



SIP Renegotiation

The Cisco Unified Border Element (SP Edition) supports two Session Initiation Protocol (SIP) renegotiation related features:

- Delta Renegotiation

The Delta Renegotiation feature determines which SIP renegotiation mode will be used by the session border controller (SBC) when renegotiating media: Delta Renegotiation or Make-Before-Break Renegotiation.

- Support Renegotiated Call Over NAT

The Support Renegotiated Call Over NAT feature allows you to ensure that pinholes are preserved for deleted streams so that if the stream is re-enabled, Cisco Unified Border Element (SP Edition) will re-use the same pinhole.

These features significantly reduce the situations in which media ports change mid-call, which provides interoperability and Network Address Translation (NAT) traversal benefits.



Note

For Cisco IOS XE Release 2.4, the Delta Renegotiation and Support Renegotiated Call Over NAT features are supported in the unified model only.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html.

For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

Feature History for SIP Renegotiation

Release	Modification
Cisco IOS XE Release 2.4	The Delta Renegotiation and Support Renegotiated Call Over NAT features were introduced on the Cisco IOS XR along with support for the unified model.

Contents

This module contains the following sections:

- [Restrictions for Delta Renegotiation, page 29-2](#)
- [Information About Delta Renegotiation, page 29-2](#)
- [Restriction for Support Renegotiated Call Over NAT, page 29-3](#)
- [Information About Support Renegotiated Call Over NAT, page 29-3](#)
- [Configuring Support Renegotiated Call Over NAT, page 29-3](#)
- [Configuration Example—Support Renegotiated Call Over NAT, page 29-7](#)

Restrictions for Delta Renegotiation

The restrictions for Delta Renegotiation are:

- When Delta Renegotiation mode is in use, stream statistics and Secure Device Provisioning (SDP) billing information will be output at call termination, not at Delta Renegotiation.
- When Delta Renegotiation mode is in use, the following precepts apply:
 - Renegotiation may cause a change in the Differentiated Services Code Point (DSCP) marking policy.
 - The port range depends on the initial incarnation of the stream.
- Under certain scenarios, if the Cisco Unified Border Element (SP Edition) fails over while a Delta Renegotiation is in progress, media resources (such as pinholes and bandwidth allowances) may be unnecessarily allocated.

Information About Delta Renegotiation

The Delta Renegotiation feature determines which SIP renegotiation mode will be used by the Cisco Unified Border Element (SP Edition) when renegotiating media:

- **Delta Renegotiation mode**

When the Cisco Unified Border Element (SP Edition) performs a Delta Renegotiation, it retains the existing media pinholes and modifies their variables. Delta Renegotiation mode is used for SIP/H.323 interworked calls and for IP Multimedia Subsystem (IMS) calls.
- **Make-Before-Break Renegotiation mode**

When the Cisco Unified Border Element (SP Edition) performs a Make-Before-Break Renegotiation, it creates new pinholes with the proposed media properties, then removes the pre-existing pinholes when the renegotiation completes. These new pinholes temporarily exist in parallel with the existing (old) media pinholes. When the renegotiation completes, Cisco Unified Border Element (SP Edition) deletes the old media pinholes, leaving just the new ones. (Or, if the renegotiation fails, it rolls back to the old state by deleting the new pinholes.)

Delta Renegotiation mode is the default SIP renegotiation mode for all SIP-to-SIP negotiations on the Cisco Unified Border Element (SP Edition) with the following exceptions:

- Change of address family

If the renegotiation changes the address family from IPv4 to IPv6, or vice versa, a new media address is required, and therefore Make-Before-Break Renegotiation mode will be used.

- Mid-call media rerouting

If the renegotiation causes a call to switch between media bypass and non-media bypass mode, the endpoints will perceive a change in the media address, and therefore Make-Before-Break Renegotiation mode will be used.

Restriction for Support Renegotiated Call Over NAT

The restriction for the Support Renegotiated Call Over NAT feature is:

- Stream statistics and SDP billing information will be output at call termination, not at Delta Renegotiation.

Information About Support Renegotiated Call Over NAT

The Support Renegotiated Call Over NAT feature allows you to ensure that media pinholes are preserved for deleted streams so that if a stream is re-enabled, the Cisco Unified Border Element (SP Edition) will re-use the same pinhole.

This feature is used to avoid de-allocation of a video pinhole in a NAT scenario where Delta Renegotiation mode is in effect and a video transmission is paused. Although the standard SDP protocol when a video transmission is paused is to set the video stream to “a=inactive” (which indicates that SBC should keep the stream allocated), there are known devices that do not set the video stream to “a=inactive” to pause it. Instead, these devices delete the video stream by setting its port to 0. To ensure that the stream remains allocated and the pinhole is preserved even when the SBC receives a port value of 0 during a media stream renegotiation, you can enable the Support Renegotiated Call Over NAT feature.

Use the **media address preserve** command to enable the Support Renegotiated Call Over NAT feature on a per-call basis.

Configuring Support Renegotiated Call Over NAT

This section contains the steps to configure the Support Renegotiated Call Over NAT feature, which preserves media pinholes for deleted streams on a per-call basis.

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **cac-policy-set** *policy-set-id*
5. **first-cac-table** *table-name*
6. **cac-table** *table-name*
7. **table-type** { **policy-set** | **limit** {*list of limit tables*}}

8. **entry** *entry-id*
9. **cac-scope** {*list of scope options*}
10. **[no] media address preserve**
11. **action cac complete**
12. **complete**
13. **active-cac-policy set** *policy-set-id*
14. **show sbc** *service-name sbe cac-policy-set policy-set-id table table-name entry entry-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: Router# configure	Enables global configuration mode.
Step 2	sbc <i>service-name</i> Example: Router(config)# sbc mysbc	Enters the mode of an SBC service. <ul style="list-style-type: none"> Use the <i>service-name</i> argument to define the name of the service.
Step 3	sbe Example: Router(config-sbc)# sbe	Enters the mode of an SBE entity within an SBC service.
Step 4	cac-policy-set <i>policy-set-id</i> Example: Router(config-sbc-sbe)# cac-policy-set 1	Enters the mode of CAC policy set configuration within an SBE entity, creating a new policy set if necessary.
Step 5	first-cac-table <i>table-name</i> Example: Router(config-sbc-sbe-cacpolicy)# first-cac-table 1	Configures the name of the first policy table to process when performing the admission control stage of policy.
Step 6	cac-table <i>table-name</i> Example: Router(config-sbc-sbe-cacpolicy)# cac-table 1	Enters the mode for configuration of an admission control table (creating one if necessary) within the context of an SBE policy set.

Command or Action	Purpose
<p>Step 7</p> <pre>table-type {policy-set limit {list of limit tables}}</pre> <p>Example: Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set</p>	<p>Configures the table type of a CAC table within the context of an SBC policy set.</p> <p><i>list of limit tables</i> can be one of the following values:</p> <ul style="list-style-type: none"> • account—Compare the name of the account. • adj-group—Compare the name of the adjacency group. • adjacency—Compare the name of the adjacency. • all—No comparison type. All events match this type. • call-priority—Compare with call priority. • category—Compare the number analysis assigned category. • dst-account—Compare the name of the destination account. • dst-adj-group—Compare the name of the destination adjacency group. • dst-adjacency—Compare the name of the destination adjacency. • dst-prefix—Compare the beginning of the dialed digit string. • event-type—Compare with CAC policy event types. • src-account—Compare the name of the source account. • src-adj-group—Compare the name of the source adjacency group. • src-adjacency—Compare the name of the source adjacency. • src-prefix—Compare the beginning of the calling number string. <p>Features can be enabled or disabled per adjacency group through CAC configuration the same way this is done per individual adjacencies. The adj-group table type matches on either source or destination adjacency group.</p> <p>When the policy-set keyword is specified, use the cac-scope command to configure the scope within each entry at which limits are applied in a CAC Policy Set table.</p>
<p>Step 8</p> <pre>entry entry-id</pre> <p>Example: Router(config-sbc-sbe-cacpolicy-cactable)# entry 1</p>	<p>Enters the mode to create or modify an entry in an admission control table.</p>

Command or Action	Purpose
<p>Step 9 <code>cac-scope {list of scope options}</code></p> <p>Example: Router(config-sbc-sbe-cacpolicy-cactable-entry) # cac-scope src-adjacency</p>	<p>Choose a scope at which CAC limits are applied within each entry in a Policy Set table.</p> <p><i>list of scope options</i>—Specifies one of the following strings used to match events:</p> <ul style="list-style-type: none"> • <i>account</i>—Events that are from the same account. • <i>adjacency</i>—Events that are from the same adjacency. • <i>adj-group</i>—Events that are from members of the same adjacency group. • <i>call</i>—Scope limits are per single call. • <i>category</i>—Events that have same category. • <i>dst-account</i>—Events that are sent to the same account. • <i>dst-adj-group</i>—Events that are sent to the same adjacency group. • <i>dst-adjacency</i>—Events that are sent to the same adjacency. • <i>dst-number</i>—Events that have the same destination. • <i>global</i>—Scope limits are global • <i>src-account</i>—Events that are from the same account. • <i>src-adj-group</i>—Events that are from the same adjacency group. • <i>src-adjacency</i>—Events that are from the same adjacency. • <i>src-number</i>—Events that have the same source number.
<p>Step 10 <code>media address preserve</code></p> <p>Example: Router(config-sbc-sbe-cacpolicy-cactable-entry) # media address preserve</p>	<p>Ensures that media pinholes are preserved (disabled) for deleted streams.</p> <ul style="list-style-type: none"> • [no]—Allows media pinholes to be deleted for deleted streams.
<p>Step 11 <code>action cac-complete</code></p> <p>Example: Router(config-sbc-sbe-cacpolicy-cactable-entry) # action cac complete</p>	<p>When an event matches, this CAC policy is complete.</p>
<p>Step 12 <code>complete</code></p> <p>Example: Router(config-sbc-sbe-cacpolicy)# complete</p>	<p>Completes the CAC policy set when you have committed the full set.</p>

	Command or Action	Purpose
Step 13	active cac-policy-set <i>policy-set-id</i> Example: Router(config-sbc-sbe)# active cac-policy-set 1	Sets the active CAC policy set within an SBE entity.
Step 14	show sbc <i>service-name</i> sbe cac-policy-set <i>policy-set-id</i> table <i>table-name</i> entry <i>entry-id</i> Example: Router# show sbc mysbc sbe cac-policy-set 1 table 1 entry 1	Lists detailed information for a given entry in a CAC policy table, including whether the Support Renegotiated Call Over NAT feature is enabled. When this feature is enabled, the “Media Address” field shows a value of “Preserve.”

Configuration Example—Support Renegotiated Call Over NAT

The following example enables the Support Renegotiated Call Over NAT feature described in this chapter on a per-call basis

```
sbc mysbc
sbe
  cac-policy-set 1
  first-cac-table 1
  cac-table 1
  table-type policy-set
  entry 1
  media address preserve
  action cac-complete
  complete
  active-cac-policy-set 1
```

The following example shows detailed output for the CAC policy set 1, table 1, entry 1, including the “Media Address” field that shows a value of “Preserve,” indicating the Support Renegotiated Call Over NAT feature is enabled

```
Router# show sbc mysbc sbe cac-policy-set 1 table 1 entry 1
SBC Service "mysbc"
Policy set 1 table 1 entry 1
Match value
Action                               Next table
Next-table
Max calls                             Unlimited
Max call rate                         Unlimited
Max in-call rate                      Unlimited
Max out-call rate                     Unlimited
Max registrations                     Unlimited
Max reg. rate                         Unlimited
Max bandwidth                         Unlimited
Max channels                          Unlimited
Transcoder                            Allowed
Caller privacy setting                 Never hide
Callee privacy setting                Never hide
Early media                           Allowed
Early media direction                  Both
Early media timeout                    None
Restrict codecs to list                default
Restrict caller codecs to list         default
Restrict callee codecs to list         default
Media bypass                           Allowed
```

■ Configuration Example—Support Renegotiated Call Over NAT

```
SRTP Transport           Trusted-Only (by default)
Callee hold setting     Standard
Caller hold setting     Standard
Media Address         Preserve
Renegotiate             Delta
Number of calls rejected by this entry    0
```