-sip-hdr-src)# header-prio 2 header-name From
ASR-1002(config-sbc-sbe-sip-hdr-src)# end
ASR-1002#

```

The following example shows how to configure a list of headers to derive a source address of a diverted call:

```

ASR-1002# configure terminal
ASR-1002(config)# sbc mySBC
ASR-1002(config-sbc)# sbe
ASR-1002(config-sbc-sbe)# sip header-profile Hprof1
ASR-1002(config-sbc-sbe-sip-hdr)# div-address
ASR-1002(config-sbc-sbe-sip-hdr-div)# header-prio 1 header-name Diversion
ASR-1002(config-sbc-sbe-sip-hdr-div)# end
ASR-1002#

```

The following is an example of the show command output after the header list for destination address, source address, and diversion address is configured on an SBC:

```

ASR-1002# show sbc mine sbe sip header-profile Hprof1
Header profile "Hprof1"
Description:
Type:      Whitelist
dst-address: (inbound only)
    header-prio 1 header-name P-Called-ID
    header-prio 2 header-name To
    header-prio 3 header-name Request-uri
src-address: (inbound only)
    header-prio 1 header-name Remote-Party-ID
    header-prio 2 header-name P-Preferred-Identity
    header-prio 3 header-name From
div-address (inbound only)
    header-prio 1 Diversion
store-rules:
    No store-rule entries found.
request-line:
    No request-line entries found.
headers:
    test
        entry 1
            description:
            action add-first-header value "cisco"
            condition is-request eq true
    Not in use with any adjacencies
    Not in use with any method-profile

```

Related Commands	Command	Description
	activate (enum)	Activates ENUM client.
	dial-plan-suffix	Configures the dial plan suffix used for the ENUM query.
	div-address	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	dst-address	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
	entry (enum)	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
	enum	Configures the ENUM client ID number and enter the ENUM configuration mode.
	header-prio header-name	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
	max-recursive-depth	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
	max-responses	Configures the maximum number of ENUM records returned to the routing module.
	req-timeout	Configures the ENUM request timeout period.
	src-address	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
	server ipv4	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
	show sbc sbe call-policy-set	Displays configuration and status information about call policy sets.
	show sbc sbe enum	Displays the configuration information about an ENUM client.
	show sbc sbe enum entry	Displays the contents of an ENUM client entry.

header-prio header-name (editor)

To configure the priority of a header that is used to derive a source, destination, or diverted-by address, use the **header-prio header-name** command in the appropriate session initiation protocol (SIP) Header Address configuration mode. To remove the priority from a header, use the **no** form of this command.

header-prio *priority-level* **header-name** *header-name* [**request-uri**]

no header-prio *priority-level*

Syntax Description	<i>priority-level</i>	Priority number to be assigned to the header. Priority levels are 1 to 10.
	<i>header-name</i>	Name of the existing header that is used to derive the source, destination, or diverted-by address to which the <i>priority-level</i> is assigned.
	request-uri	(Optional) Specifies that the Request URI is to be used for the extraction of the destination address. (Available only in Destination address mode.)

Command Default No default behavior or values are available.

Command Modes SIP header destination address configuration (config-sbc-sbe-sip-hdr-dst)
SIP header source address configuration (config-sbc-sbe-sip-hdr-src)
SIP header diverted-by address configuration (config-sbc-sbe-sip-hdr-div)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

This command can be used multiple times to set the priorities of multiple headers.

Examples The following example shows how to configure the priority of a header that uses the Request URI to derive a destination address:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor HP1
Router(config-sbc-sbe-mep-hdr) dst-address
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 1 header-name request-uri
Router(config-sbc-sbe-mep-hdr-dst)#
```

The following example shows how to configure a list of headers to derive a destination address:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Hprof1
Router(config-sbc-sbe-mep-hdr)# dst-address
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 1 header-name P-Called-ID
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 2 header-name To
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 2 header-name Request-uri
Router(config-sbc-sbe-mep-hdr-dst)# end
```

The following example shows how to configure a list of headers to derive a source address:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Hprof1
Router(config-sbc-sbe-mep-hdr)# src-address
Router(config-sbc-sbe-mep-hdr-src)# header-prio 1 header-name Remote-Party-ID
Router(config-sbc-sbe-mep-hdr-src)# header-prio 2 header-name P-Preferred-Identity
Router(config-sbc-sbe-mep-hdr-src)# header-prio 2 header-name From
Router(config-sbc-sbe-mep-hdr-src)# end
Router#
```

The following example shows how to configure a list of headers to derive the source address of a diverted call:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Hprof1
Router(config-sbc-sbe-mep-hdr)# div-address
Router(config-sbc-sbe-mep-hdr-div)# header-prio 1 header-name Diversion
Router(config-sbc-sbe-mep-hdr-div)# end
Router#
```

Related Commands

Command	Description
div-address	Enables entry into the Diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
dst-address	Enables entry into the Destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
src-address	Enables entry into the Source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
sip header-editor	Configures a header editor.

header-profile

To set a specified header profile for inbound and outbound signaling on a specified SBE SIP adjacency, use the **header-profile** command in adjacency sip configuration mode.

header-profile {inbound | outbound} *profile-name*

Syntax Description	inbound outbound	Sets the inbound and outbound SIP header profiles.
	<i>profile-name</i>	Specifies the name of the header profile to be set for inbound or outbound signaling on a specified adjacency. The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names. Note If you enter the name default , the default header profile is set for inbound or outbound signaling.

Command Default No default behavior or values are available.

Command Modes Adjacency sip configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how the **header-profile** command sets header profiles for inbound and outbound signaling on an SBE SIP adjacency test:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# header-profile inbound profile1
Router(config-sbc-sbe-adj-sip)# header-profile outbound profile2
Router(config-sbc-sbe-adj-sip)#
```

header (editor)

To add a header to a SIP message editor, use the **header** command in the SIP Header Editor configuration mode. To remove a header, use the **no** form of this command.

header *header-name* [**entry** *entry-number*]

no header *header-name* [**entry** *entry-number*]

Syntax Description

<i>header-name</i>	Name of the header to be added to the header editor. Valid names are 1 to 32 characters in length (inclusive) and case-sensitive.
entry	Specifies the filtered entry number. By default, it is 1.
<i>entry-number</i>	Entry number that can range from 1 to 99.

Command Default

By default, the entry number is 1.

Command Modes

SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

The following example shows how the **header** command adds a header, test, to the Myeditor header editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Myeditor
Router(config-sbc-sbe-sip-hdr)# header test
```

Related Commands

Command	Description
blacklist	Configures a SIP header or method blacklist editor on a SIP message.
description	Configures descriptive text for a SIP header.
sip header-editor	Configures a header editor.

header (session border controller)

To add a header with a specified name to a SIP message profile, use the **header** command in SIP header-profile configuration mode. To remove the method from the profile, use the **no** form of this command.

header *header-name*

no header *header-name*

Syntax Description	<i>header-name</i>	Specifies the name of the header added to the header profile. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.
---------------------------	--------------------	--

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	SIP header configuration (config-sbc-sbe-sip-hdr)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how the header command adds the header “test” to the header profile Myprofile:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile Myprofile
Router(config-sbc-sbe-sip-hdr)# header test
```

Related Commands	Command	Description
	blacklist	Configures SIP header or method blacklist profiles on a SIP message.
	description	Configures descriptive text for a SIP header.

heart-beat terminate

To configure the interval during which only one heartbeat request from an H.248 terminal device can pass through the Border Access Controller (BAC), and terminate the other heartbeat requests sent during this interval, use the **heart-beat terminate** command in the H248 BAC adjacency configuration mode. To return to the default value, use the **no** form of this command.

heart-beat terminate *terminate-interval*

no heart-beat terminate *terminate-interval*

Syntax Description

<i>terminate-interval</i>	Interval during which heartbeat requests are terminated, in seconds. The range is from 0 to 3600. The default value is 60.
---------------------------	--

Command Default

The default terminate interval is 60 seconds.

Command Modes

H248 BAC adjacency configuration (config-h248-bac-adj)

Command History

Release	Modification
Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To disable the heartbeat termination function, set the *terminate-interval* to 0 seconds. If the *terminate-interval* is 0 seconds, then all the heartbeat requests are passed through the BAC and none are terminated.

This command can be configured only in the access adjacency submode and not in the core adjacency submode.

Examples

The following example shows how the **heart-beat terminate** command is used to configure the terminate interval:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# heart-beat terminate 80
```

hold-media-timeout

To configure the time an SBE will wait after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down, use the **hold-media-timeout** command in SBE configuration mode. To set the number to its default, use the **no** form of this command.

hold-media-timeout timeout

Syntax Description	<i>timeout</i>	Specifies the time in milliseconds an SBE will wait after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down.
--------------------	----------------	--

Command Default	The default value is 0 milliseconds.
-----------------	--------------------------------------

Command Modes	SBE configuration (config-sbc-sbe)
---------------	------------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following command configures the SBE to wait two hours after receiving the last media packet on an on-hold call before cleaning up the call resources:
----------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# hold-media-timeout 7200
Router(config-sbc-sbe)#
```

hunt-on-reject

To set the trigger on hunting, use the **hunt-on-reject** command in the signaling border element (SBE) SIP body element configuration mode. To stop the trigger, use the **no** form of this command.

hunt-on-reject

no hunt-on-reject

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values are available.

Command Modes SBE SIP body element configuration (config-sbc-sbe-mep-bdy-ele)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples The following example shows how to create a body editor named bodyeditor1, describe the body type that is to act on the messages with the *application/ISUP* Content Type header, and set the trigger on hunting:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-editor bodyeditor1
Router(config-sbc-sbe-mep-bdy)# body application/ISUP
Router(config-sbc-sbe-mep-bdy-ele)# hunt-on-reject
Router(config-sbc-sbe-mep-bdy-ele)#
```

Related Commands	Command	Description
	body	Names a body type or content header type for a non-SDP message body that is a part of a body editor.
	body-editor	Associates a body editor at a SIP adjacency level to an adjacency in the SIP adjacency mode.
	sip body-editor	Creates a body editor to filter the non-SDP bodies from the incoming and outgoing SIP messages.

hunting-mode

To configure the form of H.323 hunting to perform if hunting is triggered, use the **hunting-mode** command in one of its supported modes: H.323 (global H.323 scope) and adjacency h323 (destination H.323 adjacency). The **no** form of the command resets to the default of alternate end points.

hunting-mode {altEndps | multiARQ}

no hunting-mode

Syntax Description	<i>altEndps</i>	Specifies alternate end points hunting. When H.323 has a list of alternate endpoints for a call, H.323 tries each endpoint in turn before reporting a routing failure.
	<i>multiARQ</i>	Specifies multiARQ hunting. This is a non-standard H.323 mechanism for hunting for other routes or destination adjacencies. It is based on issuing multiple Admission Requests (ARQs) to a Gatekeeper for a single call.

Command Default Default is alternate end points (altEndps) if user does not configure a hunting-mode or configures **no hunting-mode**. It does not disable hunting completely.

Command Modes H.323 configuration (config-sbc-sbe-h323)
Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines The SBC hunts for other routes or destination adjacencies in the event of a failure. Hunting re-routes the call in response to a specific user-configured event or error code. The hunting mode is typically set after the hunting-trigger is configured.

The Examples section shows the hierarchy of modes required to run the command.

Examples The following example shows how to configure H.323 to perform multiARQ hunting and to retry routing if it receives a noBandwidth or securityDenied error:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# h323
Router (config-sbc-sbe-h323)# hunting-trigger noBandwidth securityDenied
Router (config-sbc-sbe-h323)# hunting-mode multiARQ
```

Related Commands	Command	Description
	hunting-trigger	Configures failure return codes to trigger hunting.

hunting-trigger

To configure failure return codes to trigger hunting, use the **hunting-trigger** command in one of its supported modes: SIP (global SIP scope), H.323 (global H.323 scope), adjacency SIP (destination SIP adjacency), and adjacency h323 (destination H.323 adjacency). The **no** form of the command clears all error codes.

If you enter **no hunting-trigger x y**, then just codes x and y are removed from the configured list.

hunting-trigger {error-codes | disable} error-codes

no hunting-trigger {error-codes | disable} error-codes

Syntax Description

<i>error-codes</i> (SIP and adjacency modes)	Signifies a space-separated list of SIP numeric error codes.
<i>error-codes</i> (h323 and adjacency h323 modes)	Specifies one of the following values: - noBandwidth—H.225 no bandwidth response. - unreachableDestination—H.225 unreachable destination response. - destinationRejection—H.225 destination rejection response. - noPermission—H.225 no permission response. - gatewayResources—H.225 gateway Resources response. - badFormatAddress—H.225 bad format address response. - securityDenied— H.225 security denied response. connectFailed—Internal response. noRetry—Specifies that routing should never be retried for this adjacency no matter what failure return code is received.

Command Default

No default behavior or values are available.

Command Modes

SBE SIP configuration (config-sbc-sbe)
H.323 configuration (config-sbc-sbe-h323)
Adjacency SIP configuration (config-sbc-sbe-adj-sip)
Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If both adjacency level and SBE level hunting triggers are configured, the adjacency level takes priority.

If you enter **hunting-trigger x** followed by **hunting-trigger y**, the value of **x** is replaced with **y**.

To set both **x** and **y** to be hunting triggers, you must enter **hunting-trigger x y**.

The Examples section shows the hierarchy of modes required to run the command.

In the adjacency SIP or H.323 adjacency modes, if you specify the special hunting-trigger value of **disable**, routes are never retried to this adjacency, even if the error code is on the global retry list.

To configure more than one H.323 hunting trigger, you must enter the commands as separate lines, such as in the following example:

```
sbc mySBC
sbe
  adjacency h323 h1
    hunting-trigger badFormatAddress
    hunting-trigger connectFailed
```

Examples

SIP mode

The following example shows how to configure SIP to retry routing if it receives a 415 (media unsupported) or 480 (temporarily unavailable) error:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# sip hunting-trigger 416 480
```

H.323 mode

The following example shows how to configure H.323 to retry routing if it receives a noBandwidth or securityDenied error. Note that for multiple error codes, each hunting trigger must be configured on a separate line:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# h323
Router (config-sbc-sbe-h323)# hunting-trigger noBandwidth
Router (config-sbc-sbe-h323)# hunting-trigger securityDenied
```

SIP adjacency mode

The following example shows how to configure SIP to retry routing to the SIP adjacency SipAdj1 if it receives a 415 (media unsupported) or 480 (temporarily unavailable) error:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router (config-sbc-sbe-adj-sip)# hunting-trigger 415 480
```

H.323 adjacency mode

The following example shows how to configure H.323 to retry routing to the H.323 adjacency h323Adj1 if it receives a noBandwidth or securityDenied error. Note that for multiple error codes, each hunting trigger must be configured on a separate line:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323Adj1
Router (config-sbc-sbe-adj-h323)# hunting-trigger noBandwidth
```

```
Router (config-sbc-sbe-adj-h323) # hunting-trigger securityDenied
```

import-map

To configure flexible policy handling by a BGP route server, use the **import-map** command in route server context address family configuration mode. To remove the route server’s flexible policy handling, use the **no** form of this command.

import-map *route-map-name*

no import-map *route-map-name*

Syntax Description	<i>route-map-name</i>	Name of the route map that controls which routes will be added to the route server client virtual table.
--------------------	-----------------------	--

Command Default	No import map exists and no flexible policy handling by a route server exists.
-----------------	--

Command Modes	Route server context address family configuration (config-router-rsctx-af)
---------------	--

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE 3.3S</td><td>This command was introduced.</td></tr></table>	Release	Modification	Cisco IOS XE 3.3S	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3S	This command was introduced.				

Usage Guidelines	Use this command if your BGP route server needs to support flexible policies. In order to configure flexible policy handling, you must create a route server context, which includes an import map. The import map references a standard route map. You may match on nexthop, AS path, communities, and extended communities.
------------------	---

 Note	Do not confuse the import-map command with the import map command in VRF configuration submode, which configures an import route map for a VPN routing and forwarding (VRF) instance.
---	---

Examples	In the following example, the local router is a BGP route server. Its neighbors at 10.10.10.12 and 10.10.10.13 are its route server clients. A route server context named ONLY_AS27_CONTEXT is created and applied to the neighbor at 10.10.10.13. The context uses an import map that references a route map named only_AS27_routemap. The route map matches routes permitted by access list 27. Access list 27 permits routes that have 27 in the autonomous system path.
----------	--

```
router bgp 65000
  route-server-context ONLY_AS27_CONTEXT
    address-family ipv4 unicast
      import-map only_AS27_routemap
    exit-address-family
  exit-route-server-context
  !
  neighbor 10.10.10.12 remote-as 12
  neighbor 10.10.10.12 description Peer12
  neighbor 10.10.10.13 remote-as 13
```

```

neighbor 10.10.10.13 description Peer13
neighbor 10.10.10.21 remote-as 21
neighbor 10.10.10.27 remote-as 27
!
address-family ipv4
  neighbor 10.10.10.12 activate
  neighbor 10.10.10.12 route-server-client
  neighbor 10.10.10.13 activate
  neighbor 10.10.10.13 route-server-client context ONLY_AS27_CONTEXT
  neighbor 10.10.10.21 activate
  neighbor 10.10.10.27 activate
exit-address-family
!
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
  match as-path 27
!
```

Related Commands

Command	Description
description (route server context)	Describes a route server context for a user-friendly way to see the purpose of the route server context.
route-map	Enables policy routing.
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

ims media-service

To configure a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources, use the **ims media-service** command in CAC table entry configuration mode. To return to the default condition where only Rx is used, use the no form of this command.

ims media-service

no ims media-service

Syntax Description

This command has no arguments or keywords.

Command Default

When media service is not configured, only Rx is in use.

Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

By default, only Rx is in use, and media and 3rd-party transcoding resources cannot be used. When IMS media service is configured, Rx is used as well as media resources and 3rd party transcoding resources.



Note

Media bypass takes precedence over IMS media service configuration.

Examples

The following example shows how to configure a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# ims media-service
```

Related Commands	Command	Description
	diameter	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	origin-realm	Configures the domain name of an IMS local realm.
	origin-host	Configures the domain name of an IMS local host.
	peer	Creates an IMS peer and configure the name and IPv4 address of the peer.
	realm (diameter)	Configures a peer and assign the peer to a realm.
	show sbc sbe diameter	Displays the configuration information for the Diameter protocol.
	show sbc sbe diameter peers	Displays the configuration information for IMS peers.
	show sbc sbe diameter stats	Displays the transport statistics for an IMS peer.
	ims rx	Configures an IMS Rx interface for access adjacency
	ims pani	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
	ims realm	Configures an IMS realm for use by an IMS Rx interface.
	ims rx preliminary-aar-forbid	Prevents preliminary AAR messages from being sent in an IMS Rx session.
	ims media-service	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

ims pani

To configure the P-Access-Network-Info (PANI) header process preference for an adjacency, use the **ims pani** command in adjacency SIP configuration mode. To remove a PANI header process preference from an adjacency, use the no form of this command.

```
ims pani [received | rx | received rx | rx received]

no ims pani [received | rx | received rx | rx received]
```

Syntax Description

received	Specifies that information in the PANI header of a received message has preference over information from the Rx interface. The received message PANI is passed through.
rx	Specifies that information from the Rx interface has preference and overrides the information in the PANI header of a received message.
received rx	Specifies that if a received message contains a PANI header, it is passed through. Otherwise, a PANI header is added to the received message, using information from the Rx interface.
rx received	Specifies that information from the Rx interface has preference if there is any. Otherwise, the PANI header of the received message is passed through.

Command Default

If no keywords are specified, the default is **rx received**.

Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



Note

This command may be used when the adjacency is active, but it will only apply to new calls. It will not effect existing calls.

Examples

The following example shows how to configure the PANI header process preference for an adjacency:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
```

```
Router(config-sbc-sbe-adj-sip)# ims pani
```

Related Commands

Command	Description
diameter	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
origin-realm	Configures the domain name of an IMS local realm.
origin-host	Configures the domain name of an IMS local host.
peer	Creates an IMS peer and configure the name and IPv4 address of the peer.
realm (diameter)	Configures a peer and assign the peer to a realm.
show sbc sbe diameter	Displays the configuration information for the Diameter protocol.
show sbc sbe diameter peers	Displays the configuration information for IMS peers.
show sbc sbe diameter stats	Displays the transport statistics for an IMS peer.
ims rx	Configures an IMS Rx interface for access adjacency
ims pani	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
ims realm	Configures an IMS realm for use by an IMS Rx interface.
ims rx preliminary-aar-forbid	Prevents preliminary AAR messages from being sent in an IMS Rx session.
ims media-service	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

ims realm

To configure an IMS realm for use by either an IMS Rx interface or an IMS Rf interface, use the **ims realm** command in adjacency SIP configuration mode. To remove an IMS realm, use the no form of this command.

```
ims realm realm-name

no ims realm realm-name
```

Syntax Description	realm-name	Specifies a case sensitive, unique name for the realm. The maximum length is 63 characters.
--------------------	------------	---

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.1S	This command was updated to support an IMS Rf interface.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to configure an IMS realm for use by an IMS Rx interface:
----------	---

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# ims realm Realm_1
```

Related Commands	Command	Description
	diameter	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	origin-realm	Configures the domain name of an IMS local realm.
	origin-host	Configures the domain name of an IMS local host.
	peer	Creates an IMS peer and configure the name and IPv4 address of the peer.

Command	Description
realm (diameter)	Configures a peer and assign the peer to a realm.
show sbc sbe diameter	Displays the configuration information for the Diameter protocol.
show sbc sbe diameter peers	Displays the configuration information for IMS peers.
show sbc sbe diameter stats	Displays the transport statistics for an IMS peer.
ims rx	Configures an IMS Rx interface for access adjacency
ims pani	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
ims realm	Configures an IMS realm for use by an IMS Rx interface.
ims rx preliminary-aar-forbid	Prevents preliminary AAR messages from being sent in an IMS Rx session.
ims media-service	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

ims rf

To enable the IP Multimedia Subsystem (IMS) Rf interface for an access adjacency on the Cisco Session Border Controller (SBC), use the **ims rf** command in the SBC SBE adjacency SIP configuration mode. To disable the IMS Rf interface for an access adjacency, use the **no** form of this command.

ims rf

no ims rf

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

SBC SBE adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command cannot be modified unless the operational state of the access adjacency is down.

Examples

The following example shows how to disable the IMS Rf interface for an access adjacency on the SBC:

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# no ims rf
```

ims rx

To configure an IMS Rx interface for access adjacency, use the **ims rx** command in adjacency SIP configuration mode. To remove an IMS Rx interface, use the no form of this command.

ims rx [**pcrf** *pcrf-name*]

no ims rx [**pcrf** *pcrf-name*]

Syntax Description

pcrf <i>pcrf-name</i>	(Optional) Specifies the name of (and provides the contact point to) the Policy and Charging Rule Function (PCRF) operating in Rx mode. The PCRF configures the destination-host AVP used for Diameter messages. The PCRF name must be a case sensitive, unique, fully qualified domain name (FQDN). The maximum is length 128 characters.
------------------------------	--

Command Default

When PCRF is not specified, Rx messages are routed by realm.

Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



Note

This command can only be used when the operational state of the adjacency is down.

Examples

The following example shows how to configure an IMS Rx interface for access adjacency:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# ims rx
```

Related Commands

Command	Description
diameter	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
origin-realm	Configures the domain name of an IMS local realm.

Command	Description
origin-host	Configures the domain name of an IMS local host.
peer	Creates an IMS peer and configure the name and IPv4 address of the peer.
realm (diameter)	Configures a peer and assign the peer to a realm.
show sbc sbe diameter	Displays the configuration information for the Diameter protocol.
show sbc sbe diameter peers	Displays the configuration information for IMS peers.
show sbc sbe diameter stats	Displays the transport statistics for an IMS peer.
ims rx	Configures an IMS Rx interface for access adjacency
ims pani	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
ims realm	Configures an IMS realm for use by an IMS Rx interface.
ims rx preliminary-aar-forbid	Prevents preliminary AAR messages from being sent in an IMS Rx session.
ims media-service	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

ims rx preliminary-aar-forbid

To prevent preliminary AAR messages from being sent in an IMS Rx session, use the **ims rx preliminary-aar-forbid** command in CAC table entry configuration mode. To return to the default condition where preliminary AAR messages are sent, use the no form of this command.

ims rx preliminary-aar-forbid

no ims rx preliminary-aar-forbid

Syntax Description

This command has no arguments or keywords.

Command Default

Preliminary AAR messages are sent.

Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following example shows how to prevent preliminary AAR messages from being sent in an IMS Rx session:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# ims rx preliminary-aar-forbid
```

Related Commands

Command	Description
diameter	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
origin-realm	Configures the domain name of an IMS local realm.
origin-host	Configures the domain name of an IMS local host.

Command	Description
peer	Creates an IMS peer and configure the name and IPv4 address of the peer.
realm (diameter)	Configures a peer and assign the peer to a realm.
show sbc sbe diameter	Displays the configuration information for the Diameter protocol.
show sbc sbe diameter peers	Displays the configuration information for IMS peers.
show sbc sbe diameter stats	Displays the transport statistics for an IMS peer.
ims rx	Configures an IMS Rx interface for access adjacency
ims pani	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
ims realm	Configures an IMS realm for use by an IMS Rx interface.
ims rx preliminary-aar-forbid	Prevents preliminary AAR messages from being sent in an IMS Rx session.
ims media-service	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

inbound secure

To configure the incoming calls from an H.323 adjacency as secure calls, use the **inbound secure** command in the H.323 Adjacency configuration mode. To restore the insecure status to the incoming calls, use the **no** form of this command.

inbound secure

no inbound secure

Syntax Description

This command has no arguments or keywords.

Command Default

By default, all the incoming calls are insecure calls.

Command Modes

H.323 Adjacency configuration mode (config-sbc-sbe-adj-h323)

Command History

Release	Modification
3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

To ensure that the calls coming from an H323 adjacency are treated as secure calls, define the incoming calls from an H.323 adjacency as secure calls using the **inbound secure** command in the H.323 Adjacency configuration mode. By default, all incoming calls are insecure calls.

To configure the incoming secure calls as not secured, use the **no inbound secure** command from H.323 adjacency configuration mode.



Note

If an H.323 adjacency is configured as untrusted, you cannot configure an incoming calls as secure calls.

Examples

The following example shows how to configure incoming calls from an H.323 adjacency as secure calls:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h.323 trust-h323-adj
Router(config-sbc-sbe-adj-h323)# inbound secure
```

Related Commands

Command	Description
trunk trusted	Configures an H.323 adjacency as trusted.

inherit profile

To configure a global inherit profile for the SIP adjacency, use the **inherit profile** command in adjacency SIP configuration mode. To deconfigure the global inherit profile, use the **no** form of this command.

```
inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external |
                preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering |
                preset-standard-non-ims}

no inherit profile
```

Syntax Description

preset-access	Specifies a preset access profile for an adjacency that faces an access device on a User-Network Interface (UNI) location.
preset-core	Specifies a preset core profile for an adjacency that faces a core device on a UNI location. This is the default.
preset-ibcf-ext-untrusted	Specifies a preset IBCF external untrusted profile.
preset-ibcf-external	Specifies a preset IBCF external profile.
preset-ibcf-internal	Specifies a preset IBCF internal profile.
preset-p-cscf-access	Specifies a preset P-CSCF-access profile.
preset-p-cscf-core	Specifies a preset P-CSCF-core profile.
preset-peering	Specifies a preset peering profile for an adjacency that faces a peer device on a Network-Network Interface (NNI) location.
preset-standard-non-ims	Specified a preset standard-non-IMS profile.

Command Default

The default inherit profile setting is preset-core.

Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 2.4	The command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

This adjacency-specific configuration overrides any global configuration of the adjacency that was configured using the **sip inherit profile** command.

Examples

The following example shows how the **inherit profile** command is used to configure a P-CSCF-access inherit profile on a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-access
```

Related Commands

Command	Description
adjacency	Configures an adjacency for an SBC.

interwork cost

To specify the resource cost for an audio stream using inband DTMF interworking or to specify the resource cost for an audio or video stream using SRTP encryption and decryption, use the **transcode cost** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

interwork {**inband-dtmf** | **srtp**} **cost** *number*

no interwork {**inband-dtmf** | **srtp**} **cost**

Syntax Description

inband-dtmf	Specifies that the resource cost is to be set for an audio stream that is using inband DTMF interworking.
srtp	Specifies that the resource cost is to be set for an audio or video stream that is using SRTP encryption and decryption.
<i>number</i>	Resource cost. The range is from 1 to 4294967295.

Command Default

The default resource cost for an audio stream using inband DTMF interworking is 4. Similarly, the default resource cost for an audio or video stream using SRTP encryption and decryption is 15. When you use the **no** form of this command, the resource cost is changed to the default value.

Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

Examples

In the following example, the **interwork cost** command is used to set the resource cost for an audio stream using inband DTMF interworking to 8. This command is also used to set the resource cost for an audio or video stream using SRTP encryption and decryption to 20.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway policy type default
Router(config-sbc-sbe-media-pol)# interwork inband-dtmf cost 8
Router(config-sbc-sbe-media-pol)# interwork srtp cost 20
```

Related Commands	Command	Description
	interwork maximum	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	interwork cost	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	ipsec maximum	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	media-gateway policy type	Configures a media gateway policy.
	media limits	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	media-policy	Configures a media policy.
	show sbc sbe media-gateway-policy	Displays the details of media gateway policies.
	show sbc sbe media-policy	Displays the details of media policies.
	total resource maximum	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	transcode cost	Specifies the resource cost for transcoding an audio or video stream.
	transcode maximum	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	transrate audio cost	Specifies the resource cost for transrating an audio stream.
	transrate audio maximum	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	type	Configures a media policy as a CAC-policy type policy or a gateway type policy.

interwork maximum

To specify the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time, use the **interwork maximum** command in the SBE media policy configuration mode. To remove the maximum limit, use the **no** form of this command.

interwork {inband-dtmf | srtp} maximum *number*

no interwork {inband-dtmf | srtp} maximum

Syntax Description

<i>number</i>	Maximum number of media streams that can use the interworking service specified in the command.
---------------	---

Command Default

*The default maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time is 4294967295. When you use the **no** form of this command, any maximum limit set earlier is changed to this default value.*

Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

In the following example, the **interwork maximum** command is used to set the maximum number of calls that use the SRTP interworking service at any point of time to 500:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
Router(config-sbc-sbe-media-pol)# type cac-policy
Router(config-sbc-sbe-media-pol)# interwork srtp maximum 500
```

Related Commands	Command	Description
	interwork maximum	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	interwork cost	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	ipsec maximum	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	media-gateway policy type	Configures a media gateway policy.
	media limits	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	media-policy	Configures a media policy.
	show sbc sbe media-gateway-policy	Displays the details of media gateway policies.
	show sbc sbe media-policy	Displays the details of media policies.
	total resource maximum	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	transcode cost	Specifies the resource cost for transcoding an audio or video stream.
	transcode maximum	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	transrate audio cost	Specifies the resource cost for transrating an audio stream.
	transrate audio maximum	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	type	Configures a media policy as a CAC-policy type policy or a gateway type policy.

invite-timeout

To configure the time that SBC waits for a final response to an outbound SIP invite request, use the **invite-timeout** command in IP timer configuration mode. To return to the default value, use the **no** form of this command.

invite-timeout {interval-value}

no invite-timeout

Syntax Description	<i>interval-value</i> Time, in seconds, SBC waits before timing out an outbound invite request.	
Command Default	The default wait interval is 180 seconds. If no response is received during that time, an internal 408 request timeout response is generated and is sent to the caller.	
Command Modes	SIP timer (config-sbc-sbe-sip-tmr)	
Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command. If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.	
Examples	The following example shows how to configure the SBC to time out invite transactions after 60 seconds: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# sip timer Router(config-sbc-sbe-sip-tmr)# invite-timeout 60 Router(config-sbc-sbe-sip-tmr)# exit</pre>	
Related Commands	Command	Description
	udp-response-linger-period	Configures the time period that SBC retains negative UDP responses to invite requests.

ipsec maximum

To specify the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, use the **ipsec maximum** command in the SBE CAC table CAC policy configuration mode. To remove this configuration, use the **no** form of this command.

ipsec maximum {registers | calls} *number*

no ipsec maximum {registers | calls}

Syntax Description

<i>number</i>	Specifies one of the following: - Maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link - Maximum number of calls that can use IPsec-protected signaling
---------------	---

Command Default

The default maximum number of media streams that can use IPsec encryption and decryption on their signaling link or that can use IPsec-protected signaling, at any point of time, is 4294967295. When you use the no form of this command, any maximum limit set earlier is changed to this default value.

Command Modes

SBE CAC table CAC policy configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

In the following example, the **ipsec maximum** command is used to set the maximum number of media streams that can use IPsec encryption and decryption on their signaling link to 200. In addition, the command is used to set the maximum number of media streams that can use IPsec-protected signaling to 80.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table t1
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media limits mp1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry) # ipsec maximum registers 200
Router(config-sbc-sbe-cacpolicy-cactable-entry) # ipsec maximum calls 80
```

Related Commands

Command	Description
interwork maximum	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
interwork cost	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
ipsec maximum	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
media-gateway policy type	Configures a media gateway policy.
media limits	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
media-policy	Configures a media policy.
show sbc sbe media-gateway-policy	Displays the details of media gateway policies.
show sbc sbe media-policy	Displays the details of media policies.
total resource maximum	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
transcode cost	Specifies the resource cost for transcoding an audio or video stream.
transcode maximum	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
transrate audio cost	Specifies the resource cost for transrating an audio stream.
transrate audio maximum	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
type	Configures a media policy as a CAC-policy type policy or a gateway type policy.

ipv4

To create an IPv4 address within a DBE media address pool, use the **ipv4** command in media address configuration mode. To delete an IPv4 address within a DBE media address pool, use the **no** form of this command.

```

ipv4 ipv4_address [vrf vrf-name]

no ipv4 ipv4_address [vrf vrf-name]
  
```

Syntax Description	<i>ipv4_address</i>	Specifies the IPv4 media address.
	<i>vrf vrf-name</i>	(Optional) Specifies the VRF name.

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	Media address (config-sbc-dbe-media-address)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to configure address 10.0.1.1 for use both for non-VPN media and for media to or from vpn3: <pre> Router# configure terminal Router(config)# sbc mySbc dbe Router(config-sbc-dbe)# media-address Router(config-sbc-dbe-media-address)# media-address ipv4 10.0.1.1 Router(config-sbc-dbe-media-address)# media-address ipv4 10.0.1.1 vrf vpn3 </pre>
----------	--

ipv4 (blacklist)

To enter the mode for applying blacklisting options to a single IP address or for configuring the default event limits for the source addresses in a given VPN (where the IP address is under the VPN), use the **ipv4** command in the SBE blacklist configuration mode. Use the no form of the command to remove the blacklist entry for an address.

ipv4 ip address

Syntax Description	<i>IP address</i>	Specifies the IPv4 H.248 control address.
--------------------	-------------------	---

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	SBE blacklist configuration (config-sbc-sbe-blacklist)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to enter the mode for applying blacklisting options to a single IP address:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 1.1.1.1
Router(config-sbc-sbe-blacklist-ipv4)#
```

Related Commands	Command	Description
	blacklist	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	ipv4 (blacklist)	Enters the mode for applying blacklisting options to a single IP address.
	reason	Enters a mode for configuring a limit to a specific event type on the source.
	timeout	Defines the length of time that packets from the source are blocked, should the limit be exceeded.

Command	Description
trigger-period	Defines the period over which events are considered.
trigger-size	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.

ipv4 (SBE H.248)

To configure an SBE to use a given IPv4 H.248 control address, use the **ipv4** command in H.248 control address configuration mode. To delete a given IPv4 H.248 control address, use the **no** form of this command.

```
ipv4 IP address
no ipv4 IP address
```

Syntax Description	IP address	Specifies the IPv4 H.248 control address.
--------------------	------------	---

Command Default	No default behavior or values are available.	
-----------------	--	--

Command Modes	H.248 control address (config-sbc-sbe-ctrl-h248)	
---------------	--	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.	
------------------	--	--

Examples	The following example shows how to configure an SBE to use a given IPv4 H.248 control address: Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# control address h248 index 0 Router(config-sbc-sbe-ctrl-h248)# ipv4 1.1.1.1 Router(config-sbc-sbe-ctrl-h248)#	
----------	--	--

Related Commands	Command	Description
	control address h248 index	Selects index value and enters H.248 control address mode.
	port (SBE H.248)	Configures an SBE to use a given IPv4 H.248 port.
	transport (SBE H.248)	Configures an SBE to use a certain transport for H.248 communications.

ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

```
ip access-list { {standard | extended} } { access-list-name | access-list-number } |
helper egress check
```

```
no ip access-list { {standard | extended} } { access-list-name | access-list-number } |
helper egress check
```

Syntax Description	standard	Specifies a standard IP access list.
	extended	Specifies an extended IP access list. Required for object-group ACLs.
	<i>access-list-name</i>	Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
	<i>access-list-number</i>	Number of the access list. - A standard IP access list is in the ranges 1–99 or 1300–1999. - An extended IP access list is in the ranges 100–199 or 2000–2699.
	helper egress check	Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address.

Command Default	No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.
------------------------	--

Command Modes	Global configuration (config)
----------------------	-------------------------------

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.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.4(20)T	This command was modified. Object-group ACLs are now accepted when the deny and permit commands are used in standard IP access-list configuration mode or extended IP access-list configuration mode.
	Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.
	15.0(1)M	This command was modified. The helper , egress , and check keywords were added.

Usage Guidelines

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Named access lists are not compatible with Cisco IOS software releases prior to Release 11.2.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

Examples

The following example defines a standard access list named Internetfilter:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_service_object_group:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list helper egress check
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or in an object-group ACL that will deny packets.
ip access-group	Applies an ACL or an object-group ACL to an interface or a service policy map.
object-group network	Defines network object groups for use in object-group ACLs.
object-group service	Defines service object groups for use in object-group ACLs.
permit	Sets conditions in a named IP access list or in an object-group ACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or object-group ACLs.
show object-group	Displays information about object groups that are configured.

ip host

To resolve host names to IP addresses in evaluation cases where a DNS server is not available, use the **ip host** command in Global configuration mode. To return to the default value, use the **no** form of this command.

```
ip host hostname ip_address
no ip host hostname ip_address
```

Syntax Description	hostname	Specifies the host name.
	The following guidelines apply:	
	- The <i>hostname</i> can include upto 63 characters. - Host names must start with a letter and can end with a letter or a digit.	
	ip_address	Specifies the IP address.

Command Default	The default wait interval is 180 seconds. If no response is received during that time, an internal 408 request timeout response is generated and is sent to the caller.
-----------------	---

Command Modes	Global configuration (config)
---------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command. If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.
------------------	--



Caution

The **ip host** command provides a mechanism to resolve host names to IP addresses in evaluation cases where a DNS server is not available. Properly designed networks rely on DNS infrastructure to manage the mapping of host names to IP addresses in a scalable and consistent network-wide manner. Use of the **ip host** command in conjunction with a DNS server may result in an undesirable result when the local configuration conflicts with the global DNS mapping.

Examples	The following example shows how to configure the SBC to time out invite transactions after 60 seconds: <pre>Router# configure terminal Router(config)# ip host host_1 172.18.51.20</pre>
----------	---

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing [**vrf** *vrf-name*] [**distributed**]

no ip multicast-routing [**vrf** *vrf-name*]

Cisco IOS XE Release 3.3S

ip multicast-routing {[**vrf** *vrf-name*] **distributed**}

no ip multicast-routing {[**vrf** *vrf-name*] **distributed**}

Syntax Description

vrf <i>vrf-name</i>	(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
distributed	(Optional) Enables Multicast Distributed Switching (MDS).

Command Default

IP multicast routing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The distributed keyword was added.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the no form of this command now disables IP multicast routing on the Multicast Multilayer Switching (MMLS) Route Processor (RP) and purges all multicast MLS cache entries on the MMLS-SE.
12.0(23)S	The vrf keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The vrf keyword and <i>vrf-name</i> argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S. This command without the distributed keyword was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.3S	This command was modified. Either the distributed keyword or the vrf <i>vrf-name</i> distributed keyword and argument combination is required with this command in Cisco IOS Release 3.3S.

Usage Guidelines

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets. The optional **distributed** keyword for this command is not supported in Cisco IOS XE Release 3.2S. Either the **distributed** keyword or the **vrf vrf-name distributed** keyword and argument combination for this command is required in Cisco IOS XE Release 3.3S and later releases.

**Note**

For IP multicast, after enabling IP multicast routing, PIM must be configured on all interfaces. Disabling IP multicast routing does not remove PIM; PIM still must be explicitly removed from the interface configurations.

Examples

The following example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Router(config)# no ip multicast-routing
```

The following example shows how to enable MDS in Cisco IOS XE Release 3.3S a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1 distributed
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip multicast rpf mofrr

To enable a Provider Edge (PE) router to perform Reverse Path Forwarding (RPF) lookups using multicast only fast re-route (MoFRR) on an IP address of the exit router in the global table or a specific VPN, use the **ip multicast rpf mofrr** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **rpf mofrr** {*access-list-number* | *access-list-name*} [**sticky**]

no ip multicast [**vrf** *vrf-name*] **rpf mofrr** {*access-list-number* | *access-list-name*} [**sticky**]

Syntax Description	vrf <i>vrf-name</i>	(Optional) Enables a PE router to perform an RPF lookup using MoFRR on the exit router for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
	<i>access-list-name</i>	Name of the IP access list or object group access control list (OGACL). Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
	<i>access-list-number</i>	Number of the access control list (ACL). MoFRR is enabled for the mroute matching the ACL. An extended IP access list is in the range 100 to 199 or 2000 to 2699. Note MoFRR accepts extended ACLs only. It does not accept standard ACLs.
	sticky	(Optional) Ensures that the primary RPF does not change even if a better primary comes along. It changes only if for some reason the current primary RPF is unreachable. The sticky keyword ensures that there is no RPF flapping happening on mroutes if the unicast routes are fluctuating for some reason.

Command Default The RPF MoFRR functionality is disabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines Use the **ip multicast rpf mofrr** command to enable a PE router to perform RPF lookups using MoFRR on an IP address of the exit router in the global table or a specific VPN. MoFRR uses standard Protocol Independent Multicast (PIM) join messages to set up a primary and a secondary multicast forwarding path by establishing a primary and a secondary RPF interface on each router that receives a PIM join

message. Data is received from both the primary and backup paths. If the router detects a forwarding error in the primary path, it switches RPF to the secondary path and immediately has packets available to forward out to each outgoing interface.

MoFRR accepts extended ACLs only. It does not accept standard ACLs.

Examples

The following example shows how to enable a PE router to perform RPF lookups using MoFRR for the mroute matching the ACL numbered 150:

```
ip multicast rpf mofrr 150
```

Related Commands

Command	Description
show ip mroute	Displays information about the multicast routing (mroute) table.
show ip rpf	Displays the information that IP multicast routing uses to perform the RPF check for a multicast source.

ip multicast rpf select topology

To associate a multicast topology with a multicast group with a specific mroute entry, use the **ip multicast rpf select topology** command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip multicast rpf select topology { **multicast** | **unicast** } *topology-name access-list-number*

no ip multicast rpf select topology { **multicast** | **unicast** } *topology-name access-list-number*

Syntax Description

multicast	Associates a multicast topology with an (S,G) mroute entry.
unicast	Associates a unicast topology with an (S,G) mroute entry.
<i>topology-name</i>	Name of the topology instance.
<i>access-list-number</i>	Number of the access list.

Command Default

The topology is not associated with an (S,G) mroute entry.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **ip multicast rpf select topology** command associates a multicast topology with an (S,G) mroute entry. One (S,G) mroute entry can be associated with multiple topologies. During RPF lookup, PIM MT-ID will be used (smaller ID has higher priority) to select a topology.

One access list could be associated with multiple (S,G) mroute entries. The sequence number in the access list is used to determine the order of (S,G) mroute entry lookup within the access list.

One topology can be associated with only one access list.

Examples

The following example shows how to associate a multicast topology with an (S,G) mroute entry:

```
ip multicast rpf select topology multicast topology live-A 111
```

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast topology	Configures topology selection for multicast streams.
show ip multicast topology	Displays IP multicast topology information.

ip multicast topology

To configure topology selection for multicast streams, use the **ip multicast topology** command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip multicast topology { **multicast** | **unicast** } *topology-name* **tid** *topology-number*

no ip multicast topology { **multicast** | **unicast** } *topology-name* **tid** *topology-number*

Syntax Description

multicast	Configures a multicast topology instance.
unicast	Configures a unicast topology instance.
<i>topology-name</i>	Name of the topology instance.
tid <i>topology-number</i>	Specifies the number of the topology identifier.

Command Default

All multicast streams are associated with the multicast base topology.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **ip multicast topology** command configures topology selection for multicast streams, which is usually only required for first hop and last hop routers (and may not be required for transit routers in between). The stream, specified by an extended IP access list, can be source based, group based, or a combination of both. The sequence number in the access list will decide the order of the (S,G) mroute entries.

Examples

The following example shows how to configure topology selection for multicast streams:

```
ip multicast topology multicast live-A 111
```

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast rpf select topology	Associates a multicast topology with a multicast group with a specific mroute entry.
show ip multicast topology	Displays IP multicast topology information.

ip precedence

To configure an IP precedence with which to mark IP packets belonging to the given QoS profile, use the **ip precedence** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

ip precedence *value*

no ip precedence

Syntax Description	<i>value</i> Specifies the IP precedence with which to mark packets. Range is 0 to 7.
--------------------	---

Command Default	<i>value</i> : 0
-----------------	------------------

Command Modes	Qos sig configuration (config-sbc-sbe-qos-sig) QoS video configuration (config-sbc-sbe-qos-video) QoS voice configuration (config-sbc-sbe-qos-voice)
---------------	--

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE Release 2.4</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr></table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to configure the QoS profile to mark IP packets with a precedence of 1: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# qos sig residential Router(config-sbc-sbe-qos-sig)# ip precedence 1 Router(config-sbc-sbe-qos-sig)#</pre>
----------	--

ip service reflect

To match and rewrite multicast packets routed onto a Vif1 interface, use the **ip service reflect** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address* **mask-len** *number* **source** *new-source-address*

no ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address* **mask-len** *number* **source** *new-source-address*

Syntax Description		
<i>input-interface</i>		Interface type and number.
destination		Identifies packets with the specified destination address.
<i>destination-address</i>		Destination IP address in the packets, in A.B.C.D format.
to		Modifies the destination IP address in reflected packets to a new IP address.
<i>new-destination-address</i>		New destination address to be used, in A.B.C.D format.
mask-len <i>number</i>		Specifies the mask length of the destination address to match. The <i>number</i> argument is a value from 0 to 32.
source		Modifies the source address in reflected packets. The source address must be on the same subnet as the Vif1 interface.
<i>new-source-address</i>		New source address to be used, in A.B.C.D format.

Command Default The multicast service reflection feature is disabled.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	12.4(4)T	This command was introduced.
	12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.
	Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines Use the **ip service reflect** command to match and rewrite multicast packets routed onto a Vif1 interface. The matched and rewritten packet is sent back into Cisco multicast packet routing, where it is handled like any other packet arriving from an interface.

More than one multicast service reflection operation can be configured to match the same packet, allowing you to replicate the same received traffic to multiple destination addresses.

Examples

The following example shows how to translate any multicast packet with a destination address of 239.1.1.0/24 to a destination of 239.2.2.0/24 with a new source address of 10.1.1.2. For example, a packet with a source and destination of (10.10.10.10, 239.1.1.15) would be translated to (10.1.1.2, 239.2.2.15).

```
Router(config)# interface Vif1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip service reflect Ethernet 0/0 destination 239.1.1.0 to 239.2.2.0
mask-len 24 source 10.1.1.2
Router(config-if)# ip igmp static-group 239.1.1.0
Router(config-if)# ip igmp static-group 239.1.1.1
```

ip TOS (session border controller)

To configure an IP ToS (type of service) with which to mark IP packets belonging to the QoS profile, use the **ip TOS** command in the appropriate configuration mode. To return the QoS profile to setting the default IP ToS, use the **no** form of this command.

ip TOS *value*

no ip TOS

Syntax Description	value	Specifies the IP ToS with which to mark packets. This may be a value of 0 (normal service) or a bit field consisting of one or more of the following bits:
		8: Minimize delay. 4: Maximize throughput. 2: Maximize reliability. 1: Minimize monetary cost.

Command Default	The default IP ToS is 0 (normal service).
-----------------	---

Command Modes	Qos sig configuration (config-sbc-sbe-qos-sig) QoS video configuration (config-sbc-sbe-qos-video) QoS voice configuration (config-sbc-sbe-qos-voice)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to configure an IP TOS:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos sig residential
Router(config-sbc-sbe-qos-sig)# ip tos 12
Router(config-sbc-sbe-qos-sig)#
```

ip wccp outbound-acl-check

To check the outbound access control list (ACL) for Web Cache Communication Protocol (WCCP), use the **ip wccp outbound-acl-check** command in global configuration mode. To disable the outbound check, use the **no** form of this command.

ip wccp outbound-acl-check

no ip wccp outbound-acl-check

Syntax Description This command has no arguments or keywords.

Command Default Check of the outbound ACL services is not enabled.

Command Modes Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines This command performs the same function as the **ip wccp check acl outbound** command.

Examples

The following example shows how to configure a router to check the outbound ACL for WCCP:

```
Router(config)# ip wccp outbound-acl-check
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp check acl outbound	Checks the outbound ACL for WCCP.
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP to use on a router.

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**in** | **out**}

no ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**in** | **out**}

Syntax Description		
vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.	
web-cache	Enables the web cache service.	
<i>service-number</i>	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.	
in	Specifies packet redirection on an inbound interface.	
out	Specifies packet redirection on an outbound interface.	

Command Default	Redirection checking on the interface is disabled.
-----------------	--

Command Modes	Interface configuration (config-if)
---------------	-------------------------------------

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.0(11)S	The in keyword was added.
	12.1(3)T	The in keyword was added.
	12.2(17d)SXB	Support for this command on the Cisco 7600 series router Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
	12.2(18)SXD1	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 720.
	12.2(18)SXF	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 32.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. Note The out keyword is not supported in Cisco IOS XE Release 2.2.
	15.0(1)M	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Release	Modification
12.2(33)SRE	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.
Cisco IOS XE Release 3.1S	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added. Support for the out keyword was added.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

The **ip wccp redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ip wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.



Tips

Be careful not to confuse the **ip wccp redirect {out | in}** interface configuration command with the **ip wccp redirect exclude in** interface configuration command.



Note

This command has the potential to affect the **ip wccp redirect exclude in** command. (These commands have opposite functions.) If you have **ip wccp redirect exclude in** set on an interface and you subsequently configure the **ip wccp redirect in** command, the “exclude in” command will be overridden. The opposite is also true: configuring the “exclude in” command will override the “redirect in” command.

Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when fast/CEF switching is enabled:

```
Router(config)# interface multilink2
Router(config-if)# ip address 10.21.21.1 255.255.255.0
Router(config-if)# ip access-group IDS_Multilink2_in_1 in
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ip nat outside
Router(config-if)# ip inspect FSB-WALL out
Router(config-if)# max-reserved-bandwidth 100
Router(config-if)# service-policy output fsb-policy
Router(config-if)# no ip route-cache
Router(config-if)# load-interval 30
Router(config-if)# tx-ring-limit 3
Router(config-if)# tx-queue-limit 3
Router(config-if)# ids-service-module monitoring
```

```
Router(config-if)# ppp multilink  
Router(config-if)# ppp multilink group 2  
Router(config-if)# crypto map abc1
```

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp 99  
Router(config)# interface ethernet 0  
Router(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 is redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp web-cache  
Router(config)# interface ethernet 0/1  
Router(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP global configuration and statistics.

ip wccp source-interface

To specify the interface that Web Cache Communication Protocol (WCCP) uses as the preferred router ID and generic routing encapsulation (GRE) source address, use the **ip wccp source-interface** command in global configuration mode. To enable the WCCP default behavior for router ID selection, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] **source-interface** *source-interface*

no ip wccp [**vrf** *vrf-name*] **source-interface**

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
<i>source-interface</i>	The type and number of the source interface.

Command Default

If this command is not configured, WCCP selects a loopback interface with the highest IP address as the router ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Use this command to set the interface from which WCCP may derive the router ID and GRE source address. The router ID must be a reachable IPv4 address.

The interface identified by the *source-interface* argument must be assigned an IPv4 address and be operational before WCCP uses the address as the router ID. If the configured source interface cannot be used to derive the WCCP router ID, a Cisco IOS error message similar to the following is displayed:

```
%WCCP-3-SIFIGNORED: source-interface interface ignored (reason)
```

The *reason* field in the error output indicates why the interface has been ignored and can include the following:

- **VRF mismatch**—The VRF domain associated with the interface does not match the VRF domain associated with the WCCP command.
- **interface does not exist**—The interface has been deleted.
- **no address**—The interface does not have a valid IPv4 address.
- **line protocol down**—The interface is not fully operational.

This command provides control only of the router ID and GRE source address. This command does not influence the source address used by WCCP control protocol (“Here I Am” and Removal Query messages). The WCCP control protocol is not bound to a specific interface and the source address is always selected based on the destination address of an individual packet.

Examples

The following example shows how to select Gigabit Ethernet interface 0/0/0 as the WCCP source interface:

```
Router(config)# ip wccp source-interface gigabitethernet0/0/0
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
show ip wccp	Displays the WCCP global configuration and statistics.
show ip wccp global counters	Displays global WCCP information for packets that are processed in software.
show platform software wccp	Displays platform specific configuration and statistics related WCCP information on Cisco ASR 1000 Series Routers.

ip wccp version

To specify the version of Web Cache Communication Protocol (WCCP), use the **ip wccp version** command in global configuration mode.

ip wccp version {1 | 2}

Syntax Description

1	Specifies Web Cache Communication Protocol Version 1 (WCCPv1).
2	Specifies Web Cache Communication Protocol Version 2 (WCCPv2).

Command Default

WCCPv2

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	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.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. Only WCCP version 2 is supported in Cisco IOS XE Release 2.2.

Usage Guidelines

Configuring this command does not have any impact on Cisco ASR 1000 Series Routers because these routers support only WCCPv2. WCCPv2 is enabled by default on Cisco ASR 1000 series routers when a service group is configured or a service group is attached to an interface.

Examples

In the following example, the user changes the WCCP version from the default of WCCPv2 to WCCPv1, starting in privileged EXEC mode:

```
Router(config)# ip wccp version 1
```

```
Router# show ip wccp
```

```
% WCCP version 2 is not enabled
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
show ip wccp	Displays the WCCP global configuration and statistics.

key (session border controller)

To configure the authentication key of the accounting and authentication servers, use the **key** command in the appropriate server configuration mode. To disable any previously set authentication key, use the **no** form of this command.

key *key*

no key

Syntax Description	<i>key</i> Specifies the authentication key. This is only valid if authentication is turned on.
---------------------------	---

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	Server accounting (config-sbc-sbe-acc-ser) Server authentication (config-sbc-sbe-auth)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how to configure the <i>acctsvr</i> accounting server with the <i>HJ5689</i> authentication key and <i>acctsvr2</i> accounting server with the <i>cisco</i> authentication key on mySbc for RADIUS client instance radius1:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting radius1
Router(config-sbc-sbe-acc)# server acctsvr
Router(config-sbc-sbe-acc-ser)# key HJ5689
Router(config-sbc-sbe-acc-ser)# exit
Router(config-sbc-sbe-acc)# server acctsvr2
Router(config-sbc-sbe-acc-ser)# key cisco
Router(config-sbc-sbe-acc-ser)# exit
Router(config-sbc-sbe-acc)# exit
Router(config-sbc-sbe)# exit
```

ldr-check

To configure the time of day (local time) to run the Long Duration Check (LDR), use the **ldr-check** command in SBE billing configuration mode. To return to 00:00, use the **no** form of this command.

ldr-check {*HH MM*}

no ldr-check

Syntax Description	<i>HH:MM</i> Time in hours and minutes using a 24-hour clock. The range of the <i>HH</i> argument is 0 to 23. The range of the <i>MM</i> argument is 0 to 59.
---------------------------	---

Command Default	<i>HH MM</i> : 00 00
------------------------	----------------------

Command Modes	SBE billing configuration (config-sbc-sbe-billing)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command. If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.
-------------------------	--

Examples	The following example shows how to configure the remote long-duration-call check to occur at 10.30 p.m., to specify the time each day when SBC should check for any call whose duration is over 24 hours: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# billing Router(config-sbc-sbe-billing)# ldr-check 22 30</pre>
-----------------	---

Related Commands	Command	Description
	activate (radius)	Activates the billing functionality after configuration is committed.
	billing	Configures billing.
	local-address ipv4	Configures the local IPv4 address that appears in the CDR.

Command	Description
method packetcable-em	Enables the packet-cable billing method.
packetcable-em transport radius	Configures a packet-cable billing instance.
show sbc sbe billing remote	Displays the local and billing configurations.

ldr-check (XML billing)

To configure the time at which to check all calls over 24-hour-long, use the **ldr-check** *hour min* command in the SBE billing XML configuration mode. To disable the configuration, use the **no** form of this command.

ldr-check *hour min*

no ldr-check

Syntax Description	<i>hour</i>	Number to indicate the hour at which calls that are more than 24-hours-long will be checked. The hour format should be set using the 24-hour clock.
	<i>min</i>	Number to indicate the minutes at which long duration records will be checked.

Command Default By default, the LDR checks are done at 00:00 hours.

Command Modes SBE billing XML configuration (config-sbc-sbe-billing-xml)

Command History	Release	Modification
	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines It is important to take a note of calls that are more than 24-hours-long. To report long duration calls that are more than 24 hours, use the **ldr-check** *hour min* command from SBE billing XML configuration mode. The initial value is inherited from the value in the Billing-MGR table. The hour and minute values must be set using the 24-hour clock. The **no** form of the command does not require any parameter. The default duration at which LDR checks are performed is 00 hour and 00 minutes.

Examples The following example shows how to configure the time 23 hour and 30 minutes to check long duration calls:

```
Router(config)# sbc sbcbilling
Router(config-sbc)# sce
Router(config-sbc-sce)# billing
Router(config-sbc-sce-billing)# xml method
Router(config-sbc-sce-billing)# xml 1
Router(config-sbc-sce-billing-xml)# ldr-check 23 30
```

Related Commands	Command	Description
	xml (billing)	Configures the method index for XML billing.
	method xml	Configures the billing method as XML.
	cdr path	Configures the time at which long duration records are checked.

load-order

To specify the load order of a script in a script set, use the **load-order** command in the SBE script-set script configuration mode.

load-order *load-order-number*

Syntax Description	<i>load-order-number</i>	Order in which the script must be loaded. The range is from 1 to 4294967295.
---------------------------	--------------------------	--

Command Default	The default load order number of the first script set that you configure without using the load-order command, is 100. For scripts that are subsequently added without using the load-order command, the default order index number is set in multiples of 100, that is, 200, 300, 400, and so on.
------------------------	--

Command Modes	SBE script-set script configuration (config-sbc-sbe-scrpset-script)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command. Note that scripts are loaded in ascending order of the order index number. For example, a script with the order index number 4 is loaded before a script with the order index number 6.
-------------------------	---

Examples	In the following example, the load-order command is used to specify 2 as the load order:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# script-set 10 lua
Router(config-sbc-sbe-script-set)# script mySBCScript
Router(config-sbc-sbe-scrpset-script)# load-order 2
```

Related Commands	Command	Description
	active-script-set	Activates a script set,
	clear sbc sbe script-set-stats	Clears the stored statistics related to a script set.
	complete	Completes a CAC policy set, call policy set, or script set after committing the full set.
	editor	Specifies the order in which a particular editor must be applied.

Command	Description
editor-list	Specifies the stage at which the editors must be applied.
editor type	Configures an editor type to be applied on a SIP adjacency.
filename	Specifies the path and name of the script file written using the Lua programming language.
script	Configures a script written using the Lua programming language.
show sbc sbe editors	Displays a list of all the editors registered on the SBC.
show sbc sbe script-set	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
script-set lua	Configures a script set composed of scripts written using the Lua programming language.
sip header-editor	Configures a header editor.
sip method-editor	Configures a method editor.
sip option-editor	Configures an option editor.
sip parameter-editor	Configures a parameter editor.
test sbc message sip filename script-set editors	Tests the message editing functionality of the SBC.
test script-set	Tests the working of a script set.
type	Specifies the type of a script written using the Lua programming language.

local-address ipv4

To configure the local IPv4 address that appears in the CDR, use the **local-address ipv4** command in SBE billing configuration mode. To deconfigure the local IPV4 address, use the **no** form of this command.

local-address ipv4 {*A.B.C.D.*}

no local-address ipv4

Syntax Description	<i>A.B.C.D.</i> Local IPv4 address to be configured.
---------------------------	--

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	SBE billing configuration
----------------------	---------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
	If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.



Note

This field cannot be reconfigured when billing is active.

Examples	The following example shows how to configure the local-address to 10.20.1.1 for the billing:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing remote
Router(config-sbc-sbe-billing)# local-address ipv4 10.20.1.1
```

Related Commands	Command	Description
	billing	Configures billing.
	ldr-check	Configures the time of day (local time) to run the Long Duration Check (LDR).

Command	Description
local-address ipv4	Configures the local IPv4 address that appears in the CDR.
method packetcable-em	Enables the packet-cable billing method.
packetcable-em transport radius	Configures a packet-cable billing instance.
show sbc sbe billing remote	Displays the local and billing configurations.

local-address ipv4 (packet-cable)

To configure the local address of the packet-cable billing instance, use the **local-address ipv4** command in the packetcable-em configuration mode. To disable the local address, use the **no** form of this command.

local-address ipv4 A.B.C.D.

no local-address ipv4

Syntax Description	A.B.C.D. Local IPv4 address to be configured.	
Command Default	0.0.0.0	
Command Modes	Packet-cable em configuration (config-sbc-sbe-billing-packetcable-em)	
Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command. If no address is configured, the SBC uses any local address.	
Examples	The following example shows how to enter the billing mode for mySbc: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc) # sbe Router(config-sbc-sbe) # billing (config-sbc-sbe-billing) # packetcable-em 4 transport radius test (config-sbc-sbe-billing-packetcable-em) # local-address ipv4 10.10.10.10</pre>	
Related Commands	Command	Description
	activate (radius)	Activates the billing functionality after configuration is committed.
	attach	activate the billing for a RADIUS client
	batch-size	Configures the batching or grouping of RADIUS messages sent to a RADIUS server.
	batch-time	Configures the maximum number of milliseconds for which any record is held in the batch before the batch is sent
	deact-mode	Configures the deactivate mode for the billing method.

Command	Description
ldr-check	Configures the time of day (local time) to run the Long Duration Check (LDR).
local-address ipv4	Configures the local IPv4 address that appears in the CDR.
local-address ipv4 (packet-cable)	Configures the local address of the packet-cable billing instance.
method packetcable-em	Enables the packet-cable billing method.
packetcable-em transport radius	Configures a packet-cable billing instance.
show sbc sbe billing remote	Displays the local and billing configurations.

local-id host

To configure the local identify name on a SIP adjacency, use the **local-id** command in adjacency SIP configuration mode. To remove this configuration, use the **no** form of this command.

local-id host *name*

no local-id host

Syntax Description	<i>name</i> Specifies the local identity name to present on outbound SIP messages. The following guidelines apply: • Upto 30 alphanumeric characters are allowed. • Except for the underscore sign (_), it is recommended that you do not use any special character. • The <i>name</i> can be a DNS name. The <i>name</i> must not contain a port.				
Command Default	When the name field is not set, the local signaling address is used in SIP messages.				
Command Modes	Adjacency SIP configuration (config-sbc-sbe-adj-sip)				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Release 2.4</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				
Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.				
Examples	The following example shows how to set the SIP local identity of SIP adjacency SipToIsp42 to mcarthur: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# adjacency sip SipToIsp42 Router(config-sbc-sbe-adj-sip)# local-id host mcarthur</pre>				

local-jitter-ratio

To specify the percentage of calls that must be used to calculate the local jitter ratio, use the **local-jitter-ratio** command in the adjacency H.323 configuration mode or adjacency SIP configuration mode. To remove this configuration, use the **no** form of this command.

local-jitter-ratio *call-percentage*

no local-jitter-ratio

Syntax Description	<i>call-percentage</i>	Percentage of calls. The range is from 0 to 1000. For example, if you enter 305 as the value of <i>call-percentage</i> , the SBC uses 30.5 percent of the calls for measuring local jitter.
--------------------	------------------------	---

Command Default	By default, the value of <i>call-percentage</i> is 0 because jitter determination is a performance drain on the MPF. When the value is 0, measurements of the jitter ratio and the MOS-CQE are not available for the adjacency.	
-----------------	---	--

Command Modes	Adjacency H.323 configuration (config-sbc-sbe-adj-h323) Adjacency SIP configuration (config-sbc-sbe-adj-sip)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.
------------------	---

Examples	In the following example, the local-jitter-ratio command is used to specify that 20.5 percent of the calls must be used to calculate the local jitter ratio:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 adj1
Router(config-sbc-sbe-adj-h323)# local-jitter-ratio 305
```

Related Commands	Command	Description
	calc-moscqe	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
	current15minutes	Specifies that QoS statistics must be calculated for 15-minute intervals.

Command	Description
current5minutes	Specifies that QoS statistics must be calculated for 5-minute intervals.
currentday	Specifies that statistics must be calculated for 24-hour intervals.
currenthour	Specifies that QoS statistics must be calculated for 60-minute intervals.
currentindefinite	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
g107 bpl	Sets a value for the Packet-Loss Robustness (Bpl) factor.
g107 ie	Sets a value for the Equipment Impairment (Ie) factor.
g107a-factor	Sets a value for the Advantage (A) factor.
show sbc sbe adjacencies	Displays details of the adjacencies configured on the SBE.
show sbc sbe call-stats	Displays the statistics pertaining to all the calls on a the SBE.
snmp-server enable traps sbc	Enables SBC notification types.
statistics	Specifies the QoS statistic for which alert levels must be set.

local-port (session border controller)

To configure a data border element (DBE) to use a specific local port when connecting to the default media gateway controller (MGC), use the **local-port** command in either SBC configuration mode or VDBE configuration mode. To disable this configuration, use the **no** form of this command.

```
local-port {abcd}

no local-port {abcd}
```

Syntax Description	<i>abcd</i> This is the number of the local port the DBE uses.
--------------------	--

Command Default	Default is to use local port 2944. Note that use-any-local-port should not be used when there is a redundant Session Border Controller (SBC). If it is, the connection to the MGC may be lost with an SBC switch over.
-----------------	--

Command Modes	VDBE configuration (config-sbc-dbe-vdbe) for distributed SBC
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for distributed SBC.

Usage Guidelines	The Examples section shows the hierarchy of modes required to run the command. The local port cannot be modified after any controller has been configured on the DBE. You must delete the controller before you can modify or configure the local port.
------------------	---

Examples	The following example creates a DBE service on a distributed SBC called mySbc and configures the DBE to use the local port number 5090: <pre>Router# configure terminal Router(config)# sbc mySbc dbe Router(config-sbc-dbe)# vdb Router(config-sbc-dbe-vdbe)# local-port 5090 Router(config-sbc-dbe-vdbe)# end</pre> The following example creates a DBE service on a unified SBC called mySbc and configures the DBE to use the local port number 5090: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc)# vdb Router(config-sbc-vdbe)# local-port 5090 Router(config-sbc-vdbe)# end</pre>
----------	---

Related Commands	Command	Description
	use-any-local-port	Configures a DBE to use any available local port when connecting to the default MGC.

location-id (session border controller)

To configure the location ID for a DBE service of the Session Border Controller (SBC), use the **location-id** command in SBC-DBE configuration mode. To set the location ID to the default, use the **no** form of this command.

```
location-id location-id
no location-id location-id
```

Syntax Description	location-id The location ID of the DBE. The location ID range is from -1 to 65535.
--------------------	---

Command Default	The default location-id is -1
-----------------	-------------------------------

Command Modes	SBC-DBE configuration (config-sbc-dbe)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The **no** form of the command does not take an argument and sets the location-id to the default, which is 0xFFFFFFFF (-1).

A location ID is configured on each DBE. The SBE may associate endpoints with a particular location ID and then use the location IDs to route calls between different DBEs.

Use the **dbe** command to enter into SBC-DBE configuration mode prior to entering the **location-id** command.

Examples

The following example creates a DBE service on an SBC called mySbc, enters into SBC-DBE configuration mode, and sets the location ID for a DBE to be 1:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# location-id 1
Router(config-sbc-dbe)# exit
```

Related Commands	Command	Description
	dbe	Creates the DBE service on a SBC and enters into DBE-SBE configuration mode.

max-call-rate-per-scope

To configure the maximum call rate for an entry in an admission control table and specify the averaging period to be used in rate calculation, use the **max-call-rate-per-scope** command in the CAC table configuration mode. To unconfigure the maximum call rate for an entry in an admission control table and to remove the averaging period, use the **no** form of this command.

max-call-rate-per-scope *limit* [**averaging-period** *period-num*]

no max-call-rate-per-scope *limit* [**averaging-period** *period-num*]

Syntax Description	<i>limit</i>	A positive integer specifying the maximum number of subscriber registrations per minute to permit at the relevant scope. Only one parameter should be supplied for each command. The range is from 0 to 2147483647.
	averaging-period	Specifies the averaging period to be used in rate calculation. By default, 1 is selected.
	<i>period-num</i>	The rate based on the specified averaging period. The range is from 1 to 2.

Command Default No default behavior or values are available.

Command Modes CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The max-call-rate command was renamed as the max-call-rate-per-scope command. The averaging-period keyword and the <i>period-num</i> argument were also added

Usage Guidelines Only one parameter should be supplied for each command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples The following example shows how to configure the maximum call rate for an entry CAC table 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry) # max-call-rate-per-scope 10  
averaging-period 2
```

Related Commands

Command	Description
max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
max-channels	Configures the maximum number of channels for an entry in an admission control table.
max-num-calls	Configures the maximum number of calls pertaining to an entry in an admission control table.
max-regs	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
max-reg-rate-per-scope	Configures the maximum call number of subscriber registrations for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
max-updates	Configures the maximum call updates for an entry in an admission control table.

max-connections

To configure the maximum number of SIP connections that will be made to each remote address, use the **max-channels** command in SBE configuration mode. To set this to an unlimited number of connections, use the **no** form of this command.

max-connections *number-of-connections*

no max-connections *number-of-connections*

Syntax Description	number-of-connections The maximum number of connections.
---------------------------	---

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following command configures the maximum number of connections to each remote address to 1: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# sip max-connections 1</pre>
-----------------	---

Related Commands	Command	Description
	max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
	max-call-rate-per-scope	Configures the maximum call rate for an entry in an admission control table.
	max-channels	Configures the maximum number of channels for an entry in an admission control table.
	max-num-calls	Configures the maximum number of calls of an entry in an admission control table.
	max-regs	Configures the maximum number of subscriber registrations of an entry in an admission control table.

Command	Description
max-regs-rate-per-scope	Configures the maximum call number of subscriber registrations for an entry in an admission control table.
max-updates	Configures the maximum call updates for an entry in an admission control table.

max-in-call-msg-rate

To configure the maximum in-call rate and specify the averaging period to be used in rate calculation, use the **max-in-call-msg-rate** command in the CAC table entry configuration mode. To deconfigure the maximum in-call rate and remove the specified averaging period, use the **no** form of this command.

max-in-call-msg-rate limit [averaging-period *period-num*]

no max-in-call-msg-rate limit [averaging-period *period-num*]

Syntax Description	limit	The maximum number of in-call messages per minute. The range is from 0 to 2147483647.
	averaging-period	Specifies the averaging period to be used in the rate calculation. By default, 1 is selected.
	<i>period-num</i>	The rate based on the specified averaging period. Valid range is from 1 to 2.

Command Default No limit.

Command Modes CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The max-in-call-rate command was renamed as max-in-call-msg-rate . The averaging-period keyword and the <i>period-num</i> argument were also added

Usage Guidelines In-call messages include all the messages within the context of a call, including provisional responses during call setup and call renegotiation messages, but not including call setup or tear-down messages. When configuring the maximum rate of in-call messages in Call Admission Control (CAC), note that the following messages are not rate-limited:

- SIP INVITE requests: 200 responses and ACK messages
- SIP PRACK messages and response
- SIP BYE messages and responses
- Any SIP message with nonduplicate SDP on
- For H.323 calls: Q.931 SETUP, Q.931 CONNECT, and Q.931 RELEASE messages

The Cisco Unified Border Element (SP Edition) will reject the in-call messages when the rate exceeds the rate that is specified in the CAC.

The averaging period must be configured using the **cac-policy-set** command before the averaging period is specified in this command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

The following command shows how to configure the maximum number of connections to each remote address to 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 200
Router(config-sbc-sbe)# cac-policy-set averaging-period 2 500
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-in-call-msg-rate 500 averaging-period
2
```

Related Commands

Command	Description
max-out-call-msg-rate	Configures the maximum out-call rate in an admission control table and specifies the averaging period to be used in rate calculation.
max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
max-call-rate-per-scope	Configures the maximum call rate for an entry in an admission control table and specifies the averaging period to be used in the rate calculation.
max-channels	Configures the maximum number of channels for an entry in an admission control table.
max-num-calls	Configures the maximum number of calls pertaining to an entry in an admission control table.
max-regs	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
max-regs-rate-per-scope	Configures the maximum call number of subscriber registrations for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
max-updates	Configures the maximum call updates for an entry in an admission control table.

max-num-calls

To configure the maximum number of calls of an entry in an admission control table, use the **max-num-calls** command in CAC table configuration mode. To delete the maximum number of calls in the given entry in the admission control table, use the **no** form of this command.

max-num-calls *mnc*

no max-num-calls *mnc*

Syntax Description	<i>mnc</i>	Positive integer specifying the maximum number of calls to permit at the relevant scope.
---------------------------	------------	--

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	CAC table configuration (config-sbc-sbe-cacpolicy-cactable)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how to configure the maximum number of calls for an entry in the new admission control table MyCacTable:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-num-calls 50
```

Related Commands	Command	Description
	max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
	max-call-rate-per-scope	Configures the maximum call rate for an entry in an admission control table.
	max-channels	Configures the maximum number of channels for an entry in an admission control table.

Command	Description
max-connections	Configures the maximum number of SIP connections that will be made to each remote address.
max-regs	Configures the maximum number of subscriber registrations of an entry in an admission control table.
max-regs-rate-per-scope	Configures the maximum call number of subscriber registrations for an entry in an admission control table.
max-updates	Configures the maximum call updates for an entry in an admission control table.

max-out-call-msg-rate

To configure the maximum out-call rate and specify the averaging period to be used in rate calculation, use the **max-out-call-msg-rate** command in the CAC table entry configuration mode. To disable the maximum out-call rate and remove the specified averaging period, use the **no** form of this command.

max-out-call-msg-rate limit [averaging-period *period-num*]

no max-out-call-msg-rate limit [averaging-period *period-num*]

Syntax Description	limit	The maximum number of call-out messages per minute. The range is from 0 to 2147483647.
	averaging-period	Specifies the averaging period to be used in rate calculation. By default, 1 is selected.
	<i>period-num</i>	The rate based on the specified averaging period. The range is from 1 to 2.

Command Default No limit.

Command Modes CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The max-out-call-rate command was renamed as max-out-call-msg-rate . The averaging-period keyword and the <i>period-num</i> argument were also added

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

The averaging period must be configured using the **cac-policy-set** command before the averaging period is specified in this command.

Examples The following command shows how to configure the maximum number of connections to each remote address to 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 200
Router(config-sbc-sbe)# cac-policy-set averaging-period 2 500
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
```

```
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-out-call-msg-rate 500
averaging-period 2
```

Related Commands

Command	Description
max-in-call-msg-rate	Configures the maximum in-call rate in an admission control table and specifies the averaging period to be used in rate calculation.
max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
max-call-rate-per-scope	Configures the maximum call rate for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
max-channels	Configures the maximum number of channels for an entry in an admission control table.
max-num-calls	Configures the maximum number of calls pertaining to an entry in an admission control table.
max-regs	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
max-regs-rate-per-scope	Configures the maximum call number of subscriber registrations for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
max-updates	Configures the maximum call updates for an entry in an admission control table.

max-recursive-depth

To configure the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR), use the **max-recursive-depth** command in ENUM configuration mode. To return the maximum number of recursive ENUM look-ups to the default value, use the no form of this command.

max-recursive-depth *number*

no max-recursive-depth *number*

Syntax Description	<i>number</i>	Maximum number of look-ups. The range is 1 to 2147483647.
---------------------------	---------------	---

Command Default	The default 5.
------------------------	----------------

Command Modes	ENUM configuration (config-sbc-sbe-enum)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how to configure the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
-----------------	--

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# max-recursive-depth 100
```

Related Commands	Command	Description
	activate (enum)	Activates ENUM client.
	dial-plan-suffix	Configures the dial plan suffix used for the ENUM query.
	div-address	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	dst-address	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
	entry (enum)	Configures the ENUM client entry name and enter the ENUM entry configuration mode.

Command	Description
enum	Configures the ENUM client ID number and enter the ENUM configuration mode.
header-prio header-name	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
max-recursive-depth	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
max-responses	Configures the maximum number of ENUM records returned to the routing module.
req-timeout	Configures the ENUM request timeout period.
src-address	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
server ipv4	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
show sbc sbe call-policy-set	Displays configuration and status information about call policy sets.
show sbc sbe enum	Displays the configuration information about an ENUM client.
show sbc sbe enum entry	Displays the contents of an ENUM client entry.

max-regs-rate-per-scope

To configure the maximum call number of subscriber registrations for an entry in an admission control table and specify the averaging period to be used in rate calculation, use the **max-regs-rate-per-scope** command in the CAC table configuration mode. To delete the maximum number of subscriber registrations in a given entry in the admission control table and to remove the averaging period, use the **no** form of this command.

max-regs-rate-per-scope *limit* [**averaging-period** *period-num*]

no max-regs-rate-per-scope *limit* [**averaging-period** *period-num*]

Syntax Description	<i>limit</i>	A positive integer specifying the maximum number of subscriber registrations per minute to permit at the relevant scope. Only one parameter should be supplied for each command. The range is from 0 to 2147483647.
	averaging-period	Specifies the averaging period to be used in rate calculation. By default, 1 is selected.
	<i>period-num</i>	The rate based on the specified averaging period. The range is from 1 to 2.

Command Default No default behavior or values are available.

Command Modes CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The max-regs-rate was renamed as max-regs-rate-per-scope . The averaging-period keyword and the <i>period-num</i> argument were also added

Usage Guidelines

Only one parameter should be supplied for each command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

The averaging period must be configured using the **cac-policy-set** command before the averaging period is specified in this command.

Examples

The following example shows how to configure the maximum registration rate for an entry in the new admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 200
```

```

Router(config-sbc-sbe)# cac-policy-set averaging-period 2 500
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-regs-rate-per-scope 300
averaging-period 2

```

Related Commands

Command	Description
max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
max-call-rate-per-scope	Configures the maximum call rate for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
max-channels	Configures the maximum number of channels for an entry in an admission control table.
max-num-calls	Configures the maximum number of calls pertaining to an entry in an admission control table.
max-regs	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
max-updates	Configures the maximum call updates for an entry in an admission control table.

max-regs

To configure the maximum number of subscriber registrations of an entry in an admission control table, use the **max-regs** command in CAC table configuration mode. To delete the maximum number of subscriber registrations in the given entry in the admission control table, use the **no** form of this command.

max-regs *mr*

no max-regs *mr*

Syntax Description	<i>mrr</i>	Positive integer specifying the maximum number of subscriber registrations to permit at the relevant scope.
---------------------------	------------	---

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	CAC table configuration (config-sbc-sbe-cacpolicy-cactable)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how to configure the maximum number of subscriber registrations for an entry in the new admission control table MyCacTable:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-regs 500
```

Related Commands	Command	Description
	max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
	max-call-rate-per-scope	Configures the maximum call rate for an entry in an admission control table.

Command	Description
max-channels	Configures the maximum number of channels for an entry in an admission control table.
max-connections	Configures the maximum number of SIP connections that will be made to each remote address.
max-num-calls	Configures the maximum number of calls of an entry in an admission control table.
max-regs-rate-per-scope	Configures the maximum call number of subscriber registrations for an entry in an admission control table.
max-updates	Configures the maximum call updates for an entry in an admission control table.

max-responses

To configure the maximum number of ENUM records returned to the routing module, use the **max-response** command in ENUM configuration mode. To return the number of records returned to the default value, use the no form of this command.

max-responses *number*

no max-responses *number*

Syntax Description	<i>number</i>	Maximum number of ENUM records. The range is 0 to 2147483647.
---------------------------	---------------	---

This command has no arguments or keywords.

Command Default	The default is zero (0).
------------------------	--------------------------

Command Modes	ENUM configuration (config-sbc-sbe-enum)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how to configure the maximum number of ENUM records returned to the routing module:
-----------------	---

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# max-responses 100
```

Related Commands	Command	Description
	activate (enum)	Activates ENUM client.
	dial-plan-suffix	Configures the dial plan suffix used for the ENUM query.
	div-address	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	dst-address	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).

Command	Description
entry (enum)	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
enum	Configures the ENUM client ID number and enter the ENUM configuration mode.
header-prio header-name	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
max-recursive-depth	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
max-responses	Configures the maximum number of ENUM records returned to the routing module.
req-timeout	Configures the ENUM request timeout period.
src-address	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
server ipv4	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
show sbc sbe call-policy-set	Displays configuration and status information about call policy sets.
show sbc sbe enum	Displays the configuration information about an ENUM client.
show sbc sbe enum entry	Displays the contents of an ENUM client entry.

max-updates

To configure the maximum call updates for an entry in an admission control table, use the **max-updates** command in CAC table configuration mode. To delete the maximum call updates in the given entry in the admission control table, use the **no** form of this command.

max-updates *mu*

no max-updates *mu*

Syntax Description	<i>mu</i>	Positive integer specifying the maximum number of updates to call media to permit at the relevant scope.
---------------------------	-----------	--

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	CAC table configuration (config-sbc-sbe-cacpolicy-cactable)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how to configure the maximum number of call updates for an entry in the new admission control table MyCacTable:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-updates 500
```

Related Commands	Command	Description
	max-bandwidth	Configures the maximum bandwidth for an entry in an admission control table.
	max-call-rate-per-scope	Configures the maximum call rate for an entry in an admission control table.

Command	Description
max-channels	Configures the maximum number of channels for an entry in an admission control table.
max-connections	Configures the maximum number of SIP connections that will be made to each remote address.
max-num-calls	Configures the maximum number of calls of an entry in an admission control table.
max-regs	Configures the maximum number of subscriber registrations of an entry in an admission control table.
max-regs-rate-per-scope	Configures the maximum call number of subscriber registrations for an entry in an admission control table.

media

To enable the media bypass feature or the media down detect feature on a Border Access Controller (BAC) adjacency, use the **media** command in the H248 BAC adjacency configuration mode. To disable the media bypass feature or the media down detect feature on a BAC adjacency, use the **no** form of this command.

media {bypass | down}

no media {bypass | down}

Syntax Description	bypass	Enables the media bypass feature on a BAC adjacency.
	down	Enables the media down detect feature on a BAC adjacency.

Command Default	None
-----------------	------

Command Modes	H248 BAC adjacency configuration (config-h248-bac-adj)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples	The following example shows how to enable the media bypass feature on a BAC adjacency:
----------	--

```
Router> enable
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access vrfex
Router(config-h248-bac-adj)# media bypass
```

media-address

To add an IPv4 or IPv6 address to the set of addresses that can be used by the data border element (DBE) as a local media address, use the **media-address** command in either the SBC configuration mode or the SBC-DBE configuration mode. To remove an IPv4 or IPv6 address from the set of local media addresses, use the **no** form of this command.

```
media-address {ipv4 | ipv6} {addr} [nat-mode twice-nat | vrf vrf-name | managed-by {dbe | mgc}]
```

```
no media-address {ipv4 | ipv6} {addr} [nat-mode twice-nat | vrf vrf-name | managed-by {dbe | mgc}]
```

Syntax Description	<i>A.B.C.D</i>	Local IP address on a Session Border Controller (SBC) interface, which can be used for media arriving on the DBE.
	<i>nat-mode twice-nat</i>	(Optional) Allows local addresses to be reserved for Twice-NAT pinholes.
	vrf <i>vrf-name</i>	(Optional) Specifies that the IP address is associated with a specific VPN routing and forwarding (VRF) instance. If the VRF is not specified, the address is assumed to be an address on the global VPN.
	<i>managed-by</i>	(Optional) Specifies whether the DBE or the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.
	dbe	(Optional) Specifies that only the DBE is allowed to select these addresses as local addresses for flows.
	mgc	(Optional) Specifies that only the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.

Command Default No default behavior or values are available.

Command Modes

- SBC configuration (config-sbc) for unified SBC
- SBC-DBE configuration (config-sbc-dbe) for distributed SBC
- Voice service VoIP for TDM gateways and CUBE(config-voi-serv)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	This command was modified. The <i>nat-mode twice-nat</i> keyword was introduced.
	Cisco IOS XE Release 2.4	This command was modified for unified SBC.
	Cisco IOS XE Release 3.2S	This command was modified. The IPv6 support was added.
	Cisco IOS XE Release 3.9S	This command was modified to be supported under voice service VoIP configuration.

Usage Guidelines

Use the **media-address** command to configure a local media address for the traffic arriving on the DBE for each IP address that you specified under the SBC virtual interface with the **ip address** command.

After you have configured a local media address, it cannot be modified while the DBE service is active. You must first deactivate the DBE with the **no activate** command.

Media address is a pool of IP addresses on the DBE for the media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All the vDBEs within the DBE draw media addresses from this pool.

Examples

The following example for a unified SBC shows how the IP address 10.0.1.1, which is configured on an SBC interface, is used when media traffic arrives on the DBE from the global VPN:

```
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc)# media-address ipv4 10.0.1.1
Router(cfg-sbc-media-address)# end
```

The following example for a distributed SBC shows that the IPv4 address 10.0.1.1, which is configured on an SBC interface, is the local address used when media traffic arrives on the DBE, and is reserved for Twice-NAT pinholes:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv4 10.0.1.1 managed-by mgc nat-mode twice-nat
Router(config-sbc-dbe-media-address)# end
```

The following example for a distributed SBC shows that the IP address 10.0.1.1, which is an address configured on an SBC interface, is used when media traffic arrives on the DBE from the global VPN:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv4 10.0.1.1
Router(config-sbc-dbe-media-address)# end
```

The following example for a distributed SBC tries to delete the media address 1.1.1.1 before deactivating the DBE, and receives an error message:

```
Router(config-sbc-dbe)# no media-address ipv4 1.1.1.1
SBC: Unable to delete a media address whilst the DBE is active.
SBC: Please deactivate the DBE and try again.
```

The following example configures port ranges for a media-address range:

```
Router(config)# voice service voip
Router (conf-voi-serv)# media-address range 1.3.6.3 1.3.6.4
Router (conf-voi-serv)# port-range 32766 32766
```

Related Commands

Command	Description
media-address pool	Creates a pool of sequential IPv4 and IPv6 media addresses that can be used by the DBE as local media addresses.
ip address	Configures the IPv4 address and the subnet mask on an SBC interface.
sbc dbe	Creates the DBE service on an SBC and enters into the SBC-DBE configuration mode.
activate	Initiates the DBE service of the SBC.

media-address ipv4

To add an IPv4 H.248 Border Access Controller (BAC) address to the set of addresses that the BAC can use as local media address, use the **media-address ipv4** command in the H248 BAC configuration mode. To remove an IPv4 address from the set of local media addresses, use the **no** form of this command.

media-address ipv4 *ipv4-address* **realm** *realm-number* **vrf** *vrf-name*

no media-address ipv4 *ipv4-address* **realm** *realm-number* **vrf** *vrf-name*

Syntax Description	ipv4	Configures an IPv4 H.248 BAC media address.
	<i>ipv4-address</i>	IPv4 address assigned to an H.248 association.
	realm	Configures the realm for an IPv4 H.248 BAC media address.
	<i>realm-number</i>	Specifies the realm number.
	vrf	Configures a VPN routing and forwarding (VRF) instance.
	<i>vrf_name</i>	Name of the VRF for the H.248 adjacency.

Command Default None

Command Modes H248 BAC configuration (config-h248-bac)

Command History	Release	Modification
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

A realm group can contain multiple media addresses. When you configure a realm group under an adjacency, the IP address and port for the media stream of this adjacency is allocated from the media addresses in this realm group.

The **media-address ipv4** command includes the **port-range** *port-range* subcommand that configures the port range of the media address.

Examples

The following example shows how the **media-address ipv4** command is used to configure an H.248 media address instance:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# media-address ipv4 192.168.0.2 realm 5 vrf cisco
Router(config-h248-bac-media-addr)# port-range 20000 30000
```

Related Commands	Command	Description
	realm (H.248 BAC)	Configures an IP realm of the BAC under an adjacency.

media-address pool

To create a pool of sequential IPv4 or IPv6 media addresses that can be used by the data border element (DBE) as local media addresses, use the **media-address pool** command in the appropriate configuration mode. This pool of addresses is added to the set of local media addresses that can be used by the DBE. To remove this pool of IPv4 addresses from the set of local media addresses, use the **no** form of this command.

media-address pool {**ipv4** | **ipv6**} {*start-addr*} {*end-addr*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

no media-address pool {**ipv4** | **ipv6**} {*start-addr*} {*end-addr*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

Syntax Description		
<i>start-addr</i>		Starting the IPv4 or IPv6 media address in a range of addresses. An IPv4 or IPv6 media address is a local IP address on a Session Border Controller (SBC) interface that can be used when media traffic arrives on the DBE.
<i>end-addr</i>		Ending an IPv4 or IPv6 media address in a range of addresses. The ending IPv4 or IPv6 address must be numerically greater than the starting address.
nat-mode twice-nat		(Optional) Allows local addresses to be reserved for the Twice-NAT pinholes.
vrf <i>vrf-name</i>		(Optional) Specifies that the IP addresses are associated with a specific VPN routing and forwarding (VRF) instance. If the VRF instance is not specified, the address is assumed to be an address on the global VPN.
managed-by		(Optional) Specifies whether the DBE or the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.
dbe		(Optional) Specifies that only the DBE is allowed to select these addresses as local addresses for flows.
mgc		(Optional) Specifies that only the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.

Command Default If a pool of IPv4 or IPv6 media addresses is specified, but the optional parameters are not specified, the following default values are used:

- Addresses in the pool are members of the global VRF.
- Only the DBE is allowed to select these addresses as local addresses for flows.

Command Modes

SBC configuration (config-sbc): for unified SBC

SBC-DBE configuration (config-sbc-dbe): for distributed SBC

Voice service VoIP(config-voi-serv): for TDM gateways and CUBE

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	This command was modified. The nat-mode twice-nat keyword was introduced.
Cisco IOS XE Release 2.4	This command was modified for unified SBC.
Cisco IOS XE Release 3.2S	This command was modified. The IPv6 support was added.
Cisco IOS XE Release 3.9S	This command was modified to be supported under the voice service VoIP configuration.

Usage Guidelines

Depending on whether you are running an unified SBC or a distributed SBC, use this command in the appropriate configuration mode.

The media address pool size is limited to 1024 IPv4 addresses. If more IPv4 addresses are required, we recommend that you create multiple SBC interfaces, and then configure the address pools from the subnets on those interfaces.

After you configure a local media address, it cannot be modified while the DBE service is active. Deactivate the DBE with the **no activate** command before modifying the media-address pool ipv4 specification.

A media address is a part of a pool of IP addresses on the DBE that are used for the media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All the virtual data border elements (vDBEs) within the DBE draw media addresses from this pool.

Examples

The following example for a unified SBC shows how to create a DBE service on an SBC called “global” and how to configure addresses from 10.0.2.1 to 10.0.2.10 in the global VRF:

```
Router(config)# sbc global
Router(config-sbc)# media-address pool ipv4 10.0.2.1 10.0.2.10
Router(cfg-sbc-media-address-pool)# end
```

The following example for a distributed SBC shows how to add IPv4 addresses from 10.0.2.1 to 10.0.2.10 to the media address pool as local addresses reserved for the Twice-NAT pinholes:

```
Router(config)# sbc mySbc db
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.1 10.0.2.10 nat-mode twice-nat
Router(config-sbc-dbe-media-address-pool)# end
```

The following example for a distributed SBC shows how to create a DBE service on an SBC called “mySbc,” and enters into the SBC-DBE configuration mode, and how to configure addresses from 10.0.2.1 to 10.0.2.10 in the global VRF:

```
Router(config)# sbc mySbc db
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.1 10.0.2.10
Router(config-sbc-dbe-media-address-pool)# end
```

The following example for a distributed SBC shows how to create a DBE service on an SBC called “mySbc,” and enters into the SBC-DBE configuration mode, and how to configure addresses from 10.0.2.20 to 10.0.2.25 in vpn3:

```
Router(config)# sbc mySbc dbe  
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.20 10.0.2.25 vrf vpn3  
Router(config-sbc-dbe-media-address-pool)# exit
```

The following example for a distributed SBC tries to delete the media address 10.0.2.1 before deactivating the DBE, and receives an error message:

```
Router(config-sbc-dbe)# no media-address ipv4 10.0.2.1  
SBC: Unable to delete a media address whilst the DBE is active.  
SBC: Please deactivate the DBE and try again.
```

Related Commands

Command	Description
activate	Initiates the DBE service of the SBC.
media-address	Adds an IPv4 address to the set of addresses that can be used by the DBE as a local media address.

media-gateway

To configure a media gateway, use the **media-gateway** command in SBE configuration mode. To remove a media gateway configuration, use the **no** form of this command.

```
media-gateway ipv4 A.B.C.D

no media-gateway ipv4 A.B.C.D
```

Syntax Description	ipv4 A.B.C.D	Specifies the IPv4 media gateway address.
--------------------	--------------	---

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	SBE configuration (config-sbc-sbe)
---------------	------------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to access media gateway mode from where you configure a media gateway. <pre>Router# configure terminal Router(config)# sbc mysbc Router(config-sbc)# sbe Router(config-sbc-sbe)# media-gateway ipv4 10.0.0.1 Router(config-sbc-sbe-mg)#</pre>
----------	--

Related Commands	Command	Description
	codecs	Configures the codecs supported by the media gateway.
	show sbc sbe media-gateway-associations	Displays a list of known media gateways with an active association.
	transcoder	Configures the media gateway as a transcoder.

media-gateway policy type

To configure a media gateway policy, use the **media-gateway policy type** command in the SBE configuration mode. To remove the policy, use the **no** form of this command.

media-gateway policy type {default | local | {remote {ipv4 | ipv6} ip-address [port port-number]}}

no media-gateway policy type {default | local | {remote {ipv4 | ipv6} ip-address [port port-number]}}

Syntax Description

default	Specifies that the media gateway policy must be applied to all media gateways configured on the SBC. A default media gateway policy is applied on a media gateway (local or remote) when no other media policy is applied on the media gateway.
local	Specifies that the media gateway policy must be applied to the media gateway that is locally configured on the SBC.
remote	Specifies that the media gateway policy must be applied to a remote media gateway.
ipv4	Specifies that the remote media gateway has an IPv4 IP address.
ipv6	Specifies that the remote media gateway has an IPv6 IP address.
<i>ip-address</i>	IP address of the remote media gateway. The IP address can be in the IPv4 format or IPv6 format.
port	Specifies the port number of the remote media gateway.
<i>port-number</i>	Port number of the remote media gateway.

Command Default

No default behavior or values are available.

Command Modes

SBE configuration (config-sbc-sbe)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

In the following example, the **media-gateway policy type** command is used to configure a remote-type media gateway policy on the media gateway at 192.0.2.26:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway policy type remote ipv4 192.0.2.26 6886
```

Related Commands

Command	Description
interwork maximum	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
interwork cost	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
ipsec maximum	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
media-gateway policy type	Configures a media gateway policy.
media limits	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
media-policy	Configures a media policy.
show sbc sbe media-gateway-policy	Displays the details of media gateway policies.
show sbc sbe media-policy	Displays the details of media policies.
total resource maximum	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
transcode cost	Specifies the resource cost for transcoding an audio or video stream.
transcode maximum	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
transrate audio cost	Specifies the resource cost for transrating an audio stream.
transrate audio maximum	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
type	Configures a media policy as a CAC-policy type policy or a gateway type policy.

media-late-to-early-iw

To configure late-to-early media interworking (iw), use the **media-late-to-early-iw** command in Adjacency SIP configuration mode. To deconfigure late-to-early media interworking (iw), use the **no** form of this command.

media-late-to-early-iw {incoming | outgoing}

no media-late-to-early-iw {incoming | outgoing}

Syntax Description	<i>incoming</i>	Enable late-to-early media iw for calls from caller on this adjacency.
	<i>outgoing</i>	Enable late-to-early media iw for calls to callee on this adjacency.

Command Default	<i>No default behavior or values are available.</i>
------------------------	---

Command Modes	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

Examples	The following example shows how to configure late-to-early media iw for calls from caller on this adjacency.
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# media-late-to-early-iw incoming
```

Related Commands	Command	Description
	adjacency	Configures an adjacency for an SBC service.

media-line

To add a media description line to an entry in an SDP media profile, use the **media-line** command in SBC SBE SIP SDP media profile entry configuration mode. To delete a line, use the **no** form of this command.

media-line *index* "*media-description*"

no media-line *index*

Syntax Description

<i>index</i>	Specifies the SDP line number in an SDP media profile. Must be an integer.
<i>"media-description"</i>	The <i>media_description</i> argument must be enclosed in quotes (" "). The value inside the quotes must be syntactically valid SDP as defined in RFC 2327. The following rules apply: - An SDP entry must contain exactly one m-line. The m-line must appear first in the entry. The m-line port must be zero. SBC replaces the zero with the appropriate port. - An SDP entry must not contain a c-line. The Cisco command line interface handles the contents of <i>media_description</i> as a string value. It does not check the syntax of the configured information. If the syntax is incorrect, outbound offers by the SBC are rejected.

Command Default

No default behavior or values are available.

Command Modes

SBC SBE SIP SDP media profile entry configuration (config-sbc-sbe-sip-sdp-media-ele)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Use the **media-line** command to add media description lines into an entry of an SDP media profile.

Examples

The following example shows how to create lines in an SDP media profile entry :

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip sdp-media-profile Mediaprofile
Router(config-sbc-sbe-sip-sdp-media)# entry 1
Router(config-sbc-sbe-sip-sdp-media-ele)# media-line 1 "m=audio 0 RTP/AVP 31"
Router(config-sbc-sbe-sip-sdp-media-ele)# media-line 2 "a=aaa:testing"
```

```
Router(config-sbc-sbe-sip-sdp-media-ele) # Ctrl Z
```

Related Commands

Command	Description
entry	Creates an entry in a table or SDP media profile.
sdp-media-profile	Creates or modifies a customized SDP media profile.
show sbc sbe sip sdp-media-profile	Shows all SDP media profiles in an SBC service or details for a specified profile.

media-policy

To configure a media policy, use the **media-policy** command in the SBE configuration mode. To remove the media policy configuration, use the **no** form of this command.

```
media-policy policy-name

no media-policy policy-name
```

Syntax Description

<i>policy-name</i>	Name of the media policy. The <i>policy-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Except for the underscore character, do not use any special character to specify field names.
--------------------	--

Command Default

No default behavior or values are available.

Command Modes

SBE configuration (config-sbc-sbe)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

```
In the following example, the media-policy command is used to create the my_media_policy media policy:

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
```

Related Commands	Command	Description
	interwork maximum	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	interwork cost	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	ipsec maximum	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	media-gateway policy type	Configures a media gateway policy.
	media limits	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	media-policy	Configures a media policy.
	show sbc sbe media-gateway-policy	Displays the details of media gateway policies.
	show sbc sbe media-policy	Displays the details of media policies.
	total resource maximum	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	transcode cost	Specifies the resource cost for transcoding an audio or video stream.
	transcode maximum	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	transrate audio cost	Specifies the resource cost for transrating an audio stream.
	transrate audio maximum	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	type	Configures a media policy as a CAC-policy type policy or a gateway type policy.

media-timeout (session border controller)

To set the maximum time a DBE waits after receiving the last media packet on a call and before cleaning up the call resources, use the **media-timeout** command in SBC-DBE configuration mode. To reset the **timeout** value to the default value of 30 seconds, use the **no** form of this command.

```
media-timeout {timeout} first-packet

no media-timeout timeout
```

Syntax Description	timeout This is the timeout value in seconds.
--------------------	---

Command Default	The default is 30 seconds if media-timeout is not configured.
-----------------	--

Command Modes	SBC-DBE configuration (config-sbc-dbe)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	The first-packet keyword was added.

Usage Guidelines

This command sets the maximum time the DBE waits after receiving the last media packet on a call before the DBE determines that the call has ceased and begins to clear up the call resources and to signal the signaling border element (SBE) to do the same. This command is used when the SBE is not able to clear up the calls itself. The normal method for clearing a call is for the SBE to explicitly signal the DBE.

You can halt detection of the media timeout event with the **first-packet** keyword of the **media-timeout** command. The **first-packet** keyword instructs the DBE to wait until it has received the first packet since the call has been established before starting the media timeout timer to start counting the number of seconds for which it has not seen an SBC packet. By the DBE waiting, SBC packets can continue to be forwarded because there is no media timeout yet. After waiting for the first packet and counting the configured number of seconds, then the DBE generates an alert to the SBE.

Use the **sbc dbe** command to enter into SBC-DBE configuration mode before using the **media-timeout** command.

Examples

The following example configures the DBE to wait 10 seconds after receiving the last media packet and before cleaning up the call resources:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-timeout 10
```

Related Commands	Command	Description
	db e	Enters into SBC-DBE configuration mode.

media address preserve

To ensure that media pinholes are preserved for deleted streams so that if a stream is re-enabled, the Cisco Unified Border Element (SP Edition) will re-use the same pinhole, use the **media address preserve** command in CAC table entry configuration mode. To preserve media addresses allocated during the initial call negotiation process, use the **init-negotiation** keyword. To allow a media pinhole for a deleted stream to be deleted, use the **no** form of this command.

media address preserve

media address preserve init-negotiation

no media address preserve

Syntax Description

init-negotiation	Enable or disable Media Address Preservation during initial call negotiaiton.
-------------------------	---

Command Default

If the **media address preserve** command is not configured or the **no media address preserve** command is used, the media pinhole for a deleted stream will be deleted.

Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.5.1	Enhancement for Media Address Preservation during initial negotiation introduced.

Usage Guidelines

The **media address preserve** command configures the Support Renegotiated Call Over NAT feature. This feature is used to avoid de-allocation of a video pinhole in a Network Address Translation (NAT) scenario where Delta Renegotiation mode is in effect and a video transmission is paused. Although the standard Secure Device Provisioning (SDP) protocol when a video transmission is paused is to set the video stream to “a=inactive” (which indicates that SBC should keep the stream allocated), there are known devices that do not set the video stream to “a=inactive” to pause it. Instead, these devices delete the video stream by setting its port to 0. To ensure that the stream remains allocated and the pinhole is preserved even when the SBC receives a port value of 0 during a media stream renegotiation, you can enable the **media address preserve** command on a per-call basis. When the **media address preserve** command is enabled, stream statistics and SDP billing information will be output at call termination, not at Delta Renegotiation.

The **init-negotiation** keyword enables you to preserve media addresses allocated during the initial call negotiation process. This means that a media address/port allocated due to SDP in an initial offer remains allocated for the lifetime of the call.

Examples

The following example ensures that media pinholes are preserved for deleted streams so that if a stream is re-enabled, the Cisco Unified Border Element (SP Edition) will re-use the same pinhole. Note that the **media address preserve** command is applied on a per-call basis.

```
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media address preserve
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac complete
Router(config-sbc-sbe-cacpolicy)# complete
Router(config-sbc-sbe)# active cac-policy-set 1
```

Related Commands

Command	Description
show sbc sbe cac-policy-set table entry	Lists detailed information for a given entry in a CAC policy table, including whether the media address preserve command is enabled. When the media address preserve command is enabled, the “Media Address” field shows a value of “Preserve.”

media bandwidth-fields ignore

To set the media flag to ignore the b-line and use CODEC to calculate the baseline bandwidth required for the media stream, use the **media bandwidth-fields ignore** command in the CAC table entry configuration mode. To return to the default state, use the **no** form of this command.

media bandwidth-fields ignore

no media bandwidth-fields

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values are available.

Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following example shows how to set the AMB_CAC_MEDIA_FLAG_IGN_EXPL_BW media flag to ignore the b-line and use CODEC to calculate the baseline bandwidth required for the media stream:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table StandardListByAccount
Router(config-sbc-sbe-cacpolicy)# cac-table StandardListByAccount
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media bandwidth-fields ignore
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

Related Commands

Command	Description
show sbc sbe	Displays detailed information for a given entry in a CAC policy table.
cac-policy-set table entry	

media bypass

To configure the Multiple SBC Media Bypass feature on a Session Initiation Protocol (SIP) adjacency, use the **media bypass** command in the adjacency SIP configuration mode. To disable the Multiple SBC Media Bypass feature, use the **no** form of this command.

media bypass { **max-data-len** *data-length* | **tag** *sequence-number* *tag-name* | **auto-nat-tag-gen** }

no media bypass { **max-data-len** | **tag** *sequence-number* | **auto-nat-tag-gen** }

Syntax Description		
max-data-len		Specifies the maximum length of the multiple SBC media bypass data that can be transmitted through the outbound signaling messages on an adjacency.
<i>data-length</i>		Maximum multiple SBC media bypass data length, in bytes. The range is from 100 to 2048. The default is 1000.
tag		Specifies the tag that can be used to control the groups to which the endpoints on an adjacency belong to in the Multiple SBC Media Bypass feature.
<i>sequence-number</i>		Sequence number of a media bypass tag in the tag list. The tag list is formed from the set of tags that are arranged according to their sequence number. The range is from 1 to 20.
<i>tag-name</i>		Name of a multiple SBC media bypass tag. The total length of all the tags in an adjacency cannot exceed 255 characters. A tag name can contain letters (alphabets), numerals, special characters, and all printable characters other than commas, semicolons, and spaces.
auto-nat-tag-gen		Configures the Common IP Address Media Bypass feature to generate a media bypass tag for registered endpoints that are behind a NAT device associated with this adjacency. The default is that the SBC does not generate media bypass tags on the basis of the NAT device behind which the endpoints are located.

Command Default The SBC relays media for all the endpoints associated with the adjacency.

Command Modes Adjacency SIP configuration mode (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The media-bypass and media-bypass forbid commands were replaced with the media bypass command.
	Cisco IOS XE Release 3.6S	This command was modified. The auto-nat-tag-gen keyword was added with the introduction of the Common IP Address Media Bypass feature.

Usage Guidelines

On any particular adjacency, you can configure both the **media bypass tag** *sequence-number tag-name* command and the **media bypass auto-nat-tag-gen** command.

To use the **media bypass** command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.



Note

Media bypass is not supported for H.323 calls.

Examples

The following example shows how to use the **media bypass** command to configure the Multiple SBC Media Bypass feature and to set the maximum length of the multiple SBC media bypass data that can be transmitted on the outbound signaling messages on the adjacency to 150 bytes. The second **media bypass** command in this example is used to set TAG1 as the name of the tag that is used to control the groups that belong to the endpoints on the adjacency.

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# media bypass max-data-len 150
Router(config-sbc-sbe-adj-sip)# media bypass tag 1 TAG1
```

The following example shows how to use the **media bypass** command to configure the Multiple SBC Media Bypass feature and to specify that a media bypass tag must be automatically generated for each endpoint that is behind a NAT device on the adjacency.

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# media bypass auto-nat-tag-gen
```

Related Commands

Command	Description
adjacency	Configures an adjacency for the SBC service.

media bypass type

To configure the Multiple SBC Media Bypass feature for a Call Admission Control (CAC) policy set, use the **media bypass type** command in the CAC table entry configuration mode. To deconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

media bypass type [all | none | full [hairpin partial] | hairpin [full partial] | partial [full hairpin]

no media bypass type

Syntax Description		
all		Enables all types of media bypass, such as partial, hairpin, and full, for a CAC table entry.
none		Disables all types of media bypass for a CAC table entry.
full		Enables media bypass on the SBC if adjacent and nonadjacent downstream and upstream hops have direct media connectivity, and common tags in the bypass tag list, or the same VPN.
hairpin		Enables media bypass for hairpin calls.
partial		Enables media bypass if the SBC is a member of a group of SBCs that share the same IP realm, and if even one SBC within that group is on the media path.

Command Default No default behavior or values are available.

Command Modes CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples The following example shows how to configure the Multiple SBC Media Bypass feature to enable all types of media bypass:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media bypass type all
```

Related Commands	Command	Description
	cac-table	Configures the admission control tables.
	table-type	Configures a CAC table type to enable the priority of the call to be used as a criterion in the CAC policy.

media limits

To specify the media policy to be associated with the CAC policy table entry or applied on the media gateway, use the **media limits** command in the SBE CAC table CAC policy configuration mode or the SBE media gateway configuration mode. To remove this configuration, use the **no** form of this command.

media limits *policy-name*

no media limits *policy-name*

Syntax Description

<i>policy-name</i>	The <i>policy-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
Note	Except for the underscore character, do not use any special character to specify field names.

Command Default

No default behavior or values are available.

Command Modes

The configuration mode can be one of the following:

- SBE CAC table CAC policy configuration (config-sbc-sbe-cacpolicy-cactable-entry)
- SBE media gateway configuration (config-sbc-sbe-mg-pol)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

In the following example, the **media limits** command is used to specify that the mp1 policy must be applied as entry 1 in the t1 CAC table.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table t1
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media limits mp1
```

In the following example, the **media limits** command is used to specify that the `audio_limit1` media policy must be applied on the remote media gateway at 192.0.2.82:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy audio_limit1
Router(config-sbc-sbe-media-pol)# type gateway
Router(config-sbc-sbe-media-pol)# transcode audio maximum 15000
Router(config-sbc-sbe-media-pol)# exit
Router(config-sbc-sbe)# media-gateway policy type remote ipv4 192.0.2.82 port 2000
Router(config-sbc-sbe-mg-pol)# media limits audio_limit1
```

Related Commands

Command	Description
interwork maximum	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
interwork cost	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
ipsec maximum	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
media-gateway policy type	Configures a media gateway policy.
media limits	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
media-policy	Configures a media policy.
show sbc sbe media-gateway-policy	Displays the details of media gateway policies.
show sbc sbe media-policy	Displays the details of media policies.
total resource maximum	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
transcode cost	Specifies the resource cost for transcoding an audio or video stream.
transcode maximum	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
transrate audio cost	Specifies the resource cost for transrating an audio stream.
transrate audio maximum	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
type	Configures a media policy as a CAC-policy type policy or a gateway type policy.

media police

To configure how SBC handles media streams that exceed bandwidth limits for media calls, use the **media police** command in CAC table entry configuration mode. To return the policing conditions to the default value, use the no form of this command.

media police strip | reject | degrade

no media police strip | reject | degrade

Syntax Description		
strip	Sets the following conditions:	- If an individual media stream exceeds the bandwidth limit for a call, that media stream is disabled by setting the port to zero (0). - If after the above stage has completed, the sum of the bandwidths of all remaining streams exceeds the bandwidth limit for a call, the request is rejected.
reject	Sets the following conditions:	If an individual media stream exceeds the bandwidth limit for a call, the request is rejected. If the sum of the bandwidths of all media streams exceeds the bandwidth limit for a call, the request is rejected.
degrade	If a media stream exceeds the bandwidth limit for a call, the video stream is downgraded to a lower (non-zero) bandwidth that brings the media stream within the bandwidth limit for the call.	Note Only the video stream is downgraded. Audio streams are not downgraded. If the audio stream exceeds the bandwidth for a call, the media stream cannot be downgraded.

Command Default	When media police is not configured, the default is to inherit the conditions from the interface, which in most cases is equivalent to the conditions for strip.
------------------------	--

Command Modes	CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

The degrade option is not supported on H.323 calls.

Using the degrade option may cause a 2 to 5 percent performance degradation.

Examples

The following example shows how to configure SBC to degrade media streams to lower bandwidths when requests exceed bandwidth limits.

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table cac-tbl-1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media police degrade
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

Related Commands

Command	Description
bandwidth	Configures the maximum and minimum bandwidth limits for media calls.
caller-bandwidth-field	Configures SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the caller.
callee-bandwidth-field	Configures the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the callee
max-bandwidth-per-scope	Configures the maximum limit for the bandwidth in bps, Kbps, Mbps or Gbps for an entry in an admission control table.

method-editor

To configure a method editor, use the **method-editor** command in the Adjacency SIP configuration mode. To remove a method editor, use the **no** form of this command.

method-editor {inbound | outbound} {editor-name | default}

no method-editor {inbound | outbound} {editor-name | default}

Syntax Description		
inbound	Sets the inbound SIP method editor.	
outbound	Sets the outbound SIP method editor.	
<i>editor-name</i>	Name of the method editor to be set for inbound or outbound signaling on the adjacency.	
	The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.	
	Note Except for the underscore character, do not use any special character to specify field names.	
default	Sets the method editor to the default settings.	

Command Default No default behavior or values are available.

Command Modes Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples The following example shows how the **method-editor** command configures an inbound method editor named test1:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-sip)# method-editor inbound test1
```

Related Commands	Command	Description
	sip method-editor	Configures a method editor.

method-profile

To configure a method profile in the mode of an SBE entity, use the **method-profile** command in Adjacency SIP configuration mode. To remove the method profile, use the **no** form of this command.

method-profile {inbound | outbound} *profile-name*

no method-profile {inbound | outbound}

Syntax Description	inbound outbound	Sets the inbound and outbound SIP method profiles.
	<i>profile-name</i>	Specifies the name of the method profile. If you enter the <i>name</i> default , the default profile is configured. This profile is used for all adjacencies that do not have a specific profile configured.
		The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
	Note	Except for the underscore character, do not use any special character to specify field names.

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how the method-profile command configures a method profile with the name of test1:
----------	---

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# method-profile test1
```

method 3GPP-RF

To enable the 3GPP-RF billing method on the Cisco Session Border Controller (SBC), use the **method 3GPP-RF** command in the SBC SBE billing configuration mode. To disable the 3GPP-RF billing method, use the **no** form of this command.

method 3GPP-RF

no method 3GPP-RF

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	SBC SBE billing configuration (config-sbc-sbe-billing)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples	The following example shows how to enable the 3GPP-RF billing method on the SBC:
-----------------	--

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# method 3gpp-rf
```

method (editor)

To add a method to an method editor, use the **method** command in the session initiation protocol (SIP) Method Editor configuration mode. To remove a method from an editor, use the **no** form of this command.

method *method-name*

no method *method-name*

Syntax Description	<i>method name</i> Name of the method to be added to the method editor. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.					
Command Default	No default behavior or values are available.					
Command Modes	SIP Method Editor configuration (config-sbc-sbe-mep-mth)					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE Release 3.3S</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr></table>		Release	Modification	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification					
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.					
Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.					
Examples	The following example shows how the method command adds a method, test, to the Myeditor method editor: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# sip method-editor Myeditor Router(config-sbc-sbe-mep-mth)# method test</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>sip method-editor</td><td>Configures a method editor.</td></tr></table>		Command	Description	sip method-editor	Configures a method editor.
Command	Description					
sip method-editor	Configures a method editor.					

method packetcable-em

To enable the packet-cable billing method, use the `method packetcable-em` in the SBE billing configuration mode. To disable the packet-cable billing method, use the **no** form of this command.

method packetcable-em

no method packetcable-em

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values are available.

Command Modes SBE billing configuration (config-sbc-sbe-billing)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples *The following example shows how to enable the packet-cable billing method:*

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
(config-sbc-sbe)# billing
(config-sbc-sbe-billing)# method packetcable-em
```

Related Commands	Command	Description
	activate (radius)	Activates the billing functionality after configuration is committed.
	billing	Configures billing.
	ldr-check	Configures the time of day (local time) to run the Long Duration Check (LDR).
	local-address ipv4	Configures the local IPv4 address that appears in the CDR.
	packetcable-em transport radius	Configures a packet-cable billing instance.
	show sbc sbe billing remote	Displays the local and billing configurations.

method (session border controller)

To add a method with a specified name to a SIP message profile, use the **method** command in the SIP method-profile mode. To remove the method from the profile, use the **no** form of this command.

method *method-name*

no method *method-name*

Syntax Description	<i>method name</i>	Specifies the name of the method added to the method profile. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.
--------------------	--------------------	--

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	SIP method-profile configuration (config-sbc-sbe-sip-mth)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how the method command adds a method test to the method profile Myprofile:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile Myprofile
Router(config-sbc-sbe-sip-mth)# method test
```

method xml

To configure the Billing Manager such that it enables enabling the XML billing method, use the **method xml** command in the SBE billing configuration mode. To disable the XML billing method, use the **no** form of this command.

method xml

no method xml

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes SBE billing configuration (config-sbc-sbe-billing)

Command History	Release	Modification
	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines The XML method has been introduced to provision IP-centric logging information. Because the PacketCable billing method was too telephonic-specific, and uses the BAF format, the XML method has been introduced.

To enable the XML billing method on Billing Manager, you need to execute the **method xml** command from SBE billing configuration mode. To disable, the XML billing method, execute the **no method xml** command.



Note

If XML billing instances are configured, the **no method xml** command cannot be successfully executed.

Examples The following example shows how to enable the XML billing method on the Billing Manager:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# method xml
```

Related Commands	Command	Description
	xml (billing)	Configures the method index for XML billing.
	cdr path	Indicates the path in which to store CDR billing records on the local machine.
	ldr-check	Configures the time at which long duration records are checked.

minor-alert-size

To configure the number of specified events before a minor alert is triggered, use the **minor-alert-size** command in the blacklist reason mode. To disable the number of specified events, use the no form of this command.

minor-alert-size *number-of-events*

no minor-alert-size

Syntax Description	<i>number-of-events</i>	The number of events for alert to be triggered. This can be of any value ranging from 1 to 65535.
---------------------------	-------------------------	---

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Blacklist reason mode (config-sbc-sbe-blacklist-reason)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.
-------------------------	---

Examples	The following example shows how to configure the number of specified events for a minor alert to be triggered using the minor-alert-size command in the blacklist reason mode:
-----------------	---

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist)# reason na-policy-rejection
Router(config-sbc-sbe-blacklist-reason)# minor-alert-size 20
```

Related Commands	Command	Description
	critical-alert-size	Configures the number of specified events before a critical alert is triggered.
	major-alert-size	Configures the number of specified events before a major alert is triggered.
	reason	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).

Command	Description
trigger-period	Defines the period over which events are considered. For details, see the description of the trigger-size command.
trigger-size	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
timeout	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
snmp-server enable traps sbc blacklist	To enable SNMP SBC Blacklist traps.
show sbc sbe blacklist configured-limits	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.

mode (session border controller)

To enter a mode for configuring the mode of a RADIUS Authentication server or RADIUS accounting server, use the **server mode** command in the server authentication mode. To exit the mode for configuring of RADIUS Authentication server mode, use the **no** form of this command.

```
mode {local |remote}

no mode {local |remote}
```

Syntax Description

<i>server-name</i>	Specifies the name of the server.
local	Specifies local authentication.
remote	Specifies remote authentication.

Command Default

No default behavior or values are available.

Command Modes

Server authentication (config-sbc-sbe-auth-ser)
Server accounting (config-sbc-sbe-acc-ser)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following example shows how to configure server mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius authentication
Router(config-sbc-sbe-auth)# server panther
Router(config-sbc-sbe-auth-ser)# mode local
Router(config-sbc-sbe-auth-ser)#
```

monitor event-trace sbc ha (EXEC)

To monitor and control the event trace function of the Session Border Controller (SBC), use the **monitor event-trace sbc ha** command in privileged EXEC mode.

monitor event-trace sbc ha { **clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot** }

Syntax Description		
ha		Monitors and controls the event trace messages pertaining to the SBC high availability.
clear		Clears the existing trace messages pertaining to the SBC.
continuous		Continuously displays the latest event trace entries.
cancel		(Optional) Cancels the continuous display of the latest trace entries.
disable		Turns off event tracing for the SBC.
dump		Writes the event trace results to the file that has been configured using the monitor event-trace sbc ha command in global configuration mode. The trace messages are saved in binary format.
pretty		(Optional) Saves the event trace messages in ASCII format.
enable		Turns on event tracing for the SBC.
one-shot		Clears existing trace information, if any, from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the monitor event-trace sbc ha command in global configuration mode.

Command Default Event tracing in the SBC is not enabled.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced.
	Cisco IOS XE Release 2.3	The sbc_ha keyword was bifurcated into two keywords, sbc and ha .
	Cisco IOS XE Release 2.4	The event tracing default for the monitor event-trace sbc ha command was changed from Enabled to Disabled.
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines Use the **monitor event-trace sbc ha** command to control when and how and what kind of event trace data pertaining to the SBC on the Cisco ASR 1000 Series Aggregation Services Routers is collected. Use this command after you have configured the event trace functionality on the Cisco ASR 1000 Series Routers using the **monitor event-trace sbc ha** command in global configuration mode.

**Note**

The amount of data collected from the trace depends on the trace message size that has been configured using the **monitor event-trace sbc ha** command in global configuration mode for each instance of a trace.

You can enable or disable SBC event tracing either by using the **monitor event-trace sbc ha** command in privileged EXEC mode or by using the **monitor event-trace sbc** command in global configuration mode. To disable event tracing, you should enter either of these commands with the **disable** keyword. To enable event tracing again, you should enter either of these commands with the **enable** keyword.

Use the **show monitor event-trace sbc ha** command to display trace messages. Use the **monitor event-trace sbc ha dump** command to save the trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace sbc ha dump pretty** command.

To configure the file in which you want to save trace information, use the **monitor event-trace sbc ha dump-file *dump-file-name*** command in global configuration mode. The trace messages are saved in binary format.

Examples

The following example shows the privileged EXEC commands that stop event tracing, clear the current contents of memory, and re-enable the trace function for the SBC high availability events. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace sbc ha disable
Router# monitor event-trace sbc ha clear
Router# monitor event-trace sbc ha enable
```

The following example shows how to configure the continuous display of the latest SBC high availability trace entries:

```
Router# monitor event-trace sbc ha continuous
```

The following example shows how to stop the continuous display of the latest trace entries:

```
Router# monitor event-trace sbc ha continuous cancel
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls the event trace function for the specified Cisco IOS software subsystem component.
monitor event-trace sbc ha (global)	Configures event tracing for the SBC.
show monitor event-trace ha	Displays the event trace messages pertaining to the Cisco IOS software subsystem components.

monitor event-trace sbc ha (global)

To configure event tracing for the Session Border Controller (SBC), use the **monitor event-trace sbc ha** command in the global configuration mode. To remove event tracing configuration from the SBC, use the **no** form of this command.

monitor event-trace sbc ha { **disable** | **dump-file** *dump-file-name* | **enable** | **size** *number* | **stacktrace** [*depth*] }

no monitor event-trace sbc ha { **dump-file** *dump-file-name* | **size** *number* | **stacktrace** [*depth*] }

Syntax Description		
ha		Configures event tracing for SBC high availability.
disable		Turns off event tracing for SBC high availability.
dump-file <i>dump-file-name</i>		Specifies the file in which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters. The path can point to the flash memory on the networking device or to a TFTP or FTP server.
enable		Turns on event tracing for the SBC high availability events, if event tracing has been disabled with the monitor event-trace sbc ha disable command.
size <i>number</i>		Sets the number of messages that can be written to memory for a single instance of a trace. Valid values are from 1 to 1000000. Note Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the show monitor event-trace sbc ha parameters command.
		When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace		Enables stack trace at tracepoints. Note Clear the trace buffer with the monitor event-trace sbc ha clear privileged EXEC command before entering the command.
<i>depth</i>		(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.

Command Default Event tracing for the SBC is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced.
	Cisco IOS XE Release 2.3	The sbc_ha keyword was bifurcated into two keywords, sbc and ha .
	Cisco IOS XE Release 2.4	The event tracing default for the monitor event-trace sbc ha command was changed from Enabled to Disabled.
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **monitor event-trace sbc ha** command to enable or disable event tracing and to configure event trace parameters for the SBC.

The Cisco IOS XE software allows the SBC to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value either by using the **monitor event-trace sbc ha** command in the privileged EXEC mode or by using the **monitor event-trace sbc ha** command in the global configuration mode.

Additionally, default settings do not appear in the configuration file. If the SBC enables event tracing by default, the **monitor event-trace sbc ha enable** command does not appear in the configuration file of the networking device. However, disabling event tracing that has been enabled by default by the subsystem creates a command entry in the configuration file.



Note

The amount of data collected from the trace depends on the trace message size that has been configured using the **monitor event-trace sbc ha size** command for each instance of a trace. Some Cisco IOS software subsystem components set the size by default. To display the size parameters, use the **show monitor event-trace sbc ha parameters** command.

To determine whether event tracing is enabled by default for the SBC, use the **show monitor event-trace sbc ha** command to display the trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer with the **monitor event-trace sbc ha clear** privileged EXEC command.

Examples

The following example shows how to enable event tracing for the SBC subsystem component in the Cisco IOS XE software, and to configure the size to 10,000 messages. The trace messages file is set to sbc-ha-dump in flash memory.

```
Router(config)# monitor event-trace sbc ha enable
Router(config)# monitor event-trace sbc ha dump-file bootflash:sbc-ha-dump
Router(config)# monitor event-trace sbc ha size 10000
```

Related Commands

Command	Description
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace sbc ha (EXEC)	Monitors and controls the event trace function pertaining to the SBC.
show monitor event-trace sbc ha	Displays event trace messages pertaining to the SBC.

na-carrier-id-table

To enter the configuration mode of a number analysis table within the context of an SBE policy set, use the **na-carrier-id-table** command in the SBE call policy set mode. To remove the number analysis table, use the **no** form of this command.

na-carrier-id-table *table-name*

no na-carrier-id-table *table-name*

Syntax Description	<i>table-name</i> Name of the number analysis table you are creating, or name of an existing table you are configuring. The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
---------------------------	---

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	SBE routing policy (config-sbc-sbe-rtgpolicy)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The na-dst-number-attr-table was renamed as na-carrier-id-table.

Usage Guidelines	The entries in this table are matched with the carrier ID. If necessary, a new number analysis table is created. Do not change the configuration of the tables in the context of the active policy set. A number analysis table should not be removed if it is in the context of the active policy set. To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
-------------------------	---

Examples	The following command shows how to enter the configuration mode of the na-table number analysis table within the context of an SBE policy set:
-----------------	---

```
Router# configure terminal
Router# mySbc sbe
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-carrier-id-table na-table
Router(config-sbc-sbe-rtgpolicy-natable)#
```

Related Commands

Command	Description
sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
sbe	Enters the mode of an SBE entity within an SBC service.
call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

na-dst-address-table

To enter the configuration mode of a number analysis table within the context of an SBE policy set, use the **na-dst-address-table** command in the SBE call policy set mode. To remove the number analysis table, use the **no** form of this command.

na-dst-address-table *table-name*

no na-dst-address-table *table-name*

Syntax Description	<i>table-name</i> Name of the number analysis table you are creating, or name of an existing table you are configuring. The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
---------------------------	---

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	SBE call policy set (config-sbc-sbe-rtgpolicy)
----------------------	--

Command History	<table> <tr> <th data-bbox="386 1108 711 1136">Release</th><th data-bbox="727 1108 1515 1136">Modification</th></tr> <tr> <td data-bbox="386 1150 711 1178">Cisco IOS XE Release 2.4</td><td data-bbox="727 1150 1515 1213">This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr> <tr> <td data-bbox="386 1224 711 1251">Cisco IOS XE Release 3.2S</td><td data-bbox="727 1224 1515 1285">This command was modified. The na-dst-number-table was renamed as na-dst-address-table.</td></tr> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.	Cisco IOS XE Release 3.2S	This command was modified. The na-dst-number-table was renamed as na-dst-address-table.
Release	Modification						
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.						
Cisco IOS XE Release 3.2S	This command was modified. The na-dst-number-table was renamed as na-dst-address-table.						

Usage Guidelines	The entries in this table are matched with the complete dialed number. If necessary, a new number analysis table is created. Do not change the configuration of the tables in the context of the active policy set. A number analysis table should not be removed if it is in the context of the active policy set. To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
-------------------------	---

Examples	The following command shows how to create the MyNaTable number analysis table with the table entries matching the complete dialed number: <pre>Router# configure terminal Router# sbc mySbc Router(config-sbc)# sbe (config-sbc-sbe)# call-policy-set 1 (config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable (config-sbc-sbe-rtgpolicy-natable)# exit</pre>
-----------------	--

```
(config-sbc-sbe-rtgpolicy)# exit
```

Related Commands

Command	Description
sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
sbe	Enters the mode of an SBE entity within an SBC service.
call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
no call-policy-set default	Deconfigures the active routing policy set.
entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

na-dst-prefix-table

To enter the mode in which to configure a number analysis table, with numbers that match the prefix of the dialed number within an SBE policy set, use the **na-dst-prefix-table** command in SBE call policy set mode. Use the **no** form of this command to destroy the number analysis table.

na-dst-prefix-table *table-name*

no na-dst-prefix-table *table-name*

Syntax Description	<i>table-name</i>	Name of the number analysis table you are creating or of an existing table you are configuring. The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
--------------------	-------------------	---

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	SBE routing policy (config-sbc-sbe-rtgpolicy)
---------------	---

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE Release 2.4</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr></table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example illustrates the use of the na-dst-prefix-table command to create a number analysis table called <i>MyNaTable</i>. <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# call-policy-set 1 Router(config-sbc-sbe-rtgpolicy)# na-dst-prefix-table MyNaTable Router(config-sbc-sbe-rtgpolicy-natable)#</pre>
----------	---

Related Commands

Command	Description
sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
sbe	Enters the mode of an SBE entity within an SBC service.
call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

na-src-account-table

To enter the mode for configuring a number analysis table within an SBE policy set, with entries that match the source account, use the **na-src-account-table** command in the SBE call policy set mode. Use the **no** form of this command to destroy the table.

na-src-account-table *table-name*

no na-src-account-table *table-name*

Syntax Description

<i>table-name</i>	Name of the number analysis table within an SBE policy set, with entries matching the source account. The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Except for the underscore character, do not use any special character to specify field names.
-------------------	---

Command Default

No default behavior or values are available.

Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

Command History

Release	Modification
Cisco IOS XE Release 2.40.00	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following commands enter the mode for the NA table *MyNaTable*, or if it does not already exist, it creates it.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-account-table MyNaTable
```

Related Commands

Command	Description
sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
sbe	Enters the mode of an SBE entity within an SBC service.

Command	Description
call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

na-src-address-table

To enter the configuration mode of a source number analysis table within the context of an SBE policy set, use the **na-src-address-table** command in the SBE call policy set mode. To remove the number analysis table, use the **no** form of this command.

na-src-address-table *table-name*

no na-src-address-table *table-name*

Syntax Description

<i>table-name</i>	Name of the number analysis table you are creating, or name of an existing table you are configuring. The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
-------------------	---

Command Default

No default behavior or values are available.

Command Modes

SBE call policy set (config-sbc-sbe-rtgpolicy)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The na-src-number-table was renamed as na-src-address-table.

Usage Guidelines

The entries in this table are matched with the complete number from which the call originated. If necessary, a new number analysis table is created. Do not change the configuration of the tables in the context of the active policy set.

A number analysis table should not be removed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

The following command shows how to enter the configuration mode of the na-table number analysis table within the context of an SBE policy set:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-address-table MySrcNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# exit
```

```
Router(config-sbc-sbe-rtgpolicy)# exit
```

Related Commands	Command	Description
	sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	sbe	Enters the mode of an SBE entity within an SBC service.
	call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
	no call-policy-set default	Deconfigures the active routing policy set.
	entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

na-src-adjacency-table

To enter the mode of configuration of a number analysis table within the context of an SBE policy set, use the **na-src-adjacency-table** command in SBE routing policy mode. The **no** form of this command destroys the number analysis table.

na-src-adjacency-table *table-name*

no na-src-adjacency-table *table-name*

Syntax Description

<i>table-name</i>	Name of the number analysis table within an SBE policy set, with entries matching the source account. The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
-------------------	---

Command Default

No default behavior or values are available.

Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The entries of this table match against the source adjacency. If necessary, a new number analysis table is created. You may not change the configuration of tables in the context of the active policy set. A number analysis table may not be destroyed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following commands enter the mode for the NA table *MyNaTable* with entries matching against the whole dialed number:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-adjacency-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
```

Related Commands

Command	Description
sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
sbe	Enters the mode of an SBE entity within an SBC service.
call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

na-src-name-anonymous-table

To enter the configuration mode of a number analysis table, to determine whether the display name or presentation number is anonymous, use the **na-src-name-anonymous-table** command in the SBE routing policy configuration mode. Use the **no** form of this command to remove the number analysis table.

na-src-name-anonymous-table *table-name*

no na-src-name-anonymous-table *table-name*

Syntax Description

table-name

Name of the number analysis table you are creating or of an existing table you are configuring.

The *table-name* can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.

Note Except for the underscore character, do not use any special character to specify field names.

Command Default

No default behavior or values are available.

Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers

Usage Guidelines

The entries of this table match against the carrier ID. If necessary, a new number analysis table is created. You may not change the configuration of tables in the context of the active policy set.

A number analysis table may not be destroyed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following command enters the mode of configuration of a number analysis table na-table within the context of an SBE policy set.

```
Router# configure terminal
Router# mySbc sbe
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-name-anonymous-table NameTable
Router(config-sbc-sbe-rtgpolicy-natable)#
```

Related Commands

Command	Description
sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
sbe	Enters the mode of an SBE entity within an SBC service.
call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.
match-anonymous	Matches the display name or presentation number to Anonymous in the na-src-name-anonymous-table number analysis table.

na-src-prefix-table

To enter the mode in which to configure a number analysis table, with numbers that match the prefix of the source number within an SBE policy set, use the **na-src-prefix-table** command in SBE call policy set mode. Use the **no** form of this command to destroy the number analysis table.

na-src-prefix-table *table-name*

no na-src-prefix-table *table-name*

Syntax Description

<i>table-name</i>	Name of the number analysis table you are creating or of an existing table you are configuring. The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Except for the underscore character, do not use any special character to specify field names.
-------------------	---

Command Default

No default behavior or values are available.

Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following example illustrates the use of the **na-src-prefix-table** command to create a number analysis table called *MySrcPrefixNaTable*.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-prefix-table MySrcPrefixNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# action accept
Router(config-sbc-sbe-rtgpolicy-natable-entry)# category CAT-1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# match-prefix 159
Router(config-sbc-sbe-rtgpolicy-natable-entry)# exit
Router(config-sbc-sbe-rtgpolicy-natable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
```

Related Commands

Command	Description
sbc	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
sbe	Enters the mode of an SBE entity within an SBC service.
call-policy-set	Enters the mode of a routing policy configuration within an SBE entity.
entry	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.
edit-cic	Manipulates a carrier identification code in number analysis and routing tables.

nat (session border controller)

To configure a SIP adjacency to assume that all endpoints are behind a NAT device, use the **nat** command in the SIP adjacency mode. To deconfigure this feature on the SIP adjacency, use the **no** form of this command.

nat {force-on | force-off}

no nat {force-on | force-off}

Syntax Description	force-on	Sets the SIP adjacency to assume that all endpoints are behind a NAT device.
	force-off	Sets the SIP adjacency to assume that the endpoints are not behind a NAT device.

Command Default	The SBC autodetects whether all the endpoints are behind a NAT device.
-----------------	--

Command Modes	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how the nat force-on command is used to configure the SIP adjacency to assumes that all endpoints are behind a NAT device:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# nat force-on
```

nat force-on

To configure all the endpoints of an access adjacency for the H.248 Border Access Controller (BAC) to be behind a NAT device, use the **nat force-on** command in the H248 BAC access adjacency configuration mode. To configure all the endpoints of an access adjacency for the H.248 BAC not to be behind a NAT device, use the **no** form of this command.

nat force-on

no nat force-on

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	All the endpoints of an H.248 BAC access adjacency are not behind a NAT device.
------------------------	---

Command Modes	H248 BAC access adjacency. (config-h248-bac-adj)
----------------------	--

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 3.7</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

Examples	The following example shows how the nat force-on command is used to configure all the endpoints of an access adjacency for the H.248 BAC to be behind a NAT device:
-----------------	---

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access access1
Router(config-h248-bac-adj)# nat force-on
```

network-id (session border controller)

To configure the network ID, use the **network-id** command in SBE configuration mode. To **deconfigure the network ID**, use the **no** form of this command.

network-id *id*

no network-id

Syntax Description	<i>id</i> Specifies the eight-digit network ID. Range is 0 to 99999.
--------------------	--

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	SBE configuration (config-sbc-sbe)
---------------	------------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to set the network ID to 88888:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# network-id 88888
```

network

To configure either an IPv4 or IPv6 network on a redundant peer, use the **network** command in adjacency Session Initiation Protocol (SIP) peer configuration mode. To deconfigure a network, use the **no** form of this command.

network {IPv4 address netmask | IPv6 address netmask}

no network {IPv4 address netmask | IPv6 address netmask}

Syntax Description

<i>address</i>	The IPv4 or IPv6 IP address.
<i>netmask</i>	The IPv4 or IPv6 netmask.

Command Default

No default behavior or values are available.

Command Modes

Adjacency SIP peer configuration (config-sbc-sbe-adj-sip-peer)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

Examples

The following example shows how the **network** command is used to configure an IPv4 network on a redundant peer on a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# redundant peer 1
Router(config-sbe-adj-sip-peer)# network IPv4 33.33.36.2 255.255.255.0
```

Related Commands

Command	Description
address	Configures either an IP address or a host name to act as a redundant peer.
port	Configures a port for a redundant peer.
priority	Configures a redundant peer's priority.
redundant peer	Configures an alternative signaling peer for an adjacency.

option-editor

To set an adjacency to use a specified editor for the whitelisting or blacklisting options, use the **option-editor** command. To remove the option editor, use the **no** form of this command.

```
option-editor [ua | proxy] [inbound | outbound] [editor-name | default]

no option-editor [ua | proxy] [inbound | outbound] [editor-name | default]
```

Syntax Description

ua	Sets the SIP user agent (UA) option editors.
proxy	Sets the SIP proxy option editors.
inbound	Sets the inbound SIP option editors.
outbound	Sets the outbound SIP option editors.
editor-name	Specifies the name of the editor to use. The editor-name can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
default	Sets the option editor to the default settings.

Command Default

No default behavior or values are available.

Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

UA editors are applied to the Supported and Require headers. Proxy editors are applied to the Proxy-Require headers.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to set the adjacency to use the specified editor for the whitelisting or blacklisting options:

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# option-editor ua inbound OP1
```

Related Commands

Command	Description
sip option-editor	Configures an option editor.

option-profile

To set the adjacency to use the specified profile for white/blacklisting options, use the **option-profile** command. Use the **no** form of the command to select the default global configuration.

option-profile [**ua** | **proxy**] [**inbound** | **outbound**] [*prof-name* | **default**]

no option-profile [**ua** | **proxy**] [**inbound** | **outbound**] [*prof-name* | **default**]

Syntax Description

ua	Sets the SIP ua header profiles.
proxy	Sets the SIP proxy header profiles.
inbound	Sets the inbound SIP header profiles.
outbound	Sets the outbound SIP header profiles.
prof-name	Name of profile to use. The prof-name can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.

Command Default

The global default is used.

Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

User agent (UA) profiles are applied to Supported and Require headers. Proxy profiles are applied to Proxy-Require headers.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following example shows how to set the adjacency to use the specified profile for white/blacklisting options:

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)#

Router(config)# sbc test sbe adjacency sip Adj1
Router(config-sbc-sbe-adj-sip)# option-profile ua inbound OP1
Router(config-sbc-sbe-adj-sip)# exit
```


options

To configure the codec that will support voice inband DTMF, use the **options** command in codec definition mode. Use the **no** form of this command to remove an existing option from this codec.

options {none | transrate | transcode | inband-dtmf}

no options {none | transrate | transcode | inband-dtmf}

Syntax Description

options	Name of option. The values for the options are: - none - transrate - transcode - inband-dtmf
---------	--

Command Default

The global default is used.

Command Modes

Codec definition (config-sbc-sbe-codec-def)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command:

Examples

The following example shows how to add an option to the codec.

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system GSM id 3
Router(config-sbc-sbe-codec-def)# inband-dtmf
```

option (editor)

To add an option to an editor, use the **option** command in the Session Initiation Protocol (SIP) Option Editor configuration mode. To remove an option, use the **no** form of this command.

option *opt-name*

no option *opt-name*

Syntax Description	opt-name Name of the option.				
Command Default	No default behavior or values are available.				
Command Modes	SIP Option Editor configuration (config-sbc-sbe-mep-opt)				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Release 3.3S</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr> </table>	Release	Modification	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				
Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.				
Examples	The following example shows how to add an option to an editor: <pre>Router# configure terminal Router(config)# sbc sanity Router(config-sbc)# sbe Router(config-sbc-sbe)# sip option-editor optedi Router(config-sbc-sbe-mep-opt)# option opt1</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>sip option-editor</td><td>Configures an option editor.</td></tr> </table>	Command	Description	sip option-editor	Configures an option editor.
Command	Description				
sip option-editor	Configures an option editor.				

option (session border controller)

To add an option to a profile, use the **option** command in SIP option mode. Use the **no** form of this command to remove an existing option from this profile.

```
option opt-name

no option opt-name
```

Syntax Description	opt-name Name of profile to use. The <i>opt-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. Note Except for the underscore character, do not use any special character to specify field names.
--------------------	--

Command Default	The global default is used.
-----------------	-----------------------------

Command Modes	SIP option (sip-opt)
---------------	----------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command:
------------------	--

Examples	The following example shows how to add an option to the profile.
----------	--

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-profile optpr1
Router(config-sbc-sbe-sip-opt)# option opt1
```

origin-host

To configure the domain name of an IMS local host, use the **origin-host** command in Diameter configuration mode. To remove the origin host, use the no form of this command.

origin-host *host-name*

no origin-host *host-name*

Syntax Description	<i>host-name</i>	Specifies the name of the local host. The maximum length is 255 characters.
---------------------------	------------------	---

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	Diameter configuration (config-sbc-sbe-diameter)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

The domain name of the local host (origin-host) is reported in the Diameter Origin-host AVP.

Examples	The following example shows how to configure the domain name of an IMS local host.
-----------------	--

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# diameter
Router(config-sbc-sbe-diameter)# origin-host Host1
```

Related Commands	Command	Description
	diameter	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	origin-realm	Configures the domain name of an IMS local realm.
	origin-host	Configures the domain name of an IMS local host.
	peer	Creates an IMS peer and configure the name and IPv4 address of the peer.
	realm (diameter)	Configures a peer and assign the peer to a realm.
	show sbc sbe diameter	Displays the configuration information for the Diameter protocol.

Command	Description
show sbc sbe diameter peers	Displays the configuration information for IMS peers.
show sbc sbe diameter stats	Displays the transport statistics for an IMS peer.
ims rx	Configures an IMS Rx interface for access adjacency
ims pani	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
ims realm	Configures an IMS realm for use by an IMS Rx interface.
ims rx preliminary-aar-forbid	Prevents preliminary AAR messages from being sent in an IMS Rx session.
ims media-service	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

origin-host (Rf interface)

To specify the domain name of an origin host for Rf support on the Session Border Element (SBE) of the Session Border Controller (SBC), use the **origin-host** command in the SBC SBE billing Rf configuration mode. To unconfigure the domain name of an origin host for Rf support on the SBE of the SBC, use the **no** form of this command.

origin-host *host-name*

no origin-host *host-name*

Syntax Description	<i>host-name</i>	Unique name (case sensitive) for an origin host. String length range: 1 to 30.
---------------------------	------------------	--

Command Default	None
------------------------	------

Command Modes	SBC SBE billing Rf configuration (config-sbc-sbe-billing-rf)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples	The following example shows how to specify the domain name of an origin host for Rf support on the SBE of the SBC:
-----------------	--

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# rf 0
Router(config-sbc-sbe-billing-rf)# origin-host mySBC
```

Related Commands	Command	Description
	origin-realm (session border controller)	Specifies the domain name of an origin realm for Rf support on the SBE of the SBC.
	rf	Enables Rf support via billing configuration.

origin-realm

To configure the domain name of an IMS local realm, use the **origin-realm** command in Diameter configuration mode. To remove the origin realm, use the no form of this command.

origin-realm *realm-name*

no origin-realm *realm-name*

Syntax Description	<i>realm-name</i>	Specifies the domain name of the local realm. The maximum length is 63 characters.
--------------------	-------------------	--

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	Diameter configuration (config-sbc-sbe-diameter)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command. Diameter is a realm-based routing protocol, where multiple IMS peers can be configured. The domain name of the local realm (origin-realm) is reported in the Diameter Origin-Realm AVP.
------------------	--

Examples	The following example shows how to configure the domain local name of an IMS realm.
----------	---

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# diameter
Router(config-sbc-sbe-diameter)# origin-realm R1
```

Related Commands	Command	Description
	diameter	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	origin-realm	Configures the domain name of an IMS local realm.
	origin-host	Configures the domain name of an IMS local host.
	peer	Creates an IMS peer and configure the name and IPv4 address of the peer.
	realm (diameter)	Configures a peer and assign the peer to a realm.

Command	Description
show sbc sbe diameter	Displays the configuration information for the Diameter protocol.
show sbc sbe diameter peers	Displays the configuration information for IMS peers.
show sbc sbe diameter stats	Displays the transport statistics for an IMS peer.
ims rx	Configures an IMS Rx interface for access adjacency
ims pani	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
ims realm	Configures an IMS realm for use by an IMS Rx interface.
ims rx preliminary-aar-forbid	Prevents preliminary AAR messages from being sent in an IMS Rx session.
ims media-service	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

origin-realm (Rf interface)

To specify the domain name of an origin realm for Rf support on the Session Border Element of the Cisco Session Border Controller (SBC), use the **origin-realm** command in the SBC SBE billing Rf configuration mode. To unconfigure the domain name of an origin realm for Rf support on the SBE of the SBC, use the **no** form of this command.

```
origin-realm realm-name

no origin-realm realm-name
```

Syntax Description	realm-name	Unique name (case sensitive) of an origin realm. String length range: 1 to 30.
--------------------	------------	--

Command Default	None
-----------------	------

Command Modes	SBC SBE billing Rf configuration (config-sbc-sbe-billing-rf)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to specify the domain name of an origin realm for Rf support on the SBE of the SBC:

Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# rf 0
Router(config-sbc-sbe-billing-rf)# origin-realm mySBC

Related Commands	Command	Description
	origin-host (session border controller)	Specifies the domain name of an origin host for Rf support on the SBE of the SBC.
	rf	Enables Rf support via billing configuration.

outbound-flood-rate

To configure the maximum desired rate of outbound request signals on this adjacency (excluding ACK/PRACK requests) in signals per second, use the **outbound-flood-rate** command in adjacency SIP configuration mode. Use the **no** form of this command to disable flood protection.

outbound-flood-rate *rate*

no **outbound-flood-rate**

Syntax Description

rate	Desired rate of outbound request signals in signals per second.
-------------	---

Command Default

No flood protection.

Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Examples

The following example shows how to configure the maximum desired rate of outbound request signals on this adjacency to 1,000 signals per second:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# outbound-flood-rate 1000
Router(config-sbc-sbe-adj-sip)#
```

overload-time-threshold (session border controller)

To configure the threshold for media gateway (MG) overload control detection, use the **overload-time-threshold** command in SBC-DBE configuration mode. This threshold defines the maximum delay allowed by a SBC that has subscribed to overload control events for the DBE to add a new flow. If the threshold is exceeded, the DBE generates an overload event notification. To reset the threshold value to its default value of 100 milliseconds, use the **no** form of this command.

overload-time-threshold *time*

no overload-time-threshold

Syntax Description	<i>time</i>	The time threshold in milliseconds. The possible values are 0 to 0-2000000000.
--------------------	-------------	--

Command Default	If a time threshold value is not configured, the default value is 100 milliseconds.
-----------------	---

Command Modes	SBC-DBE configuration (config-sbc-dbe)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	If an SBC has subscribed for overload control events, the DBE outputs an overload event notification for every request to add a new flow whose execution takes longer than this threshold.
------------------	--

Examples	The following example configures the threshold for media gateway (MG) overload control detections with a value of 400 milliseconds:
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# overload-time-threshold 400
```

Related Commands	Command	Description
	dbe	Enters into DBE-SBE configuration mode.