100rel inbound

To configure the 100rel interworking parameters for inbound SIP adjacencies on signaling border elements (SBEs), use the **100rel inbound** command in the adjacency SIP configuration mode.

100rel inbound {strip | support}

Syntax Description

inbound	Sets the inbound SIP 100rel parameters.
strip	Strips 100rel from the Supported and Require headers in the incoming INVITE request.
support	Sends reliable provisional responses for all the requests that include a "Supported: 100rel" header, even when the request does not include a "Require: 100rel" header and responses are received as unreliable provisional responses.

Command Default

100rel interworking is disabled.

Command Modes

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

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.

Examples

The following example shows how to enable the 100rel strip option for the incoming INVITE request for inbound SIP adjacency:

```
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 adj1
Router(config-sbc-sbe-adj-sip)# 100rel inbound strip
Router(config-sbc-sbe-adj-sip)#
```

The following example shows how to enable 100rel support option to send reliable provisional responses for all the incoming SIP INVITE requests that contains "Supported:100rel" header:

```
Router(config-sbc-sbe-adj-sip)# 100rel inbound support
Router(config-sbc-sbe-adj-sip)#
```

100rel outbound

To configure the 100rel interworking parameters for outbound SIP adjacencies on signaling border elements (SBEs), use the **100rel outbound** command in the adjacency SIP configuration mode.

100rel outbound {require-add | support-add}

Syntax Description

outbound	Sets the outbound SIP 100rel parameters.
require-add	Adds 100rel Require header in the outgoing INVITE request.
support-add	Adds 100rel Support header in the outgoing INVITE request.

Command Default

100rel interworking is disabled.

Command Modes

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

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.

Examples

The following example shows how to enable 100rel Require header option in the outgoing INVITE request:

```
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 adj1
Router(config-sbc-sbe-adj-sip)# 100rel outbound require-add
Router(config-sbc-sbe-adj-sip)#
```

The following example shows how to enable 100rel Support header option in the outgoing INVITE request:

```
Router(config-sbc-sbe-adj-sip)# 100rel outbound support-add
Router(config-sbc-sbe-adj-sip)#
```

account (session border controller)

To define a SIP or H.323 adjacency account on an SBE, use the **account** command in the appropriate configuration mode. To remove this definition, use the **no** form of this command.

account *account-name*

no account *account-name*

Syntax Description

account-name	Specifies the SBE account name. The *account-name* can have a maximum of 32 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 account name is associated with the adjacency.

Command Modes

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

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 h323ToIsp42 to account isp42:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 SipToIsp42
Router(config-sbc-sbe-adj-h323)# account isp42
```

The following example shows how to configure the SIP adjacency SipToIsp42 to account isp42:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# account isp42
```

action (body)

To set the action to take on a body type in a SIP body profile for a non-SDP message body, use the **action (body)** command in SBE configuration mode. To restore the default behavior of **action nopass**, use the **no action** command.

action [*pass* | *nopass* | *strip* | *reject]*

no action [*pass* | *nopass* | *strip* | *reject]*

Syntax Description

pass	Instructs the SBC to pass through the body type of the non-SDP message body.
nopass	Uses the handling parameter in the message to determine whether to strip the body or reject the entire message with error code 415 (Unsupported media type).
strip	Strips the body and passes the rest of the message.
reject	Rejects the entire message with an error code.

Command Default

The command default is **action nopass**.

Command Modes

SBE SIP Body Element configuration (config-sbc-sbe-sip-body-ele)

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 **action (body)** command is used in conjunction with the **sip body-profile** {*profile_name*} and **body** {*body_name*} commands to complete the configuration.

After creating a body profile with the **sip body-profile** {*profile_name*} command, you can associate the body profile at the following levels and configuration modes:

- At the SIP signaling entity level (ingress or egress), under SBE mode, using the **sip default body-profile** [[**inbound**|**outbound**] {*profile_name*}] command. The body profile is associated for the entire signlaing instance (that is all messages, either ingress or egress, passing through the SBC).
- SIP adjacency level, under SIP adjacency mode, using the **body-profile** [[**inbound**|**outbound**] {*profile_name*}] command. The body profile is associated to an adjacency.
- At SIP method profile level, under method profile mode, using the **body-profile** {*profile_name*} command. The body profile is associated to a method profile.

SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

Examples

The following example creates a body profile named bodyprofile1, associates the body profile at the SIP signaling level for all inbound calls passing through the SBC, describes the body type that is to act on messages with the "application/ISUP" content-type header, and instructs SBC to strip that particular message body and pass the rest of the message.

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-profile bodyprofile1
Router(config-sbc-sbe)# sip default body-profile inbound bodyprofile1
Router(config-sbc-sbe-sip-body)# body application/ISUP
Router(config-sbc-sbe-sip-body-ele)# action strip
Router(config-sbc-sbe-sip-body-ele)#
```

Related Commands

Command	Description
sip default body-profile	Associates a body profile at the SIP signaling level under the SBE mode.
body-profile	Associates a body profile to a method profile under the method profile mode.
body-profile (sip adj)	Associates a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
sip body-profile	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
body	Names a body type or content header type for a non-SDP message body that is part of the body profile.

action (body editor)

To set an action to be taken on a body type in a SIP body editor for a non-SDP message body, use the **action** command in the signaling border element (SBE) SIP body element configuration mode. To remove the action, use the **no** form of this command.

action [*pass* | *nopass* | *strip* | *reject]*

no action

Syntax Description

pass	Instructs the session border controller (SBC) to pass through the body type of the non-SDP message body.
nopass	Uses the handling parameter in the message to determine whether to strip the body or reject the entire message with the error code 415, which is unsupported media type.
strip	Strips the body and passes the rest of the message.
reject	Rejects the entire message.

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

The **action (body)** command is used in conjunction with the **sip body-editor** {*editor-name*} and **body** {*word*} commands to complete the configuration.

The SBC uses a body editor that you have created and associated, to filter the non-SDP bodies from the incoming and outgoing SIP messages, based on the Content Type header field. A body editor allows a message containing a specific non-SDP body to be passed (without altering the message), stripped off the body (and pass the rest of the message), or rejected.

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 instruct the SBC to strip that particular message body and pass the rest of the message:

```
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)# action strip
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.

action (CAC)

To configure the action to perform after this entry in an admission control table, use the **action** command in CAC table entry configuration mode.

action {**cac-complete** | **next-table** *goto-table-name*}

no action {**cac-complete** | **next-table** *goto-table-name*}

Syntax Description

cac-complete	Indicates an event matches, this CAC policy is complete.
next-table	Specifies the name of the next cac table.
goto-table-name	Table name identifying the next CAC table to process (or cac-complete, if processing should stop).

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 configure the next table to process for the 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)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# table-type limit src-account
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
```

Related Commands

Command	Description
action (NA-)	Configures the action to perform after an entry in an admission control table.
action (RTG-SRC)	Configures the action to take if a routing entry is chosen.

action drop-msg

To add an action of dropping the message to a SIP message profile, use the **action drop-msg** command in SIP header-profile configuration mode. To remove the method from the profile, use the **no** form of this command.

action drop-msg

no action drop-msg

Syntax Description

This command has no arguments or keywords.

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 action of dropping the message to a SIP message profile 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)# action drop-msg
```

Related Commands

Command	Description
sip header-profile	Configures a header profile.

action (header-editor)

To configure an action that is to be taken on an element type in a header editor or parameter editor, use the **action** command in the appropriate configuration mode. To remove an action from the element type, use the **no** form of this command.

action {**add-first-header**| **add-header** | **replace-name** | **replace-value**} {**value** *word*}

action {**as-editor** | **drop-msg** | **pass** | **strip**}

action reject [**status-code** *code-number*]

no action

Syntax Description

add-first-header	Adds the first occurrence of a header (no action occurs if a header already exists).
add-header	Adds a header irrespective of whether or not a header already exists.
as-editor	Default editor action (whitelist or blacklist).
drop-msg	Drops the message.
pass	Passes on the header.
reject	Rejects a request if this header is present, specifically for INVITE headers.
replace-name	Replaces the header name.
replace-value	Replaces the header content (value).
strip	Unconditionally strips the matched body, header, or parameter element.
value	Specifies the string used in conjunction with the action.
word	String used in the action. It can be upto 256 characters.
status-code	Specifies the SIP status code for the response.
code-number	SIP status-code number that can range from 300 to 699. By default, it is 488.

Command Default

By default, the *code-number* is 488.

Command Modes

SBE Header Editor Header configuration (config-sbc-sbe-mep-hdr-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.

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, you must remove the existing configuration first.

Examples

The following example shows how to set the as-editor action for the To header element type in the headerprof1 parameter editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor headerprof1
Router(config-sbc-sbe-mep-hdr)# header To
Router(config-sbc-sbe-mep-hdr-ele)# action as-editor
```

Related Commands

Command	Description
header	Configures a header element in a header editor.
parameter-editor	Configures a parameter element in a parameter editor.
sip header-editor	Configures a header editor.

action (method-editor)

To configure an action to be taken on a method editor, use the **action** command in the signaling border element (SBE) method editor element configuration mode. To deconfigure an action, use the **no** form of this command.

action {**as-editor** | **pass** | **reject**}

no action

Syntax Description

as-editor	Passes the method for the whitelist method editor, and rejects for the blacklist method editor.
pass	Passes the method.
reject	Rejects the method.

Command Default

The default is the **as-editor** keyword.

Command Modes

SBE method editor element configuration (config-sbc-sbe-mep-mth-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 the reject action:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-editor editor1
Router(config-sbc-sbe-mep-mth)# description mysbc editor1
Router(config-sbc-sbe-mep-mth)# blacklist
Router(config-sbc-sbe-mep-mth)# method test
Router(config-sbc-sbe-mep-mth-ele)# action reject
Router(config-sbc-sbe-mep-mth-ele)# end
```

Related Commands

Command	Description
header	Configures a header element in a header editor.
parameter-editor	Configures a parameter element in a parameter editor.

action (method profile)

To configure the action to take on a method profile, use the **action** command in the SBE method profile element configuration mode. To remove the action on a method profile, use the **no** form of this command.

action {**as-profile** | **pass** | **reject**}

no action

Syntax Description

as-profile	Drops the method. This is the default
pass	Passes the method.
reject	Rejects the method.

Command Default

The default is as-profile.

Command Modes

SBE method profile element configuration (config-sbc-sbe-sip-mth-ele)

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 the action to drop the method:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile profile1
Router(config-sbc-sbe-sip-mth)# description mysbc profile1
Router(config-sbc-sbe-sip-mth)# blacklist
Router(config-sbc-sbe-sip-mth)# pass-body
Router(config-sbc-sbe-sip-mth)# method test
Router(config-sbc-sbe-sip-mth-ele)# action as-profile
Router(config-sbc-sbe-sip-mth-ele)# end
```

Related Commands

Command	Description
header	Configures a header element in a header profile.
parameter-profile	Configures a parameter element in a parameter profile.

action (NA-)

To configure the action of an entry in the number analysis table with entries of the table matching a source number (prefix or whole number), a dialed number (prefix or whole number) or the source adjacency or account, use the **action (NA-)** command in the Number analysis table configuration mode. To deconfigure the action, use the **no** form of this command.

action {**next-table** *goto-table-name* | **accept** | **reject**}

no action

Syntax Description

next-table *goto-table-name*	Specifies the next number analysis table to process, if the event matches this entry.
accept	Configures the call to be accepted if it matches the entry in the table.
reject	Configures the call to be rejected if it matches the entry in the table.

Command Default

No default behavior or values are available.

Command Modes

Number analysis table configuration (config-sbc-sbe-rtgpolicy-natable-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 2.6	This command was updated to support source number analysis.

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 call to be accepted if it matches the entry in the new number analysis table MyNaTable:

```
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-number-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# action accept
```

The following example shows how to configure the call to be accepted if it matches the start of the entry in the new number analysis table MyNaTable:

```
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)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# action accept
```

The following example shows how to configure the call to be accepted if it matches the source adjacency entry in the new number analysis table MyNaTable:

```
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-adjacency-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# action accept
```

The following example shows how to configure the call to be accepted if it matches the source account entry in the new number analysis table MyNaTable:

```
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
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# action accept
```

Related Commands

Command	Description
action (CAC)	Configures the action to perform after an entry in an admission control table.
action (RTG-SRC)	Configures the action to take if a routing entry is chosen.

action (parameter)

To configure the action to take on an element type in a parameter, use the **action** command in the appropriate configuration mode. To remove an action from the element type, use the **no** form of this command.

action {**add-not-present** | **add-or-replace** | **strip**}

no action {**add-not-present** | **add-or-replace** | **strip**}

Syntax Description

add-not-present	Adds the parameter if it is not present.
add-or-replace	Adds the parameter if it is not present or replace the parameter if it is present.
strip	Strips out the parameter if it is present.

Command Default

The default parameter action is **strip**.

The default header action is **strip**.

Command Modes

SBE header profile header configuration (config-sbc-sbe-sip-hdr-ele)

SBE parameter profile parameter configuration (config-sbc-sbe-sip-prm-ele)

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 set the action for parameter element type user in parameter profile paramprof1 to add-not-present:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-profile paramprof1
Router(config-sbc-sbe-sip-prm)# parameter user
Router(config-sbc-sbe-sip-prm-ele)# action add-not-present value phone
```

The following example shows how to set the action for header element type To in parameter profile headerprof1 to as-profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile headerprof1
Router(config-sbc-sbe-sip-hdr)# header To
Router(config-sbc-sbe-sip-hdr-ele)# action as-profile
```

Related Commands

Command	Description
header	Configures a header element in a header profile.
parameter	Configures a parameter element in a parameter profile.

action (parameter editor)

To configure an action to be taken on an element type in a parameter editor, use the **action** command in the SIP Parameter Editor Element configuration mode. To remove an action from an element type, use the **no** form of this command.

action {**add-not-present** | **add-or-replace**} {**value**} {*word* | **private-ip-address** | **public-ip-address**}

action strip

no action

Syntax Description

add-not-present	Adds the parameter if it is not present.
add-or-replace	Adds the parameter if it is not present, or replaces the parameter if it is present.
value	Specifies the value of the parameter to be added or replaced.
word	Description of the action. Length can be a maximum of 30 characters.
private-ip-address	Specifies the value of the parameter as the private IP address.
public-ip-address	Specifies the value of the parameter as the public IP address.
strip	Strips out the parameter if it is present.

Command Default

By default, **strip** is used.

Command Modes

SIP Parameter Editor Element configuration (config-sbc-sbe-mep-prm-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 set the add-not-present action for the parameter element type user in the paramedit1 parameter editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-editor paramedit1
Router(config-sbc-sbe-mep-prm)# parameter user
Router(config-sbc-sbe-mep-prm-ele)# action add-not-present value phone
```

Related Commands

Command	Description
parameter	Configures a parameter element in a parameter editor.
sip parameter-editor	Configures a parameter editor.

action (RTG-)

To configure the action to take if a routing entry is chosen, use the **action** command in the RTG routing table configuration mode. To delete the action, use the **no** form of this command.

action {**next-table** *goto-table-name* | **complete** | **reject**}

no action

Syntax Description

next-table *goto-table-name*	Specifies the next routing table to process if the event matches the entry.
complete	Completes the action.
reject	Rejects the indicated action.

Command Default

No default behavior or values are available.

Command Modes

RTG routing table configuration (config-sbc-sbe-rtgpolicy-rtgtable-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 configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action reject
```

The following example shows how to configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency 1471
```

```
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action reject
```

The following example shows how to configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-account-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-account 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action reject
```

The following example shows how to configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-round-robin-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
```

The following example configures the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
```

Related Commands

Command	Description
action (NA-)	Configures the action of an entry in the number analysis table with entries of the table matching a dialed number (prefix or whole number) or the source adjacency or account.
action (CAC)	Configures the action to perform after an entry in an admission control table.

action (SDP)

To configure an SDP policy table action, use the **action** command in sdp match table configuration mode. To return to the default, use the **no** form of this command.

action {**whitelist** | **blacklist**}

no action

Syntax Description

whitelist	Allow the defined set of attributes and block the rest.
blacklist	Block the defined set of attributes and allow the rest. This is the default.

Command Default

The default action is blacklist.

Command Modes

SDP match table configuration (config-sbc-sbe-sdp-match-tbl)

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 action of dropping the message to a SIP message profile to the header profile Myprofile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sdp-match-table 1
Router(config-sbc-sbe-sdp-match-tbl)# action blacklist
```

Related Commands

Command	Description
sdp-match-table	Creates an SDP match table.
match-string	Configures an SDP attribute matching string.
sdp-policy-table	**Configures** an SDP policy table.

action (SIP)

To configure the action to take on an element type in a header or parameter profile, use the **action** command in the appropriate configuration mode. To remove an action from the element type, use the **no** form of this command.

action {**add-first-header**| **add-header** | **as-profile** | **drop-msg** | **pass** | **replace-name** | **replace-value** | **strip**}

no action {**add-first-header**| **add-header** | **as-profile** | **drop-msg** | **pass** | **replace-name** | **replace-value** | **strip**}

Syntax Description

add-first-header	Adds the first occurrence of a header (no action if a header exists).
add-header	Adds a header whether on not one already exists.
as-profile	Default profile action (whitelist or blacklist).
drop-msg	Drops the message.
pass	Pass on the header.
replace-name	Replace the header name.
replace-value	Replace the header content (value).
strip	Unconditionally strips the matched body, header, or parameter element.

Command Default

The default body action is **strip**.

The default parameter action is **strip**.

The default header action is **strip**.

Command Modes

SBE header profile header configuration (config-sbc-sbe-sip-hdr-ele)

SBE parameter profile parameter configuration (config-sbc-sbe-sip-prm-ele)

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 set the action for parameter element type user in parameter profile paramprof1 to add-not-present:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-profile paramprof1
Router(config-sbc-sbe-sip-prm)# parameter user
Router(config-sbc-sbe-sip-prm-ele)# action add-not-present value phone
```

The following example shows how to set the action for header element type To in parameter profile headerprof1 to as-profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile headerprof1
Router(config-sbc-sbe-sip-hdr)# header To
Router(config-sbc-sbe-sip-hdr-ele)# action as-profile
```

Related Commands

Command	Description
header	Configures a header element in a header profile.
parameter-profile	Configures a parameter element in a parameter profile.

activate (billing)

To activate billing once it is configured, use the **activate** command in SBE billing configuration mode.

activate

Syntax Description

This command has no arguments or keywords.

Command Default

By default, billing is not activated.

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.

You can activate billing only after the RADIUS configuration has been activated.

Examples

The following example shows how to activate the billing functionality after configuration is committed:

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

Related Commands

Command	Description
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.
method packetcable-em	Enables the packet-cable billing method.

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

activate (enum)

To activate ENUM client, use the **activate** command in ENUM configuration mode. To deactivate ENUM client, use the no form of this command.

activate

no activate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values are available.

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 activate ENUM client:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# activate
```

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.

activate (radius)

To activate the RADIUS client, use the **activate** command in the appropriate configuration mode. To disable this command, use the **no** form of this command.

activate

no activate

Syntax Description

This command has no arguments or keywords.

Command Default

Default is the **no** form of the command.

Command Modes

Server accounting (config-sbc-sbe-acc)

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 activate the RADIUS client**.**

```
Router# configure terminal
Router(config)# sbc uut105-1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting SBC1-account-1
Router(config-sbc-sbe-acc)# activate
```

Related Commands

retry-interval	Sets the retry interval to connect to the RADIUS server.
retry-limit	Sets the retry interval to the RADIUS server.
concurrent-requests	Sets the maximum number of concurrent requests to the RADIUS server.

activate (session border controller)

To start the Session Border Controller (SBC) service when all signaling border element (SBE) or data border element (DBE) address configuration have been successfully committed, use the **activate** command in the appropriate configuration mode. To deactivate the SBE service of the SBC, use the **no** form of this command.

activate

no activate

Syntax Description

This command has no arguments or keywords.

Command Default

Default is the **no** form of the command.

Command Modes

DBE configuration (config-sbc-dbe)

SBE configuration (config-sbc-sbe)

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 2.4	SBE support added for unified SBC.

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 command is not completed even when the CLI returns; there is an asynchronous process (activation or deactivation) going on and the new instruction is not actioned until the last one completes.

Examples

The following example shows how to activate the DBE on the service mySbc:

```
Router# configur
Router(config)# sbc mySbc dbe
Router (config-sbc-dbe)# activate
```

The following example shows how to activate the SBE on the service mySbc:

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

Related Commands

Command	Description
deact-mode	Indicates how to implement the deactivation of an SBE.

cac-policy-set global

To activate the global call admission control (CAC) policy set within an signaling border element (SBE) entity, use the **cac-policy-set global** command in the SBE configuration mode.

cac-policy-set global *policy-set-id*

Syntax Description

policy-set-id	Integer identifying the policy set that should be made global. Range is from 1 to 2147483647.

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.
Cisco IOS XE Release 3.2S	This command was replaced by the **cac-policy-set global** command.

Usage Guidelines

The active CAC policy set cannot be modified.

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 activate policy set 1 on mySbc:

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

Related Commands

Command	Description
cac-policy-set	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
show sbc sbe cac-policy-set	Lists detailed information pertaining to a CAC policy table.

call-policy-set default

To activate a default policy set within a signaling border element (SBE) entity, use the **call-policy-set default** command in the SBE configuration mode. To deactivate a default policy set, use the **no** form of this command.

call-policy-set default *policy-set-id*

no call-policy-set default

Syntax Description

policy-set-id	Number that identifies the default call policy set. The range is from 1 to 2147483647.

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.
Cisco IOS XE Release 3.2S	This command was replaced by the **call-policy-set default** command.

Usage Guidelines

If another policy set was previously active, it is made inactive by executing this command. The SBE is created with no active routing policy set; an active routing policy set must be explicitly configured using 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 example shows how to set policy set 1 as the default on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# call-policy-set default 20
```

Related Commands

Command	Description
call-policy-set	Creates a policy set on the session border controller (SBC).
first-inbound-na-table	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
first-outbound-na-table	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
show sbc sbe call-policy-set	Lists the details of the policy sets configured on the SBC.
show sbc sbe call-policy-set default	Lists the summary of the default policy set configured on the SBC.

active-script-set

To activate a script set, use the **active-script-set** command in the SBE configuration mode. To change the active script set to the inactive state, use the **no** form of this command. Only one script set can be active on the SBC at any given point in time. When you use the **no** form of this command, script-based editing is temporarily disabled.

active-script-set *script-set-number*

no active-script-set

Syntax Description

script-set-number	Script set number. This is the number that you set when you run the **script-set lua** command.

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 Aggregation Services Routers.

Usage Guidelines

At any particular point of time, only one script can be in the active state on the SBC. When you run the **active-script-set** command for a particular script set, the script set that was previously active automatically goes to the inactive state. The editors in an inactive script set are not applied to SIP messages. You can switch an inactive script set to the active state by running the **active script-set** command on it. 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 **active-script-set** command is used to activate the script set with the number 10:

```
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
Router(config-sbc-sbe-scrpset-script)# type wrapped edit-point both
Router(config-sbc-sbe-scrpset-script)# filename bootflash:mySBCScript.lua
Router(config-sbc-sbe-scrpset-script)# exit
Router(config-sbc-sbe-script-set)# complete
```

```
Router(config-sbc-sbe-script-set)# exit
Router(config-sbc-sbe)# active-script-set 10
```

Related Commands

Command	Description
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.
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.
load-order	Specifies the load order of a script in a script set.
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.

address ipv4 (session border controller)

To configure the address of the RADIUS server, use the **address** command in the Server accounting configuration mode. To deconfigure the active accounting server address, use the **no** form of this command.

address ipv4 *A.B.C.D.*

no address ipv4 *A.B.C.D.*

Syntax Description

A.B.C.D.	IP address of the RADIUS server.

Command Default

No default behavior or values are available.

Command Modes

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

Any number of accounting servers can be specified. Call Detail Reports are sent to the accounting server with the highest priority upon call termination.

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 accounting servers castor and pollux on mySbc for Remote Authentication Dial-In User Service (RADIUS) client instance radius1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# radius accounting radius1
(config-sbc-sbe-acc)# server castor
(config-sbc-sbe-acc-ser)# address ipv4 10.0.0.1
(config-sbc-sbe-acc-ser)# exit
(config-sbc-sbe-acc)# server pollux
(config-sbc-sbe-acc-ser)# address pollux
(config-sbc-sbe-acc-ser)# exit
```

address (session border controller)

To configure either an IP address or a host name to act as a redundant peer, use the **address** command in adjacency Session Initiation Protocol (SIP) peer configuration mode. To deconfigure an IP address or a host name, use the **no** form of this command.

address *address*

no address *address*

Syntax Description

address	The IP address or host name of a peer.

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 required to run the command.

Examples

The following example shows how the **address** command is used to configure an IP address or a host name to act as 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)# address sbc1
```

Related Commands

Command	Description
network	Configures either an IPv4 or IPv6 network in a redundant peer.
port	Configures a port for redundant peer.
priority	Configures a redundant peer's priority.
redundant peer	Configures an alternative signaling peer for an adjacency.

adjacency

To configure an adjacency for an Session Border Controller (SBC) service, use the **adjacency** command in SBE configuration mode. To deconfigure the adjacency, use the **no** form of this command.

adjacency {**sip | h323**} *adjacency-name*

no adjacency {**sip | h323**} *adjacency-name*

Syntax Description

sip	Enters the mode of an SBE SIP adjacency, often called adjacency sip mode, to configure a destination SIP adjacency.
h323	Enters the mode of an SBE H.323 adjacency, often called adjacency h323, to configure a destination H.323 adjacency.
adjacency-name	Specifies the name of the SBE SIP or H.323 adjacency. The *adjacency-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 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 below shows the hierarchy of modes required to run the command.

Examples

The following example shows how the **adjacency** command configures a SIP adjacency named sipGW, and enters into adjacency sip mode.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip sipGW
Router(config-sbc-sbe-adj-sip)#
```

The following example shows how the **adjacency** command configures an H.323 adjacency named H323ToIsp42, and enters into adjacency h323 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)#
```

adjacency h248

To configure an H.248 Border Access Controller (BAC) access adjacency and core adjacency, use the **adjacency h248** command in the H248 BAC configuration mode. To unconfigure an H.248 BAC access adjacency and core adjacency, use the **no** form of this command.

adjacency h248 {access *access-adjacency name***}**

adjacency h248 {core *core-adjacency name***}**

no adjacency h248 {access *access-adjacency name***} | {core** *core-adjacency name***}**

Syntax Description

h248	Specifies an adjacency for an H.248 BAC.
access	Specifies an access adjacency.
access-adjacency name	Name of the access adjacency. The *access-adjacency 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.
core	Specifies a core adjacency.
core-adjacency name	Name of the core adjacency. The *core-adjacency 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

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

When you configure an access adjacency, the **adjacency h248** command enters the access adjacency submode.

When you configure a core adjacency, the **adjacency h248** command enters the core adjacency submode.

Examples

The following example shows how the **adjacency h248** command is used to configure an H.248 BAC access adjacency:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
```

The following example shows how the **adjacency h248** command is used to configure an H.248 BAC core adjacency:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 core core_spec2
```

Related Commands

Command	Description
core-adj	Binds an H.248 BAC core djacency with its corresponding H.248 BAC access adjacency.

adjacency timeout

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

adjacency timeout *value*

no adjacency timeout *value*

Syntax Description

value	Specifies the timeout period in milliseconds. Valid values are from 10000 to 30000. The default value is 30 seconds.

Command Default

The default value is 30 seconds.

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 **adjacency timeout** command configures adjacency retry timeout 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)# adjacency timeout 10000
```

The following example shows how the **adjacency timeout** command configures adjacency retry timeout 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)# adjacency timeout 10000
```

admin-domain

To configure an administrative domain, use the **admin-domain** command in the Signaling border element (SBE) configuration mode. To deconfigure an administrative domain, use the **no** form of this command.

admin-domain *name*

no admin-domain *name*

Syntax Description

name	The name of an administrative domain. The *name* field 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 configuration mode (config-sbc-sbe)

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.

The command enables the user to enter into the administrative domain mode. The policy set that is to be used for an administrative domain is defined in the administrative domain mode. A user can specify only one CAC policy set to be used for the administrative domain. A user can also define separate call policy sets for inbound number analysis, routing policy, and outbound number analysis. If the policies are not specified, the default call policy set is used.

The policy sets must be in a complete state before they can be assigned to an administrative domain. A default call policy set must be configured before the administrative domain mode can be entered.

Examples

The following example shows how to configure an administrative domain in the SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set default 25 priority 1
Router(config-sbc-sbe)# admin-domain ADMINDOMAIN
Router(config-sbc-sbe-ad)# description This is the description of the admin-domain 1
```

```
Router(config-sbc-sbe-ad)# call-policy-set inbound-na 2 priority 1
Router(config-sbc-sbe-ad)# call-policy-set outbound-na 3 priority 1
Router(config-sbc-sbe-ad)# call-policy-set rtg 2 priority 1
Router(config-sbc-sbe-ad)# cac-policy-set 2
Router(config-sbc-sbe-ad)# exit
```

Related Commands

Command	Description
cac-policy-set (admin-domain)	Configures the call admission control (CAC) policy set for an administrative domain.
call-policy-set (admin-domain)	Configures the inbound and outbound number analysis and routing policy set for an administrative domain.
show sbc sbe admin-domain	Lists the administrative domains on the Session Border Controller (SBC) and per adjacency.

admin-domain (adjacency)

To associate an administrative domain to an adjacency, use the **admin-domain** command in the Session Initiation Protocol (SIP) adjacency and an H.323 adjacency configuration mode. To remove the association of an administrative domain from an adjacency, use the **no** form of this command.

admin-domain *name*

no admin-domain *name*

Syntax Description

name	Specifies the name of an administrative domain. The *name* field 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

SIP adjacency mode (config-sbc-sbe-adj-sip)

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

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.

In the SIP and H.323 adjacency modes, the user can configure up to two optional administrative domains on an adjacency. A separate **admin-domain** command is configured for every administrative domain. An administrative domain can be configured for both the SIP adjacency and the H323 adjacency. However, the H.323 adjacency must be unattached in order to be able to add, delete, or modify the administrative domain.

Examples

The following example shows how to assign the administrative domain to a 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)# admin-domain ADMINDOMAIN
Router(config-sbc-sbe-adj-sip)#
```

Related Commands

Command	Description
cac-policy-set (admin-domain)	Configures the call admission control (CAC) policy set for an administrative domain.
call-policy-set (admin-domain)	Configures the inbound and outbound number analysis and routing policy set for an administrative domain.
show sbc sbe admin-domain	Lists the administrative domains on the Session Border Controller (SBC) and per adjacency.

alias (session border controller)

To configure the endpoint alias of an H.323 adjacency, use the **alias** command in adjacency H.323 configuration mode. To remove this configuration, use the **no** form of this command.

alias *alias-name*

no alias

Syntax Description

alias-name	Specifies the alias of the H.323 adjacency endpoint. The *alias-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

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 to configure the H.323 adjacency h323ToIsp42 endpoint alias to end1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# alias end1
```

Related Commands

Command	Description
attach-controller	Configures a DBE to attach to a controller.

allow diff-med-sig-vpn

To allow media and signaling to use different VPN IDs in a call leg, use the **allow diff-med-sig-vpn** command in the session border controller (SBC) configuration mode. To allow media and signaling to use the same VPN ID in a call leg, use the **no** form of this command.

allow diff-med-sig-vpn

no allow diff-med-sig-vpn

Syntax Description

This command has no arguments or keywords.

Command Default

No default values are available.

Command Modes

SBC configuration (config-sbc)

Command History

Release	Modification
Cisco IOS XE Release 3.5.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Ensure that the SBC is deactivated before running the **allow diff-med-sig-vpn** command.

If the SBC is active and you run the **allow diff-med-sig-vpn** command, the system issues a warning message, asking you to first deactivate the SBC. You can reactivate the SBC using the **activate** command.

Use the **show run** command to display the output of the **allow diff-med-sig-vpn** command.

Examples

The following example shows how the **allow diff-med-sig-vpn** command allows media and signaling to use different VPN IDs in a call leg:

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# no activate
Router(config-sbc)# allow diff-med-sig-vpn
Router(config-sbc)# activate
Router(config-sbc)# exit
```

allow private info

To configure an H.323 adjacency to allow private information on messages sent out by the adjacency, use the **allow private info** command in the adjacencyH.323 configuration mode. To disallow private information on messages sent out by the adjacency, use the **no** form of this command.

allow private info

no allow private info

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the H.323 adjacency does not send private information.

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.

Please note that if you configure the H.323 adjacency to allow private information, then it will allow private information on messages even if the CAC policy is configured to apply privacy service or the user requests privacy service.

Examples

The following example shows how the **allow private info** command is used to configure an H.323 adjacency to allow private information on messages sent by the adjacency.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323ToIsp422
Router(config-sbc-sbe-adj-h323)# allow private info
```

Related Commands

Command	Description
privacy restrict outbound	Configures an H.323 adjacency to apply privacy restriction on outbound messages if the user requests it.

associate dspfarm profile

To associate the session border controller (SBC) with a digital signal processor (DSP) farm profile, use the **associate dspfarm profile** command in the SBC and SBC-DBE configuration modes. To remove the association with a DSP farm profile, use the **no** form of this command.

associate dspfarm profile {*profile-number* | **all**}

no associate dspfarm profile {*profile-number* | **all**}

Syntax Description

profile-number	The DSP farm profile number the SBC is to associate with.
all	The SBC picks one of the DSP farm profiles associated with the SBC for its transcoding session.

Command Default

No default behavior or values.

Command Modes

SBC and SBC-DBE configuration (config-sbc-dbe)

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 associate the SBC with a DSP farm profile using the **associate dspfarm profile** command in the SBC-DBE mode:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# sbc mySBC dbe
Router(config-sbc-dbe)# associate dspfarm profile 1
```

attach-controllers (session border controller)

To configure a DBE to attach to an H.248 controller, use the **attach-controllers** command in VDBE configuration mode. To detach the DBE from its controller, use the **no** form of this command.

attach-controllers

no attach-controllers

Syntax Description

This command has no arguments or keywords.

Command Default

The default is that no controllers are attached.

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.

Usage Guidelines

The attachment and detachment of the DBE from its controller does not always complete immediately. To view the current attachment status, use the **show sbc dbe controllers** command.

Examples

In a configuration where the DBE has been created and controllers have been configured, the following example shows how to attach the DBE to a controller in VDBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# attach-controllers
```

Related Commands

Command	Description
vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.
show sbc dbe controllers	Lists the media gateway controllers configured on each vDBE and its controller address.

attach (H.248 BAC)

To set the Border Access Controller (BAC) adjacency state to Attached, use the **attach** command in the H248 BAC adjacency configuration mode. To set the BAC adjacency state to Detached, use the **no** form of this command.

attach

no attach

Syntax Description

This command has no arguments or keywords.

Command Default

None

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.

Examples

The following example shows how the **attach** command is used to set the BAC adjacency state:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# attach
```

attach (Rf billing)

To attach an origin realm or an origin host to a Rf billing on an Element (SBE), use the **attach** command in the SBC SBE billing Rf configuration mode. To detach an origin realm or an origin host to a Rf billing on an SBE, use the **no** form of this command.

attach

no attach

Syntax Description

This command has no arguments or keywords.

Defaults

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 attach the an origin realm to an Rf billing on an SBE:

```
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
Router(config-sbc-sbe-billing-rf)# attach
```

attach (session border controller)

To attach an adjacency to an account on an SBE, use the **attach** command in the appropriate configuration mode. To detach the adjacency from an account on an SBE, use the **no** form of this command.

attach

no attach *force [**abort** | **normal**]*

Syntax Description

force	Executes a forced detach.
abort	Tears down calls without signaling an end.
normal	Tears down calls gracefully.

Command Default

Default is the **no** form of the command.

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 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

You can only modify adjacencies when the adjacency is detached. Before modifying an adjacency, you can detach the adjacency first with the **no attach** command. The adjacency stays in the going down state when a call is active or when the ping enable feature is running. During this state, existing calls are not torn down and new calls are not accepted. The adjacency does not go to detached state until all calls have ended. An adjacency cannot be attached until the adjacency is in detached state.

If you wish to override the option to wait till active calls on the adjacency end, the adjacency can be detached immediately using the following commands:

- **no attach force abort**—Executes a forced detach, tearing down calls without signaling their end.
- **no attach force normal**—Executes a forced detach, tearing down calls gracefully.

To check the state of the adjacency, you can use the **show sbc sbe adjacencies** command.

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 attach the H.323 adjacency to 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)# attach
```

audit (H.248 BAC)

To force the Border Access Controller (BAC) to send an audit to an H.248 terminal device, ignoring the audit initiated by the H.248 terminal device, use the **audit force** command in the H248 BAC adjacency configuration mode. To auto audit (default), which means the BAC will not send an audit to an H.248 terminal device if the audit initiated by the H.248 terminal device is received within the audit interval, use the **no** form of this command.

To change the audit interval in the BAC, use the **audit interval** command in the H248 BAC adjacency configuration mode. To return to the default value, use the **no** form of this command.

audit force

audit interval *idle time*

no audit {force | interval *idle time*}

Syntax Description

force	Forces the H.248 BAC to send an audit to the terminal devices. Default is auto audit.
interval	Specifies the audit interval.
idle time	Audit time interval, in seconds. The range is from 0 to 3600. The default value is 60.

Command Default

The default is the **no** form of the command.

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

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 **audit force** command forces the BAC to send an audit to the H.248 terminal devices:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# audit force
```

The following example shows how the **audit interval** command is used to change the audit interval in the BAC:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# audit interval 300
```

authentication mode (session border controller)

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

authentication mode {local | remote}

no authentication mode {local | remote}

Syntax Description

local	Configures the SIP adjacency for local authentication.
remote	Configures the SIP adjacency for remote authentication.

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 **authentication mode** command is used to configure the SIP adjacency for local authentication:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# authentication mode local
```

Related Commands

Command	Description
authentication nonce timeout	Configures the authentication nonce timeout for a SIP adjacency.

authentication (session border controller)

To configure the H.323 adjacency authentication, use the **authentication** command in the adjacency H.323 configuration mode. To deconfigure the H.323 adjacency authentication mode, use the **no** form of this command.

authentication ***auth-type***

no authentication

Syntax Description

auth-type	The authentication type; currently this can only be **endpoint**.

Command Default

Default 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.

Usage Guidelines

This command causes the SBC to authenticate itself with a Gatekeeper. The gatekeeper is responsible for performing the endpoint authentication.

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 sets H.323 adjacency "h323ToIsp42" to use endpoint authentication.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# isp42 adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# authentication endpoint
Router(config-sbc-sbe-adj-h323)# exit
```

bandwidth-fields mandatory

To set the bandwidth description of Session Description Protocol (SDP) as mandatory, use the **bandwidth-fields mandatory** command in Virtual Data Border Element (VDBE) configuration mode. To set the bandwidth description as optional, use the **no** form of this command.

bandwidth-fields mandatory

no bandwidth-fields

Syntax Description

This command has no arguments or keywords.

Command Default

The default behaviour is that the bandwidth description of SDP is optional.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

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 a user group that is 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 that follows shows the hierarchy of the modes and submodes required to run the command.

Examples

The following example shows how to set the bandwidth description of the SDP as mandatory in the VDBE configuration mode:

```
Router# configure terminal
Router# sbc sbc dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# bandwidth-fields mandatory
```

Related Commands

Command	Description
vdbe	Enters VDBE configuration mode.

bandwidth (session border controller)

To configure the maximum and minimum bandwidth limits for media calls, use the **bandwidth** command in codec definition mode mode. To return the bandwidth to the default value, use the no form of this command.

bandwidth *bandwidth-value* [**min** *bandwidth-value*]

no bandwidth *bandwidth-value* [**min** *bandwidth-value*]

Syntax Description

bandwidth	Specifies the maximum bandwidth in bits per second (bps) for media calls. Decimal points are allowed.
min *bandwidth-value*	(Optional) Specifies the minimum bandwidth in bits per second (bps) for media calls. Decimal points are allowed.

Command Default

The default minimum bandwidth is 128 kbps.

Command Modes

Codec definition mode (config-sbc-sbe-codec-def)

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.

This command configures the bandwidth for the analog-to-digital codec (enCOder/DECoder) hardware. The codec name must be one of the system codecs that SBC can recognize. To see a list of the system codecs, use the **show sbc sbc sbe codecs** command.

The minimum bandwidth setting is for use with the **media police degrade** command. It specifies the minimum acceptable bandwidth for the video codec. If the available bandwidth is smaller than the configured **min** *bandwidth-value*, the call is rejected under the degrade policy. The minimum bandwidth setting applies only to the unidirectional bandwidth of the media stream, and does not include the packet overhead.

The **bandwidth min** command specifies the unidirectional, minimum bandwidth limit bandwidth and does not include packet overhead.

Examples

The following example shows how to configure the maximum bandwidth limit to 400,000 bps for media calls:

```
Router# configure terminal
Router(config)# sbc mySBC
```

```
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system H263 id 34
Router(config-sbc-sbe-codec-def)# bandwidth 400000
```

The following example shows how to configure the minimum bandwidth limit to 328,000 bps, specifically for video type media calls:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router (config-sbc-sbe)# codec custom h263-c id 96
Router (config-sbc-sbe-codec-def)# type variable
Router (config-sbc-sbe-codec-def)# media video
Router (config-sbc-sbe-codec-def)# bandwidth min 328000
```

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.

batch-size

To configure the batching or grouping of RADIUS messages sent to a RADIUS server, use the **batch** command in the packetcable-em configuration mode. To disable the batch, use the **no** form of this command.

batch-size *number*

no batch-size

Syntax Description

number	Specifies the batch size in bytes. The range is 0 through 4096.

Command Default

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.

A value of 0 indicates no batching. A platform may choose to set a non-zero default value (this may increase performance.)

Examples

The following example shows how to configure the maximum size of a batch of CDRs:

```
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)# batch-size 256
```

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.

batch-time

To configure the maximum number of milliseconds for which any record is held before the batch is sent, use the **batch-time** command in the packetcable-em configuration mode. To disable the waiting period, use the **no** form of this command.

batch-time *number*

no batch-time

Syntax Description

number	Specifies the batch time in milliseconds. The range is 1 through 3600000.

Command Default

1000 milliseconds

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.

Examples

The following example shows how to configure the maximum number of milliseconds for which any record is held before the batch is sent:

```
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)# batch-size 256
(config-sbc-sbe-billing-packetcable-em)# batch-time 22
```

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.

bgp additional-paths select

To have the system calculate a second BGP bestpath, use the **bgp additional-paths select** command in address family configuration mode. To remove this mechanism for calculating a second bestpath, use the **no** form of the command.

bgp additional-paths select {**best-external** [**backup**] | **backup**}

no bgp additional-paths select

Syntax Description

best-external	(Optional) Calculates a second bestpath from among those received from external neighbors. Configure this keyword on a PE or RR. This keyword enables the BGP Best External feature on an RR.
backup	(Optional) Calculates a second bestpath as a backup path.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The BGP Diverse Path feature can be enabled on a route reflector to calculate a bestpath and an additional path per address family.

Computation of a diverse path per address family is triggered by any of the following commands:

- **bgp additional-paths install**
- **bgp additional-paths select**
- **maximum-paths ebgp**
- **maximum-paths ibgp**

The **bgp additional-paths install** command will install the type of path that is specified in the **bgp additional-paths select** command Either the **best-external** keyword or the **backup** keyword is required; both keywords can be specified. If both keywords (**best-external** and **backup**) are specified, the system will install a backup path.

Examples

In the following example, the system computes a second best path from among those received from external neighbors:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
```

```
neighbor 10.1.1.1 activate
maximum-paths ibgp 4
bgp bestpath igp-metric ignore
bgp additional-paths select best-external
bgp additional-paths install
neighbor 10.1.1.1 advertise diverse-path backup
```

Related Commands

Command	Description
bgp additional-paths install	Enables BGP to calculate a backup path for a given address and to install it into the RIB and CEF.
bgp bestpath igp-metric ignore	Specifies that the system ignore the IGP metric during best path selection.
maximum-paths ebgp	Configures multipath load sharing for eBGP and iBGP routes.
maximum-paths ibgp	Controls the maximum number of parallel iBGP routes that can be installed in a routing table.

bgp bestpath igp-metric ignore

To have the system ignore the Interior Gateway Protocol (IGP) metric during BGP best path selection, use the **bgp bestpath igp-metric ignore** command in address family configuration mode. To remove the instruction to ignore the IGP metric, use the **no** form of this command.

bgp bestpath igp-metric ignore

no bgp bestpath igp-metric ignore

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The IGP metric is a configurable metric for EIGRP, IS-IS, or OSPF that is related to distance. The **bgp bestpath igp-metric ignore** command can be used independently, or in conjunction with the BGP Diverse Path feature. This command does not enable the BGP Diverse Path feature.

Similarly, enabling the BGP Diverse Path feature does not necessarily require that the IGP metric be ignored. If you enable the BGP Diverse Path feature and the RR and its shadow RR are not co-located, this command must be configured on the RR, shadow RR, and PE routers.

This command is supported in the following address families:

- ipv4 unicast
- vpnv4 unicast
- ipv6 unicast
- vpnv6 unicast
- ipv4+label
- ipv6+label

Note This command is not supported per VRF; if you use it per VRF, it is at your own risk.

This command applies per VRF as follows (which is consistent with the BGP PIC/Best External feature):

- When configured under address-family vpnv4 or vpnv6, it applies to all VRFs, but it will be nvgened only under vpnv4/vpnv6 global.

- When configured under a particular VRF, it applies only to that VRF and will be nvgened only for that VRF.
- When configured under vpnv4 or vpnv6 global, this command can be disabled for a particular VRF by specifying **no bgp bestpath igp-metric ignore**. The **no** form will be nvgened under that VRF, while under vpnv4 or vpnv6 **bgp bestpath igp-metric ignore** is nvgened and the command applies to all other VRFs.

Examples

In the following example, the IGP metric is ignored during calculation of the BGP best path:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select backup
 bgp additional-paths install
 neighbor 10.1.1.1 advertise diverse-path backup
```

Related Commands

Command	Description
bgp additional-paths select	Specifies that the system compute a second BGP bestpath.

bgp consistency-checker

To enable the BGP Consistency Checker feature, use the **bgp consistency-checker** command in router configuration mode. To disable the BGP Consistency Checker feature, use the **no** form of this command.

bgp consistency-checker {**error-message** | **auto-repair**} [**interval** *minutes*]

no bgp consistency-checker

Syntax Description

error-message	Specifies that when an inconsistency is found, the system will only generate a syslog message.
auto-repair	Specifies that when an inconsistency is found, the system will generate a syslog message and take action based on the type of inconsistency found.
interval *minutes*	(Optional) Specifies the interval at which the BGP consistency checker process occurs. • The range is 5 to 1440 minutes. The default is 1440 minutes (one day).

Command Default

No BGP consistency check is performed.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

A BGP route inconsistency with a peer occurs when an update or a withdraw is not sent to a peer, and black-hole routing can result. The BGP consistency checker feature is a low-priority process created to address this issue. This feature performs nexthop-label, RIB-out, and aggregation consistency checks. When BGP consistency checker is enabled, it is performed for all address families. Once the process identifies such an inconsistency:

- If the **error-message** keyword is specified, the system will report the inconsistency with a syslog message, and will also perform forceful aggregation reevaluation in the case of an aggregation inconsistency.
- If the **auto-repair** keyword is specified, the system will report the inconsistency with a syslog message and also take appropriate action, such as a route refresh request or an aggregation reevaluation, depending on the type of inconsistency.

Examples

In the following example, BGP consistency checker is enabled. If a BGP route inconsistency is found, the system will send a syslog message and take appropriate action.

```
Router(config)# router bgp 65000
Router(config-router)# bgp consistency-checker auto-repair
```

Related Commands

Command	Description
show ip bgp vpnv4 all inconsistency nexthop-label	Displays routes that have nexthop-label inconsistency found by BGP consistency checker.

bgp refresh max-eor-time

To cause the router to generate a Route-Refresh End-of-RIB (EOR) message if it was not able to generate one due to route flapping, use the **bgp refresh max-eor-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

bgp refresh max-eor-time *seconds*

no bgp refresh max-eor-time

Syntax Description

seconds	Number of seconds after which, if the router was unable to generate a Route-Refresh EOR message due to route flapping, the router generates a Route-Refresh EOR message. • Valid values are from 600 to 3600, or 0. • The default is 0, meaning the command is disabled.

Command Default

0 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The BGP Enhanced Route Refresh feature is enabled by default. The **bgp refresh max-eor-time** command is not needed under normal circumstances. You might configure the **bgp refresh max-eor-time** command in the event of continuous route flapping, when the router is unable to generate a Route-Refresh EOR message, in which case a Route-Refresh EOR is generated after the timer expires.

Examples

In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.

```
router bgp 65000
 bgp refresh stalepath-time 800
 bgp refresh max-eor-time 800
```

Related Commands

Command	Description
bgp refresh stalepath-time	Causes the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message.

bgp refresh stalepath-time

To cause the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message, use the **bgp refresh stalepath-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

bgp refresh stalepath-time *seconds*

no bgp refresh stalepath-time

Syntax Description

seconds	Number of seconds the router waits to receive a Route-Refresh End-of-RIB (EOR) message, and then removes the stale paths from BGP table if the router hasn't received an EOR message. • Valid values are 600 to 3600, or 0. • The default is 0, meaning the command is disabled.

Command Default

0 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The BGP Enhanced Route Refresh feature is enabled by default. The **bgp refresh stalepath-time** command is not needed under normal circumstances. You might configure the **bgp refresh stalepath-time** command in the event of continuous route flapping, when the router does not receive a Route-Refresh EOR after an Adj-RIB-Out, in which case the router removes the stale routes from the BGP table after the timer expires. The stale path timer is started when the router receives a Route-Refresh SOR.

Examples

In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.

```
router bgp 65000
 bgp refresh stalepath-time 800
 bgp refresh max-eor-time 800
```

Related Commands

Command	Description
bgp refresh max-eor-time	Causes the router to generate a Route-Refresh EOR message if it was not able to generate one due to route churn.

billing

To configure billing, use the **billing** command in SBE configuration mode. Use the **no** form of this command to remove all the billing configuration.

billing

no billing

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 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.

There is only one billing per SBC.

Examples

The following example shows how to enter the billing mode for mySbc:

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

Related Commands

Command	Description
activate (radius)	Activates the billing functionality after configuration is committed.
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.
method packetcable-em	Enables the packet-cable billing method.

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

billing (CAC)

To configure billing, use the **billing** command in the CAC table entry configuration mode. To unconfigure the billing configuration, use the **no** form of this command.

billing {**filter** {**disable** | **enable**} | **methods** {**packetcable-em** | **xml**}}

no billing {**filter** | **methods** {**packetcable-em** | **xml**}}

Syntax Description

filter	Specifies whether the billing filter scheme is enabled or disabled.
disable	Disables the billing filter.
enable	Enables the billing filter.
methods	Specifies the billing methods that are allowed for calls relating to different adjacencies.
packetcable-em	Configures the PacketCable billing method for billing.
xml	Configures the XML billing method for billing.

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 3.3S	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.

There is only one billing per SBC.

Examples

The following example shows how to enter the billing mode for mySbc:

```
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 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)# billing filter enable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# billing methods xml
```

Related Commands

Command	Description
cac-policy-set	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
cac-table	Configures admission control tables.
table-type	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

blacklist

To enter the mode for configuring the event limits of a given source, use the **blacklist** command in the SBE configuration mode. To return the event limits to the default values, use the **no** form of this command.

[**no**] **blacklist** [**critical**] **global** [address-default | {**ipv4** {*addr*} | **ipv6** {*addr*}} [**tcp** {*tcp-port*} | **udp** {*udp-port*} | default-port-limit]]

[**no**] **blacklist** [**critical**] **vpn** {*vpn-name*} [**address-default** [**address-family** {**ipv4** | **ipv6**}] | **address-family** {**ipv4** | **ipv6**} | **ipv4** *addr* [**tcp** {*tcp-port*} | **udp** {*udp-port*} | **default-port-limit**] | **ipv6** *addr* [**tcp** {*tcp-port*} | **udp** {*udp-port*} | **default-port-limit**]]

Syntax Description

global	(Required) Allows blacklisting limits or critical blacklisting limits to be configured for the global VPN. Sets limits for total traffic from global VPN. This keyword is required when the command is used on the global VPN. Either global or vpn name must be specified for the blacklist.
critical	Configures critical blacklisting limits for the global VPN or a specific VPN.
vpn {*vpn_name*}	(Required) Enters the mode for configuring the event limits or critical event limits for the given VPN. Sets limits for total traffic from the named VPN. *vpn_name* is the VPN name. Either global or vpn name must be specified for the blacklist.
address-default	(Optional) Enters the mode for configuring the default event limits for the source addresses in the given VPN. Sets default traffic limits to apply to each IP address within the global VPN, except where overridden by the **ipv4 or ipv6** command option.
address-family	(Optional) Enters the mode for configuring the default event limits for the IPv4 or IPv6 address family in the given VPN.
ipv4 *addr*	(Optional) Enters the mode for configuring the default event limits for the IPv4 address in the given VPN. Sets traffic limits for total traffic from this IP address within the global VPN. *addr* is the IPv4 address.
ipv6 *addr*	(Optional) Enters the mode for configuring the default event limits for the IPv6 address in the given VPN. Sets traffic limits for total traffic from this IP address within the global VPN. *addr* is the IPv6 address.
tcp *tcp-port*	(Optional) Sets traffic limit for traffic from this IP address and TCP port within the global VPN.
udp *udp-port*	(Optional) Sets traffic limit for traffic from this IP address and UDP port within the global VPN.
default-port-limit	(Optional) Sets traffic limits to apply to each port within the IP address in the global VPN, except where overridden by either the **tcp** or **udp** command option.

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.
Cisco IOS XE Release 2.4.2	The **critical** keyword and options were added.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added.
Cisco IOS XE Release 3.1S	The **ipv6** keyword was added under **address-family**. The **ipv6** *addr* and options were also added.

Usage Guidelines For IPv4, either “global” or “vpn_name” must be specified for the blacklist. However, if a vpn_name is entered, a VPN token is required.

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 **vpn** keyword and the VPN token of 800 are used to enter the mode for configuring the event limits for the VPN test:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist vpn 800
Router(config-sbc-sbe-blacklist)#
```

The following example shows how to enter the mode for configuring the default event limits for all addresses:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global address-default
```

The following example shows how to enter the mode for configuring blacklisting to apply to all addresses:

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

The following example shows how to enter the mode for applying blacklisting options to a single IPv4 IP address:

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

The following example shows how to enter the mode for applying blacklisting options to a single IPv6 IP address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global ipv6 2001::10:0:0:1
Router(config-sbc-sbe-blacklist)#
```

The following example shows how to enter the mode for applying blacklisting options to an IPv6 address family in a VPN:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist vpn Mgmt-intf address-family ipv6
Router(config-sbc-sbe-blacklist)#
```

Related Commands

Command	Description
address-default	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
clear sbc sbe blacklist	Clears the blacklist for the specified SBC service.
global	Enters the mode for configuring blacklisting to apply to all addresses.
ipv4 (blacklist)	Enters the mode for applying blacklisting options to a single IPv4 IP address.
ipv6 (blacklist)	Enters the mode for applying blacklisting options to a single IPv6 IP address.
vpn	Enter the mode for configuring the event limits for a given VPN.
reason	Enters a mode for configuring a limit to a specific event type on the source.
show sbc sbe blacklist configured-limits	Lists the explicitly configured limits, showing only the sources configured.
show sbc sbe blacklist current-blacklisting	Lists the limits causing sources to be blacklisted.
tcp	Enters the mode for configuring blacklisting for TCP protocol only.
timeout	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
trigger-period	Defines the period over which events are considered.
default-port-limit	Enters a mode for configuring the default even limits for the ports of a given address.
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.
udp	Enters the mode for configuring blacklisting for UDP protocol only.
vpn	Enters the mode for configuring the event limits for a given VPN.

blacklist (profile)

To set a profile to be blacklisted, use the **blacklist** command in the appropriate profile configuration mode. To remove blacklist from this profile, use the **no** form of this command.

blacklist

no blacklist

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values are available.

Command Modes

SIP Method Profile configuration (config-sbc-sbe-mep-mth)

SIP Option Profile configuration (config-sbc-sbe-mep-opt)

SIP Header Profile 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 to blacklist an option profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-profile option1
Router(config-sbc-sbe-mep-opt)# blacklist
```

The following example shows how to blacklist a method profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile Method1
Router(config-sbc-sbe-mep-mth)# blacklist
```

The following example shows how to blacklist a header profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile header1
Router(config-sbc-sbe-mep-hdr)# blacklist
```

Related Commands

Command	Description
sip header-profile	Configures a header profile.
sip method-profile	Configures a method profile.
sip option-profile	Configures an option profile.

blacklist (sip-opt)

To set profile to be blacklisted, use the **blacklist** command in SIP option mode. Use the **no** form of this command to remove blacklist from this profile.

blacklist

no blacklist

Syntax Description

This command has no arguments or keywords.

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)# blacklist
```

blended-codec-list

To add a blended codec list, use the **blended-codec-list** command in SBC SBE CAC policy CAC table entry configuration mode. To remove a blended codec list, use the **no** form of this command.

blended-codec-list *blended-codec-li*st

no blended-codec-list *blended-codec-li*st

Syntax Description

blended-codec-list	Case-sensitive, unique name for a blended codec list. The maximum length is 63 characters.

Defaults

No blended codec list exists.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to configure a blended codec list:

```
Router> enable
Router# configure terminal
Router(config)# sbc 123
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table test
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table test
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# blended-codec-list codec-a
```

Related Commands

Command	Description
blended-transcode	Enables the Blended Transcoding feature.

blended-transcode

To enable the Blended Transcoding feature, use the **blended-transcode** command in the SBC SBE CAC policy CAC table entry configuration mode. To disable the Blended Transcode feature, use the **no** form of this command.

blended-transcode

no blended-transcode

Syntax Description

This command has no arguments or keywords.

Defaults

The Blended Transcode feature is disabled.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to enable the Blended Transcode feature:

```
Router> enable
Router# configure terminal
Router(config)# sbc 123
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table test
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table test
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# blended-transcode
```

Related Commands

Command	Description
blended-codec-list	Configures a blended codec list.

body-editor

To associate a body editor to a SIP adjacency to cause the body editor to act on the incoming and outgoing SIP messages, use the **body-editor** command in the Adjacency SIP configuration mode. To remove a body editor, use the **no** form of this command.

body-editor ***[inbound | outbound]*** *{editor-name}*

no body-editor ***[inbound | outbound]*** *{editor-name}*

Syntax Description

inbound	Associates a body editor to act on the inbound messages on a SIP adjacency. **Note** When the message is passed, the body editor should be applied in the inbound and outbound directions on the respective adjacencies on which the message is routed.
outbound	Associates a body editor to act on the outbound messages on a SIP adjacency. **Note** When the message is passed, the body editor should be applied in the inbound and outbound directions on the respective adjacencies on which the message is routed.
editor-name	Text string that describes a body editor name. 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.

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 to associate two body editors, inbound editor2 and outbound editor1, at a SIP adjacency level for the adj-1 adjacency:

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

```
Router(config-sbc-sbe)# adjacency sip adj-1
Router(config-sbc-sbe-adj-sip)# body-editor inbound editor2
Router(config-sbc-sbe-adj-sip)# body-editor outbound editor1
```

Related Commands

Command	Description
action	Sets the action to be taken on a body type in a SIP body editor for a non-SDP message body.
sip body-editor	Configures a body editor.

body-editor (method)

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

body-editor *editor-name*

no body-editor

Syntax Description

editor-name	Specifies the name of the body editor. The following guidelines apply: 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.

Command Default

No default behavior or values are available.

Command Modes

SBE SIP method element configuration (config-sbc-sbe-mep-mth-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 the **body-editor** command adds a body editor to act on a method:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
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)# body-editor bodyEditor1
```

Related Commands

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

body-profile

To associate a body profile to a method profile to cause the body profile to act on incoming and outgoing SIP messages, use the **body-profile** command in SBE method profile element configuration mode. To remove the body profile, use the **no body-profile** command.

body-profile *{profile_name}*

no body-profile *{profile_name}*

Syntax Description

profile_name	Text string that describes a body profile name. The following guidelines apply: The *profile_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 method profile element configuration mode (config-sbc-sbe-sip-mth-ele)

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

After creating a body profile with the **sip body-profile** {*profile_name*} command, you can associate the body profile at the following additional levels and configuration modes:

- At the SIP signaling entity level (ingress or egress), under SBE mode, using the **sip default body-profile** [[**inbound**|**outbound**] {*profle_name*}] command. The body profile is associated for the entire signlaing instance (that is all messages, either ingress or egress, passing through the SBC).
- SIP adjacency level, under SIP adjacency mode, using the **body-profile** [[**inbound**|**outbound**] {*profle_name*}] command. The body profile is associated to an adjacency.

SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

Examples

The following example describes how to associate body profile, bodyprofile1, to a method profile:

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

```
Router(config-sbc-sbe)# sip method-profile profile1
Router(config-sbc-sbe-sip-mth)# description mysbc profile1
Router(config-sbc-sbe-sip-mth)# method test
Router(config-sbc-sbe-sip-mth-ele)# body-profile bodyprofile1
Router(config-sbc-sbe-sip-mth-ele)#
```

Related Commands

Command	Description
sip default body-profile	Associates a body profile at the SIP signaling level under the SBE mode.
body-profile (sip adj)	Associates a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
sip body-profile	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
body	Names the body type or content header type for a non-SDP message body that is part of the body profile.
action	Sets the action to be taken on a body type in a SIP body profile for a non-SDP message body
sip method-profile	Configures a method profile in the mode of an SBE entity

body-profile (sip adj)

To associate a body profile to a SIP adjacency to cause the body profile to act on incoming and outgoing SIP messages, use the **body-profile (sip adj)** command in adjacency SIP configuration mode. To remove the body profile, use the **no body-profile (sip adj)** command.

body-profile ***[inbound | outbound]*** *{profile_name}*

no body-profile ***[inbound | outbound]*** *{profile_name}*

Syntax Description

inbound	Associates the body profile to act on inbound messages on the SIP adjacency. **Note** When the message is 'passed,' the body profile should be applied both in the inbound and outbound direction on the respective adjacencies on which the message is routed.
outbound	Associates the body profile to act on outbound messages on the SIP adjacency. **Note** When the message is 'passed,' the body profile should be applied both in the inbound and outbound direction on the respective adjacencies on which the message is routed.
profile_name	The *profile_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

Adjacency SIP configuration (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

After creating a body profile with the **sip body-profile** {*profile_name*} command, you can associate the body profile at the following additional levels and configuration modes:

- At the SIP signaling entity level (ingress or egress), under SBE mode, using the **sip default body-profile** [[**inbound**|**outbound**] {*profile_name*}] command. The body profile is associated for the entire signlaing instance (that is all messages, either ingress or egress, passing through the SBC).
- At SIP method profile level, under method profile mode, using the **body-profile** {*profile_name*} command. The body profile is associated to a method profile.

SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

Examples

The following example describes how to associate two body profiles, inbound profile2 and outbound profile1, at the SIP adjacency level for adjacency adj-1:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj-1
Router((config-sbc-sbe-adj-sip))# body-profile inbound profile2
Router((config-sbc-sbe-adj-sip))# body-profile outbound profile1
```

Related Commands

Command	Description
sip default body-profile	Associates a body profile at the SIP signaling level under the SBE mode.
body-profile	Associates a body profile to a method profile under the method profile mode.
sip body-profile	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
body	Names the body type or content header type for a non-SDP message body that is part of the body profile.
action	Sets the action to be taken on a body type in a SIP body profile for a non-SDP message body

body

To name the body type or content header type for a non-SDP message body that is part of the body profile, use the **body** command in SBE SIP Body configuration mode. To remove the body type or content header type, use the **no body** command.

body {*WORD*}

no body {*WORD*}

Syntax Description

WORD	Specifies the body type or content header type. This is a string of maximum 64 characters. The body name must be in the form of <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive. For more information, see Usage Guidelines.

Command Default

No default behavior or values are available.

Command Modes

SBE SIP Body configuration (config-sbc-sbe-sip-body)

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

This command describes the body type or content header type for SBC to act on messages with the specified body type or content header type.

The **body** command is used in conjunction with the **sip body-profile** command that is used to create the body profile.

The body name must be in the form of <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive.

Asterisk (*) is used to match *all* non-SDP body types. Note that * is also interpreted as a string by the CLI, and is just a token used to indicate wild-card match.

The following Content-Type descriptions are not allowed: application/sdp and multipart/mixed

Only one body element with such a wildcard can co-exist with other bodies per body profile. The wildcard body is applied if there is no other matching body in that profile. The body name is matched using regular ‘string compare.’ Note that there is no provision to match body names using any regular expression matching techniques.

Examples

The following example does the following: creates a body profile named bodyprofile1; describes the body type, that is to act on messages with Content-Type header “application/ISUP”; and instructs SBC to strip that particular message body and pass the rest of the message:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-profile bodyprofile1
Router(config-sbc-sbe-sip-body)# body application/ISUP
Router(config-sbc-sbe-sip-body-ele)# action strip
Router(config-sbc-sbe-sip-body-ele)#
```

Related Commands

Command	Description
sip default body-profile	Associates a body profile at the SIP signaling level under the SBE mode.
body-profile	Associates a body profile to a method profile under the method profile mode.
body-profile (sip adj)	Associates a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
sip body-profile	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
action	Sets the action to be taken on a body type in a SIP body profile for a non-SDP message body.

body (editor)

To name a body type or content header type for a non-SDP message body that is a part of the body editor, use the **body** command in the signaling border element (SBE) session initiation protocol (SIP) body configuration mode. To remove a body type or content header type, use the **no** form of this command.

body *word*

no body *word*

Syntax Description

word	The *word* field can have a maximum of 64 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. The body name must be in the form <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive.

Command Default

No default behavior or values are available.

Command Modes

SIP Body Editor configuration (config-sbc-sbe-mep-bdy)

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

This command describes the body type or content header type for the SBC to act on messages of the specified body type or content header type.

The **body** command is used in conjunction with the **sip body-editor** command that is used to create the body editor.

The body name must be in the form <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive.

Asterisk (*) is used to match *all* the non-SDP body types. Note that * is also interpreted as a string by the CLI, and is a token used to indicate wildcard match.

Examples

The following example shows how to create a body editor named bodyeditor1 and describe the body type as application/ISUP:

```
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
```

Related Commands

Command	Description
sip body-editor	Creates a body editor to filter the non-SDP message bodies from the incoming and outgoing SIP messages.

branch bandwidth-field

To configure the SBC such that it converts a specific bandwidth line format into another bandwidth line format in the outbound Session Description Protocol (SDP) sent to a caller or a callee, use the **branch bandwidth-field** command in the CAC table entry configuration mode. To unconfigure the conversion of the bandwidth line format, use the **no** form of this command.

branch bandwidth-field {as-to-tias | tias-to-as}

no branch bandwidth-field {as-to-tias | tias-to-as}

Syntax Description

as-to-tias	Configures the SBC to convert the b=AS line format into the b=TIAS line format for a specific SDP media descriptor in an outbound offer. Here, AS refers to Application Specific maximum. Similarly, TIAS refers to Transport Independent Application Specific maximum.
tias-to-as	Configures the SBC to convert the b=TIAS line format into the b=AS line format for a given SDP media descriptor in an outbound offer.

Command Default

The default is that the format of bandwidth lines is not converted.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The SBC applies the outgoing bandwidth line format that you configure. If the offerer-side adjacency is configured to apply a specific style of bandwidth line format in the SDP, this command causes the SBC to convert the answer to the specified format before it is sent back to the offerer. If there are multiple bandwidth lines, only the first line is converted into the specified bandwidth line and the remaining lines are ignored.

Note As mentioned earlier, the default is that the bandwidth line is not converted from one format to another. However, if the callee is configured to convert the bandwidth, and the message is converted, the response that is sent back to the caller is converted back even if this command is not configured for the caller.

Examples

The following example shows how to configure the SBC such that it converts an AS bandwidth line format into a TIAS bandwidth line format in the outbound SDP sent to a caller or a callee:

```
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)# cac-policy-set 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)# branch bandwidth-field as-to-tias
```

Related Commands

Command	Description
callee-bandwidth-field	Configures the SBC such that it converts a specific bandwidth line format into another bandwidth line format in an outbound SDP sent to a callee.
caller-bandwidth-field	Configures the SBC such that it converts a specific bandwidth line format into another bandwidth line format in an outbound SDP sent to a caller.

branch codec

To configure the codec options for a caller or a callee, use the **branch codec** command in the CAC table entry configuration mode. To unconfigure the codec options, use the **no** form of this command.

branch codec {convert | profile *profile-name*}

no caller codec {convert | profile}

Syntax Description

convert	Enables the codec variant conversion.
profile *profile-name*	Specifies the codec variant profile name. The *profile-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

By default, codec variant conversion is disabled, and no codec variant profile is specified.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 codec options for a caller using the **branch codec** command:

```
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)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch codec convert
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch codec profile profile-1
```

Related Commands

Command	Description
callee codec	Configures the codec options for a callee.
caller codec	Configures the codec options for a caller.

branch codec-list

To specify the codecs that the caller or the callee of a call can use, use the **branch codec-list** command in the CAC table entry configuration mode. To delete a codec list, use the **no** form of this command.

branch codec-list *list-name*

no branch codec-list *list-name*

Syntax Description

list-name	Name of the codec list. The *list-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

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 a mode to create the test codec list:

```
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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch codec-list test
```

Related Commands

Command	Description
callee-codec-list	Specifies the codecs that the callee of a call can use.
caller-codec-list	Specifies the codecs that the caller of a call can use.

branch hold-setting

To specify the caller hold settings or the callee hold settings, use the **branch hold-setting** command in the CAC table entry configuration mode. To remove the caller hold settings or the callee hold settings, use the **no** form of this command.

branch hold-setting {**hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard**}

no branch hold-setting {**hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard**}

Syntax Description

hold-c0	Branch supports and requires c=0.0.0.0.
hold-c0-inactive	Branch supports and requires c=0.0.0.0 and a=inactive.
hold-c0-sendonly	Branch supports and requires c=0.0.0.0 and a=sendonly.
hold-sendonly	Branch supports and requires a=sendonly.
standard	Branch supports and requires c=0.0.0.0 and an a= line.

Command Default

The default setting is **standard**.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 **branch hold-setting** command:

```
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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value fairchild
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch hold-setting hold-sendonly
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

Related Commands

Command	Description
callee-hold-setting	Specifies the callee hold settings.
caller-hold-setting	Specifies the caller hold settings.

branch inband-dtmf-mode

To configure the dual-tone multifrequency (DTMF) in-band mode for the caller side or the callee side, use the **branch inband-dtmf-mode** command in the CAC table entry configuration mode. To unconfigure the DTMF in-band mode, use the **no** form of this command.

branch inband-dtmf-mode {**always** | **inherit** | **maybe** | **never**}

no branch inband-dtmf-mode

Syntax Description

always	Specifies that the in-band DTMF tones are always used by the endpoint.
inherit	Specifies that the in-band DTMF mode for the endpoint is not affected by the CAC entry.
maybe	Specifies that the in-band DTMF tones are used by the endpoint unless signaling indicates that an alternative format is in use for the DTMF.
never	Specifies that the endpoint never uses the in-band DTMF mode.

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 3.5S	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 DTMF in-band mode for the caller side using the **caller inband-dtmf-mode** command in the CAC table entry configuration mode so that the endpoint never uses the inband DTMF mode:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table InbandDTMF
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch inband-dtmf-mode never
```

Related Commands

Command	Description
callee inband-dtmf-mode	Configures the DTMF in-band mode for the callee side.
caller inband-dtmf-mode	Configures the DTMF in-band mode for the caller side.

branch inbound-policy

To configure a caller inbound SDP policy table or a callee inbound SDP policy table, use the **branch inbound-policy** command in the CAC table entry configuration mode. To unconfigure an inbound SDP policy table, use the **no** form of this command.

branch inbound-policy *sdp-policy-table-name*

no branch inbound-policy *sdp-policy-table-name*

Syntax Description

sdp-policy-table-name	Name of the SDP policy table. The *sdp-policy-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

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 **branch inbound-policy** command to configure an inbound SDP policy 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)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch inbound-policy test
```

Related Commands

Command	Description
callee-outbound-policy	Configures a callee outbound SDP policy table.
caller-outbound-policy	Configures a caller outbound SDP policy table.

branch media bypass

To enable or disable the Multiple SBC Media Bypass feature on the caller side or the callee side, use the **branch media bypass** command in the CAC table entry configuration mode. To unconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

branch media bypass {**enable** | **disable**}

no branch media bypass

Syntax Description

enable	Enables the Multiple SBC Media Bypass feature on the caller side or the callee side.
disable	Disables the Multiple SBC Media Bypass feature on the caller side or the callee side.

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 3.5S	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 use the **branch media bypass** command to enable the Multiple SBC Media Bypass feature:

```
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)# branch media bypass enable
```

Related Commands

Command	Description
codec	Adds a codec to a codec list.
codec-list	Creates a codec list.

Command	Description
codec-list description	Provides a description of a codec list.
show sbc sbe codec-list	Displays information about codec lists.

branch media-caps

To configure a codec list used to announce media capabilities on behalf of a SIP caller or SIP callee in a SIP-to-H.323 or H.323-to-SIP interworking call, use the **branch media-caps** command in the CAC table entry configuration mode. To unconfigure the codec list, use the **no** form of this command.

branch media-caps *media-caps-list-name*

no branch media-caps *media-caps-list-name*

Syntax Description

media-caps-list-name	Name of media capabilities list. The *media-caps-list-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

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command configures a codec list and assigns the list to a CAC table. After a codec list is assigned, it must not be deleted before it is removed from the CAC table. A codec list must exist before it can be assigned to an entry in a CAC table.

Examples

The following example shows how to configure the caller-media-caps-list codec list and assign the list to the cac-tbl-1 CAC table in entry 1:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list caller-media-caps-list
Router(config-sbc-sbe-codec-list)# codec t38
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)# branch media-caps media-caps-list
```

Related Commands

Command	Description
callee-media-caps	Configures a codec list that is used to announce media capabilities on behalf of a SIP callee in a SIP-to-H.323 or H.323-to-SIP interworking call.
caller-media-caps	Configures a codec list that is used to announce media capabilities on behalf of a SIP caller in a SIP-to-H.323 or H.323-to-SIP interworking call.

branch media-description disabled

To configure how the SBC handles disabled media descriptions for a caller or a callee, use the **branch media-description disabled** command in the CAC table entry configuration mode. To unconfigure how the SBC handles disabled media descriptions for a caller or a callee, use the **no** form of this command.

branch media-description disabled {strip {answer | offer {all | new}} | {pad offer}}

no branch media-description disabled {strip {answer | offer {all | new}} |{pad offer}}

Syntax Description

strip	Strips the disabled media description lines.
pad	Pads with dummy disabled media description lines.
answer	Strips the disabled media description lines from answers.
offer	Strips the disabled media description lines from offers when this keyword is used with the **strip** keyword. Pads offers with dummy disabled media description lines when used with pad.
all	Strips all the disabled media descriptions from offers.
new	Strips new disabled media descriptions from offers.

Command Default

By default, the **pad** setting is configured.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 removal of disabled media streams from new forwarded offers:

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-description disabled strip
offer new
```

The following example shows how to configure the removal of disabled media streams from forwarded offers, regardless of whether it is known to the recipient of the offer:

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-description disabled strip
offer all
```

The following example shows how to configure the removal of disabled media streams from forwarded answers:

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-description disabled strip
answer
```

The following example shows how to configure the SBC so that it does not pad forwarded offers with disabled media streams:

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# no branch media-description disabled pad
offer
```

Related Commands

Command	Description
callee media-description disabled	Configures how the SBC handles disabled media descriptions for a callee.
caller media-description disabled	Configures how the SBC handles disabled media descriptions for a caller.

branch media-type

To configure the media address type settings for a caller or a callee, use the **branch media-type** command in the CAC table entry configuration mode. To unconfigure the media address type settings for a caller, use the **no** form of this command.

branch media-type {ipv4 | ipv6 | inherit | both}

no branch media-type {ipv4 | ipv6 | inherit | both}

Syntax Description

ipv4	Specifies that only IPv4 media addresses are supported.
ipv6	Specifies that only IPv6 media addresses are supported.
inherit	Specifies that the supported media IP address type from earlier CAC policy entries must be inherited. This is the default setting.
both	Specifies that both IPv4 and IPv6 media addresses are supported.

Command Default

The default is that the supported media IP address type from earlier CAC policy entries must be inherited.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 **branch media-type** command to specify that only IPv4 media addresses are supported:

```
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 mytable
Router(config-sbc-sbe-cacpolicy)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-type ipv4
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

Related Commands

Command	Description
callee media-type	Configures the media address type settings for a callee.
caller media-type	Configures the media address type settings for a caller.

branch outbound-policy

To configure an outbound Session Description Protocol (SDP) policy table for a caller or a callee, use the **branch outbound-policy** command in the CAC table entry configuration mode. To unconfigure an outbound SDP policy table, use the **no** form of this command.

branch outbound-policy *table-name*

no branch outbound-policy *table-name*

Syntax Description

table-name	Name of the SDP policy table. The *table-name* 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

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 outbound SDP policy table for a caller:

```
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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch outbound-policy test
```

Related Commands

Command	Description
callee-inbound-policy	Configures a callee inbound SDP policy table.
caller-inbound-policy	Configures a caller inbound SDP policy table.

branch port-range-tag

To configure the port range tag for a caller or a callee that is used when selecting a media address and port, use the **branch port-range-tag** command in the CAC table entry configuration mode. To unconfigure the port range tag, use the **no** form of this command.

branch port-range-tag {*adjacency-name* | **none** | **string** *tag-string*}

no branch port-range-tag

Syntax Description

adjacency-name	Source adjacency name that is used as a port range tag.
none	Prompts the SBC to not use a port range tag for calls matching the CAC entry, and removes any previously found strings.
string *tag-string*	Specifies the explicit port range tag string.

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 3.5S	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 use the **branch port-range-tag** command to configure a port range tag:

```
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)# branch port-range-tag adj1
```

Related Commands

Command	Description
callee port-range-tag	Configures the port range tag for a callee.
caller port-range-tag	Configures the port range tag for a caller.

branch privacy edit-privacy-request

To edit and update privacy indications provided by a user, use the **branch privacy edit-privacy-request** command in the CAC table configuration mode. To remove the indications, use the **no** form of this command.

branch privacy edit-privacy-request {**pass** | **strip** | **insert** | **replace** | **sip** {**strip** {**all** | **critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**} | **insert** {**critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**}}}

no branch privacy edit-privacy-request {**pass** | **strip** | **insert** | **replace** | **sip** {**strip** {**all** | **critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**} | **insert** {**critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**}}}

Syntax Description

insert	Inserts privacy restrictions, depending on the type of message: • SIP message—Inserts Privacy:header;session;user;id;critical if the header is not already present. • H323 message—Changes the presentation indicator from Allowed to Restricted.
pass	Passes on the privacy header or presentation indicators.
replace	Replaces privacy restrictions, depending on the type of message: • SIP message—Replaces Privacy:header;session;user;id;critical except when none has been requested. • H323 message—Sets the presentation indicator to Restricted.
strip	Removes all the privacy restrictions, depending on the type of message: • SIP message—Removes the Privacy header. • H323 message—Sets the presentation indicator to Allowed.
sip	Specifies the following SIP settings. These settings allow greater control and overide all generic actions: • **insert**—Inserts privacy tokens into the Privacy header. • **strip**—Removes privacy tokens from the Privacy header.
critical	Specifies the call must be discontinued if privacy cannot be achieved in the Privacy header.
header	Obscures all the header information that is related to the user, from the Privacy header.
id	Adds or removes the ID headers from the Privacy header.
none	Specifies that privacy must not be applied to the call.
session	Specifies the media privacy for the session in the Privacy header. No media bypass is performed.
token	Specifies the nonstandard user-defined privacy token in the Privacy header.
word	User-defined privacy token.
user	Removes all nonessential header information that is related to the user, from the Privacy header.

Command Default The default setting is **pass**.

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 entry to remove all the privacy restrictions from the SIP and H323 adjacencies in the MyCacTable admission control 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 MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch-privacy edit-privacy-request strip
```

Related Commands

Command	Description
callee-privacy edit-privacy-request	Edits and updates privacy indications provided by a user, from the callee side.
caller-privacy edit-privacy-request	Edits and updates privacy indications provided by a user, from the caller side.

branch privacy privacy-service

To apply privacy settings according to RFC3323, RFC3325, and the H.323 presentation restriction settings in the admission control table, use the **branch privacy privacy-service** command in the CAC table configuration mode. To unconfigure the privacy settings, use the **no** form of this command.

branch privacy privacy-service {**adj-trust-boundary | always | never**}

no branch privacy privacy-service

Syntax Description

adj-trust-boundary	Specifies the adjacency privacy trust level to determine whether the privacy service is required.
always	Specifies that the privacy service must be provided indefinitely if requested by the user.
never	Specifies that the privacy service must not be provided even if requested by the user.

Command Default

The default privacy setting value is **adj-trust-boundary**.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 entry to provide privacy service indefinitely in the MyCacTable admission control 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 MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch privacy privacy-service always
```

Related Commands

Command	Description
callee privacy privacy-service	Applies privacy settings according to RFC3323, RFC3325, and H.323 presentation restriction settings, on the callee side.
caller privacy privacy-service	Applies privacy settings according to RFC3323, RFC3325, and H.323 presentation restriction settings, on the caller side.

branch ptime

To configure the packetization time on the caller side or the callee side, use the **branch ptime** command in the CAC table configuration mode. To unconfigure the packetization time setting, use the **no** form of this command.

branch ptime *packetization-time*

no branch ptime *packetization-time*

Syntax Description

packetization-time	Packetization time, in milliseconds. The range is from 0 to 100. The default is 0.

Command Default

The default packetization time is 0 milliseconds. This value indicates that transrating must not be performed.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 packetization time to 30 milliseconds by using the **branch ptime** command:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch ptime 30
```

Related Commands

Command	Description
callee ptime	Configures the packetization time on the callee side.
caller ptime	Configures the packetization time on the caller side.

branch secure-media

To apply the granular-level Secure Media feature on the caller side or the callee side, use the **branch secure-media** command in the CAC table entry configuration mode. To remove the granular-level Secure Media feature, use the **no** form of this command.

branch secure-media

no branch secure-media

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the granular-level (Unsignaled) Secure Media feature is disabled.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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.

We recommend that you use the granular-level Secure Media feature instead of enabling Secure Media globally. The granular-level feature enables you to specify the calls and adjacencies at the location where you want to use secure media.

Examples

The following example shows an Unsignaled Secure Media configuration where the two SIP adjacencies for both legs of the call are configured for security trusted-unencrypted, and both the caller and the callee sides are configured for secure media in a CAC table entry:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# adjacency sip server
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table testSecure
Router(config-sbc-sbe-cacpolicy)# cac-table testSecure
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)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch secure-media
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```

```
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# cac-policy-set global 1
Router(config-sbc-sbe)# end
```

Related Commands

Command	Description
callee secure-media	Configures the granular-level Secure Media feature on the callee side.
caller secure-media	Configures the granular-level Secure Media feature on the caller side.

branch sig-qos-profile

To configure the Quality of Service (QoS) profile to be used for signaling packets sent to the original caller or callee, use the **branch sig-qos-profile** command in the CAC table entry configuration mode. To unconfigure the QoS profile, use the **no** form of this command.

caller-sig-qos-profile *profile-name*

no caller-sig-qos-profile *profile-name*

Syntax Description

profile-name	Name of the QoS profile. The *default* string is reserved. The *profile-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

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command can be run only at the per-call scope. The CAC policy will not be activated if this command is configured in any other scope.

Packet marking will not be applied until the CAC decision process is run. This means that some initial signaling packets sent to the caller, for example, the SIP 100 provisional response, will not receive any particular Differentiated Services Codepoint (DSCP) marking.

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 shows how to configure calls from the acme account to use the voice QoS profile enterprise for signaling packets sent from the SBC to the original caller or callee:

```
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-scope call
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 src-account
```

```
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch-sig-qos-profile enterprise
```

Related Commands

Command	Description
callee-sig-qos-profile	Configures the QoS profile to be used for the signaling packets sent to the original callee.
caller-sig-qos-profile	Configures the QoS profile to be used for the signaling packets sent to the original caller.

branch tel-event payload type

To configure the payload type to be used for the caller or the callee in H.323-SIP interworking calls, use the **branch tel-event payload-type** command in the CAC entry configuration mode. To unconfigure the payload type setting, use the **no** form of this command.

branch tel-event payload type *payload-type*

no branch tel-event payload type

Syntax Description

payload-type	See RFC 2833 for detailed information about the values of *payload-type*. The range is from 96 to 127. The default is 101.

Command Default

No default behavior or values are available.

Command Modes

CAC entry configuration (config-sbc-cac-entry)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **branch tel-event payload type** command enables support for dual tone multifrequency (DTMF) H.323-SIP interworking. The telephone-event payload type configured by this command is used by the SBC only in situations where the payload type information is not provided by the other side in an H.323-SIP interworking call.

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 **branch tel-event payload-type** command to set the payload type to 101:

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-cac-pol)# cac-table CAC-POLICY-TBL1
Router(config-sbc-cac-entry)# branch tel-event payload-type 101
```

Related Commands

Command	Description
callee tel-event payload-type	Configures the payload type to be used for the callee in H.323-SIP interworking calls.
caller tel-event payload-type	Configures the payload type to be used for the caller in H.323-SIP interworking calls.

branch video-qos-profile

To configure the QoS profile to be used for the media packets sent to the original caller or original callee, use the **branch video-qos-profile** command in the CAC table configuration mode. To remove this configuration, use the **no** form of this command.

branch video-qos-profile *profile-name*

no branch video-qos-profile *profile-name*

Syntax Description

profile-name	Name of the QoS profile. The *profile-name* 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

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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 **branch video-qos-profile** command can be executed only in the per-call scope. The CAC policy is not activated if this command is configured in any other scope.

Examples

The following example shows how to configure calls from the acme account to use the video QoS profile enterprise for the packets sent from the SBC to the original caller:

```
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-scope call
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 src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch video-qos-profile enterprise
```

Related Commands

Command	Description
callee-video-qos-profile	Configures the QoS profile to be used for the media packets sent to the original callee.
caller-video-qos-profile	Configures the QoS profile to be used for the packets sent to the original caller.

branch voice-qos-profile

To configure the QoS profile to be used for the media packets sent to the original caller or the original callee, use the **branch voice-qos-profile** command in the CAC table configuration mode. To unconfigure the QoS profile, use the **no** form of this command.

branch voice-qos-profile *profile-name*

no branch voice-qos-profile

Syntax Description

profile-name	Name of the QoS profile. The *profile-name* 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

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	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. This command can be run only in the per-call scope. The CAC policy is not activated if this command is configured in any other scope.

Examples

The following example shows how to configure the calls from the acme account to use the voice QoS profile enterprise for the packets sent from the SBC:

```
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-scope call
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 src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch voice-qos-profile enterprise
```

Related Commands

Command	Description
calle-voice-qos-profile	Configures the QoS profile to be used for the media packets sent to the original callee.
caller-voice-qos-profile	Configures the QoS profile to be used for the media packets sent to the original caller.

cac-policy-set

To create a new call admission control (CAC) policy set, copy an existing complete policy set, swap the references of a complete policy set to another policy set, or set the averaging period for rate calculations in a CAC policy set, use the **cac-policy-set** command in the Signaling border element (SBE) configuration mode. To remove a policy set or deconfigure the averaging period, use the **no** form of this command.

cac-policy-set {*policy-set-id* | **copy** {**source** *policy-set-id* **destination** *policy-set-id*} | **swap** {**source** *policy-set-id* **destination** *policy-set-id*} | **averaging-period** {*avg-number avg-period*}

no *cac-policy-set* {*policy-set-id* | **averaging-period** {*avg-number*}}

Syntax Description

policy-set-id	An integer chosen by a user to identify the policy set. The range is from 1 to 2147483647.
copy	Copies an existing policy set.
swap	Swaps the existing references of a complete policy set to another policy set.
source	Specifies the existing complete call policy set.
destination	Specifies the destination of the call policy set.
averaging-period	Specifies the averaging period for rate calculations.
avg-number	The averaging period number. It can be 1 or 2.
avg-period	The averaging period used by the CAC in rate calculations, in seconds. It can range from 1 to 3600 seconds. By default, 60 seconds is configured.

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.
Cisco IOS XE Release 3.2S	This command was modified. The copy-and-swap function was added to this command. The averaging period could also be configured for a CAC policy set.

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.

Changes are not permitted to the configuration of a global policy set. Also, a policy set cannot be removed if it is a global policy set.

Examples

The following command creates a policy set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# exit
```

The following example shows how to copy an existing complete CAC policy set and swap its references to the new policy set:

```
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)# cac-policy-set copy source 12 destination 22
Router(config-sbc-sbe)# cac-policy-set 22
Router(config-sbc-sbe-cacpolicy)# no complete
Router(config-sbc-sbe-cacpolicy)# cac-table TAB1
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# $max-call-rate-per-scope 100
Router(config-sbc-sbe)# cac-policy-set 22
Router(config-sbc-sbe-cacpolicy)# complete
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# cac-policy-set swap source 12 destination 22
Router(config-sbc-sbe-cacpolicy)# cac-policy-set global 22
Router(config-sbc-sbe)# end
```

The following example shows how to set the averaging period for rate calculations in a CAC policy set:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 100
Router(config-sbc-sbe)# cac-policy-set averaging-period 2 175
```

Related Commands

Command	Description
cac-policy-set global	Activates the global CAC policy set within an SBE entity.
show sbc sbe cac-policy-set	Lists detailed information pertaining to a CAC policy table.

cac-policy-set (admin-domain)

To configure the call admission control (CAC) policy set for an administrative domain, use the **cac-policy-set** command in **the Administrative domain** configuration mode. To **remove a policy set from the administrative domain**, use the **no** form of this command.

cac-policy-set *policy-set-id*

no cac-policy-set

Syntax Description

policy-set-id	The integer, ranging from 1 to 2147483647, that identifies a complete policy set.

Command Default

By default, no CAC policy set is configured.

Command Modes

Administrative domain configuration (config-sbc-sbe-ad)

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.

A user can specify only one CAC policy set for an administrative domain.

Examples

The following example shows how to configure the CAC policy set for the administrative domain ADMIN1 using the **call-policy-set** command in **an administrative domain** configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# admin-domain ADMIN1
Router(config-sbc-sbe-ad)# cac-policy-set 2
```

Related Commands

Command	Description
admin-domain	Configures an administrative domain.
call-policy-set (admin-domain)	Configures the inbound and outbound number analysis and routing policy set for an administrative domain.
show sbc sbe admin-domain	Lists the administrative domains on the Session Border Controller (SBC) and per adjacency.

cac-policy-set global

To activate the global call admission control (CAC) policy set within an signaling border element (SBE) entity, use the **cac-policy-set global** command in the SBE configuration mode.

cac-policy-set global *policy-set-id*

Syntax Description

policy-set-id	Integer identifying the policy set that should be made global. Range is from 1 to 2147483647.

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.
Cisco IOS XE Release 3.2S	This command was modified. The **cac-policy-set global** command was renamed as **cac-policy-set global**.

Usage Guidelines

The active CAC policy set cannot be modified.

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 activate policy set 1 on mySbc:

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

Command	Description
cac-policy-set	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
show sbc sbe cac-policy-set	Lists detailed information pertaining to a CAC policy table.

cac-table

To create or configure an admission control table, use the **cac-table** command in CAC-policy-set configuration mode. To **delete the admission control table**, use the **no** form of this command.

cac-table *table-name*

no cac-table *table-name*

Syntax Description

table-name	Specifies the admission control table. 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

CAC-policy-set configuration (config-sbc-sbe-cacpolicy)

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 create the 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)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)#
```

Related Commands

Command	Description
first-cac-table	Configures the name of the first policy table to process when performing the admission control stage of policy.
first-cac-scope	Configure the scope at which to begin defining limits when performing the admission control stage of policy.

cache-lifetime

To configure the lifetime of any DNS entry, use the **cache-lifetime** command in the DNS configuration mode. To disable the lifetime, use the **no** form of this command.

cache-lifetime *0-1879048*

no cache-lifetime

Syntax Description

0-1879048	Specifies the lifetime of any DNS entry in seconds.

Command Default

No default behavior or values are available.

Command Modes

DNS configuration (config-sbc-sbe-dns)

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 lifetime of any DNS entry,:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip dns
Router(config-sbe-dns)# cache-lifetime 444
```

Related Commands

Command	Description
cache-limit	Configures the maximum number of entries that are permitted in the DNS cache.
sip dns	Enter the SIP DNS configuration mode.

cache-limit

To configure the maximum number of entries that are permitted in the DNS cache, use the **cache-limit** command in the DNS configuration mode. To set the limit to 100, use the **no** form of this command.

cache-limit *0-4294967295*

no cache-lifetime

Syntax Description

0-4294967295	Specifies the maximum number of DNS entries.

Command Default

100

Command Modes

DNS configuration (config-sbc-sbe-dns)

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 limits on DNS entries:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip dns
Router(config-sbe-dns)# cache-limit 14
```

Related Commands

Command	Description
cache-lifetime	Configures the lifetime of any DNS entry.
sip dns	Enters the SIP DNS configuration mode.

cache (session border controller)

To enable caching and configure call detail record caching parameters on a local disk, use the **cache** command in the SBE Billing configuration mode. To disable caching and local cache parameters, use the **no** form of this command.

cache [*path {WORD}* | alarm [critical VAL] [major VAL] [minor VAL] | max-size *{0-4194303}]*

no cache [*path {WORD}* | alarm [critical VAL] [major VAL] [minor VAL] | max-size *{0-4194303}]*

Syntax Description

path	(Required to enable caching) Specifies the local CDR cache file path location.
WORD	(Required to enable caching) Specifies the local drive name, up to a maximum of 255 characters.
alarm	(Optional) Specifies the cache file alarm thresholds.
critical VAL	(Optional) Specifies a critical alarm threshold.
major VAL	(Optional) Specifies a major alarm threshold.
minor VAL	(Optional) Specifies a minor alarm threshold.
max-size	(Optional) Specifies the maximum size of the local call detail record (CDR) cache file in kilobytes.
0-4194303	(Optional) This is the maximum size of the local CDR cache file, from zero to 4194303 kilobytes. The default is zero. The **cache max-size 0** command results in no limit on how big the cache can be.

Command Default

The default size of the local CDR cache file is zero.

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

The Cisco ASR 1000 Series Routers have a local disk where records and event messages can be stored on a local cache. Local cache support is a significant advantage because call detail records and event messages (EMs) are not lost when a billing server is unavailable.

Use the **cache** command configures parameters for storing call detail records and EMs on local disk as part of Cisco Unified Border Element (SP Edition)'s integrated billing system in the unified model.

The **cache path** command enables caching and the **no cache path** command disables caching. You can use the other optional keywords to specify alarm thresholds and how large the cache size is in kilobytes.

Examples

The following example configures billing and enables caching of call detailed records and EMs on the designated hard disk:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address aaa ipv4 10.1.1.1
Router(config-sbc-sbe)# radius accounting ACCT-CLIENT-GROUP-1
Router(config-sbc-sbe-acc)# activate
Router(config-sbc-sbe-acc)# server ACCT-SERVER-1
Router(config-sbc-sbe-acc-ser)# address ipv4 20.1.1.1
Router(config-sbc-sbe-acc-ser)# key cisco
Router(config-sbc-sbe-acc)# activate
Router(config-sbc-sbe-acc)# exit
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# ldr-check 22 30
Router(config-sbc-sbe-billing)# local-address ipv4 10.20.1.1
Router(config-sbc-sbe-billing)# method packetcable-em
Router(config-sbc-sbe-billing)# cache path harddisk:
Router(config-sbc-sbe-billing)# packetcable-em 3 transport radius test
Router(config-sbc-sbe-billing-packetcable-em)# batch-size 256
Router(config-sbc-sbe-billing-packetcable-em)# batch-time 22
Router(config-sbc-sbe-billing-packetcable-em)# local-address ipv4 10.1.1.1
Router(config-sbc-sbe-billing-packetcable-em)# attach
Router(config-sbc-sbe-billing-packetcable-em)# exit
Router(config-sbc-sbe-billing)# activate
```

The following configuration example shows that the cache file alarm thresholds and maximum size of the local CDR cache file are configured:

```
 cache path disk2:
 cache alarm minor 100 major 200 critical 300
 cache max-size 1234567
```

The following configuration example shows that caching is enabled on the hard disk:

```
sbc asr
 sbe
   ! - Local radius IP address
   control address aaa ipv4 10.1.1.1

   ! - First radius accounting client group
   radius accounting ACCT-CLIENT-GROUP-1
    ! - First radius server
    server ACCT-SERVER-1
     address ipv4 20.1.1.1
     key cisco
    activate

  ! - Billing manager.
   billing
    local-address ipv4 10.1.1.1
    method packetcable-em
    cache path harddisk:
    ! - First billing method.
    packetcable-em 0 transport radius ACCT-CLIENT-GROUP-1
     local-address ipv4 10.1.1.1
     attach
    activate
```

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.
packetcable-em *method-index* **transport radius** *RADIUS-client-name*	Configures a packet-cable billing instance.
method packetcable-em	Enables the packet-cable billing method.
show sbc sbe billing remote	Displays the local and billing configurations.

cac-policy-set global

To activate the global call admission control (CAC) policy set within an signaling border element (SBE) entity, use the **cac-policy-set global** command in the SBE configuration mode. To deactivate the global CAC policy, use the **no** form of the command.

cac-policy-set global *policy-set-id*

no cac-policy-set global

Syntax Description

policy-set-id	Integer identifying the policy set that should be made global. Range is from 1 to 2147483647.

Command Default

No default behavior or values are available.

Command Modes

SBE configuration (config-sbc-sbe)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It replaces the **cac-policy-set global** command.

Usage Guidelines

From Release 3.5S onward, an active CAC policy set can be modified.

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 activate policy set 1 on mySbc:

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

Related Commands

Command	Description
cac-policy-set	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
show sbc sbe cac-policy-set	Lists detailed information pertaining to a CAC policy table.

cac-scope

To allow you to choose the scope in which CAC limits are to be applied within each entry in a policy set table, use the **cac-scope** command in the CAC table entry configuration mode. To unconfigure the scope, use the **no** form of this command.

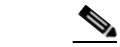
cac-scope {*list of scope options***}**

no cac-scope {*list of scope options***}**

Syntax Description

list of scope options The scope options are as follows:

- **account**—Events that are from the same account.
- **adjacency**—Events that are from the same adjacency.
- **adj-group**—Events that are from members of the same adjacency group.
- **call**—Scope limits are per single call.
- **category**—Events under the same category.
- **dst-account**—Events that are sent to the same account.
- **dst-adj-group**—Events that are sent to the same adjacency group.
- **dst-adjacency**—Events that are sent to the same adjacency.
- **dst-number**—Events that have the same destination.
- **global**—Scope limits are global.
- **src-account**—Events that are from the same account.
- **src-adj-group**—Events that are from the same adjacency group.
- **src-adjacency**—Events that are from the same adjacency.
- **src-number**—Events that have the same source number.
- **sub-category**—Limits specified at this scope are applicable to all the events sent to or received from members of the same subscriber category.
- **sub-category-pfx prefix-len**—Limits specified in this scope are applicable to all the events sent to or received from members having the same subscriber category prefix.



Note *prefix-len* is included as part of the **cac-scope** command, for example, the command is as follows:
cac-scope sub-category-pfx *prefix-len*

- **subscriber**—The limits specified in this scope apply to all the events sent to or received from individual subscribers (a device that is registered with a Registrar server).

Command Default

The default setting is **global**.

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 2.5	The **sub-category**, **sub-category-pfx**, and **subscriber** scope options were added.
Cisco IOS XE Release 3.5S	The **account** and **adjacency** scope options were added.

Usage Guidelines The **cac-scope** command allows you to choose a scope in which CAC limits are to be applied within each entry. This command is available only to the entries defined within a Policy Set table type. You can define more than one **cac-scope** command within an entry.

Use the **table-type** command to configure a Policy Set table type.

Some CAC scopes can be combined to create compound scopes. The **global** scope and **call** scope cannot be combined.

When policy-set is defined as the table type for a CAC table, you must define cac-scope and cac-scope-prefix-len within the entry, for example:

cac-scope sub-category-pfx *prefix-len*

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 call event at which limits are applied in the TAB1 CAC policy-set 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)# first-cac-table TAB1
Router(config-sbc-sbe-cacpolicy)# cac-table TAB1
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-num-calls 20
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)# complete
```

Related Commands

Command	Description
cac-table	Configures a Call Admission Control (CAC) table.
table-type	Configures a CAC table type that enables the priority of the call to be used as a criterion in the CAC policy.

calc-moscqe

To specify the percentage of calls that must be used to calculate the MOS-CQE score, use the **calc-moscqe** command in the adjacency H.323 configuration mode or adjacency SIP configuration mode. To remove this configuration, use the **no** form of this command.

calc-moscqe *call-percentage*

no calc-moscqe

Syntax Description

call-percentage	Percentage of calls. The range is from 0 to 1000. For example, if you enter 205 as the value of *call-percentage*, the SBC uses 20.5 percent of the calls for measuring local jitter.

Command Default

By default, the value of *call-percentage* is 0.

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 **calc-moscqe** command is used to specify that 20.5 percent of the calls must be used to calculate the MOS-CQE score:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 adj1
Router(config-sbc-sbe-adj-h323)# calc-moscqe 205
```

Related Commands

Command	Description
current15minutes	Specifies that QoS statistics must be calculated for 15-minute intervals.
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.

Command	Description
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.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
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.

call-policy-set

To create a new policy set, copy an existing complete policy set, or swap the references of a complete policy set to another policy set, use the **call-policy-set** command in the Signaling border element (SBE) configuration mode. To **delete a policy set**, use the **no** form of this command.

call-policy-set {*policy-set-id* | **copy** {**source** *policy-set-id* **destination** *policy-set-id*} | **swap** {**source** *policy-set-id* **destination** *policy-set-id*}}

no **call-policy-set** *policy-set-id*

Syntax Description

policy-set-id	The integer, ranging from 1 to 2147483647, for a call policy set.
copy	Copies an existing policy set.
swap	Swaps the existing references of a complete policy set to another policy set.
source	Specifies the existing complete call policy set.
destination	Specifies the destination of the call policy set.

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.
Cisco IOS XE Release 3.2S	This command was modified. The copy-and-swap function was added to this command.

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 policy set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)#
```

The following example shows how to copy an existing complete policy set and swap its references to a new policy set:

```
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)# call-policy-set copy source 2 destination 20
Router(config-sbc-sbe)# call-policy-set 20
Router(config-sbc-sbe-rtgpolicy)# no complete
Router(config-sbc-sbe-rtgpolicy)# first-inbound-na-table InTable
Router(config-sbc-sbe-rtgpolicy)# first-outbound-na-table OutTable
Router(config-sbc-sbe-rtgpolicy)# complete
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)# call-policy-set swap source 2 destination 20
```

Related Commands

Command	Description
call-policy-set	Creates a new policy set on the session border controller (SBC).
call-policy set default	Configures a default policy set on the SBE entity.
first-call-routing-table	Configures the name of the first policy table to be processed when performing the routing stage of a policy for new call events.
first-inbound-na-table	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
first-outbound-na-table	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
show sbc sbe call-policy-set	Lists the details of the policy sets configured on the SBC.
show sbc sbe call-policy-set default	Lists the summary of the default policy set configured on the SBC.

call-policy-set (admin-domain)

To configure the inbound and outbound number analysis and routing policy set for an administrative domain, use the **call-policy-set** command in **the Administrative domain** configuration mode. To **remove a policy set from an administrative domain**, use the **no** form of this command.

call-policy-set {**inbound-na** *policy-set-id* | **outbound-na** *policy-set-id* | **rtg** *policy-set-id*} [**priority** *priority-id*]

no call-policy-set {**inbound-na | outbound-na | rtg**}

Syntax Description

inbound-na	Specifies a completed inbound number analysis policy.
outbound-na	Specifies a completed outbound number analysis policy.
rtg	Specifies a completed routing policy.
policy-set-id	The integer, ranging from 1 to 2147483647, that identifies a complete policy set.
priority	Specifies the administrative domain priority
priority-id	The priority value, ranging from 1 to 10, with 10 indicating the highest priority. By default, 10 is the priority value given to a policy set.

Command Default

If the policy sets are not configured, an administrative domain uses the values defined within the default call policy set.

Command Modes

Administrative domain configuration (config-sbc-sbe-ad)

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 an inbound and outbound number analysis and routing policy set for the administrative domain ADMIN1, and allocate priority to the policy sets using the **call-policy-set** command in **the Administrative domain** configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# admin-domain ADMIN1
Router(config-sbc-sbe-ad)# call-policy-set inbound-na 2 priority 10
Router(config-sbc-sbe-ad)# call-policy-set outbound-na 3 priority 10
Router(config-sbc-sbe-ad)# call-policy-set rtg 1 priority 10
```

Related Commands

Command	Description
admin-domain	Configures an administrative domain.
cac-policy-set (admin-domain)	Configures the CAC policy set for an administrative domain.
show sbc sbe admin-domain	Lists the administrative domains on the SBC and per adjacency.

call-policy-set default

To activate a default policy set within an signaling border element (SBE) entity, use the **call-policy-set default** command in **the SBE** configuration mode. To deactivate a default policy set, use the **no** form of this command.

call-policy-set default *policy-set-id* [**priority** *priority-value*]

no call-policy-set default

Syntax Description

policy-set-id	The integer, ranging from 1 to 2147483647, that identifies a default call policy set.
priority	Specifies the priority for the administrative domains that are not configured.
priority-id	The priority value, ranging from 1 to 10, with 10 indicating the highest priority. By default, 6 is the priority value given to the policy set.

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.
Cisco IOS XE Release 3.2S	This command was modified. The **call-policy-set default** command was renamed as **call-policy-set default**. The **priority** keyword and its value were also added.

Usage Guidelines

If another policy set was previously active, it is made inactive by executing this command. The SBE is created with no active routing policy set; an active routing policy set must be explicitly configured using 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 example shows how to set policy set 1 as the default on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# call-policy-set default 1 priority 9
```

Related Commands

Command	Description
call-policy-set	Creates a new policy set on the session border controller (SBC).
first-inbound-na-table	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
first-outbound-na-table	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
show sbc sbe call-policy-set	Lists the details of the policy sets configured on the SBC.
show sbc sbe call-policy-set default	Lists the summary of the default policy set configured on the SBC.

callee-bandwidth-field

To configure 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, use the **callee-bandwidth-field** command in CAC table entry configuration mode. To remove the specific style of bandwidth line format, use the **no callee-bandwidth-field** command.

callee-bandwidth-field *[as-to-tias | tias-to-as]*

no callee-bandwidth-field *[as-to-tias | tias-to-as]*

Syntax Description

as-to-tias	This option causes the SBC to convert a b=AS line format into a b=TIAS line format, for a given SDP bandwidth modifier in an outbound offer. AS = Application Specific Maximum TIAS = Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.
tias-to-as	This option causes the SBC to convert a b=TIAS line format into a b=AS line format, for a given SDP bandwidth modifier in an outbound offer. AS = Application Specific Maximum TIAS = Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.

Command Default

The default is that the bandwidth line is not translated from one format to another.

Command Modes

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

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 follows whichever outgoing bandwidth line format is configured. If the outgoing adjacency is configured to prefer a specific style of bandwidth line, then the preferred format is used, and any b=AS or b=TIAS lines are translated to that format.

If the answerer-side adjacency is configured to prefer a specific style of bandwidth line format in the SDP, this command causes the SBC to convert the offer to the specified format before being sent to the answerer. If there are multiple bandwidth lines, only the first is converted into the specified bandwidth line and the rest are ignored.

Note The default is that the bandwidth line is not translated from one format to another. However, if the callee is configured to convert the bandwidth, and the message is converted, then the response back to the caller is converted back even if the caller-bandwidth-field option is not provisioned.

Examples

The following example shows the SBC is configured to convert an AS bandwidth line format into a TIAS bandwidth line format in an outbound SDP sent to the callee:

```
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)# cac-policy-set 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)# callee-bandwidth-field as-to-tias
```

Related Commands

Command	Description
caller-bandwidth-field *[as-to-tias | tias-to-as]*	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 caller.

callee-codec-list

To list the codecs which the callee leg of a call is allowed to use, use the **callee-codec-list** command in the CAC table entry configuration mode. To delete a codec list, use the **no** form of this command.

callee-codec-list *list-name*

no callee-codec-list *list-name*

Syntax Description

list-name	Specifies the name of the codec list. The *list-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

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 enter a mode to create a codec list using the name test:

```
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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-codec-list test
```

callee-hold-setting

To configure the callee hold settings that are supported, use the **callee-hold-setting** command in CAC table entry configuration mode. To deconfigure the callee hold settings, use the **no** form of this command.

callee-hold-setting {hold-c0 | hold-c0-inactive | hold-c0-sendonly | hold-sendonly | standard}

no ***callee-hold-setting {hold-c0 | hold-c0-inactive | hold-c0-sendonly | hold-sendonly | standard}***

Syntax Description

hold-c0	Callee supported; requires c=I 0.0.0.0.
hold-c0-inactive	Callee supported; requires c=I 0.0.0.0 or a=inactive.
hold-c0-sendonly	Callee supported; requires c=0.0.0.0 or a=sendonly
hold-sendonly	Callee supported; requires a=sendonly.
standard	Callee supported; requires c=0.0.0.0 and either a=forward-direction capability.

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 configure the callee hold settings:

```
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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value fairchild
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-hold-setting hold-sendonly
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

Related Commands

Command	Description
callee-inbound-policy	Configures a callee inbound SDP policy table.
callee-outbound-policy	Configures a callee outbound SDP policy table.

callee-inbound-policy

To configure a callee inbound SDP policy table, use the ***callee-inbound-policy*** command in CAC table entry configuration mode. To, use the **no** form of this command.

callee-inbound-policy *WORD*

no ***callee-inbound-policy*** *WORD*

Syntax Description

WORD	Specifies the name of the SDP policy table. The maximum size is 30 characters.

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 create the 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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-inbound-policy test
```

Related Commands

Command	Description
callee-hold-setting	Configures the callee hold settings that are supported.
callee-outbound-policy	Configures a callee outbound SDP policy table.

callee-media-caps

To configure a codec list used to announce media capabilities on behalf of a SIP callee in a SIP to H.323 or H.323 to SIP interworking call, use the **callee-media-caps** command in CAC table entry configuration mode. To remove the codec list, use the **no callee-media-caps** command.

callee-media-caps *{code-list-name}*

no callee-media-caps *{code-list-name}*

Syntax Description

code-list-name	This is a string text of a maximum length of 30 characters. Describes the extra codecs that a SIP callee can announce to the H.323 side.

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 2.5.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command configures a codec list and assigns the list to a CAC table.

Once a codec list has been assigned, it may not be deleted until it is removed from the CAC table entry. A codec list must exist before it can be assigned to an entry in a CAC table.

For a description of "H.323 TCS Codecs," see the "Codec Handling" chapter in the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model*.

Examples

The following example configures a codec list called "callee-media-caps-list" and assigns that list to the CAC table "cac-tbl-1" in entry 1 to announce that T.38 was added as a callee SIP media capabilities.

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list callee-media-caps-list
Router(config-sbc-sbe-codec-list)# codec t38
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)# callee-media-caps callee-media-caps-list
```

Related Commands

Command	Description
caller-media-caps	Configures a codec list used to announce media capabilities on behalf of a SIP caller in a SIP to H.323 or H.323 to SIP interworking call.
tcs-extra-caps-list	Configures a codec list used to announce media capabilities on behalf of both the SIP caller and callee in a SIP to H.323 or H.323 to SIP interworking call.

callee-outbound-policy

To configure a callee outbound SDP policy table, use the **callee-outbound-policy** command in CAC table entry configuration mode. To, use the **no** form of this command.

callee-outbound-policy *WORD*

no callee-outbound-policy *WORD*

Syntax Description

WORD	Specifies the name of the SDP policy table. The maximum size is 30 characters.

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 create the 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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-inbound-policy test
```

Related Commands

Command	Description
callee-hold-setting	Configures the callee hold settings that are supported.
callee-inbound-policy	Configures a callee inbound SDP policy table.

callee-privacy edit-privacy-request

To edit and update privacy indications provided by the user, use the **callee-privacy edit-privacy-request** command in CAC table configuration mode. To remove the indications, use the **no** form of this command.

callee-privacy edit-privacy-request {**pass** | **strip** | **insert** | **replace** | **sip** {**strip** {**all** | **critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**} | **insert** {**critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**}}}

no callee-privacy edit-privacy-request {**pass** | **strip** | **insert** | **replace** | **sip** {**strip** {**all** | **critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**} | **insert** {**critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**}}}

Syntax Description

insert	Inserts privacy restrictions: • SIP —Inserts Privacy:header;session;user;id;critical, if the header is not present already • H323—Sets presentation indicator from allowed to restricted.
pass	Passes on the privacy header or presentation indicators.
replace	Replaces privacy restrictions: • SIP—Replaces the Privacy:header;session;user;id;critical, except when none has been requested. • H323—Sets presentation indicator to restricted.
strip	Removes all privacy restrictions: • SIP—Removes Privacy header. • H323—Set presentation indicator to allowed.
sip	Specifies the following SIP settings that allows greater control and overrides all generic actions: • **insert**—Inserts Privacy tokens into the Privacy header. • **strip**—Removes privacy tokens from the Privacy header.
critical	Specifies the call to discontinue if privacy cannot be achieved in the SIP Privacy header.
header	Obscures all header information that is related to the user from the SIP Privacy header.
id	Adds or removes the ID headers from the SIP Privacy header.
none	Privacy is not applied to call.
session	Specifies the media privacy for the session in the SIP Privacy header. No media bypass is performed.
token	Specifies the non standard user defined privacy token in the SIP Privacy header.
word	Specifies the user defined privacy token.
user	Removes all non-essential header information that is related to the user from the SIP Privacy header.

Command Default *The privacy request editing* is set to Pass.

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 from **callee-privacy** to **callee-privacy edit-privacy-request**. The **callee-privacy limited-privacy-service** command has been removed.

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 entry to remove all privacy restrictions from SIP and H323 adjacencies 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)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-privacy edit-privacy-request strip
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands

Command	Description
cac-table	Configures admission control tables.
callee-privacy privacy-service	Applies privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings.
table-type	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

callee-privacy privacy-service

To apply privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings in the given entry in the admission control table, use the **callee-privacy privacy-service** command in CAC table configuration mode. To remove the privacy settings, use the **no** form of this command.

callee-privacy privacy-service {**adj-trust-boundary | always | never**}

no callee-privacy privacy-service

Syntax Description

adj-trust-boundary	Specifies the adjacency privacy trust level to determine if the privacy service is required.
always	Provides privacy service always, if requested by the user.
never	Never provides privacy service even if requested by the user.

Command Default

The privacy setting value is set to adj-trust-boundary.

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 from **callee-privacy** to **callee-privacy privacy-service**. The **callee-privacy limited-privacy-service** command has been removed.

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 entry to provide privacy service always as requested by the user 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)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-privacy privacy-service always
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands

Command	Description
cac-table	Configures admission control tables.
callee-privacy edit-privacy-request	Edits and updates privacy indications provided by the user
table-type	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

callee-sig-qos-profile

To **configure the QoS profile to be used for signaling packets sent to the original callee**, use the **callee-sig-qos-profile** command in the CAC table entry configuration mode. To **deconfigure the QoS profile**, use the **no** form of this command.

callee-sig-qos-profile *profile-name*

no callee-sig-qos-profile *profile-name*

Syntax Description

profile-name	Specifies the name of the QoS profile. The string "default" is reserved. The *profile-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

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 the **callee-sig-qos-profile** command is used to configure the QoS profile named enterprise to be used for signaling packets sent to the original callee:

```
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 MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-sig-qos-profile enterprise
```

callee tel-event payload type

To configure the payload type to be used for the callee in H.323-SIP interworking calls, use the **callee tel-event payload-type** command in the CAC entry configuration mode. To unconfigure the payload type setting, use the **no** form of this command.

callee tel-event payload type *payload-type*

no callee tel-event payload type

Syntax Description

payload-type	See RFC 2833 for detailed information about the values of *payload-type*. The range is from 96 to 127. The default is 101.

Command Default

No default behavior or values are available.

Command Modes

CAC entry configuration (config-sbc-cac-entry)

Command History

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

Usage Guidelines

The **callee tel-event payload type** command enables support for dual tone multifrequency (DTMF) H.323-SIP interworking. The telephone-event payload type configured by this command is used by the SBC only in situations where the payload type information is not provided by the other side in an H.323-SIP interworking call.

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 **callee tel-event payload-type** command to set the payload type to 101:

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-cac-pol)# cac-table CAC-POLICY-TBL1
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)# callee tel-event payload-type 101
```

Related Commands

Command	Description
branch tel-event payload-type	Configures the payload type to be used for the callee or the caller in H.323-SIP interworking calls.
caller tel-event payload-type	Configures the payload type to be used for the caller in H.323-SIP interworking calls.

callee-video-qos-profile

To configure the QoS profile to use for media packets sent to the original callee, use the **callee-video-qos-profile** command in CAC table entry configuration mode. To return to the default behavior, use the **no** form of this command.

callee-video-qos-profile *profile-name*

no callee-video-qos-profile

Syntax Description

profile-name	Name of the QoS profile. The *profile*-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

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.

Note The **callee-video-qos-profile can** be executed only at the per-call scope. CAC policy does not activate if configured at any other scope.

Examples

The following example shows how to configure calls from the acme account to use the video QoS profile enterprise for packets sent from the SBC to the original callee:

```
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-scope call
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-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-video-qos-profile enterprise
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

callee-voice-qos-profile

To configure the QoS profile to use for media packets sent to the original callee, use the **callee-voice-qos-profile** command in CAC table entry configuration mode. To return to the default behavior, use the **no** form of this command.

callee-voice-qos-profile *profile-name*

no callee-voice-qos-profile

Syntax Description

profile-name	Name of the QoS profile. The *profile-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

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.

Note This command can be executed only at the per-call scope. CAC policy does not activate if this command is configured at any other scope.

Examples

The following example shows how to configure calls from the acme account to use the voice QoS profile enterprise for packets sent from the SBC to the original callee.

```
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-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-voice-qos-profile enterprise
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

callee codec

To configure the codec options for a callee, use the **callee codec** command in the CAC table entry configuration mode. To deconfigure the codec options, use the **no** form of this command.

callee codec {convert | profile *profile-name*}

no callee codec {convert | profile}

Syntax Description

convert	Enables or disables the codec variant conversion.
profile	Specifies or removes the codec variant profile.
profile-name	The codec variant profile name. The *profile-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

By default, codec variant conversion is disabled, and no codec variant profile is specified.

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 that follows shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to configure the codec options for a callee using the **callee codec** command in the CAC table entry 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)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee codec convert
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee codec profile profile-1
```

callee inband-dtmf-mode

To configure the dual tone multifrequency (DTMF) in-band mode for the callee side, use the **callee inband-dtmf-mode** command in the CAC table entry configuration mode.To deconfigure the DTMF in-band mode for the callee side, use the **no** form of this command.

callee inband-dtmf-mode {**always** | **inherit** | **maybe** | **never**}

no callee inband-dtmf-mode

Syntax Description

always	Specifies that the in-band DTMF tones are always used by the endpoint.
inherit	Specifies that the in-band DTMF mode for the endpoint is not affected by the CAC entry.
maybe	Specifies that the in-band DTMF tones are used by the endpoint unless signaling indicates that an alternative format is in use for the DTMF.
never	Specifies that the endpoint never uses in-band DTMF.

Command Default

No default behavior or values.

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 that follows shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to configure the DTMF in-band mode for the callee side using the **callee inband-dtmf-mode** command in the CAC table entry configuration mode so that the in-band DTMF tones are always in use by the endpoint:

```
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)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table InbandDTMF
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee inband-dtmf-mode always
```

Related Commands

Command	Description
caller inband-dtmf-mode	Configures the DTMF in-band mode for the caller side

callee media-description disabled

To configure how Cisco Unified Border Element (SP Edition) handles disabled media descriptions for a callee, use the **callee media-description disabled** command in the CAC table entry configuration mode.

callee media-description disabled {strip {answer | offer {all | new}} | {pad offer}}

no callee media-description disabled {strip {answer | offer {all | new}} |{pad offer}}

Syntax Description

strip	Strips disabled media description lines.
pad	Pads with dummy disabled media description lines.
answer	Strips disabled media description lines from answers.
offer	Strips disabled media description lines from offers when used with strip. Pad offers with dummy disabled media description lines when used with pad.
all	Strips all disabled media descriptions from offers.
new	Strips new disabled media descriptions from offers.

Command Default

Pad and do-not-strip are the default behaviors.

Command Modes

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

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.

Examples

The following example shows how to remove disabled media streams in forwarded offers which are new:

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-description disabled strip
offer new
```

The following example shows how to remove all disabled media streams from forwarded offers, whether known to the recipient of the offer or not.

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-description disabled strip
offer all
```

The following example shows how to remove all disabled media streams from forwarded answers.

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-description disabled strip
answer
```

The following example shows how to stop SBC from padding forwarded offers with disabled media streams.

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# no callee media-description disabled pad
offer
```

callee media-type

To configure the media address type settings for a callee on the Cisco Unified Border Element (SP Edition), use the **callee media-type** command in the CAC table entry configuration mode. Use the **no** form of this command to disable the media address type settings for a callee.

callee media-type {ipv4 | ipv6 | inherit | both}

no callee media-type {ipv4 | ipv6 | inherit | both}

Syntax Description

ipv4	Only IPv4 media addresses are supported.
ipv6	Only IPv6 media addresses are supported.
inherit	Inherit the supported media IP address type from earlier CAC policy entries (default).
both	Both IPv4 and IPv6 media addresses are supported.

Command Default

The default behavior is inherit.

Command Modes

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

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 remove disabled media streams in forwarded offers which are new:

```
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 mytable
Router(config-sbc-sbe-cacpolicy)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-type ipv4
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

callee media bypass

To enable or disable the Multiple SBC Media Bypass feature on the callee side, use the **callee media bypass** command in the CAC table entry configuration mode. To deconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

callee media bypass {**enable** | **disable**}

no callee media bypass

Syntax Description

enable	Enables the Multiple SBC Media Bypass feature on the callee side.
disable	Disables the Multiple SBC Media Bypass feature on the callee side.

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 enable the Multiple SBC Media Bypass feature on the callee side:

```
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)# callee media bypass enable
```

Related Commands

Command	Description
cac-table	Configures admission control tables.
caller media bypass	Enables or disables the Multiple SBC Media Bypass feature on the caller side.
table-type	Configures a CAC table type to enable the priority of the call to be used as a criterion in the CAC policy.

callee port-range-tag

To configure the port range tag for a callee that is used when selecting a media address and port, use the **callee port-range-tag** command in the CAC table entry configuration mode. To deconfigure the port range tag, use the **no** form of this command.

callee port-range-tag {**adj-name** | **none** | **string** *tag-string*}

no callee port-range-tag

Syntax Description

adj-name	Uses the destination adjacency name as a port-range tag.
none	Prompts the SBC to not use a port range tag for calls matching the CAC entry, and removes any previously found strings.
string *tag-string*	Specifies the explicit port range tag string.

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 a port-range tag:

```
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)# match SIPIMSAccess
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee port-range-tag string
GenericCorePortRange
```

Related Commands

Command	Description
media-address-pool	Adds an IPv4 and IPv6 address to the set of addresses that can be used by the DBE as a local media address.

callee ptime

To configure the packetization time on the callee side, use the **callee ptime** command in the CAC table configuration mode.To deconfigure the packetization time on the callee side, use the **no** form of this command.

callee ptime *0-100*

no callee ptime *0-100*

Syntax Description

0-100	The packetization time in milliseconds (ms).

Command Default

By default, 0 ms is configured. This means that no transrating occurs.

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 that follows shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to configure the packetization time on the callee side using the **callee ptime** command in the CAC table configuration 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)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee ptime 30
```

Related Commands

Command	Description
caller ptime	Configures the packetization time on the caller side.

callee secure-media

To configure granular-level Secure Media on the callee side, use the **callee secure-media** command in CAC table entry configuration mode. To remove granular-level Secure Media, use the **no callee secure-media** command.

callee secure-media

no callee secure-media

Syntax Description

This command has no arguments or keywords.

Command Default

Granular-level (Unsignaled) Secure Media is disabled by default.

Command Modes

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

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

Restriction—Both caller and callee sides of the call need to be configured. If only one leg of the call has granular secure media configured, then the call will fail.

We recommend you use unsignaled (also called granular-level) Secure Media configuration because, instead of turning on Secure Media globally, you can specify the calls and adjacencies where you want to use Secure Media.

Examples

The following example shows an Unsignaled Secure Media configuration where the two SIP adjacencies for both legs of the call are configured for “security trusted-unencrypted” and both the caller and callee sides are configured for Secure Media in a CAC table entry:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# adjacency sip server
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table testSecure
Router(config-sbc-sbe-cacpolicy)# cac-table testSecure
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)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller secure-media
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee secure-media
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# cac-policy-set global 1
Router(config-sbc-sbe)# end
```

The following configuration example shows how to configure Unsignaled Secure Media where an adjacency is *untrusted* by using the **transport srtp allowed** command on the untrusted adjacency in a CAC policy table:

```
...
cac-policy-set 2
 first-cac-table 1
 cac-table 1
  table-type limit all
  entry 1
   match-value call-update
   transport srtp allowed
   caller secure-media
   callee secure-media
   action cac-complete
   exit
 complete
 exit
cac-policy-set global 2
```

The following configuration example shows that SIP adjacencies ‘client’ and ‘server’ are configured as “security trusted-unencrypted” and that CAC table entry 1 is configured for Secure Media on both the caller and callee sides:

```
...
cac-policy-set 2
 first-cac-table 1
 cac-table 1
  table-type policy-set
  entry 1
   action cac-complete
   caller secure-media
   callee secure-media
 complete
cac-policy-set global 2

adjacency sip client
 nat force-off
 security trusted-unencrypted
 signaling-address ipv4 10.10.100.110
 signaling-port 9060
 remote-address ipv4 10.10.100.10 255.255.255.255
 signaling-peer 10.10.100.10
 signaling-peer-port 9060
 attach
adjacency sip server
 nat force-off
 security trusted-unencrypted
 signaling-address ipv4 10.10.100.110
 signaling-port 9070
 remote-address ipv4 10.10.100.10 255.255.255.255
 signaling-peer 10.10.100.10
 signaling-peer-port 9070
 attach
```

Related Commands

Command	Description
caller secure-media	Configures granular-level Secure Media on the caller side.
security	Configures transport-level security (TLS) on a SIP adjacency.

caller-bandwidth-field

To configure the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the caller, use the **caller-bandwidth-field** command in CAC table entry configuration mode. To remove the specific style of bandwidth line format, use the **no caller-bandwidth-field** command.

caller-bandwidth-field *[as-to-tias | tias-to-as]*

no caller-bandwidth-field *[as-to-tias | tias-to-as]*

Syntax Description

as-to-tias	Configures the SBC to convert a b=AS line format into a b=TIAS line format, for a given SDP media descriptor in an outbound offer. AS —Application Specific Maximum TIAS—Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.
tias-to-as	Configures the SBC to convert a b=TIAS line format into a b=AS line format, for a given SDP media descriptor in an outbound offer. AS—Application Specific Maximum TIAS—Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.

Command Default

The default is that the bandwidth line is not translated from one format to another.

Command Modes

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

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 follows whichever outgoing bandwidth line format is configured. If the outgoing adjacency is configured to prefer a specific style of bandwidth line, then the preferred format is used, and any b=AS or b=TIAS lines are translated to that format.

If the offerer-side adjacency is configured to prefer a specific style of bandwidth line format in the SDP, this command causes the SBC to convert the answer to the specified format before being sent back to the offerer. If there are multiple bandwidth lines, only the first is converted into the specified bandwidth line and the rest are ignored.

Note The default is that the bandwidth line is not translated from one format to another. However, if the callee is configured to convert the bandwidth, and the message is converted, then the response back to the caller is converted back even if the caller-bandwidth-field option is not provisioned.

Examples

The following example shows the SBC is configured to convert an AS bandwidth line format into a TIAS bandwidth line format in an outbound SDP sent to the caller:

```
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)# cac-policy-set 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)# caller-bandwidth-field as-to-tias
```

Related Commands

Command	Description
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.

caller-codec-list

To list the codecs which the caller leg of a call is allowed to use, use the **caller-codec-list** command in the CAC table entry configuration mode. To delete a codec list, use the **no** form of this command.

caller-codec-list *list-name*

no caller-codec-list *list-name*

Syntax Description

list-name	Specifies the name of the codec list. The *list-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

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 enter a mode to create a codec list using the name test:

```
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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-codec-list test
```

caller-hold-setting

To configure the caller hold settings that are supported, use the **caller-hold-setting** command in CAC table entry configuration mode. To cancel caller hold settings, use the **no** form of this command.

caller-hold-setting {**hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard**}

no caller-hold-setting {**hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard**}

Syntax Description

hold-c0	Specifies callee supported; requires c=I 0.0.0.0.
hold-c0-inactive	Specifies callee supported; requires c=I 0.0.0.0 or a=inactive.
hold-c0-sendonly	Specifies callee supported; requires c=0.0.0.0 or a=sendonly
hold-sendonly	Specifies callee supported; requires a=sendonly.
standard	Specifies callee supported; requires c=0.0.0.0 and either a=forward-direction capability.

Command Default

The default is standard.

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 configure the caller hold settings:

```
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-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value fairchild
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-hold-setting hold-sendonly
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

Related Commands

Command	Description
caller-outbound-policy	Configures a caller outbound SDP policy table.
caller-inbound-policy	Configures a caller inbound SDP policy table.

caller-inbound-policy

To configure a caller inbound SDP policy table, use the **caller-inbound-policy** command in CAC table entry configuration mode. To deconfigure a caller inbound SDP policy table, use the **no** form of this command.

caller-inbound-policy *WORD*

no caller-inbound-policy *WORD*

Syntax Description

WORD	Specifies the name of the SDP policy table. The maximum size is 30 characters.

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 configure a caller inbound SDP policy 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)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-inbound-policy test
```

Related Commands

Command	Description
caller-hold-setting	Configures the caller hold settings.
caller-outbound-policy	Configure a caller outbound SDP policy table.
codec	Adds a codec to a codec list.
caller-codec-list	Lists the codecs which the caller of a call can use.

caller-media-caps

To configure a codec list used to announce media capabilities on behalf of a SIP caller in a SIP to H.323 or H.323 to SIP interworking call, use the **caller-media-caps** command in CAC table entry configuration mode. To remove the codec list, use the **no caller-media-caps** command.

caller-media-caps *{code-list-name}*

no caller-media-caps *{code-list-name}*

Syntax Description

code-list-name	This is a string text of a maximum length of 30 characters. Describes the extra codecs that a SIP caller can announce to the H.323 side.

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 2.5.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command configures a codec list and assigns the list to a CAC table.

Once a codec list has been assigned, it may not be deleted until it is removed from the CAC table entry. A codec list must exist before it can be assigned to an entry in a CAC table.

For a description of "H.323 TCS Codecs," see the "Codec Handling" chapter in the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model*.

Examples

The following example configures a codec list called "caller-media-caps-list" and assigns that list to the CAC table "cac-tbl-1" in entry 1 to announce that T.38 is added as a caller SIP media capabilities:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list caller-media-caps-list
Router(config-sbc-sbe-codec-list)# codec t38
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)# caller-media-caps caller-media-caps-list
```

Related Commands

Command	Description
callee-media-caps	Configures a codec list used to announce media capabilities on behalf of a SIP callee in a SIP to H.323 or H.323 to SIP interworking call.
tcs-extra-caps-list	Configures a codec list used to announce media capabilities on behalf of both the SIP caller and callee in a SIP to H.323 or H.323 to SIP interworking call.

caller-outbound-policy

To configure a caller outbound SDP policy table, use the **caller-outbound-policy** command in CAC table entry configuration mode. To deconfigure a caller outbound SDP policy table, use the **no** form of this command.

caller-outbound-policy *table_name*

no caller-outbound-policy *table_name*

Syntax Description

WORD	Specifies the name of the SDP policy table. The maximum size is 30 characters.

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 configure a caller outbound SDP Limit 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)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-outbound-policy test
```

Command	Description
caller-hold-setting	Configures the caller hold settings.
caller-inbound-policy	Configures a caller inbound SDP policy table.

caller-privacy edit-privacy-request

To edit and update privacy indications provided by the user, use the **caller-privacy edit-privacy-request** command in CAC table configuration mode. To remove the indications, use the **no** form of this command.

caller-privacy edit-privacy-request {**pass** | **strip** | **insert** | **replace** | **sip** {**strip** {**all** | **critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**} | **insert** {**critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**}}}

no caller-privacy edit-privacy-request {**pass** | **strip** | **insert** | **replace** | **sip** {**strip** {**all** | **critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**} | **insert** {**critical** | **header** | **id** | **none** | **session** | **token** *word* | **user**}}}

Syntax Description

insert	Inserts privacy restrictions: • SIP —Inserts Privacy:header;session;user;id;critical, if the header is not present already • H323—Sets presentation indicator from allowed to restricted.
pass	Passes on the privacy header or presentation indicators.
replace	Replaces privacy restrictions: • SIP—Replaces the Privacy:header;session;user;id;critical, except when none has been requested. • H323—Sets presentation indicator to restricted.
strip	Removes all privacy restrictions: • SIP—Removes Privacy header. • H323—Set presentation indicator to allowed.
sip	Specifies the following SIP settings that allows greater control and overrides all generic actions: • **insert**—Inserts Privacy tokens into the Privacy header. • **strip**—Removes privacy tokens from the Privacy header.
critical	Specifies the call to discontinue if privacy cannot be achieved in the SIP Privacy header.
header	Obscures all header information that is related to the user from the SIP Privacy header.
id	Adds or removes the ID headers from the SIP Privacy header.
none	Privacy is not applied to call.
session	Specifies the media privacy for the session in the SIP Privacy header. No media bypass is performed.
token	Specifies the non standard user defined privacy token in the SIP Privacy header.
word	Specifies the user defined privacy token.
user	Removes all non-essential header information that is related to the user from the SIP Privacy header.

Command Default

The privacy request editing is set to Pass.

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 from **caller-privacy** to **caller-privacy edit-privacy-request**. The **caller-privacy limited-privacy-service** command has been removed.

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 entry to remove all privacy restrictions from SIP and H323 adjacencies 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)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-privacy edit-privacy-request strip
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands

Command	Description
cac-table	Configures admission control tables.
caller-privacy privacy-service	Applies privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings.
table-type	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

caller-privacy privacy-service

To apply privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings in the given entry in the admission control table, use the **caller-privacy privacy-service** command in CAC table configuration mode. To remove the privacy settings, use the **no** form of this command.

caller-privacy privacy-service {**adj-trust-boundary | always | never**}

no caller-privacy privacy-service

Syntax Description

adj-trust-boundary	Specifies the adjacency privacy trust level to determine if the privacy service is required.
always	Provides privacy service always, if requested by the user.
never	Never provides privacy service even if requested by the user.

Command Default

The privacy setting value is set to adj-trust-boundary.

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 from **caller-privacy** to **caller-privacy privacy-service**. The **caller-privacy limited-privacy-service** command has been removed.

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 entry to provide privacy service always as requested by the user 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)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-privacy privacy-service always
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands

Command	Description
cac-table	Configures admission control tables.
caller-privacy edit-privacy-request	Edits and updates privacy indications provided by the user
table-type	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

caller-sig-qos-profile

To **configure** the QoS profile to use for signaling packets sent to the original caller, use the **caller-sig-qos-profile** command in the CAC table entry configuration mode. To **deconfigure the QoS profile**, use the **no** form of this command.

caller-sig-qos-profile *profile-name*

no caller-sig-qos-profile *profile-name*

Syntax Description

profile-name	Specifies the name of the QoS profile. The string "default" is reserved. The *profile-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

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

This command can only be executed at the per-call scope. CAC policy will not activate if this command is configured at any other scope.

Packet marking will not be applied until the CAC decision process is run. This means that some initial signaling packets sent to the caller (for example, the SIP 100 provisional response) will not receive any particular DSCP marking.

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 calls from the acme account to use the voice QoS profile enterprise for signaling packets sent from the SBC to the original caller:

```
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-scope call
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 src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-sig-qos-profile enterprise
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

caller tel-event payload type

To configure the payload type to be used for the caller in H.323-SIP interworking calls, use the **caller tel-event payload-type** command in the CAC entry configuration mode. To unconfigure the payload type setting, use the **no** form of this command.

caller tel-event payload type *payload-type*

no caller tel-event payload type

Syntax Description

payload-type	See RFC 2833 for detailed information about the values of *payload-type*. The range is from 96 to 127. The default is 101.

Command Default

No default behavior or values are available.

Command Modes

CAC entry configuration (config-sbc-cac-entry)

Command History

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

Usage Guidelines

The **caller tel-event payload type** command enables support for dual tone multifrequency (DTMF) H.323-SIP interworking. The telephone-event payload type configured by this command is used by the SBC only in situations where the payload type information is not provided by the other side in an H.323-SIP interworking call.

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 **caller tel-event payload-type** command to set the payload type to 101:

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-cac-pol)# cac-table CAC-POLICY-TBL1
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)# caller tel-event payload-type 101
```

Related Commands

Command	Description
branch tel-event payload-type	Configures the payload type to be used for the callee or the caller in H.323-SIP interworking calls.
callee tel-event payload-type	Configures the payload type to be used for the callee in H.323-SIP interworking calls.

caller-video-qos-profile

To configure the QoS profile to use for media packets sent to the original caller, use the **caller-video-qos-profile** command in CAC table configuration mode. To remove this configuration, use the **no** form of this command.

caller-video-qos-profile *profile-name*

no caller-video-qos-profile *profile-name*

Syntax Description

profile-name	Specifies the Qos profile. The *profile-name* 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

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.

Note The **caller-video-qos-profile** command can be executed only at the per-call scope. CAC policy does not activate if this command is configured at any other scope.

Examples

The following example shows how to configure calls from the acme account to use the video QoS profile enterprise for packets sent from the SBC to the original caller:

```
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-scope call
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 src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-video-qos-profile enterprise
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

caller-voice-qos-profile

To configure the QoS profile to use for media packets sent to the original caller, use the **caller-voice-qos-profile** command in CAC table configuration mode. To remove this configuration, use the **no** form of this command.

caller-voice-qos-profile *profile-name*

no caller-voice-qos-profile

Syntax Description

profile-name	Specifies the QoS profile. The *profile-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

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.

Note This command can be executed only at the per-call scope. CAC policy does not activate if this command is configured at any other scope.

Examples

The following example shows how to configure calls from the acme account to use the voice QoS profile enterprise for packets sent from the SBC to the original caller:

```
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-scope call
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 src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-voice-qos-profile enterprise
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

caller codec

To configure the codec options for a caller, use the **caller codec** command in the CAC table entry configuration mode. To deconfigure the codec options, use the **no** form of this command.

caller codec {convert | profile *profile-name*}

no caller codec {convert | profile}

Syntax Description

convert	Enables or disables the codec variant conversion.
profile	Specifies or removes the codec variant profile.
profile-name	The codec variant profile name.

Command Default

By default, codec variant conversion is disabled, and no codec variant profile is specified.

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 that follows shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to configure the codec options for a caller using the **caller codec** command in the CAC table entry 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)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller codec convert
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller codec profile profile-1
```

caller inband-dtmf-mode

To configure the dual tone multifrequency (DTMF) in-band mode for the caller side, use the **caller inband-dtmf-mode** command in the CAC table entry configuration mode.To deconfigure the DTMF in-band mode for the caller side, use the **no** form of this command.

caller inband-dtmf-mode {**always** | **inherit** | **maybe** | **never**}

no caller inband-dtmf-mode

Syntax Description

always	Specifies that the in-band DTMF tones are always used by the endpoint.
inherit	Specifies that the in-band DTMF mode for the endpoint is not affected by the CAC entry.
maybe	Specifies that the in-band DTMF tones are used by the endpoint unless signaling indicates that an alternative format is in use for the DTMF.
never	Specifies that the endpoint never uses in-band DTMF mode.

Command Default

No default behavior or values.

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 that follows shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to configure the DTMF in-band mode for the caller side using the **caller inband-dtmf-mode** command in the CAC table entry configuration mode so that the endpoint never uses in-band DTMF 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)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table InbandDTMF
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller inband-dtmf-mode never
```

Related Commands

Command	Description
callee inband-dtmf-mode	Configures the DTMF in-band mode for the callee side.

caller media-description disabled

To configure how Cisco Unified Border Element (SP Edition) handles disabled media descriptions for a caller, use the **caller media-description disabled** command in the CAC table entry configuration mode.

caller media-description disabled {strip {answer | offer {all | new}} | {pad offer}}

no caller media-description disabled {strip {answer | offer {all | new}} |{pad offer}}

Syntax Description

strip	Strips disabled media description lines.
pad	Pads with dummy disabled media description lines.
answer	Strips disabled media description lines from answers.
offer	Strips disabled media description lines from offers when used with strip. Pad offers with dummy disabled media description lines when used with pad.
all	Strips all disabled media descriptions from offers.
new	Strips new disabled media descriptions from offers.

Command Default

Pad and do-not-strip are the default behaviors.

Command Modes

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

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.

Examples

The following example shows how to remove disabled media streams in forwarded offers which are new:

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-description disabled strip
offer new
```

The following example shows how to remove all disabled media streams from forwarded offers, whether known to the recipient of the offer or not.

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-description disabled strip
offer all
```

The following example shows how to remove all disabled media streams from forwarded answers.

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-description disabled strip
answer
```

The following example shows how to stop SBC from padding forwarded offers with disabled media streams.

```
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 mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# no caller media-description disabled pad
offer
```

caller media-type

To configure the media address type settings for a caller on the Cisco Unified Border Element (SP Edition), use the **caller media-type** command in the CAC table entry configuration mode. Use the **no** form of this command to disable the media address type settings for a caller.

caller media-type {ipv4 | ipv6 | inherit | both}

no caller media-type {ipv4 | ipv6 | inherit | both}

Syntax Description

ipv4	Only IPv4 media addresses are supported.
ipv6	Only IPv6 media addresses are supported.
inherit	Inherit the supported media IP address type from earlier CAC policy entries (default).
both	Both IPv4 and IPv6 media addresses are supported.

Command Default

Inherit is the default behavior.

Command Modes

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

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 remove disabled media streams in forwarded offers which are new:

```
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 mytable
Router(config-sbc-sbe-cacpolicy)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-type ipv4
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

caller media bypass

To enable or disable the Multiple SBC Media Bypass feature on the caller side, use the **caller media bypass** command in the CAC table entry configuration mode. To deconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

caller media bypass {**enable** | **disable**}

no caller media bypass

Syntax Description

enable	Enables the Multiple SBC Media Bypass feature on the caller side.
disable	Disables the Multiple SBC Media Bypass feature on the caller side.

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 enable the Multiple SBC Media Bypass feature on the caller side:

```
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)# caller media bypass enable
```

Related Commands

Command	Description
cac-table	Configures the admission control tables.
callee media bypass	Enables or disables the Multiple SBC Media Bypass feature on the callee side.
table-type	Configures a CAC table type to enable the priority of the call to be used as a criterion in the CAC policy.

caller port-range-tag

To configure the port range tag for a caller that is used when selecting a media address and port, use the **caller port-range-tag** command in the CAC table entry configuration mode. To deconfigure the port range tag, use the **no** form of this command.

caller port-range-tag {**adj-name** | **none** | **string** *tag-string*}

no caller port-range-tag

Syntax Description

adj-name	Uses the source adjacency name as a port-range tag.
none	Prompts the SBC to not use a port range tag for calls matching the CAC entry, and removes any previously found strings.
string *tag-string*	Specifies the explicit port range tag string.

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 a port-range tag:

```
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)# match SIPIMSAccess
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller port-range-tag adj-name
```

Related Commands

Command	Description
media-address-pool	Adds an IPv4 and IPv6 address to the set of addresses that can be used by the DBE as a local media address.

caller ptime

To configure the packetization time on the caller side, use the **caller ptime** command in the CAC table configuration mode.To deconfigure the packetization time on the caller side, use the **no** form of this command.

caller ptime *0-100*

no caller ptime *0-100*

Syntax Description

0-100	The packetization time in milliseconds (ms).

Command Default

By default, 0 ms is configured. This means that no transrating occurs.

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 that follows shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to configure the packetization time on the caller side using the **caller ptime** command in the CAC table configuration 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)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
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)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller ptime 30
```

Related Commands

Command	Description
callee ptime	Configures the packetization time on the callee side.

caller secure-media

To configure granular-level Secure Media on the caller side, use the **caller secure-media** command in CAC table entry configuration mode. To remove granular-level Secure Media, use the **no caller secure-media** command.

caller secure-media

no caller secure-media

Syntax Description

This command has no arguments or keywords.

Command Default

Granular-level (Unsignaled) Secure Media is disabled by default.

Command Modes

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

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

Restriction—Both caller and callee sides of the call need to be configured. If only one leg of the call has granular secure media configured, then the call will fail.

We recommend you use Unsignaled (also called granular-level) Secure Media configuration because, instead of turning on Secure Media globally, you can specify the calls and adjacencies where you want to use Secure Media.

Examples

The following example shows an Unsignaled Secure Media configuration where the two SIP adjacencies for both legs of the call are configured for “security trusted-unencrypted” and both the caller and callee sides are configured for Secure Media in a CAC table entry:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# adjacency sip server
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table testSecure
Router(config-sbc-sbe-cacpolicy)# cac-table testSecure
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)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller secure-media
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee secure-media
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# cac-policy-set global 1
Router(config-sbc-sbe)# end
```

The following configuration example shows how to configure Unsignaled Secure Media where an adjacency is *untrusted* by using the **transport srtp allowed** command on the untrusted adjacency in a CAC policy table:

```
...
cac-policy-set 2
 first-cac-table 1
 cac-table 1
  table-type limit all
  entry 1
   match-value call-update
   transport srtp allowed
   caller secure-media
   callee secure-media
   action cac-complete
   exit
 complete
 exit
cac-policy-set global 2
```

The following configuration example shows that SIP adjacencies ‘client’ and ‘server’ are configured as “security trusted-unencrypted” and that CAC table entry 1 is configured for Secure Media on both the caller and callee sides:

```
...
cac-policy-set 2
 first-cac-table 1
 cac-table 1
  table-type policy-set
  entry 1
   action cac-complete
   caller secure-media
   callee secure-media
 complete
cac-policy-set global 2

adjacency sip client
 nat force-off
 security trusted-unencrypted
 signaling-address ipv4 10.10.100.110
 signaling-port 9060
 remote-address ipv4 10.10.100.10 255.255.255.255
 signaling-peer 10.10.100.10
 signaling-peer-port 9060
 attach
adjacency sip server
 nat force-off
 security trusted-unencrypted
 signaling-address ipv4 10.10.100.110
 signaling-port 9070
 remote-address ipv4 10.10.100.10 255.255.255.255
 signaling-peer 10.10.100.10
 signaling-peer-port 9070
 attach
```

Related Commands

Command	Description
callee secure-media	Configures granular-level Secure Media on the callee side.
security	Configures transport-level security (TLS) on a SIP adjacency.

call-policy-set default

To activate a default policy set within an signaling border element (SBE) entity, use the **call-policy-set default** command in **the SBE** configuration mode. To deactivate a default policy set, use the **no** form of this command.

call-policy-set default *policy-set-id* [**priority** *priority-value*]

no call-policy-set default

Syntax Description

policy-set-id	The integer, ranging from 1 to 2147483647, that identifies a default call policy set.
priority	Specifies the priority for the administrative domains that are not configured.
priority-id	The priority value, ranging from 1 to 10, with 10 indicating the highest priority. By default, 6 is the priority value given to the policy set.

Command Default

No default behavior or values are available.

Command Modes

SBE configuration (config-sbc-sbe)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It replaces the **call-policy-set default** command.

Usage Guidelines

If another policy set was previously active, it is made inactive by executing this command. The SBE is created with no active routing policy set; an active routing policy set must be explicitly configured using 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 example shows how to set policy set 1 as the default on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# call-policy-set default 1 priority 9
```

Related Commands

Command	Description
call-policy-set	Creates a new policy set on the session border controller (SBC).
first-inbound-na-table	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
first-outbound-na-table	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
show sbc sbe call-policy-set	Lists the details of the policy sets configured on the SBC.
show sbc sbe call-policy-set default	Lists the summary of the default policy set configured on the SBC.

category (NA-)

To configure the entry category in the number analysis table with entries of the table matching a part of or the whole dialed number, use the **category** command in the NA routing table configuration mode. To deconfigure the category of an entry, use the **no** form of this command.

category *category-name*

no category *category-name*

Syntax Description

category-name	Specifies a category to assign to the event. The *category-name* 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

NA routing table configuration (config-sbc-sbe-rtgpolicy-natable)

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 category of entry 1 in the new number analysis table MyNaTable matching the whole number:

```
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-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# category external
Router(config-sbc-sbe-rtgpolicy-natable-entry)# exit
Router(config-sbc-sbe-rtgpolicy-natable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)#
```

cause

To configure the cause, sub-cause, status-code, and reason of an internal error for an error profile, use the **cause** command in error profile configuration mode. To remove the cause, use the no form of this command.

cause *cause* [**sub-cause** *sub-cause*] **status-code** *status-code* [**reason** *reason*]

no cause *cause* [**sub-cause** *sub-cause*] **status-code** *status-code* [**reason** *reason*]

Syntax Description

cause	Cause of the error. For a list of the causes, use the question mark (?) online help function. The following causes are currently available: • **cac-in-call-msg-rate**—cac: The rate of mid-call messages has exceeded a maximum configured limit • **cac-max-bandwidth**—cac: The bandwidth used has exceeded a maximum configured limit • **cac-max-call-rate**—cac: Call setup rate exceeded a maximum configured limit • **cac-max-channels**—cac: The number of media channels used has exceeded a maximum limit • **cac-max-num-calls**—cac: The number of calls has exceeded a maximum limit • **cac-max-reg**—cac: The number of registrations has exceeded a maximum configured limit • **cac-max-reg-rate**—cac: The rate of registrations has exceeded a maximum configured limit • **cac-max-updates**—cac: The number of call updates has exceeded the configured limit • **cac-out-call-msg-rate**—cac: The rate of out of dialogue messages has exceeded a maximum configured limit • **cac-rtp-disallowed**—cac: Disallowing rtp caused the call to fail • **cac-srtp-disallowed**—cac: Disallowing srtp caused the call to fail • **cac-srtp-rtp-interwork**—cac: call failed due to srtp to rtp interworking disallowed • **enum-failure**—ENUM processing encountered an error • **max-media-streams**—An offer cannot be reduced to meet the maximum number of media streams • **mg-srtp-unsupported**—No MG was found which can support srtp • **na-invalid-address**—na: Number validation failure • **no-acceptable-codec**—No acceptable codec can be found for an offer • **rtg-max-routes-tried**—rtg: The maximum number of routing attempts exceeded • **rtg-no-route-found**—rtg: Routing failed to find a route • **rtg-route-unavailable**—rtg: The route selected by call-policy is unavailable

- **srtp-general-error**—srtp general error
- **sub-media-bearer-chan-fail**—subscriber media bearer channel has failed mid-call
- **sub-media-bearer-chan-rej**—subscriber media bearer channel has rejected during setup or renegotiation
- **sub-sig-bearer-chan-fail**—subscriber signaling bearer channel is unavailable

sub-cause

(Optional) Sub cause of the error. To see the list of the available sub-causes for a specific cause, use the question mark (?) online help function after you have selected the cause. The following list shows all available sub-causes:

- **na-dst-number**—Destination number based analysis
- **na-src-adjacency**—Source adjacency based analysis
- **na-src-account**—Source account based analysis
- **na-sub-category**—Subscriber category based analysis
- **na-carrier-id**—Carrier identification code based analysis
- **na-src-number**—Source number based analysis
- **na-no-src-number**—No source number present for source number based analysis
- **rtg-src-address**—Source address based routing
- **rtg-dst-address**—Destination address based routing
- **rtg-src-adjacency**—Source adjacency based routing
- **rtg-src-account**—Source account based routing
- **rtg-category**—Category based routing
- **rtg-sub-category**—Subscriber category based routing
- **rtg-src-domain**—Source domain based routing
- **rtg-dst-domain**—Destination domain based routing
- **rtg-time**—Time based routing
- **rtg-dst-tgid**—Destination trunk group Identifier based routing
- **rtg-src-tgid**—Source trunk group identifier based routing
- **rtg-carrier-id**—Carrier identification code based routing
- **rtg-round-robin**—Round robin based routing
- **rtg-least-cost**—Least cost based routing
- **cac-unknown**—Unknown call admission control error
- **cac-per-call-scope**—Call admission control call scope error
- **cac-src-number-scope**—Call admission control source number scope error
- **cac-downstream-scope**—Call admission control downstream scope attribute error
- **cac-upstream-scope**—Call admission control upstream scope attribute error
- **sub-rx-reg-bearer-loss**—Failed to route to a subscriber because the Rx session for the subscriber registration suffered loss of bearer

	• **sub-rx-reg-bearer-rel**—Failed to route to a subscriber because the rx session for the subscriber registration suffered release of bearer • **sub-rx-reg-bearer-term**—Failed to route to a subscriber because the rx session for the subscriber registration was terminated • **sub-rx-media-policy-rej**—Rx session for a call was rejected for policy reasons (for example, unsupported media) • **sub-rx-media-error**—Rx session for a call was rejected for non-policy reasons (for example, service unavailable) • **sub-rx-reg-bearer-loss**—Rx session for a call suffered loss of bearer • **sub-rx-reg-bearer-rel**—Rx session for a call suffered release of bearer • **sub-rx-reg-bearer-term**—Rx session for a call was terminated • **enum-resource**—enum - encountered a resource shortage • **enum-dst-not-number**—enum - destination address which was not a telephone number • **enum-unknown-number**—enum - unable to resolve a telephone number • **enum-interface-failure**—enum - failed in the enum interface • **enum-regex-error**—enum - failed because a regex in a NAPTR record was invalid
status-code	Maps a SIP status-code to the selected cause/sub-cause. The SIP status-code numbers range from 400 to 699.
reason	(Optional) The reason that the error occurred. The reason allows system administrators to optionally configure a SIP "Reason:" header, which is inserted into the error response and displayed when an error occurs. The configured reason header must conform to the syntax rules defined in RFC 3326.

Command Default No default behavior or values are available.

Command Modes Error profile configuration (config-sbc-sbe-sip-err)

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 cause of an internal error for an error profile:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip error-profile Error_profile_1
Router(config-sbc-sbe-sip-err)# cause rtg-no-route-found sub-cause rtg-src-adjacency
status-code 604 reason "SBC: No route found based on src adjacency"
Router(config-sbc-sbe-sip-err)#
```

Related Commands

Command	Description
error-profile	Configures an existing error profile as the outbound SIP error profile.
sip error-profile	Creates an error profile and enters error profile configuration mode.
cause	Configures the cause of an internal error for an error profile.
show sbc sbe sip error-profile	Displays the configuration information of an error profile.

cdr

To add media information or endpoint information of a call to a billing record, use the **cdr** command in SBE billing configuration mode. To disable adding media information or endpoint information to billing records, use the **no** form of this command.

cdr {media-info | endpoint-info {addressing | adjacency}}

no cdr {media-info | endpoint-info {addressing | adjacency}}

Syntax Description

media-info	Adds media information to billing records.
endpoint-info	Adds endpoint information to billing records
addressing	Adds address information and adjacency name to billing records in the format *IP address,port,transport type,adjacency name.* (For example, *2.0.0.36,5078,UDP,SIPPB)*
adjacency	Adds adjacency names to billing records.

Command Default

By default, the media information and the adjacency names are not included in the call details records.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 2.5	Call details record CLI with **media-info** key word was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.6.1	The **adj-info** keyword was added.
Cisco IOS XE Release 2.6.2	The **adj-info** keyword was removed. The **endpoint-info**, **addressing**, and **adjacency** keywords were added.

Usage Guidelines

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

Examples

The following example shows how to add media information to a billing record:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# cdr media-info
Router(config-sbc-sbe-billing)# end
```

The following example shows how to include endpoint addressing information to a billing record:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# cdr endpoint-info addressing
Router(config-sbc-sbe-billing)# end
Router#
```

Related Commands

Command	Description
billing	Configures billing.
method packetcable-em	Enables the packet-cable billing method.
packetcable-em *transport radius*	Configures a packet-cable billing instance.
show sbc sbe billing instance	Displays whether media creation information and endpoint information are included in the billing records for a specific billing instance.

cdr alarm (XML Billing)

To configure the free disk space sizes, which, when exceeded, should generate, different types of alarms, use the **cdr alarm** command in SBE billing XML configuration mode. To disable the configuration of free disk space sizes, use the **no** form of this command.

cdr alarm {critical | major | minor} *kilobytes*

no cdr alarm [critical | major | minor]

Syntax Description

critical	Configures a critical alarm if the free disk space is less than the configured size in kilobytes.
major	Configures a major alarm if the free disk space is less than the configured size in kilobytes.
minor	Configures a minor alarm if the free disk space is less than the configured size in kilobytes.
kilobytes	The free disk space size, which, if exceeded, will trigger a critical, major or minor alarm. The default value for a critical alarm is 100 MB, a major alarm is 500 MB, and a minor alarm is 1 GB.

Command Default

By default, the free disk space alarm size that is set for a critical alarm is 100 MB, a major alarm is 500 MB, and a minor alarm is 1 GB.

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

To inform the administrator for freeing disk space to store the XML billing records, the CDR alarm feature has been introduced. If there are too many calls, the free disk space available to store the XML billing records might be less. However, even if there is no space on the local machine, the calls will be active, although, because of non availability of disk space, the calls may not be billed.

To avoid such a situation, alarms must be configured using the **cdr alarm** command. Based on the free disk space size configured, minor, major, or critical alarms are generated.

Examples

The following example shows how to configure a minor alarm for free disk space less than 800 MB:

```
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)# cdr alarm minor 800
```

The following example shows how to configure a major alarm for free disk space less than 600 MB:

```
Router(config-sbc-sce-billing-xml)# cdr alarm major 600
```

The following example shows how to configure a major alarm for free disk space less than 200 MB:

```
Router(config-sbc-sce-billing-xml)# cdr alarm critical 200
```

Related Commands

Command	Description
xml (billing)	Configures the method index for XML billing.
method xml	Configures the billing method as XML for the Billing Manager.
ldr-check	Configures the time at which long duration records are checked.

cdr path

To store the CDR XML billing records on the local machine (Cisco ASR 1000 Series Router), use the **cdr path** *path* command in the SBE billing XML configuration mode. To disable the cdr path, use the **no** form of this command.

cdr path *path*

no cdr path

Syntax Description

path	Indicates the path in which to store the XML billing records locally on the Cisco ASR 1000 Series Router. The maximum length of the path is 128 bytes, and the directory should not be a root directory. The valid options to set CDR path are harddisk:, usb0:, and usb1:.

Command Default

No default behavior or values

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

To store the XML billing records on the local machine (Cisco ASR 1000 Series Router), set the path using the **cdr path** *path* command from the SBE billing XML configuration mode. The maximum length of path is 128 bytes, and the directory should not be a root directory. Moreover, before the path is defined using the **cdr path** command, ensure that a directory has been created using the **mkdir** command from Privilege EXEC mode. The valid options to store the XML billing records are: harddisk:, usb0, and usb1:.

Examples

The following example shows how to define the path to store the XML billing records on the Cisco ASR 1000 Series Router:

```
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)# cdr path harddisk:cdrbilling
```

Related Commands

Command	Description
xml (billing)	Configures the method index for XML billing.

Command	Description
method xml	Configures the billing method as XML for the Billing Manager.
ldr-check	Configures the time at which long duration records are checked.

clear platform hardware qfp active feature sbc sfx

To clear the Cisco QuantumFlow Processor SIP Fast-Register (SFX) counters, use the **clear platform hardware qfp active feature sbc sfx** command in Exec mode.

clear platform hardware qfp active feature sbc sfx [global]

Syntax Description

global	Specifies SIP Fast-Register (SFX) global state information.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example clears information about the parsing of SIP fast-register (SFX) messages in the Cisco QuantumFlow Processor (QFP):

```
Router# clear platform hardware qfp active feature sbc sfx global
```

Related Commands

Command	Description
show platform hardware qfp active feature sbc sfx	Displays information about SFX messages in Cisco QFP.

clear platform software wccp

To clear Web Cache Communication Protocol version 2 statistics on the Cisco ASR 1000 Series Routers, use the **clear platform software wccp** command in privileged EXEC mode.

clear platform software wccp {*slot* [**active** | **standby**] **statistics**} | {**counters** | **statistics**}

Syntax Description

slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot. Valid options are: • **F0**—Embedded Service Processor slot 0 • **F1**—Embedded Service Processor slot 1 • **FP**—Embedded Service Processor • **R0**—Route Processor slot 0 • **R1**—Route Processor slot 1 • **RP**—Route Processor
active	Clears active instances.
standby	Clears standby instances.
statistics	Clears statistics counters.
counters	Clears packet processing counters.

Command Default

WCCPv2 statistics are not cleared.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to clear WCCPv2 statistics on Embedded-Service-Processor slot 0:

```
Router# clear platform software wccp F0 statistics
```

Related Commands

Command	Description
clear ip wccp	Removes WCCP statistics (counts) maintained on the router for a particular service.

clear sbc

To clear a data border element (DBE), redundancy group, or signaling border element (SBE) information, use the **clear sbc** command in Privileged EXEC mode.

clear sbc *sbc-name* **{dbe | rg | sbe}**

Syntax Description

sbc-name	The name of the Session Border Controller (SBC) service.
dbe	Clears DBE information.
rg	Clears redundancy group statistics. The SBC redundancy group creates and transports establishment.
sbe	Clears SBE information.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

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	The keyword **rg** was added to this command.

Examples

The following example shows how to clear the DBE configuration:

```
Router# clear sbc mySbc dbe
```

clear sbc dbe media-stats (session border controller)

To clears all the statistics collected by the media gateway manager of the DBE, use the **clear sbc dbe media-stats** command in Exec mode.

clear sbc *sbc-name* **dbe media-stats**

Syntax Description

sbc-name	Name of the SBC service.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command clears the statistics displayed by the **show sbc dbe media-stats** command.

Examples

The following example clears all the statistics collected by the media gateway manager of a DBE on an SBC called mySbc:

```
Router(config)# clear sbc mySbc dbe media-stats
```

Related Commands

Command	Description
show sbc dbe media-stats	Lists the statistics of one or more media flows collected on the DBE.

clear sbc h248 bac

To clear the information pertaining to the Session Border Controller (SBC) H.248 Border Access Controller-related call context sessions, use the **clear sbc h248 bac** command in the privileged EXEC mode.

clear sbc h248 bac {**context- sessions** [**correlator** *context-correlator*} | {**iad-sessions** [**correlator** *iad-correlator*]}

Syntax Description

context-sessions	Clears the information pertaining to the SBC H.248 Border Access Controller (BAC) call context sessions.
correlator	Clears an SBC H.248 BAC call context session along with the specific context correlator.
context-correlator	Number of the context session correlator. Range: 1 to 4294967295.
iad-sessions	Clears the information pertaining to the SBC H.248 BAC Integrated Access Device (IAD) registry sessions.
correlator	Clears an SBC H.248 BAC IAD session along with the specific IAD correlator.
iad-correlator	Number of the IAD session correlator. Range: 0 to 4294967295.

Command Modes

Privileged EXEC (#)

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

There is no **no** form of this command.

Examples

The following example shows how to clear the information pertaining to the SBC H.248 BAC context sessions:

```
Router> enable
Router# clear sbc h248 bac context-sessions
```

clear sbc sbe adjacency statistics

To clear the SIP method statistics counters and reset them to zero, use the **clear sbc sbe adjacency statistics** command in Privileged EXEC mode.

clear sbc *sbc-name* **sbe adjacency** *adj-name* **adjacency**

Syntax Description

sbc-name	Specifies the name of the SBC service.
adj-name	Specifies the name of the adjacency.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command clears request and response counters that are displayed in the output of the **show sbc sbe sip-method-stats** command.

Examples

The following example clears the SIP method statistics counters for the sipGW adjacency:

```
Router# clear sbc mySbc sbe adjacency sipGW statistics
```

Related Commands

Command	Description
show sbc sbe sip-method-stats	Displays summary or detailed statistics for a SIP method.
statistics-setting	Configures an adjacency to support SIP method statistics.

clear sbc sbe blacklist

To clear the blacklist for the specified Session Border Controller (SBC) service, use the **clear sbc sbe blacklist** command in privileged EXEC mode.

clear sbc *sbc-name* **sbe blacklist [critical]** {**WORD**}[**ipv4** addr [{udp | tcp} port]]

clear sbc *sbc-name* **sbe blacklist [critical]** {**ipv4** *addr* | **ipv6** *addr*} [{udp | tcp} port]

Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.
critical	Allows you to clear critical blacklists.
WORD	Specifies the VPN ID for which you want to clear critical blacklisting information.
ipv4 *addr*	Clears configured critical blacklisting for a single IPv4 address.
tcp	Clear blacklisting for TCP protocol only.
udp	Clear blacklisting for UDP protocol only.
ipv6 addr	Clears configured blacklisting for a single IPv6 address.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

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 2.4.2	The **critical** keyword and **critical** options were added.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added.

Examples

The following example clears all the blacklists for the TCP port 1 for VRF test for the ipv4 address of 2.2.2.2:

```
Router# clear sbc aa sbe blacklist test ipv4 2.2.2.2 tcp 1
```

Related Commands

Command	Description
blacklist	Enter the mode for configuring the event limits of a given source.

clear sbc sbe cac-policy-set-stats

To clear all the call admission control (CAC) policy statistics, use the **clear sbc sbe cac-policy-set-stats** command in the Privileged EXEC mode.

clear sbc ***sbc-name*** **sbe cac-policy-set-stats** [**all** | **policy-set** *cac-policy-number*]

Syntax Description

sbc-name	Name of the SBC service.
all	Clears all the CAC policy set statistics.
policy-set	Clears the CAC statistics pertaining to the specified policy set number.
cac-policy-number	CAC policy set number that can range from 1 to 2147483647.

Command Default

By default, the **all** keyword is used.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.3S	This command was modified. The **all** and **policy-set** keywords and the *cac-policy-number* argument were added.

Examples

The following example shows how to clear all the CAC policy statistics in SBC global:

```
Router# clear sbc global sbe cac-policy-set-stats
```

The following example shows how to clear the CAC policy statistics for the CAC policy set number 21:

```
Router# clear sbc global sbe cac-policy-set-stats policy-set 21
```

clear sbc sbe cac-rejection-stats

To clear all the call admission control policy rejection statistics, use the **clear sbc sbe cac-rejection-stats** command in privileged EXEC mode.

clear sbc *sbc-name* ***sbe cac-rejection-stats***

Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example clears all the call admission control policy rejection statistics for the SBE mysbc:

```
Router# clear sbc mySbc sbe cac-rejection-stats
```

clear sbc sbe call-policy-set-stats

To clear call policy set statistics, use the **clear sbc sbe call-policy-set-stats** command in privileged EXEC mode.

clear sbc *sbc-name* sbe call-policy-set-stats [all | na | rtg]

Syntax Description

sbc-name	Specifies the name of the SBC service.
all	Clears all policy routing rejection statistics.
na	Clears all policy number analysis rejection statistics.
rtg	Clears call policy routing rejection statistics.

Command Default

By default, clears **all** policy routing rejection statistics.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following examples shows how to clear policy number analysis rejection statistics in sbc “global”:

```
Router# clear sbc global sbe call-policy-stats na
```

clear sbc sbe call-rate-stats

To clear all the call rate statistics, use the **clear sbc sbe call-rate-stats** command in privileged EXEC mode.

clear sbc *sbc-name* ***sbe call-rate-stats***

Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example clears all the call rate statistics for the SBE mysbc:

```
Router# clear sbc mySbc sbe call-rate-stats
```

clear sbc sbe call-rejection-stats

To clear all the call admission control policy rejection statistics, use the **clear sbc sbe call-rejection-stats** command in privileged EXEC mode.

clear sbc *sbc-name* ***sbe call-rejection-stats***

Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example clears all the call admission control policy rejection statistics for the SBE mysbc:

```
Router# clear sbc mySbc sbe call-rejection-stats
```

clear sbc sbe call-stats

To clear the call statistics on the SBE, use the **clear sbc sbe call-stats** command in the privileged EXEC mode.

clear sbc *sbc-name* ***sbe call-stats [all | dst-account*** *account-name* **|** ***dst-adjacency*** *adjacency-name* **|** ***global* | *src-account*** *account-name* **|** ***src-adjacency*** *adjacency-name* **| per-adjacency** *adjacency-name*] [**all** | **current-indefinite**]

clear sbc *sbc-name* ***sbe call-stats*** **reject-threshold memory**

Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.
account-name	Name of the source or destination account.
adjacency-name	Name of the source or destination adjacency.
all	Clears all the call statistics.
dst-account	Clears the statistics pertaining to a destination account.
dst-adjacency	Clears the statistics pertaining to a destination adjacency.
global	Clears the global call statistics.
per-adjacency	Clears the statistics pertaining to a per adjacency. • **all**—Clears the statistics for all the summary periods. • **current-indefinite**—Clears the statistics for only the current indefinite period.
reject-threshold	Clears the statistics related to reject threshold.
memory	Clears the statistics related to call denials because of low memory.
src-account	Clears the statistics pertaining to a source account.
src-adjacency	Clear the statistics pertaining to a source adjacency.

Command Default

By default, the **all** keyword is used.

Command Modes

Privileged EXEC (#)

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 3.3S	This command was modified. The **per-adjacency** keyword and the *currentindefinite* parameter were added to the command.

Examples

The following example shows how to clear all the call statistics pertaining to the mysbc SBE:

Router# **clear sbc mysbc sbe call-stats**

The following example shows how to clear the call statistics pertaining to the current indefinite period for the mysbc SBC:

```
Router# clear sbc mysbc sbe call-stats global current-indefinite
```

clear sbc sbe call

To clear an identified call, use the **clear sbc sbe call** command in privileged EXEC mode.

clear sbc *sbc-name* **sbe call {***0-2147483647***}**

Syntax Description

sbc-name	Specifies the name of the SBC service.
0-2147483647	Specifies the call index number that is to be cleared.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following examples shows how to display calls on the global SBC service; how to clear specified call number 1; and how to show that call number 1 has been cleared:

```
Router# show sbc global sbe calls

SBC Service "global"
  Call           State        Type          Src Adjacency        Dest Adjacency
  ------------------------------------------------------------------------------
    1             Active      Audio         glophone             registrar

Router#
Router#
Router# clear sbc global sbe call 1
Router#

Router# show sbc global sbe calls

SBC Service "global"
  Call           State        Type          Src Adjacency        Dest Adjacency
  ------------------------------------------------------------------------------
No call information found.

Router#
```

clear sbc sbe policy-failure-stats

To clear all the policy failure statistics of all adjacencies and accounts, **use the clear sbc sbe policy-failure-stats command in** privileged EXEC **mode.**

clear sbc *sbc-name* **sbe policy-failure-stats [src-adjacency | src-account | dst-adjacency | dst-sccount]** *name*

Syntax Description

sbc-name	Specifies the name of the Session Border Controller (SBC) service.
src-adjacency	(Optional) Clears statistic for a source adjacency.
src-account	(Optional) Clears statistic for a source account.
dst-adjacency	(Optional) Clears statistic for a destination adjacency.
dst-account	(Optional) Clears statistic for a destination account.
name	Specifies the adjacency name or the account name.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to clear all of the policy failure statistics for an adjacency named YY:

```
Router# clear sbc mysbc sbe policy-failure-stats src-adjacency YY
```

clear sbc sbe policy-rejection-stats

To clear all the policy rejection statistics by the SBE, use the **clear sbc sbe policy-rejection-stats** command in privileged EXEC mode.

clear sbc *sbc-name* ***sbe policy-rejection-stats***

Syntax Description

sbc-name	Specifies the name of the Session Border Controller (SBC) service.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

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

This clears all recorded policy rejection stats including the current and previous intervals.

Examples

The following example clears all the policy rejection statistics by the SBE.

```
Router# clear sbc mySbc sbe policy-rejection-stats
```

clear sbc sbe radius-client-stats

To clear all the statistics for the local RADIUS clients, use the **clear sbc sbe radius-client-stats** command in privileged EXEC mode.

clear sbc *sbc-name* ***sbe radius-client-stats {accounting*** *word* **| authentication}***

Syntax Description

sbc-name	Specifies the name of the Session Border Controller (SBC) service.
word	The RADIUS client name. The maximum size is 80 characters.
accounting	Clears accounting client statistics.
authentication	Clears authentication client statistics.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example clears all the authentication statistics:

```
Router# clear sbc mySbc sbe radius-client-stats authentication
```

The following example clears all the accounting statistics for the local RADIUS client, radius1:

```
Router# clear sbc mySbc sbe radius-client-stats accounting radius1
```

clear sbc sbe radius-client

To clear all the statistics for the specified RADIUS server, use the **clear sbc sbe radius-client** command in privileged EXEC mode.

clear sbc *sbc-name* ***sbe radius-client {accounting*** *word* **| *authentication* | *radius-server-stats*** *word}*

Syntax Description

sbc-name	Specifies the name of the Session Border Controller (SBC) service.
accounting	Clears accounting client statistics.
authentication	Clears authentication client statistics.
radius-server-stats	Identifies the RADIUS server name.
word	For **accounting**, the RADIUS client name. The maximum size is 80 characters. For **radius-server-stats**, the RADIUS server name. The maximum size is 80 characters.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example clears all the authentication statistics for the RADIUS server called svr:

Router# **clear sbc mySbc sbe radius-client authentication radius-server-stats svr**

The following example clears all the accounting client statistics for the local RADIUS client, acc, for the RADIUS server svr:

```
Router# clear sbc mySbc sbe radius-client accounting acc radius-server-stats svr
```

clear sbc sbe script-set-stats

To clear the stored statistics related to a script set, use the **clear sbc sbe script-set-stats** command in the privileged EXEC mode.

clear sbc *sbc-name* **sbe script-set-stats** *script-set-number* **[editors-stats** *editor-name***]**

Syntax Description

sbc-name	Name of the SBC.
script-set-number	Script set number. The range is from 1 to 2147483647.
editor-stats	Specifies that the script-set statistics must be cleared for a specific editor.
editor-name	Name of the editor.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

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

These statistics cleared by this command are the same as those displayed when you run the **show sbc sbe script-set** command.

Examples

In the following example, the **clear sbc sbe script-set-stats** command is used to clear stored statistics related to script set 10.

```
Router# clear sbc mySbc sbe script-set-stats 10
```

Related Commands

Command	Description
active-script-set	Activates 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.
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.

Command	Description
filename	Specifies the path and name of the script file written using the Lua programming language.
load-order	Specifies the load order of a script in a script set.
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.

clear sbc sbe sip statistics

To clear aggregated SIP statistics handled by the Cisco Unified Border Element (SP Edition) process on the Cisco ASR 1000 Series Routers, use the **clear sbc sbe sip statistics** command in Privileged EXEC mode.

clear sbc ***service-name*** **sbe {sip statistics [global | adjacency** *adj-name* **method] blacklist | cac-policy-set-stats | call-policy-set-stats [all | na | rtg] call-stats {global | all | src-account** *name* **| dst-account** *name* **| src-adjacency** *name* **| dst-adjacency** *name***} | radius-client | radius-client-stats }**

Syntax Description

service-name	Name of the Session Border Controller (SBC) service.
adj-name	Name of the adjacency.
name	Name of the account for which you would like to display statistics. The maximum length of this value is 30 characters.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	Added new parameters to the command.

Usage Guidelines

This command resets to zero all the packet counters of SIP statistics aggregated by the SBC.

Examples

The following example resets to zero the packet counters of SIP statistics aggregated by the Cisco Unified Border Element (SP Edition) process on the Cisco ASR 1000 Series Routers:

```
Router# clear sbc global sbe sip statistics
```

Related Commands

Command	Description
show sbc sbe sip statistics	Displays the aggregated SIP statistics handled by the Cisco Unified Border Element (SP Edition).

clear sbc sbe sip subscriber aor

To clear the stuck registrations, use the **clear sbc sbe sip subscriber aor** command in privileged EXEC mode.

clear sbc *sbc-name* **sbe sip subscriber aor** *address-of-record*

Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.
address-of-record	Subscriber's Address of Record.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

To use this command, you must know the corresponding subscriber's Address of Record (AOR). The **show sbc sbe sip subscribers** command displays the details of all the Session Initiation Protocol (SIP) endpoints that have been registered with the SBC, including the AOR for each subscriber.

Examples

The following example shows how the **clear sbc sbe sip subscriber aor** command is used to clear the stuck registrations in the privileged EXEC mode:

```
Router# clear sbc asr sbe sip subscriber aor sip:alice@open-ims.test
```

Related Commands

Command	Description
show sbc sbe sip subscribers	Displays the details of all the SIP endpoints that have been registered with the SBC.

clear sbc sbe statistics

To clear the summary statistics and the detailed response code statistics, use the **clear sbc sbe statistics** command in privileged EXEC mode.

clear sbc *sbc-name* ***sbe*** *adj-name* ***statistics***

Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.
adj-name	Name of the RADIUS client. The maximum size is 80 characters.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example clears all summary statistics and the detailed response code statistics:

```
Router# clear sbc mySbc sbe ttt statistics
```

clear sbc sbe transcoding-stats

To clear the transcoding-related statistics, use the **clear sbc sbe transcoding-stats** command in the Privileged EXEC mode.

clear sbc *sbc-name* **sbe transcoding-stats** [**adjacency** *adjacency-name* | **global**] [**all** | **currentindefinite**]

Syntax Description

sbc-name	Name of the SBC service.
adjacency	Clears the statistics pertaining to the specified adjacency.
adjacency-name	Name of the specified adjacency.
global	Clears the transcoding-related statistics globally.
all	Clears statistics pertaining to all the summary periods.
currentindefinite	Clears statistics pertaining to only the current indefinite period.

Command Default

No default behavior or values are available.

Command Modes

Privileged EXEC (#)

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.

Examples

The following example shows how to clear the voice transcoding-related statistics pertaining to the SIPP1 adjacency for the current indefinite period:

```
Router# clear sbc mySBC sbe transcoding-stats adjacency SIPP1 currentindefinite
```

Related Commands

Command	Description
show sbc sbe transcoding-stats	Displays the voice transcoding-related statistics.

codec-list description

To provide a description of a codec list, use the **codec-list description** command in codec list configuration mode. To delete the description for the codec list, use the **no** form of this command.

codec-list description *text*

no description

Syntax Description

text	An arbitrary text string that describes the codec list. The *text* field 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

Codec list (sbe-codec-list)

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 provide the my_codecs codec list with a description (Legitimate codecs):

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
Router(config-sbc-sbe-codec-list)# codec-list description Legitimate codecs
```

codec-preference-list

To configure the CAC to add preference to a codec list, use the **codec-preference-list** command in CAC table entry configuration mode. To remove the preference on the codeclist, use the **no** form of this command.

codec-preference-list *list-name*

no codec-preference-list *list-name*

Syntax Description

list-name	Specifies the name of the codec list.

Command Default

Default codec preference priority is 100.

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

Not setting this command, or issuing the **no** form of the command, means that the CAC entry does not impose any restriction on the codecs that can be used (but also it does not lift any restrictions set by entries encountered earlier).

Examples

The following command configures the entry to restrict codecs to those named on the list my_codecs:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table Mycactable
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)# codec-preference-list my_codecs
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

codec-restrict-to-list

To configure the CAC to restrict the codecs used in signaling a call to the set of codecs given in the named list, use the **codec-restrict-to-list** command in CAC table entry configuration mode. To impose no restrictions on the codecs that can be used with the CAC entry, use the **no** form of this command.

codec-restrict-to-list *list-name*

no codec-restrict-to-list *list-name*

Syntax Description

list-name	Specifies the name of the codec list.

Command Default

Not setting this command, or issuing the **no** form of the command, means that the CAC entry does not impose any restriction on the codecs that can be used (but also it does not lift any restrictions set by entries encountered earlier).

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

For each codec on this list, CAC restricts the packetization period for any stream using that codec to be greater than or equal to the packetization period configured along with that codec in the list. If a stream uses more than one codec in the list, the greater of all the packetization periods configured for each codec in the list is applied to the stream.

If the codec list is empty, all codecs recognized by the SBE will be allowed.

To clear all restrictions set by an earlier CAC entry, you must configure a **codec-restrict-to-list** *list-name*, where *list-name* is the name of a list containing no codecs.

You are not allowed to use this command if the table is part of the active policy set. You can only configure the **codec-restrict-to-list** command at per-call scope. If it is configured at any other scope, an error will be flagged when you type “complete” in the CAC policy set configuration.

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 entry to restrict codecs to those named on the list my_codecs:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table Mycactable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
```

```
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable)# cac-scope dst-adjacency
Router(config-sbc-sbe-cacpolicy-cactable-entry)# codec-restrict-to-list my_codecs
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)# exit
```

codec

To add a codec to a codec list, use the **codec** command in the Codec list configuration mode. To remove a named codec from a codec list, use the **no** form of this command.

codec *codec-name*

no codec *codec-name*

Syntax Description

codec-name	Name of a codec. This value must be one of the list of codecs that the SBE is hard-coded to recognize. Otherwise, when you execute this command, the SBE displays an error. The format of the codec name is the same as the string used to represent it in Session Description Protocol (SDP). For example, PCMU or VDVI. A codec can only be added to each list one time.

Command Default

No default behavior or values are available.

Command Modes

Codec list (sbe-codec-list)

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 assign the PCMU codec to the my_codecs codec list:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
Router(config-sbc-sbe-codec-list)# codec PCMU
```

codecs

To configure the codecs supported by the media gateway, use the **codecs** command in media gateway configuration mode. To set the codec support to nothing, use the **no** form of this command.

codecs *codec-list*

no codecs

Syntax Description

codec-list	Specifies the supported codecs.

Command Default

No default behavior or values are available.

Command Modes

Media gateway configuration (config-sbc-sbe-mg)

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 media gateway 10.0.0.1's supported codecs to *m=audio 6000 RTP/AVP 4* and *a=rtpmap:0 PCMU/8000* (as defined in RFC 1890):

```
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)# codecs m=audio 1234 RTP/AVP 0 18,a=rtpmap:=rtpmap:18 G729/80000
PCMU/8000,a=rtpmap:18 G729/8000
```

codec custom

To configure or modify an existing hard coded codec, use the **codec custom** command in the config sbc sbe configuration mode. To delete a new codec or to restore a custom codec, use the **no** form of this command.

codec custom *custom-name id payload id*

no ***codec custom*** *custom-name id payload id*

Syntax Description

custom-name	Unique name for the custom codec. This name is case insensitive and can contain a maximum of 30 characters.
payload id	Static payload id. The range is from 0 to 96.

Command Default

No default value.

Command Modes

Configure SBC SBE (config-sbc-sbe)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The following table contains details of the modes:

Mode	Values	Default Value
media	AUDIO, VIDEO, APPLICATION, DATA, CONTROL, IMAGE, OMIT, TEL-EVENT	AUDIO
rate (in Hz)	1–2147483647	8000
packet-time	1–65535	10
bandwidth	1–9223372036854775807	64000
sample-size	0–255	8
channels	0–255	1
max-frames-per-packet	0–65535	1
options	none, transrate, transcode	none
codec-type	fixed, sampling, format, variable, redundancy	N/A, mandatory

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

Examples

The following example shows how to define a custom codec from a codec hardcoded in SBC:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec custom G726-40-4 id 4
Router(config-sbc-sbe-codec-def)# rate 64000
Router(config-sbc-sbe-codec-def)# packet time 100
Router(config-sbc-sbe-codec-def)# bandwidth 128000
Router(config-sbc-sbe-codec-def)# sample size 4
Router(config-sbc-sbe-codec-def)# channels 16
Router(config-sbc-sbe-codec-def)# max-frames-per-packet 12
Router(config-sbc-sbe-codec-def)# media video
Router(config-sbc-sbe-codec-def)# options transcode
Router(config-sbc-sbe-codec-def)# type sampling
```

codec list

To create a codec list, use the **codec list** command in the signaling border element (SBE) configuration mode. To delete a codec list, use the **no** form of this command.

codec list *list-name*

no codec list *list-name*

Syntax Description

list-name	The name of the codec list. The *list-name* 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 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 a mode to create a codec list using the name my_codecs:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
```

Related Commands

Command	Description
codec packetization-period	Sets a minimum packetization period for a codec.
policy	Configures the packetization period policy.

codec packetization-period

To set a minimum packetization period for a codec, use the **codec packetization-period** command in the codec list configuration mode. To remove a packetization period from a codec, use the **no** form of this command.

codec *codec-name* **packetization-period** *packet-period* **[priority** *priority-value***]**

no codec *codec-name* **packetization-period** *packet-period* **[priority** *priority-value***]**

Syntax Description

codec-name	The name of a codec. This value must be taken from the list of codecs that the signaling border element (SBE) is hard-coded to recognize. Otherwise, when you execute this command, the SBE displays an error. The format of the codec name is the same as the string used to represent it in Session Description Protocol (SDP), for example, PCMU, or VDVI.
packet-period	The minimum acceptable packetization period in milliseconds as indicated by **packetization-period**. For example, **codec PCMU packetization-period 20** adds the codec PCMU to the list with a minimum acceptable packetization period of 20 ms. The range of packetization period is 0 to 1000.
priority	Specifies the priority used for reordering purposes.
priority-value	The value of the priority.

Note For each minimum packetization period, only one codec can be added to each list once.

Command Default

No default behavior or values are available.

Command Modes

Codec list (sbe-codec-list)

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	The **priority** keyword and the *priority-value* argument were added to the command.

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 a minimum packetization period for the PCMU and G729 codecs that are in the my_codecs codec list. It also shows how to set the priority for the G729 codec:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
Router(config-sbc-sbe-codec-list)# codec PCMU packetization-period 20
Router(config-sbc-sbe-codec-list)# codec G729 packetization-period 10 priority 2
```

Related Commands

Command	Description
codec list	Creates a codec list.
policy	Configures the packetization period policy.

codec system

To modify a codec, use the **codec system** command in the configure sbc sbe mode.

codec system *sys-codec id payload id*

Syntax Description

sys-codec	Codec included in the SBC.
id payload id	Static payload id. Value can be from 0 to 96.

Command Default

No default value.

Command Modes

Configure SBC SBE (config-sbc-sbe)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

To use this command, you must be in the correct configuration mode. The following table contains details of the modes:

Mode	Values	Default Value
media	AUDIO, VIDEO, APPLICATION, DATA, CONTROL, IMAGE, OMIT, TEL-EVENT	AUDIO
rate (in Hz)	1–2147483647	8000
packet-time	1–65535	10
bandwidth	1–9223372036854775807	64000
sample-size	0–255	8
channels	0–255	1
max-frames-per-packet	0–65535	1
options	none, transrate, transcode	none
codec-type	fixed, sampling, format, variable, redundancy	N/A, mandatory

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

Examples

The following example removes the rate configured on G726-40 codec:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system G726-40
Router(config-sbc-sbe-codec)# no clock rate
```

codec variant

To configure the codec variants and the codec variant profiles, use the **codec variant** command in the Signaling border element (SBE) configuration mode. To remove the codec variants and the codec variant profiles, use the **no** form of this command.

codec variant {**codec** *variant-name* | **profile** *profile-name*}

no codec variant {**codec** *variant-name* | **profile** *profile-name*}

Syntax Description

codec	Enters the codec variant mode to configure, modify, or delete a codec variant.
variant-name	The codec variant name.
profile	Enters the Codec variant profile mode to configure a codec variant profile.
profile-name	The codec profile name.

Command Default

No default behavior or values are available.

Command Modes

SBE configuration (config-sbc-sbe)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	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 enter the Codec variant mode to configure, modify, and delete a codec variant:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant codec G723-H-1
Router(config-sbc-sbe-codec-var-codec)#
```

The following example shows how to enter the Codec variant profile mode to configure the codec variant profile:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant profile profile-1
Router(config-sbc-sbe-codec-var-prof)#
```

concurrent-requests

To set the maximum number of concurrent requests to the RADIUS server, use the **concurrent-request** command in the appropriate configuration mode. To set the default, use the **no** form of this command.

concurrent-requests ***0-4000***

no concurrent-requests ***0-4000***

Syntax Description

0-4000	Maximum number of concurrent requests to the RADIUS server. The range is from 0 to 4000. The default value is 250.

Command Default

Default value is 250.

Command Modes

Server accounting (config-sbc-sbe-acc)

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 maximum number of concurrent requests to the RADIUS server**.**

```
Router# configure terminal
Router(config)# sbc uut105-1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting SBC1-account-1
Router(config-sbc-sbe-acc)# concurrent-requests 34
```

Related Commands

retry-interval	Sets the retry interval to connect to the RADIUS server.
retry-limit	Sets the retry interval to the RADIUS server.
activate	Activates the RADIUS client.

condition (editor)

To specify a condition to match before taking an action on a SIP message editor, use the **condition** command in the SIP Header Editor header action configuration mode. To remove a condition from the editor, use the **no** form of this command.

condition *[comparison-type | boolean-operator | operator | comparison-value]*

no ***condition*** *[comparison-type | boolean-operator | operator | comparison-value]*

Syntax Description

comparison-type	The supported comparison types are: • status-code—Response code value • header-value—Current header content • header-name *name* header-value—Content of a different header • variable—Match on variable content • adjacency—Match on adjacency settings • header-uri—Match on parts of the URI (username) • request-uri—Match on parts of the request URI (username) • *word*—Match on static strings • src-address—Match the source address • dst-address—Match the destination address
boolean-operator	The supported boolean operators are: • is-sip-uri—Does the header contain a sip: URI • is-tel-uri—Does the header contain a tel: URI • is-request—Is the message a request • is-100rel-required—Is the call performing 100rel • is-defined—Test if a variable is defined • is-private—Has privacy been invoked by the CAC policy: True
operator	The supported operators are: • [not] eq—Equals or not equal • [not] contains—Contains or does not contain • [not] regex-match—Regular expression matching (BRE) • store-as—Store rules only • and—Logical AND to add another condition to an existing condition • or—Logical OR to add another condition to an existing condition
comparison-value	Specifies a character string or numeric value to compare.

Command Default

No default behavior or values are available.

Command Modes SIP Header Editor header action configuration (config-sbc-sbe-mep-hdr-ele-act)

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.

Examples The following example shows how the **header** command adds the *test* header 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
Router(config-sbc-sbe-sip-hdr-ele)# action drop-msg
Router(config-sbc-sbe-sip-hdr-ele-act)# condition header-value contains "Cisco"
Router(config-sbc-sbe-sip-hdr-ele-act)# condition is-request eq true
```

Related Commands

Command	Description
dst-address	Enables you to enter the Destination address configuration mode to create a list of prioritized headers to derive a destination address.
src-address	Enables you to enter the Source address configuration mode to create a list of prioritized headers to derive a source address.

condition (session border controller)

To specify a condition to match before taking an action on a SIP message profile, use the **condition** command in SIP header-profile configuration mode. To remove the condition from the profile, use the **no** form of this command.

condition *[comparison-type | boolean-operator | operator | comparison-value]*

no ***condition*** *[comparison-type | boolean-operator | operator | comparison-value]*

Syntax Description

comparison-type	The supported comparison types are: • status-code—Response code value • header-value—Current header content • header-name *name* header-value—Content of a different header • variables—Match on variable content • adjacency—Match on adjacency settings • transport—Match on transport addresses or ports • header-uri—Match on parts of the URI (username) • request-uri—Match on parts of the request-URI (username) • *word*—Match on static strings • src-address—Match the source address • dst-address—Match the destination address
boolean-operator	The supported boolean operators are: • is-sip-uri—Does the header contain a sip: URI • is-tel-uri—Does the header contain a tel: URI • is-request—Is the message a request • is-100rel-required—Is the call performing 100rel • is-defined—Test if a variable is defined
operator	The supported operators are: • [not] eq—Equals or not equal • [not] contains—Contains or does not contain • [not] regex-match—Regular expression matching (BRE) • store-as—Store-rules only
comparison-value	Specifies any character string or numeric value to compare.

Command Default

No default behavior or values are available.

Command Modes

SIP header configuration (config-sbc-sbe-sip-hdr-ele-act)

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	The comparison types, boolean operators, and operators comparison types were added.
Cisco IOS XE Release 3.1S	The dst-address and src-address comparison types were added.

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.

Examples

The following example shows how the **header** command adds the *test* header to the *Myprofile* header profile:

```
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
Router(config-sbc-sbe-sip-hdr-ele)# action drop-msg
Router(config-sbc-sbe-sip-hdr-ele-act)# condition condition header-value contains "Cisco"
Router(config-sbc-sbe-sip-hdr-ele-act)# condition is-request eq true
```

Related Commands

Command	Description
action drop-msg	Adds an action of dropping a message to a SIP message profile.
dst-address	Enables you to enter the destination address configuration mode to create a list of prioritized headers to derive the destination address.
src-address	Enables you to enter the source address configuration mode to create a list of prioritized headers to derive the source address.

congestion-cleared

To configure that the congestion has cleared when the level of system resources reaches the congestion cleared threshold, use the **congestion-cleared** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

congestion-cleared [*percentage]*

no **congestion-cleared** [*percentage]*

Syntax Description

percentage	(Optional) This is the percentage value of system resources to signal congestion to the SBE. The range is from 1 to 100.

Command Default

The system default percentage is 60 if you do not configure the **congestion-cleared** command or if you configure **no congestion-cleared**.

Command Modes

VDBE configuration (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 the distributed model.

Usage Guidelines

When the data border element (DBE) has previously signaled a congestion event to the signaling border element (SBE), the DBE will signal that the congestion has cleared when the level of system resources used reaches the congestion cleared threshold. Congestion cleared must be less than or equal to the threshold, however, equal to the threshold is not recommended because it may cause excessive messaging between the MG and media gateway controller (MGC).

Examples

The following example creates a DBE service on a session border controller (SBC) called mySbc and configures the DBE to signal to the SBE that congestion has cleared at 90% percent of system resources consumed:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# congestion-cleared 90
```

Related Commands

Command	Description
congestion-threshold	Configures the DBE to signal a congestion event to the SBE when a maximum percentage has been reached.

congestion-threshold

To configure the DBE to signal a congestion event to the SBE when a maximum percentage has been reached, use the **congestion-threshold** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

congestion-threshold [*percentage]*

no **congestion-threshold** [*percentage]*

Syntax Description

percentage	(Optional) This is the percentage value of system resources to signal congestion to the SBE. The range is from 1 to 100.

Command Default

The system default percentage is 80 if you do not configure the congestion-threshold, or if you issue the default **congestion-threshold** command, or if you configure **no congestion-threshold**.

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.

Usage Guidelines

When the DBE reaches the maximum configured congestion-threshold percentage for either number of calls or media bandwidth, it sends a congestion message to the SBE.

Examples

The following example creates a DBE service on an SBC called mySbc, enters into SBC-DBE configuration and VDBE configuration modes, and shows how to configure the DBE to signal a congestion event to the SBE when 95% percent of capacity is reached.

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# congestion-threshold 95
```

Related Commands

Command	Description
congestion-cleared	Configures that the congestion has cleared when the level of system resources reaches the congestion cleared threshold.

congestion sip reject-code

To change the reject message code for signaling congestion handling, use the **congestion sip reject-code** command in the SBE configuration mode.

congestion sip reject-code *valid-reject-code*

Syntax Description

valid-reject-code	The reject message code sent back to sender during congestion. Range is from 300 to 999.

Command Default

Signaling congestion handling is on by default. The default reject message code is 503.

Command Modes

SBE configuration (config-sbc-sbe)

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.

Examples

The following example shows how to change the reject message code for signaling congestion handling:

```
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)# congestion sip reject-code 600
Router(config-sbc-sbe)#
```

control-address h248 ipv4

To configure a DBE to use a specific IPv4 H.248 control address, use the **control-address h248 ipv4** command in VDBE configuration mode. To deconfigure a DBE from using an IPv4 H.248 control address, use the **no** form of this command.

control-address h248 ipv4 {*A.B.C.D}*

no control-address h248 ipv4 {*A.B.C.D}*

Syntax Description

A.B.C.D	This is the IP address for the IPv4 H.248 control address of the DBE, which is the local IP address used to connect to the SBE.

Command Default

No default behavior or values are available.

Command Modes

VDBE configuration (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.

Usage Guidelines

Neither the control-address nor the local-port can be changed when the controller exists. The controller must be deleted to change these parameters. To delete the controller, use the **no control-address h248 ipv4** command.

Examples

The following command configures the DBE to use address 10.0.0.1 as its control address.

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# control address h248 ipv4 10.0.0.1
Router(config-sbc-sbe-vdbe)# controller h248 1
```

Related Commands

Command	Description
attach-controllers	Configures a DBE to attach to an H.248 controller.

control-address ipv4

To configure a local IPv4 H.248 signaling address for the Border Access Controller (BAC), use the **control-address ipv4** command in the H248 BAC adjacency configuration mode. To unconfigure the BAC from using a local IPv4 H.248 signaling address, use the **no** form of this command.

control-address ipv4 *ipv4-address* {**port** *port-number*}

control-address ipv4 *ipv4-address* {**port-range** *minimum-port number maximum-port number*}

no control-address ipv4 *ipv4-address* {**prt** *port-number*} | {**port-range** *minimum-port number maximum-port number*}

Syntax Description

ipv4	Configures an IPv4 media address.
ipv4-address	IPv4 address assigned to an H.248 association.
port	Specifies the port for the adjacency address.
port-number	Number for the adjacency address port. The range is from 1 to 65535.
port-range	Specifies the port range for the adjacency address.
minimum-port number	Starting port number of the range. The possible values are from 1 to 65535, but the minimum port number specified must be less than or equal to the maximum port number specified.
maximum-port number	Ending port number of the range. The possible values are from 1 to 65535, but the maximum port number specified must be greater than the minimum port number specified.

Command Default

None

Command Modes

H.248 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

The BAC handles two types of Message Identifiers (MIDs): domain name and IP address.

If the **control-address ipv4** command is configured in the core adjacency submode and the MID of an IAD is IP address, only the **port-range** is configured and not the **port**.

If the **control-address ipv4** command is configured in the access adjacency submode, irrespective of the MID type, only the **port** is configured.

Examples

The following example shows how the **control-address ipv4** command is used to configure a local IPv4 H.248 signaling address for the BAC in the core adjacency submode:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 core core_spec2
Router(config-h248-bac-adj)# control-address ipv4 192.168.102.222 port-range 2944 4000
```

The following example shows how the **control-address** command is used to configure a local IPv4 H.248 signaling address for the BAC in the access adjacency submode:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# control-address ipv4 172.16.104.14 port 2940
```

Related Commands

Command	Description
adjacency h248	Configures an H.248 BAC access adjacency and core adjacency.

controller h248

To configure the H.248 controller for a data border element (DBE) or enter into Controller H.248 configuration mode, use the **controller h248** command in VDBE configuration mode. To delete the H.248 controller, use the **no** form of this command.

controller h248 {*controller-index}*

no controller h248 {*controller-index}*

Syntax Description

controller-index	The number that identifies the H.248 controller for the DBE, in case you want to configure more than one controller.

Command Default

No default behavior or values are available.

Command Modes

VDBE configuration (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.

Usage Guidelines

Once a controller is configured and attached, it must be detached with the **no attach-controllers** command before you can modify any controller information.

Note This command is invalid for the unified model, where both the SBE and DBE logical entities co-exist on the same network element.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures an H.248 controller with index 1.

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# controller h248 1
```

The following example configures an H.248 controller with index 1 and tries to configure an IPv4 remote address on the controller. The message indicates that the controller must be detached first before the remote address can be modified.

```
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 210.229.108.253
SBC: remote-address cannot be changed while controllers are attached.
```

Related Commands

Command	Description
sbc dbe	Creates the DBE service on an SBC and enters into SBC-DBE configuration mode.
vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.

control address aaa

To configure an SBE to use a given IPv4 AAA control address when contacting an authentication or billing server, use the **control address aaa ipv4** command in **SBE** configuration mode. To deconfigure the IPv4 AAA control address, use the **no** form of this command.

control address aaa ipv4 *ip_address [***vrf** *vrf-name]*

no control address aaa ipv4 *ip_address*

Syntax Description

ipv4 *ip_address*	Specifies the IPv4 AAA control address.
vrf *vrf-name*	(Optional) Specifies the VRF name.

Command Default

No default behavior or values are available.

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 configure the SBE to use address 10.1.0.1 as its AAA control address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address aaa ipv4 10.1.0.1 vrf myvrf
```

Related Commands

Command	Description
control address h248 index	Configures IPv4 H.248 control addresses.

control address h248 index

To configure an SBE to use a given IPv4 H.248 control address, port, or transport for H.248 communications when acting as a media gateway controller, use the **control address h248 index** command in SBE configuration mode. To deconfigure the given IPv4 H.248 control address when acting as a media gateway controller, use the **no** form of this command.

control address h248 index *index-number*

no control address h248 index *index-number*

Syntax Description

index-number	Specifies the unique identifier of the H.248 control address to set. The index number range is from 0 to 2147483647.

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.

See the related commands: **control-address h248 ipv4**, **control address h248 port**, and **control address h248 transport** commands.

Examples

The following example shows the options available when you enter into SBC SBE CTRL-H248 configuration mode, after entering the **control address h248 index** *index-number* command:

```
Router(config-sbc-sbe)# control address h248 index 0
Router(config-sbc-sbe-ctrl-h248)# ?
SBC SBE CTRL-H248 Configuration Commands:
  default    Set a command to its defaults
  exit       Exit the SBC SBE CTRL-H248 configuration mode
  ipv4       IPv4 address
  no         Negate a command or set its defaults
  port       Listening port number
  transport  Transport method to use for connection to H.248 controller

Router(config-sbc-sbe-ctrl-h248)#
```

The following example shows how to configure the SBE to use address 10.1.0.1 as its H.248 control address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 index 1
Router(config-sbc-sbe-ctrl-h248)# ipv4 10.1.0.1
Router(config-sbc-sbe-ctrl-h248)# exit
```

Related Commands

Command	Description
ipv4 (SBE H.248)	Configures an SBE to use a given IPv4 H.248 control address.
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.

control address h248 port

To configure an SBE to use a given port for H.248 communications when acting as a media gateway controller, use the **control-address h248 port** command in SBE configuration mode. To deconfigure a h248 controller, use the **no** form of this command.

control address h248 port *port-number*

no control address h248 port *port-number*

Syntax Description

port-number	Port number assigned.

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 change or remove this configuration, deconfigure the h248 controller by issuing the **no control address h248** command, then configure a new h248 control address.

If the port is not configured, or is configured with the value zero, then the H.248 default port number, 2944, is used.

Examples

The following command configures the SBE to use port 123 as its H.248 port:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 port 123
Router(config-sbc-sbe)# exit
```

Related Commands

Command	Description
control-address h248 transport	Configures an SBE to use a given transport for H.248 communications.

control address h248 transport

To configure an SBE to use a given transport for H.248 communications when acting as a media gateway controller, use the **control-address h248 transport** command in SBE configuration mode. To deconfigure a h248 controller, use the **no** form of this command.

control address h248 transport [udp | tcp]

no ***control address h248 transport [udp | tcp]***

Syntax Description

udp	Selects UDP as the underlying transport.
tcp	Selects TCP as the underlying transport.

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 change or remove this configuration, deconfigure the h248 controller by issuing the **no control address h248** command, then configure a new h248 control address.

Examples

The following command configures the SBE to use TCP as its H.248 transport:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 transport tcp
Router(config-sbc-sbe)# exit
```

Related Commands

Command	Description
control-address h248 port	Configures an SBE to use a given port for H.248 communications.

copy logs

To to transfer debug and system logs off of the ACE for analysis, use the ***copy logs*** *uri* command in Exec mode.

copy logs *uri*

Syntax Description

uri	Specifies either image:/filename.tar or disk0:/filename.tar.

Command Default

No default behavior or values are available.

Command Modes

Exec (#)

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

You can specify the filename but it must end in *.tar*.

Examples

The following example copies the log files to the ku040708.tar file:

Router# **copy logs image:/ku040708.tar**

```
Copying logs to tar file image:/ku040708.tar..
```

core-adj

To bind an H.248 Border Access Controller (BAC) core adjacency with its corresponding H.248 BAC access adjacency, use the **core-adj** command in the H248 BAC adjacency configuration mode. To unbind an H.248 BAC core adjacency from its corresponding H.248 BAC access adjacency, use the **no** form of this command.

core-adj *core adjacency-name*

no core-adj *core adjacency-name*

Syntax Description

core adjacency-name	Name of the core adjacency. The *core adjacency-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

None

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

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 **core-adj** command is used to bind an H.248 BAC core adjacency with its corresponding H.248 BAC access adjacency:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# core-adj core_spec2
```

Related Commands

Command	Description
adjacency h248	Configures an H.248 BAC access adjacency and core adjacency.

cost

To assign a cost to this route, use the **cost** command in the RTG routing table entry configuration mode. To destroy the cost given to the route, use the **no** form of this command.

cost *cost*

no ***cost*** *cost*

Syntax Description

cost	Range: [1-0xFFFFFFFF] The value of "0" is not accepted. Enter "na" to mean this entry will never be matched.

Command Default

The default is "na".

Command Modes

RTG routing table entry configuration (config-sbc-sbe-rtgpolicy-rtgtable-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 create an entry in the new admission control table, MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-least-cost-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# cost
Router(config-sbc-sbe-rtgpolicy-entry)# exit
```

Related Commands

Command	Description
rtg-least-cost-table	Configures the least-cost routing table.

critical-alert-size

To configure the number of specified events before a critical alert is triggered, use the **critical-alert-size** command in the blacklist reason mode. To disable the number of specified events, use the no form of this command.

critical-alert-size *number-of-events*

no critical-alert-size

Syntax Description

number-of-events	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 critical alert to be triggered using the **critical-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)# critical-alert-size 655
```

Related Commands

Command	Description
major-alert-size	Configures the number of specified events before a major alert is triggered.
minor-alert-size	Configures the number of specified events before a minor 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.

current15minutes

To specify that QoS statistics must be calculated for 15-minute intervals, use the **current15minutes** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

current15minutes {adjacency *adjacency-name* **{critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value***] | minor low** *value* **upper** *value* **[[critical low value upper value] | [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]} **| default {critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value*] **| minor low** *value* **upper** *value* **[[critical low** *value* **upper** *value*] **| [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]}}

no current15minutes {adjacency *adjacency-name* **| default}**

Syntax Description

adjacency	Specifies that alert levels must be set for the specified adjacency.
adjacency-name	Name of the adjacency.
critical	Specifies the lower limit and upper limit for the Critical alert level.
low	Specifies the lower limit for the alert level.
value	Value of the lower limit or upper limit.
upper	Specifies the upper limit for the alert level.
major	Specifies the lower limit and upper limit for the Major alert level.
minor	Specifies the lower limit and upper limit for the Minor alert level.
default	Specifies that alert levels must be set for all adjacencies on the SBC.

Command Default

No default behavior or values are available.

Command Modes

Statistics SBE configuration (config-sbc-sbe-stats)

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

The following example shows how to specify that statistics must be calculated for 15-minute intervals using the **current15mins** command in the statistics SBE configuration mode:

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

```
Router(config-sbc-sbe)# statistics lcl-jit
Router(config-sbc-sbe-stats)# current15minutes default critical low 30 upper 50
```

Related Commands

Command	Description
calc-moscqe	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
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.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
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.

current5minutes

To specify that QoS statistics must be calculated for 5-minute intervals, use the **current5minutes** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

current5minutes {adjacency *adjacency-name* **{critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value***] | minor low** *value* **upper** *value* **[[critical low value upper value] | [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]} **| default {critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value*] **| minor low** *value* **upper** *value* **[[critical low** *value* **upper** *value*] **| [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]}}

no current5minutes {adjacency *adjacency-name* **| default}**

Syntax Description

adjacency	Specifies that alert levels must be set for the specified adjacency.
adjacency-name	Name of the adjacency.
critical	Specifies the lower limit and upper limit for the Critical alert level.
low	Specifies the lower limit for the alert level.
value	Value of the lower limit or upper limit.
upper	Specifies the upper limit for the alert level.
major	Specifies the lower limit and upper limit for the Major alert level.
minor	Specifies the lower limit and upper limit for the Minor alert level.
default	Specifies that alert levels must be set for all adjacencies on the SBC.

Command Default

No default behavior or values are available.

Command Modes

Statistics SBE configuration (config-sbc-sbe-stats)

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

The following example shows how to specify that statistics must be calculated for 5-minute intervals using the **current5mins** command in the statistics SBE configuration mode:

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

```
Router(config-sbc-sbe)# statistics mpl-pct
Router(config-sbc-sbe-stats)# current5minutes default major low 10 upper 29 critical low
30 upper 50
```

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.
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.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
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.

currentday

To specify that statistics must be calculated for 24-hour intervals (starting from midnight), use the **currentday** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

currentday {adjacency *adjacency-name* **{critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value***] | minor low** *value* **upper** *value* **[[critical low value upper value] | [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]} **| default {critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value***] | minor low** *value* **upper** *value* **[[critical low** *value* **upper** *value***] | [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]}}

no currentday {adjacency *adjacency-name* **| default}**

Syntax Description

adjacency	Specifies that alert levels must be set for the specified adjacency.
adjacency-name	Name of the adjacency.
critical	Specifies the lower limit and upper limit for the Critical alert level.
low	Specifies the lower limit for the alert level.
value	Value of the lower limit or upper limit.
upper	Specifies the upper limit for the alert level.
major	Specifies the lower limit and upper limit for the Major alert level.
minor	Specifies the lower limit and upper limit for the Minor alert level.
default	Specifies that alert levels must be set for all adjacencies on the SBC.

Command Default

No default behavior or values are available.

Command Modes

Statistics SBE configuration (config-sbc-sbe-stats)

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

The following example shows how to specify that statistics must be calculated for 15-minute intervals using the **currentday** command in the statistics SBE configuration mode:

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

```
Router(config-sbc-sbe)# statistics mos-cqe
Router(config-sbc-sbe-stats)# currentday default critical low 2 upper 3
```

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.
current5minutes	Specifies that QoS statistics must be calculated for 5-minute 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.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
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.

currenthour

To specify that QoS statistics must be calculated for 60-minute intervals, use the **currenthour** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

currenthour {adjacency *adjacency-name* **{critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value*] **| minor low** *value* **upper** *value* **[[critical low value upper value] | [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]} **| default {critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value*] **| minor low** *value* **upper** *value* **[[critical low** *value* **upper** *value*] **| [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]}}

no currenthour {adjacency *adjacency-name* **| default}**

Syntax Description

adjacency	Specifies that alert levels must be set for the specified adjacency.
adjacency-name	Name of the adjacency.
critical	Specifies the lower limit and upper limit for the Critical alert level.
low	Specifies the lower limit for the alert level.
value	Value of the lower limit or upper limit.
upper	Specifies the upper limit for the alert level.
major	Specifies the lower limit and upper limit for the Major alert level.
minor	Specifies the lower limit and upper limit for the Minor alert level.
default	Specifies that alert levels must be set for all adjacencies on the SBC.

Command Default

No default behavior or values are available.

Command Modes

Statistics SBE configuration (config-sbc-sbe-stats)

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

The following example shows how to specify that statistics must be calculated for 60-minute intervals using the **currenthour** command in the statistics SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# statistics mpd-pct
```

```
Router(config-sbc-sbe-stats)# currenthour adjacency adj1 minor low 5 upper 19 critical low
20 upper 30
```

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.
current5minutes	Specifies that QoS statistics must be calculated for 5-minute intervals.
currentday	Specifies that statistics must be calculated for 24-hour 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.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
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.

currentindefinite

To specify that statistics must be calculated indefinitely starting from the last explicit reset, use the **currentindefinite** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

currentindefinite {adjacency *adjacency-name* **{critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value***] | minor low** *value* **upper** *value* **[[critical low value upper value] | [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]} **| default {critical low** *value* **upper** *value* **| major low** *value* **upper** *value* **[critical low** *value* **upper** *value*] **| minor low** *value* **upper** *value* **[[critical low** *value* **upper** *value*] **| [major low** *value* **upper** *value* **[critical low** *value* **upper** *value*]]]}}

no currentindefinite {adjacency *adjacency-name* **| default}**

Syntax Description

adjacency	Specifies that alert levels must be set for the specified adjacency.
adjacency-name	Name of the adjacency.
critical	Specifies the lower limit and upper limit for the Critical alert level.
low	Specifies the lower limit for the alert level.
value	Value of the lower limit or upper limit.
upper	Specifies the upper limit for the alert level.
major	Specifies the lower limit and upper limit for the Major alert level.
minor	Specifies the lower limit and upper limit for the Minor alert level.
default	Specifies that alert levels must be set for all adjacencies on the SBC.

Command Default

No default behavior or values are available.

Command Modes

Statistics SBE configuration (config-sbc-sbe-stats)

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

The following example shows how to specify that statistics must be calculated indefinitely starting from the last explicit reset using the **currentindefinite** command in the statistics SBE configuration mode:

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

```
Router(config-sbc-sbe)# statistics mpl-pct
Router(config-sbc-sbe-stats)# currentindefinite adjacency adj1 minor low 31 upper 40 major
low 41 upper 50 critical low 51 upper 60
```

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.
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.
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.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
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.