CUCM 10.5 / CUBE 9.5

BT SIP Trunk Configuration Guide

This document covers service specific configuration required for interoperability with the BT SIP Trunk service. Anything which could be considered as normal CUCM configuration (such as dial plan, device pools etc.) are not within the scope of this document unless a specific configuration parameter is required in order to ensure the greatest level of interoperability with the BT SIP Trunk service.

This configuration guidance can be split into five distinct areas:

1. CUCM service parameters required for correct SIP behaviour (with regards to the BT SIP Trunk platform)
2. SIP Trunk configuration specific parameters
3. CUBE device configuration required for correct SIP behaviour (with regards to the BT SIP Trunk platform)
4. Hardware resources required for correct interaction of CUCM and the BT SIP Trunk platform
5. End device specific parameters required for correct operation

It should be further noted that the document reflects the configuration of the test environment used to execute the BT SIP Trunk platform compliance testing. Only configuration which is non-default will be covered.

1 Service Parameters

Cluster-wide parameters for the “Cisco CallManager” service:

Parameter	Default	New Setting
SIP Min-SE Value	1800	900
Fail Call Over SIP Trunk if MTP Allocation Fails	False	True

More detailed information on these changes is as follows:

SIP Min-SE Value

By default, a SIP:INVITE message sent from the BT SIP Trunk platform to CUCM had a Minimum Session Expiry (Min-SE) value set to 450ms. CUCM’s default value is 1800ms. If CUCM receives a message with a Min-SE value lower than the configured service parameter it will reject the message with a SIP:422 – Session Time Too Small error. In order to prevent this, the service parameter was reduced to “**900ms**” to accommodate the requests coming from the platform.

Fail Call Over SIP Trunk if MTP Allocation Fails

By default if MTP is required for a connection CUCM will attempt to allocate one from its configured resources, however if one is unavailable it will still allow the call to proceed without allocating the MTP. For interaction with the BT SIP Trunk, MTP is sometimes required for correct device / feature operation such as DTMF tone generation with RFC-2833 non-compliant devices. As such, MTP must be allocated to guarantee a consistent and reliable service will be received by the caller and so if MTP resource is unavailable the call should not proceed. Hence the parameter is set to “**True**”.

2 SIP Trunk Configuration Specific Parameters

The configuration of a SIP Trunk in CUCM can be split into three distinct categories:

1. SIP Profile
2. SIP Trunk Security Profile
3. SIP Trunk Configuration

SIP Profile Configuration

When interfacing between a Cisco CUBE device and CUCM where the CUBE performs the Early Offer / Delayed Offer interworking to establish early media without the need for MTP, a default SIP Profile is mostly used. However, one core parameter needs to be configured on a dedicated SIP profile as follows:

Parameter	Default Setting	New Setting
Early Offer support for voice and video calls	Disable (Default value)	Mandatory (insert MTP if needed)
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type “None (Default)”	Unchecked	Checked
Ping Interval for In-service and Partially In-service Trunks (seconds)	60	10

More detailed information on these changes is as follows:

Early Offer support for voice and video calls (insert MTP if needed)

In order to interoperate with the BT SIP Trunk platform correctly CUCM must perform Early Offer and negotiate Early Media in certain scenarios. The Cisco CUBE device has the capability to perform Early Offer to Delayed Offer interworking however doing so may impose limitations on the CUBE modes of operation (for example media flow-through rather than media flow-around). To ensure maximum flexibility in deployments CUCM should be configured to do perform Early Offer where possible. Introduced in CUCM 8.5 is the capability to do exactly that. However this feature must be explicitly enabled on the SIP profile configuration as it is not enabled by default. It should be noted that some devices running the right level of firmware will natively support this feature, whereas others will require MTP in order to interoperate correctly (see later).

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type “None (Default)”

In a CUCM / CUBE deployment it is the CUBE device which performs failover functionality between platform SBC’s when one is taken out of service. During testing a single CUBE device was used, however in a production deployment it is common to have multiple CUBE devices to remove any single points of failure in the design. There are multiple ways to do this, however to ensure optimal failover behaviours CUCM should be configured to detect any potential out-of-service CUBE devices so that it can use alternative routing where available. Introduced in CUCM 8.5 is the ability to poll an SBC (or a CUBE device in this instance) using a SIP:OPTIONS message to illicit a response and determine whether the SBC is in service or not. If no satisfactory response is gained within a pre-determined time span then the SIP Trunk which uses this profile is taken out of service for CUCM call routing purposes and CUCM will not attempt to pass any further calls to the CUBE until it is returned to service. The net effect will be that after a defined interval of polling CUCM will detect this failure and no further calls will route via the failed CUBE device. This facility is not enabled by default on CUCM and must be explicitly enabled on the SIP profile.

Ping Interval for In-service and Partially In-service Trunks (seconds)

By default if SIP:OPTIONS polling of an SBC is enabled CUCM will poll that SBC every 60 seconds and wait a further 3 seconds for a response. If there is a failure of the CUBE device it is possible to experience an extended dialling delay (up to almost 64 seconds in certain circumstances) until the CUBE is detected out of service. By reducing this parameter from the default 60 seconds down to 10 seconds this reduces that window to 22.5 seconds.

SIP Trunk Security Profile Configuration

A default SIP Trunk Security Profile is used, the core configuration parameters are:

Parameter	Default Setting	New/Suggested Setting
Device Security Mode	Non Secure	Non Secure
Incoming Transport Type	TCP+UDP	TCP+UDP
Outgoing Transport Type	**TCP**	**TCP**
Enable Digest Authentication	Unchecked	Unchecked
Nonce Validity Time (mins)	600	600
X.509 Subject Name	<Blank>	<Blank>
Incoming Port	5060	5060
Enable Application Level Authorization	Unchecked	Unchecked
Accept Presence Subscription	Unchecked	Unchecked
Accept Out-of-Dialog REFER	Unchecked	Unchecked
Accept Unsolicited Notification	Unchecked	Unchecked
Accept Replaces Header	Unchecked	Unchecked
Transmit Security Status	Unchecked	Unchecked
Allow charging header	Unchecked	Unchecked
SIP V.150 Outbound SDP Offer Filtering	Use Default Filter	Use Default Filter

The only real point to note is the Outgoing Transport Type – this is set to TCP rather than the platform default of UDP. As a Cisco CUBE device is employed then there is no reason to deviate from the default TCP mechanism of CUCM; furthermore, TCP mechanisms allow faster failure detection by CUCM (realising the TCP session is down rather than waiting for signalling timeout) so potentially allows a faster failover between multiple CUBE devices should they be deployed.

All other parameters essentially remain at default.

SIP Trunk Configuration

SIP Trunk specific configuration parameters that need to be changed from default or must be a specific parameter are:

Parameter	Default Setting	Required / New Setting
Call Routing Information – Asserted-Identity	Checked	Checked
Call Routing Information – Asserted-Type	Default	PAI
SIP Trunk Security Profile	-- Not Selected --	<Pre-configured profile>
SIP Profile	-- Not Selected --	<Pre-configured profile>
DTMF Signalling Method	No Preference	RFC 2833

More detailed information on these changes is as follows:

Call Routing Information – Asserted-Identity and Asserted-Type

By default the BT SIP Trunk platform requires that the Privacy-Asserted-ID field in SIP messaging is included to correctly populate caller identity, particularly for emergency calls. Therefore to ensure that CUCM populates this field this should be set from Default to “PAI”.

SIP Trunk Security Profile / SIP Profile

Both a SIP Trunk Security profile and a SIP Profile need to be configured to reflect the BT SIP Trunk platform requirements (as detailed previously). These then need to be applied to the specific trunks when configured.

DTMF Signalling Method

The BT SIP Trunk platform requires that all DTMF signalling uses the RFC 2833 specified mechanism. Therefore to ensure that CUCM adheres to this requirement the SIP Trunk should be configured accordingly and the DTMF Signalling Method changed from No Preference to “RFC 2833”.

3 CUBE Device Configuration

The configuration of the CUBE device can be split into three distinct categories:

1. Voice Services and General Protocol Behaviour
2. Voice Classes
3. Dial Peers

Voice Services and General Protocol Behaviour

The first part of the configuration sets up how the CUBE device behaves with SIP signalling, with the following sample configuration:

```
!
no voice hunt no-response
no voice hunt invalid-number
!
!
voice service voip
 ip address trusted list
  ipv4 <SBC 1 IP>
  ipv4 <SBC 2 IP>
  ipv4 <SBC 3 IP>
  ipv4 <SBC 4 IP>
  ipv4 <CUCM Node 1 IP>
  ipv4 <CUCM Node 2 IP>
mode border-element
allow-connections sip to sip
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
sip
 bind control source-interface <Signalling Interface>
 bind media source-interface <Media Interface>
 min-se 450 session-expires 900
 session refresh
 header-passing
 error-passthru
 asserted-id pai
 options-ping 60
 g729 annexb-all
!
!
sip-ua
 retry invite 3
 timers trying 350
!
!
```

The above configuration alters the SIP signalling timers and privacy settings ensuring that:

- Session timers allow the lower-than-default platform session refresh timers
- Error signalling is passed through the CUBE to CUCM
- Privacy-Asserted-Identity headers are allowed (a platform requirement)
- The CUBE device can probe SBC's and dynamically shut-down corresponding dial peers when the SBC is out of service
- Fail over a call in 2.5 seconds rather than the default of 32 seconds when an SBC fails while waiting for the OPTIONS pings to take the dial peer out of service.
- Treat all variants of the g.729 codec as a valid codec (to avoid on-net G.729 codec interoperability negotiation failures)

Voice Classes

The second part of the configuration deals with filtering preferred / allowed codecs and manipulating the outbound SIP signalling headers on a per-call basis:

```
voice class codec 100
 codec preference 1 g711alaw
 codec preference 2 g711ulaw
 codec preference 3 g729r8
!
voice class sip-profiles 100
 request INVITE sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone SIP/2.0"
 request REINVITE sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone SIP/2.0"
 request INVITE sip-header SIP-Req-URI modify " SIP/2.0" ";user=phone SIP/2.0"
 request REINVITE sip-header SIP-Req-URI modify " SIP/2.0" ";user=phone SIP/2.0"
!
!
```

The above configuration alters the list of allowed / negotiated codecs (along with corresponding preferences) so that:

- Only G.711 A-law, G.711 µ-law, or G.729 / G.729a (**not** Annex-B) codecs are permitted
- Invite requests to the platform correctly format the request URI to contain the "user=phone" parameter.

Dial Peers

The last part of the configuration handles the core call routing between the CUBE device and both the platform and the CUCM server(s). While dial peer configuration is fairly straightforward, there are some key parameter requirements that must be fulfilled in order to apply the voice classes and behaviours configured in the previous step and to ensure that the signalling from the CUBE device is compliant with the platform requirements.

Configuration of dial peers can be split into four distinct sections, namely:

i. CUBE device to CUCM
ii. CUCM to CUBE device
iii. CUBE device to SIP trunking platform
iv. SIP trunking platform to CUBE device

The following is a sample configuration covering the dial peers that deal with call legs from the CUBE device to CUCM. It is taken from a base configuration for three CUCM servers allowing priority routing for each server.

```
dial-peer voice 301 voip
 description CUCM Sub (Outbound)
 preference 1
 destination-pattern +44<DDI Number Range>
 session protocol sipv2
 session target ipv4:<CUCM Server 1 IP>
 session transport tcp
 voice-class codec 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 302 voip
 description CUCM Pub (Outbound)
 preference 2
 destination-pattern +44<DDI Number Range>
 session protocol sipv2
 session target ipv4:<CUCM Server 2 IP>
 session transport tcp
 voice-class codec 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
!
!
```

The key components of this example configuration are highlighted in red for one of the dial-peers. These elements set the following behaviours for calls allocated to the corresponding dial peers:

- Set the signalling to use TCP (rather than the default of UDP). Though not strictly necessary using TCP where possible does have some advantages (see previous configuration for CUCM SIP Trunk Security Profile).

- Sets the call leg to only allow one of the desired / permitted codecs (i.e. G.711 A-law, G.711 µ-law or G.729 / G.729a (without Annex B revisions)) – as defined in the voice classes section.
- Configures the CUBE device to periodically probe the end target device (in this case the individual CUCM server) such that any failed or unresponsive device automatically takes the dial peer out of service for call routing.
- Configures RFC-2833 compliant DTMF signalling as the preferred / chosen signalling method during codec negotiation.
- Disable voice activity detect (VAD) silence suppression to minimise issues with firewalls and other media gateways / border devices.

The following is a sample configuration for the dial peer corresponding to call legs from CUCM to the CUBE device:

```
dial-peer voice 2000 voip
 description CUCM to CUBE
 session protocol sipv2
 session transport tcp
 incoming called-number .T
 voice-class codec 100
 dtmf-relay rtp-nte
 no vad
!
!
```

The key components of this example configuration are highlighted in red. These elements configure the following behaviours for calls allocated to the corresponding dial peer:

- Set the signalling to use TCP (rather than the default of UDP). Though not strictly necessary using TCP where possible does have some advantages (see previous configuration for CUCM SIP Trunk Security Profile).
- Sets the call leg to only allow one of the desired / permitted codec (i.e. G.711 A-law, G.711 µ-law or G.729 / G.729a (without Annex B revisions)) – as defined in the voice classes section.
- Configures RFC-2833 compliant DTMF signalling as the preferred / chosen signalling method during codec negotiation.
- Disable voice activity detect (VAD) silence suppression to minimise issues with firewalls and other media gateways / border devices.

The next section of configuration covers dial-peers corresponding to call legs from the CUBE device to the SIP trunking platform SBC's:

```
dial-peer voice 201 voip
 description BT SIP Trunk SBC 1 (Outbound)
 preference 1
 destination-pattern .T
 session protocol sipv2
 session target ipv4:<SBC 1 IP>
 session transport tcp
 voice-class codec 100
 voice-class sip profiles 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
```

```
!
!
dial-peer voice 202 voip
 description BT SIP Trunk SBC 2 (Outbound)
 preference 2
 destination-pattern .T
 session protocol sipv2
 session target ipv4:193<SBC 2 IP>
 session transport tcp
 voice-class codec 100
 voice-class sip profiles 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
!
!
dial-peer voice 203 voip
 description BT SIP Trunk SBC 3 (Outbound)
 preference 3
 destination-pattern .T
 session protocol sipv2
 session target ipv4:<SBC 3 IP>
 session transport tcp
 voice-class codec 100
 voice-class sip profiles 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
!
!
dial-peer voice 204 voip
 description BT SIP Trunk SBC 4 (Outbound)
 preference 4
 destination-pattern .T
 session protocol sipv2
 session target ipv4:<SBC 4 IP>
 session transport tcp
 voice-class codec 100
 voice-class sip profiles 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
!
!
```

The key components of this example configuration are highlighted in red. These elements configure the following behaviours for calls allocated to the corresponding dial peer:

- Set the signalling to use TCP which is the SIP trunking platform recommended transport mechanism.
- Sets the call leg to only allow one of the desired / permitted codecs (i.e. G.711 A-law, G.711 µ-law, G.729 / G.729a (without Annex B revisions)) – as defined in the voice classes section.
- Enables the CUBE device to manipulate the outbound SIP signalling to make it conform with platform requirements regarding request URI formatting.

- Configures the CUBE device to periodically probe the end target device (in this case the individual platform SBC's) such that any failed or unresponsive device automatically takes the dial peer out of service for call routing.
- Configures RFC-2833 compliant DTMF signalling as the preferred / chosen signalling method during codec negotiation.
- Disabled voice activity detect (VAD) silence suppression to minimise issues with firewalls and other media gateways / border devices.

The final section of CUBE device example configuration covers dial-peers corresponding to call legs from the SIP trunking platform SBC's to the CUBE device:

```
dial-peer voice 1010 voip
 description BT SIP Trunk (Inbound)
 session protocol sipv2
 session transport tcp
 incoming called-number +44<DDI Number Range>
 voice-class codec 100
 dtmf-relay rtp-nte
 no vad
!
!
```

The key components of this example configuration aare highlighted in red. These elements configure the following behaviours for calls allocated to the corresponding dial peer:

- Set the signalling to use UDP which is the SIP trunking platform default transport mechanism.
- Sets the call leg to only allow one of the desired / permitted codecs (i.e. G.711 A-law, G.711 µ-law or G.729 / G.729a (without Annex B revisions)) – as defined in the voice classes section.
- Configures RFC-2833 compliant DTMF signalling as the preferred / chosen signalling method during codec negotiation.
- Disable voice activity detect (VAD) silence suppression to minimise issues with firewalls and other media gateways / border devices.

4 Hardware Resources Required for the Correct Operation of CUCM

In order to successfully place outgoing calls across the BT SIP Trunk platform from CUCM, MTP is required to be configured for some non RFC-2833 DTMF compliant devices. The use of software MTP does not scale well therefore hardware MTP must be used. Cisco IOS Enhanced Software MTP is sufficient for SIP Trunking purposes.

These hardware-based MTP devices (of which Cisco IOS Enhanced Software MTP is classed as hardware-based), should be assigned to the media resources of the device endpoints (to allow local resource use) and not the SIP Trunk.

Furthermore, because of the G.729a mandatory codec support requirement for platform calls, hardware transcoding resource may be required for devices that do not natively support the G.729a codec, such as a software-based T.38 fax solution which supports the G.711 codec only. This hardware transcoding needs to be applied to the media resources of the devices which require transcoding.

Cisco IOS Enhanced Software MTP

The number of concurrent software MTP sessions which a platform can support will depend upon the hardware of the Cisco IOS device being configured. As such, the following configuration should be considered as guidance only. Additionally, each MTP resource can only support a singular codec and therefore multiple profiles must be configured for each and every codec expected to be in use across the BT SIP Trunk platform.

Note: In order to support T.38 faxing an additional codec can (and must) be configured for each MTP profile. This codec is "**pass-through**", failure to do so will result in T.38 fax calls failing.

Sample configuration for Cisco IOS Enhanced Software MTP is as follows:

```
dspfarm profile 1 mtp
 description Soft MTP - G.711ulaw
 codec g711ulaw
 codec pass-through
 maximum sessions software 16
 associate application SCCP
!
dspfarm profile 2 mtp
 description Soft MTP - G.711alaw
 codec g711alaw
 codec pass-through
 maximum sessions software 16
 associate application SCCP
!
dspfarm profile 3 mtp
 description Soft MTP - G.729a
 codec g729ar8
 codec pass-through
 maximum sessions software 16
 associate application SCCP
```

Cisco IOS Hardware Transcoding

The number of concurrent hardware transcoding sessions which a platform can support will depend upon the hardware of the Cisco IOS device being configured. As such, the following configuration should be considered as guidance only. Furthermore by default a hardware transcoder requires one call leg to be G.711, however to cover all possibilities the following example uses "**Universal transcoding**". This enables transcoding from any codec to any codec (within the configured codec list), rather than G.711 to any codec which is the default behaviour.

Each hardware transcoding profile must be configured for each and every codec expected to be in use across the BT SIP Trunk platform.

Note: In order to support T.38 faxing an additional codec can (and must) be configured for each hardware transcoder profile. This codec is "**pass-through**", failure to do so will result in T.38 fax calls failing.

Sample configuration for Cisco IOS Hardware Transcoding is as follows:

```
dspfarm profile 4 transcode universal
 description Hardware transcoder
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec pass-through
 maximum sessions 3
 associate application SCCP
!
```

5 End Device Specific Parameters Required for Correct Operation

Within the test solution a SIP gateway was configured as an analogue fax gateway and also as a local PSTN gateway (to test for potential migration scenarios). No specific requirements for SIP dial peers were required other than setting the correct DTMF relay and codec parameters (see CUBE device configuration sections).

For typical customer deployment scenarios, however, many solutions use MGCP gateways for PSTN gateways and SCCP for analogue gateways. SCCP gateways DO NOT support standards-based T.38 faxing and so for analogue faxes must be converted to MGCP in order to enable successful faxing. Any MGCP gateways in use require additional configuration to be applied on CUCM and on the MGCP controlled Cisco IOS gateways as well.

CUCM MGCP Gateway Configuration – Product Specific Configuration Layout

The following parameters were changed from default during testing:

Parameter	Default Setting	New Setting
Type of DTMF Relay	Current GW Config	NTE-CA
Cisco Fax Relay	Disable	Disable
T38 Fax Relay	Disable	Enable

More detailed information on these changes is as follows:

Type of DTMF Relay

DTMF relay towards the BT SIP Trunk is extremely restrictive (i.e. the use of RFC 2833 compliant signalling is required). Therefore to ensure that CUCM instructs the MGCP gateway to use the correct DTMF signalling the signalling needs to be set under Call Agent control by setting the Type of DTMF Relay parameter to “**NTE-CA**”.

Cisco Fax Relay

Cisco Fax Relay uses a proprietary signalling mechanism to signal switchover to using Fax Relay and therefore will not interoperate with the BT SIP Trunk platform. Accordingly the capability must be kept disabled by setting the Cisco Fax Relay parameter to “**Disable**” (which is the default setting).

T38 Fax Relay

The BT SIP Trunk platform requires the use of T.38 fax relay to allow faxes to successfully transfer and therefore this capability must be enabled by setting the T38 Fax Relay parameter to “**Enable**”.

IOS MGCP Gateway Configuration

By default a Cisco IOS voice gateway will drop the negotiated fax rate to a rate commensurate with the negotiated voice codec (i.e. 7,200 bps for a G.729a call or 14,400 bps for a G.711 call). This can be overridden using the "**mgcp fax rate <rate>**" command should solution specific configurations require it (optional – use with caution).

Additionally redundancy can also be added to the T.38 fax data stream to counter the effects of lost packets (the important parameter being high speed redundancy) using the "**mgcp fax t38 ls_redundancy <value>**" and "**mgcp fax t38 hs_redundancy <value>**" commands.

As with other devices, the MGCP gateway must also transmit RFC2833 compliant DTMF signalling. By default it does not and an additional capability package must be enabled to do so, this is done with the use of the "**mgcp dtmf-relay voip codec all mode nte-ca**" and "**mgcp package-capability fm-package**" commands.

The following example reflects the Cisco IOS voice gateway configuration that corresponds to the CUCM MGCP configuration, but further expands it to add RFC 2833 compliant DTMF signalling, implement full T.38 fax redundancy and override the negotiated fax rate beyond the default G.729a codec restriction:

```
ccm-manager mgcp
no ccm-manager fax protocol cisco
ccm-manager music-on-hold
ccm-manager config server <ip address list>
ccm-manager config
!
mgcp
mgcp call-agent <ccm server> 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode nte-ca
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
mgcp package-capability fm-package
no mgcp package-capability res-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax rate 14400
mgcp fax t38 ecm
mgcp fax t38 ls_redundancy 5
mgcp fax t38 hs_redundancy 2
!
mgcp profile default
!
!
```

Note: This configuration assumes automatic CUCM configuration rather than manual MGCP configuration via the Cisco IOS voice gateway CLI. Any additional IOS configuration commands that were manually entered are highlighted in red.