SDP Support

In this section:

- SDP Transparency
- Suppressing 183 Response Without SDP
- Passing Audio Codecs in SDP Offer
- Late Media INVITE or Re-INVITE Support
- Late Media Pass-through Calls over GW-GW
- ANAT Support
- ICE-Lite Support
- Bundling of Streams

Related Articles

- Media Services
- Video Support
- Configuring Video Best Practices
- Configuring SBC for WRTC
- ingressIpAttributes - SIP - CLI
- Ip Signaling Profile - Ingress Ip Attributes (EMA)
- commonIpAttributes - SIP - CLI
- Common Ip Attributes - Flags (EMA)
- sipTrunkGroup media - CLI
- SIP Trunk Group - Media (EMA)
- SDP Manipulation (SMM examples)

Modified: for 5.1.5

SDP Transparency

Session Description Protocol (SDP) is a set of rules defining how multimedia sessions are set up to allow all end points to effectively participate in the session.

Interactive Connectivity Establishment (ICE) is a protocol used by systems that cannot determine their own transport address as seen from the remote end, but that can provide several possible alternatives (see ICE-Lite Support below). The SDP transparency feature allows SDP and ICE media to pass through the SBC as-is to the far end.

SDP Transparency functionality includes:

- All unknown SDP attributes are transparently passed.
- All unknown components of known SDP attributes are dropped.
- Any unknown audio codecs are dropped.
- All known and unknown video codecs are transparently passed.

When SDP Transparency is enabled, all IP Signaling Profile SDP-related flags are overridden.

For additional audio/video support topics, see:

- Media Services
- Video Support
- Configuring Video Best Practices

Suppressing 183 Response Without SDP

The SBC Core supports suppressing the 183 response without SDP upon receipt of 3xx Redirect response for reasons such as:

- An endpoint perceives a 183 without SDP response as being an extra message resulting in unexpected behavior.
- Endpoints that behave irregularly upon receipt of a 183 without SDP response prior to cut-through.

Two IP Signaling Profile ingress flags are available to configure the SBC to suppress 183 response without SDP:

- suppress183For3xxRedirectResponse
- suppress183WithoutSdp
The following table describes the effects of enabling/disabling these flags.

**Table 1: Suppress 183 Response Without SDP Flags**

<table>
<thead>
<tr>
<th>Suppress 183 for 3xx Redirect Response</th>
<th>Suppress 183 without SDP</th>
<th>Action</th>
</tr>
</thead>
</table>
| Enabled                                | Enabled                  | • If 183 without SDP is due to 3xx redirect response, it is suppressed due to “Suppress 183 for 3xx Redirect Response” flag.  
• If 183 without SDP is triggered for reason other than 3xx redirect response, it is suppressed due to “Suppress 183 without SDP” flag. |
| Enabled                                | Disabled                 | 3xx redirect response triggers 183 without SDP, and hence is suppressed. |
| Disabled                               | Enabled                  | A ‘183 without SDP triggered due to 3xx redirect response’ (or for any other reason) is suppressed. |
| Disabled                               | Disabled                 | Existing behavior persists. |

For configuration details, see `ingressIpAttributes` - SIP - CLI or Ip Signaling Profile - Ingress Ip Attributes (EMA).

** Passing Audio Codecs in SDP Offer**

The SBC supports passing the list of received audio codecs in the SDP offer to PSX in the policy request. The SBC also passes the received audio codec information list as received in the ingress SDP to PSX in the policy request.

The SBC uses the modified calling number returned by the PSX in the policy response in formatting the egress call leg request. The P-CDR information is written onto the SBC accounting records, populating the “Egress External Accounting Data” field for STOP and ATTEMPT CDR records.

> This feature is not applicable when the SBC is configured for ERE mode.

** Late Media INVITE or Re-INVITE Support**

- **Do not use** `deriveFromOtherLeg` **when configuring H.323 or SIP trunk groups to use INVITEs with no SDPs.**

`sendAllAllowedCodecsForLateMediaInviteOrReInvite`

- When this flag is disabled for transcoded calls (default behavior), the SBC offers the codec used for transcoding on the leg.
- When the flag is enabled for transcoded calls, the SBC offers multiple codecs which include:
  - The subset of the codecs that the associated peer supports.
  - The transcoded codecs that the associated DSP channel supports. This includes the codec currently being used for transcoding.

For pass-through calls, the SBC always offers a subset of the codecs advertised by the associated peer. The SBC Offer...
codec list is classified as a subset because the list can be subjected to codec policy filters.

**Example 1: G711 pass-through call**

1. Ingress Offer: G711, G729
2. Egress Offer: G711, G729, AMR, G726
3. Ingress Answer: G711
4. Egress Answer: G711

If a re-INVITE with no SDP is received on egress, SBC generates an offer for G711, G729. The G726 and AMR are not offered because the call is marked as a relay call with DSP removed, and hence the transcoded codecs.

**Example 2: G711 to AMR transcoded call**

1. Ingress Offer: G711, G729
2. Egress Offer: G711, G729, AMR, G726
3. Egress Answer: AMR
4. Ingress Answer: G711

If a re-INVITE with no SDP is received on egress, by default, SBC generates an offer for AMR. If the “Send All Allowed Codecs For Late Media Invite Or Re-Invite” flag is enabled then SBC generates a codec list of G711, G729, AMR, and G726 in the Offer.

See commonIpAttributes - SIP - CLI or Common Ip Attributes - Flags (EMA) for configuration details.

**Late Media Pass-through Calls over GW-GW**

The SBC supports Late Media pass-through calls over GW-GW and also, handles Late Media (offer less) re-INVITE on either side. This functionality is supported when the flag lateMediaSupport is configured as passthru.

```
set addressContext <addressContex name> zone <zone name> sipTrunkGroup <sipTrunkGroup name> media lateMediaSupport passthru
```

When the flag lateMediaSupport is set as passthru, the Late Media INVITE/re-INVITE received on that leg is relayed to the other leg.

**Note**
The SBC SWe Cloud does not support Late Media pass-through calls over GW-GW.

**ANAT Support**

Alternative Network Address Types (ANAT) semantics for the SDP grouping framework allows the expression of alternative network addresses (e.g. different IP versions) for a particular media stream. This ability is useful in environments with both IPv4-only hosts and IPv6-only hosts.

The SBC supports ANAT formatting within the SDP offer to facilitate both an IPv4 and IPv6 address types. In addition, the SBC allows a configured address type preference whereby the user can configure which IP version takes precedence when multiple IP version types are supported. If the SBC receives an ANAT offer and only a single IP version is supported on the received interface, that IP version is used regardless of the configured IP version type preference. See sipTrunkGroup media - CLI or SIP Trunk Group - Media for configuration details.

**ICE-Lite Support**

**Overview**

Interactive Connectivity Establishment (ICE) is a protocol for Network Address Translator (NAT) traversal for multimedia sessions established with the offer/answer model. ICE uses the Session Traversal Utilities for NAT (STUN) protocol and its extension Traversal Using Relay NAT (TURN).
ICE uses STUN and TURN servers to overcome network address translation issues that can occur when an endpoint is situated behind a NAT device. ICE solves the NAT issues for media streams. Support of the ICE specification is required by WebRTC (WRTC) endpoints.

The SBC is capable of acting as an ICE-Lite agent to allow the WRTC endpoints to connect to the existing VoIP network through the SBC using the DTLS-SRTP protocol. While acting as an ICE-Lite endpoint, the SBC interconnects with endpoints that have either ICE-Lite or full-ICE implementations. ICE-Lite is a lite version of the ICE protocol, which is defined to exchange media with each other. The interconnect with ICE-Lite end points is only for the purpose of IPv4 to IPv6 inter-working and no NAT traversal procedures are supported for ICE-Lite to ICE-Lite.

ICE-Lite key points:

- **STUN message processing:**
  - Decoding received messages on media port
  - Validating the received messages
  - Authenticating the received messages
  - Encoding outgoing STUN Response messages and sending on allocated media port
  - Encrypting outgoing STUN as per the configured username/password

- **Reachable IP address:** An ICE-Lite agent has a reachable public IP address and can work with other agents that use ICE and are behind the NAT.

**ICE-Lite Implementation**

The ICE-Lite procedure starts with the offerer discovering all the IP port where it is reachable. These are known as local “candidates”. The “candidates” can be any or all of the following:

- Host candidates (Local IP port)
- Server Reflexive Candidates (External IP port allocated by NAT)
- Relay candidates (IP port on a media relay)

STUN is used to discover the Server Reflexive and Peer reflexive addresses on the NAT and TURN is used to discover the Relay candidates on the TURN relay. After the local candidates are discovered, the offerer (Full ICE Agent) sends them in the session description protocol (SDP) offer to the remote endpoints. The remote end point (SBC) discovers its own local candidates (which are only host candidates) and sends in the answer SDP to the offerer.

Once the offer/answer exchange is completed, Full ICE Agent takes the role of ICE controlling agent and performs connectivity check between the candidate pairs (from local candidate to remote candidate) by sending the STUN messages. SBC acts as controlled agent and responds to the STUN requests. Based on the success/failure of the connectivity check, a candidate pair is selected by the controlling agent to exchange the media and it sends a connectivity check on the selected pair with USE-CANDIDATE attribute to let the controlled agent know about the selected pair. The connectivity check may lead to the discovery of new local candidates due to the presence of Restricted or Symmetric NAT. These local candidates are also included in the procedure and are known as “Peer Reflexive Addresses”. SBC being a controlled ICE-Lite agent cuts thru the media after receiving USE-CANDIDATE on all components of the media stream (for example, if RTP and RTCP are required for a stream then media is only cut-through when USE-CANDIDATE is received for both RTP and RTCP).

The controlling agent sends an updated offer by using the selected local candidate in the default IP port of the media line and controlled agent (SBC) respond by sending its local candidate in the default IP port of the media line to complete the ICE-Lite procedure. The Ice-lite procedure can be restarted by the Full ice agent using ICE Restart procedures, if the Media ports changed during a call.

**Bundling of Streams**

SBC supports bundling of various streams (audio/video) over the same IP/port pair using a SDP grouping framework extension named **BUNDLE**. The **BUNDLE** is used with the SDP OFFER/ANSWER mechanism to negotiate the usage of a single address:port combination (BUNDLE...
address) for receiving media (bundled media) associated with multiple SDP media streams ("m=" lines). The address:port combination used for sending bundled media may be the same as the BUNDLE address, used to receive bundled media, depending on whether symmetric RTP is used.

The SDP media-level attribute, "bundle-only", is parsed and used to identify that specific media is only used if bundled, and resides within a BUNDLE group. The "bundle-only" attribute is a property attribute with no value.

The use of a BUNDLE group and a BUNDLE address also allows the usage of a single set of Interactive Connectivity Establishment (ICE) candidates for multiple "m=" lines.

If RTP/RTCP multiplexing is used, the same address:port combination is used for all RTP and RTCP packets.

### Single-bundle

The SBC accepts offers that express bundling with a single bundle. A bundle may have one or more streams.

#### Stream

- A stream can be tagged as bundle-only and have a port set to 0.
- The policers for the stream which represents the bundle reflect the total bandwidth for all streams within the bundle.
- Only relay scenarios are supported, any interworking causes the streams to unbundle.

#### Bundle Only

The SBC accepts offers that include bundled streams with the bundle-only attribute set.

- Offers with "m=" lines tagged as bundle-only with the port set to 0.
- Non-compliant offers which associate bundle-only with a non-zero port, the "m=" line is also accepted; the stream is treated as a bundle-only stream.
- Media attributes received with a bundle-only stream offer are handled considering that the stream is present and output in the outbound offer. (media codecs, fmtp options)

### Bundle Group

The bundling of streams is negotiated using the "a=group:BUNDLE" attribute at the session level:

- The OFFER contains the BUNDLE attribute followed by a list of streams which are part of the BUNDLE.
- The OFFER contains unique address:port combinations for each stream as the peer may not support bundling the streams.

If the peer is able to support the bundle:

- The ANSWER contains the BUNDLE attribute.
- The ANSWER contains the same address:port combination for all streams within the bundle.

### OFFER and ANSWER

The following is an example for OFFER and ANSWER mechanism.

#### OFFER
RTP and RTCP Multiplexing

The SBC allows relaying multiplexed RTP and RTCP traffic. Within a BUNDLE group, the offerer and answerer must enable RTP/RTCP multiplexing for the RTP-based media associated with the BUNDLE group.

When RTP/RTCP multiplexing is enabled, the same address:port combination is used for sending all RTP and RTCP packets associated with the BUNDLE group. Each endpoint sends the packets towards the BUNDLE address of the other endpoint. The same address:port combination may be used for receiving RTP and RTCP packets.

- SBC allows relay of multiplexed RTP and RTCP traffic for bundled and unbundled streams.
- The "a=rtcp-mux" attribute negotiates multiplexing when RTCP is enabled on both sides of the call and the call is a pass-through call.
- The rtcp-mux attribute takes precedence over the "a=rtcp." attribute when it has to accept SDPs from the peer.
- When rtcp-mux is used within a bundle it must be enabled for all streams in a bundled or disabled for all.

The above requirement also covers audio calls; the SBC supports RTP and RTCP multiplexing by relaying the rtcp-mux attribute for audio pass-through only flows. Pass-through only flows are flows where transcoding is not possible (no transcode codecs are a part of the outgoing offer).

For rtcp-mux to work on audio only calls, sdpAttributesSelectiveRelay must be enabled.

Interactions with ICE

Using bundling of media streams and the support of RTCP multiplexing ensures that only a single ICE transaction on one port is required. This limits the occurrence of NAT traversal issues and reduces the time needed to establish a call.

For the OFFER:
• The ICE data is unique for each stream.
• A candidate is included for RTCP in the initial OFFER and for RTP.
• A bundle-only "m=" line does not include ICE candidate or ufrag/pwd.

For the ANSWER:

• The ICE data matches the chosen master stream.
• A single ICE candidate line for the RTP component is only included.

**Interactions with Security**

Bundling and/or multiplexing is only allowed when security is configured to be relayed, and:

• DTLS-SRTP (and DTLS-SCTP for data) is relayed.
• SDES SRTP is relayed

⚠️ If the SBC performs security termination for any stream the call is forced to be unbundled.

**Limitations**

• Multiple bundles are not currently supported
• Bundling and rtcp-mux can only be relayed, not interworked.
• Configuration for LI or a call requiring transcoding, DTMF or security termination is unbundled.
• Bundling is not supported over the GW protocol.