Application Note

Media Path Optimization for a Webex Calling Local Gateway (LGW) using Cisco IOS-XE based SIP-TDM Gateway

July 2023

Table of Contents

Introduction....3
Network Topology....4
System Components....5
Hardware Requirements....5
Software Requirements....5
Deployment considerations....5
Configuring Cisco IOS-XE TDM-SIP LGW....6
Dial-peer and translation rule configurations....6
Inbound PSTN (TDM) call to Webex Calling via the TDM-SIP LGW....6
Outbound PSTN (TDM) call from Webex Calling via the TDM-SIP LGW....8
ICE-lite configuration (to be applied towards Webex Calling facing dial-peers)....10
Voice class Tenant and SIP-Profile configurations....10
Global Configurations....11
Codecs....12
Complete Configuration Example....13
Acronyms....21
Important Information....22

Introduction

In many regions around the world, especially in Asia-Pacific, TDM circuits remain the prevalent choice for PSTN connectivity. Customers in these regions wanting to utilize premises-based PSTN are currently unable to benefit from media path optimization between the Webex Calling endpoint and the TDM-SIP-based Local Gateway (LGW) due to ICE-Lite not being supported on a TDM-SIP-based IOS-XE gateway.

Due to this limitation, the media path cannot be directly routed between the TDM-SIP LGW and the endpoint in a call. In a Webex Calling Multitenant environment using a TDM-SIP LGW, this limitation may lead to media quality issues on a PSTN call due to poor network quality as the media is routed by default from the Webex Calling endpoint to the cloud to the LGW to the PSTN. Additionally, there are some countries, e.g. India, where for regulatory reasons, media should not be routed outside of the country.

Currently, ICE-Lite is supported on Cisco IOS-XE gateways only for SIP-SIP call flows, that is, a Cisco Unified Border Element (CUBE) being deployed as a LGW. If the customers using a TDM-SIP LGW are unable to change their PSTN connection type to a SIP Trunk as opposed to a TDM circuit (e.g. ISDN PRI) to benefit from ICE-lite, they can benefit from ICE-lite by looping the call on the TDM-SIP LGW, essentially making it a TDM ←→ [SIP ← → SIP] ←→SIP to Webex Calling call.

This application note primarily describes how to configure a Webex Calling TDM-SIP LGW with loopback dial-peer configurations so that ICE-Lite can be engaged for media path optimization for such a deployment. Loopback dial-peer configurations on a TDM-SIP LGW will route the calls back to the same gateway, simulating the SIP-SIP call legs for ICE negotiations towards Webex Calling and enabling media optimization whenever possible.

This document assumes the reader is knowledgeable with the terminology and configuration of Webex Calling, Webex Calling Local Gateway, Cisco IOS-XE gateways (TDM-SIP), and CUBE (SIP-SIP). The TDM-SIP gateway configuration detailed in this document is based on a lab environment using a simple dial plan to ensure a proper media path optimization functionality is achieved based on ICE negotiations via a TDM-SIP IOS-XE gateway.

- Feature configuration and most importantly the dial plan is customer specific and need an individual approach
- The features verified include – basic inbound and outbound calls, hold-resume, call transfers, call forwarding, and long-duration calls.

Network Topology

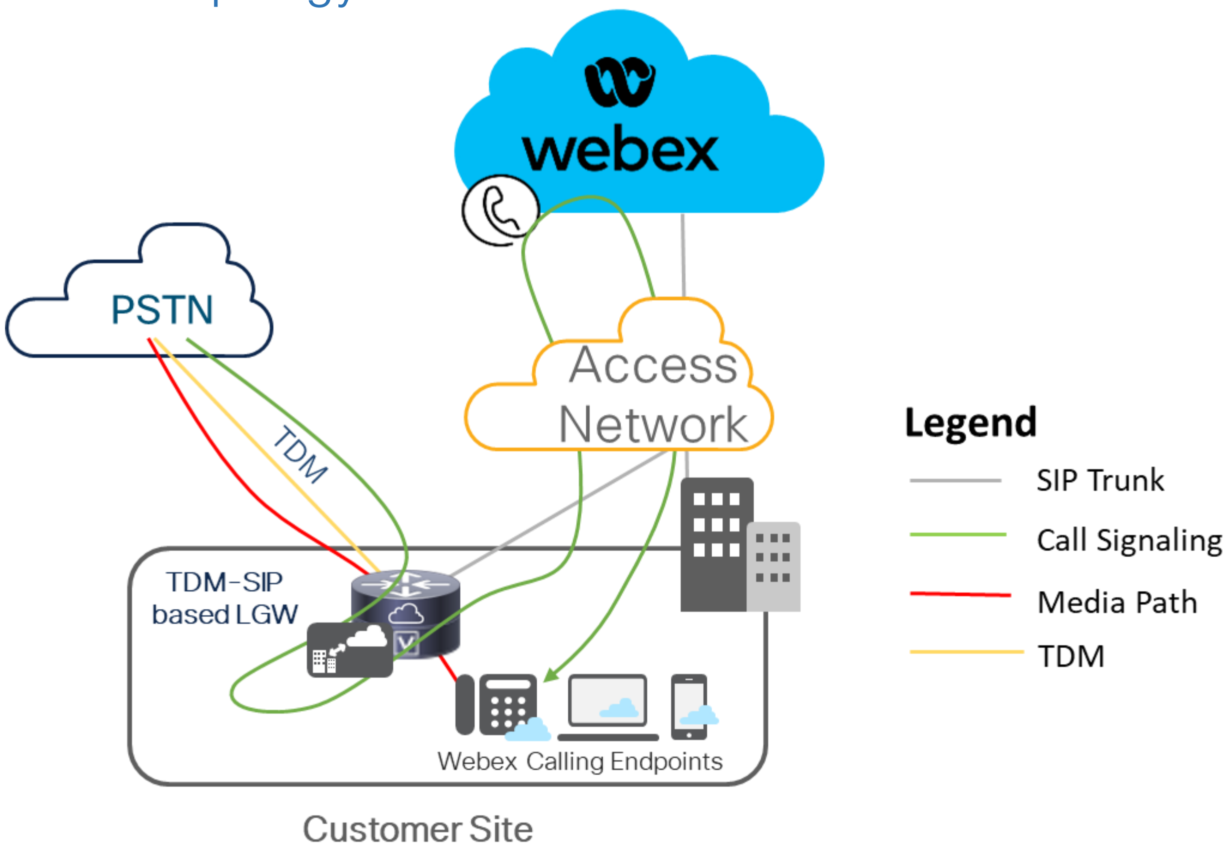

Figure 1: Network Topology

The network topology includes TDM-SIP-based LGW (registration-based) and Webex Calling Endpoints that include Cisco MPP phones, and the Webex App.

Cisco Webex Calling and Cisco TDM-SIP Local Gateway Settings:

Setting	Value
Transport from TDM-SIP GW to Webex Calling	TLS with SRTP
Transport from TDM-SIP GW to PSTN	PSTN Interface

System Components

Hardware Requirements

- Cisco TDM-SIP Gateway on Cisco ISR 4000/Cat8200/Cat8300 supported router.
- Cisco IP Phones with Multiplatform Firmware
- Cisco Webex App

Software Requirements

- Cisco SIP-TDM gateway running IOS-XE 17.12.1

Note: Earlier IOS-XE recommended releases are still valid as no explicit code changes have been made for the loopback option.

Deployment considerations

- This application note includes the relevant configuration required for a TDM-SIP-based Local Gateway to benefit from ICE-lite for media path optimization and does not present the complete Local Gateway configuration. For a complete LGW configuration, refer to https://help.webex.com/en-us/article/jr1i3r/

- If the LGW configuration does not require media path optimization, then the default configuration guidelines presented at this link should be followed. https://help.webex.com/en-us/article/jr1i3r/

- In a deployment where CUCM is present, the default configuration guideline recommends that all call routing decisions be made by the CUCM. Any incoming call onto the LGW is first sent to CUCM, and then CUCM determines if it is intended for PSTN or Webex Calling. As such, a TDM-SIP LGW will already be doing an IP-IP path {TDM ←→ [SIP to CUCM ← → SIP from CUCM] ←→SIP to Webex Calling} and will not require the loopback configuration presented in this application note as it will automatically invoke ICE-Lite for media path optimization.

- The loopback configuration presented in this application note is based on registration-based TDM-SIP LGW. However, it can be utilized for a certificate-based TDM-SIP LGW as well.

- The configuration guidelines provided in this application note assume a dedicated LGW platform with no existing voice configuration. If an existing PSTN GW deployment is being modified to also utilize the LGW function for Webex Calling, please pay careful attention to the configuration applied to ensure existing call flows and functionality are not interrupted as a result of the specific configuration being applied from this application note.

Configuring Cisco IOS-XE TDM-SIP LGW

This section covers the TDM-SIP LGW loopback dial-peer and translation rule configuration settings for inbound and outbound PSTN calls via the TDM-SIP LGW to Webex Calling.

Dial-peer and translation rule configurations

Inbound PSTN (TDM) call to Webex Calling via the TDM-SIP LGW

[PSTN (TDM) → LGW → Webex Calling]

Inbound PSTN (TDM) calls first match the incoming pots dial-peer (tag 100) and apply the translation profile to replace the DNIS (called number) by prefixing 888.

```
voice translation-rule 100
 rule 1 /^/ /888/

voice translation-profile 100
 translate called 100

voice class dpg 401
 dial-peer 401 preference 1

dial-peer voice 100 pots
 description Incoming dial-peer from PSTN
 translation-profile incoming 100
 destination dpg 401
 incoming called-number .T
 direct-inward-dial
 port 0/2/0:23
```

The call then proceeds by matching the outbound loopback dial-peer (tag 401), the session target of which points to the TDM-SIP LGW's loopback interface IP address.

```
dial-peer voice 401 voip
 description Outgoing dial-peer loopback call
 destination-pattern .T
 session protocol sipv2
 session target ipv4:10.64.100.179
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 voice-class sip bind media source-interface GigabitEthernet0/0/0
 voice-class codec 1
 no vad
```

The loopback call then comes back to the TDM-SIP LGW by matching the inbound loopback dial-peer (tag 888) and applies a translation profile to remove the 888 prefix that was added earlier.

```
voice translation-rule 888
 rule 1 /^888/ //

voice translation-profile 888
 translate called 888

voice class dpg 301
 dial-peer 301 preference 1

dial-peer voice 888 voip
 description Incoming Loopback dial-peer for PSTN to WxC
 translation-profile incoming 888
 destination dpg 301
 incoming called-number 888T
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 voice-class sip bind media source-interface GigabitEthernet0/0/0
 voice-class codec 1
 no vad
```

Finally, the outbound dial-peer facing towards Webex Calling is matched, which has the ICE-Lite configuration (voice -class stun-usage 1).

```
dial-peer voice 301 voip
 description Outgoing dial-peer to Webex Calling
 destination-pattern .T
 session protocol sipv2
 session target sip-server
 voice-class stun-usage 1
 no voice-class sip localhost
 voice-class sip tenant 5000
 srtp
 voice-class codec 1
 no vad
```

Outbound PSTN (TDM) call from Webex Calling via the TDM-SIP LGW

[Webex Calling → LGW → PSTN (TDM)]

Outgoing calls to PSTN (TDM) from Webex calling first matches the incoming Webex Calling facing VoIP dial-peer (tag 300), which applies the translation profile to replace the DNIS (called number) by prefixing 777.

```
voice translation-rule 300
 rule 1 /^/ /777/

voice translation-profile 300
 translate called 300

voice class dpg 401
 dial-peer 401 preference 1

dial-peer voice 300 voip
 description Incoming dial-peer from Webex Calling
 translation-profile incoming 300
 session protocol sipv2
 destination dpg 401
 incoming uri via 300
 voice-class stun-usage 1
 voice-class sip tenant 5000
 srtp
 voice-class codec 1
 no vad
```

The call then proceeds by matching the outbound loopback dial-peer (tag 401), the session target of which points to the TDM-SIP LGW's loopback interface IP address. This is the same loopback dial-peer that was used for inbound PSTN calls.

```
dial-peer voice 401 voip
 description Outgoing dial-peer loopback call
 destination-pattern .T
 session protocol sipv2
 session target ipv4:10.64.100.179
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 voice-class sip bind media source-interface GigabitEthernet0/0/0
 voice-class codec 1
 no vad
```

The loopback call then comes back to the TDM-SIP LGW by matching the inbound loopback dial-peer (tag 777) and applies a translation profile to remove the 777 prefix that was added earlier.

```
voice translation-rule 777
 rule 1 /^777/ //

voice translation-profile 301
 translate called 777

voice class dpg 201
 dial-peer 201 preference 1

dial-peer voice 777 voip
 description Incoming Loopback dial-peer for WxC to PSTN
 translation-profile incoming 301
 session protocol sipv2
 destination dpg 201
 incoming called-number 777T
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 voice-class sip bind media source-interface GigabitEthernet0/0/0
 voice-class codec 1
 no vad
```

Finally, the outbound PSTN facing POTS dial-peer is matched to route the call to the TDM PSTN.

```
dial-peer voice 201 pots
 description Outgoing dial-peer to PSTN
 destination-pattern .T
 port 0/2/0:23
```

The subsequent configuration shown here is similar to the Webex Calling Local Gateway configuration guide as available on https://help.webex.com/en-us/article/jr1i3r/

ICE-lite configuration (to be applied towards Webex Calling facing dial-peers)

```
voice class stun-usage 1
 stun usage firewall-traversal flowdata
 stun usage ice lite
```

Voice class Tenant and SIP-Profile configurations

```
voice class tenant 5000
 registrar dns:47846594.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
 credentials number BLR_Trunk8055_LGU username BLR_Trunk9876_LGU password 6
TIiH^cNiibfXNPdaJNdKUBGiTYFDhJd[V]HF realm BroadWorks
 authentication username BLR_Trunk9876_LGU password 6
UeTSM\MQO^bMdiEIUcVS^PFOXYEHiiRWaWPd realm BroadWorks
 authentication username BLR_Trunk9876_LGU password 6
UeTSM\MQO^bMdiEIUcVS^PFOXYEHiiRWaWPd realm 47846594.cisco-bcld.com
 no remote-party-id
 sip-server dns:47846594.cisco-bcld.com
 connection-reuse
 srtp-crypto 5000
 session transport tcp tls
 url sips
 error-passthru
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/0
 bind media source-interface GigabitEthernet0/0/0
 no pass-thru content custom-sdp
 sip-profiles 5000
 outbound-proxy dns:sy11.sipconnect-au.bcld.webex.com
 privacy-policy passthru


voice class sip-profiles 5000
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=blr_trunk9876_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
```

Global Configurations

```
voice service voip
 ip address trusted list
  ipv4 x.x.x.x y.y.y.y
  exit
 mode border-element
 media statistics
 media bulk-stats
 allow-connections sip to sip
 no supplementary-service sip refer
 no supplementary-service sip handle-replaces
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 trace
 stun
 stun flowdata agent-id 1 boot-count 4
 stun flowdata shared-secret 0 Password123$
 sip
  conn-reuse
  early-offer forced
  g729 annexb-all
  end
```

Explanation

Command	Description
allow-connections sip to sip	Allow IP2IP connections between two SIP call legs
media statistics	Enables media monitoring on the LGW
media bulk-stats	Enables the control plane to poll the data plane for bulk call statistics
fax protocol	Specifies the fax protocol
no supplementary-service sip refer no supplementary-service sip handle-replaces	Disable forwarding SIP REFER message for call transfers and replace the Dialog-ID in the Replaces header with the peer Dialog-ID
stun stun flowdata agent-id 1 boot-count 4 stun flowdata shared-secret 0 Password123$	Enable STUN globally. The STUN binding feature on the local gateway allows locally generated STUN requests to be sent over the negotiated media path. The shared secret is arbitrary as STUN is only used to open the pinhole in the firewall and allow media latching to take place in Webex Calling's Access SBC. STUN password is a pre-requisite for LGW/CUBE to send STUN message out.
early-offer forced	Forces local gateway to send the SDP information in the initial INVITE message

Codecs

G711u-Law and G711alaw voice codecs are configured for this testing and validated with g711ulaw codec. Codec preferences/list to be changed according to the need.

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g711alaw
```

Complete Configuration Example

The **show run** from the TDM-SIP LGW is being included for reference.

```
 Building configuration...

Current configuration : 14727 bytes
!
! Last configuration change at 16:21:17 IST Mon Jul 3 2023
!
version 17.12
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname TDM-SIP-ICE-DUT
!
boot-start-marker
boot system bootflash:isr4300-universalk9.17.12.01prd3.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
card type t1 0 2
logging queue-limit 1000000
logging buffered 100000
no logging rate-limit
no logging console
no aaa new-model
clock timezone IST 5 30
!
ip vrf vrf1
 rd 1:1
!
ip vrf vrf2
 rd 2:1
!
ip name-server 72.163.128.140
!
login on-success log
!
ipv6 unicast-routing
!
subscriber templating
!
vtp version 1
multilink bundle-name authenticated
!
isdn switch-type primary-5ess
!
```

```
trunk group PSTN
 hunt-scheme sequential
!
crypto pki trustpoint TP-self-signed-3603010091
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3603010091
 revocation-check none
 rsakeypair TP-self-signed-3603010091
 hash sha256
!
crypto pki trustpoint SLA-TrustPoint
 enrollment terminal
 revocation-check none
 hash sha256
!
crypto pki trustpoint dummyTp
 revocation-check crl
 hash sha256
!
crypto pki certificate chain TP-self-signed-3603010091
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33363033 30313030 3931301E 170D3230 30333031 31323137
  34345A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 36303330
  31303039 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 01008C64 9890E67E 12A504A0 0EA068AD FF66893D F7DE506A 07058EB6
  86D94D2E 96C38422 3B918238 28FD78C5 AD639201 4309B3AB 1D67A4BA 9338555D
  F03FF987 21AF8FFC 2993F0A3 8B75F4AA 96A71E6E 2C7396EB 37F924A7 076111A9
  39CD47FC ABA49C61 A2E16D39 C2A4EAAE 647B0464 4E8CF546 4BC6F468 EE9F70D6
  4F5340FE DF3FE510 90A3E927 A681F9C4 97EE35DF 799D9BBA 54933C03 26E744FA
  E5B0FE23 AC3B3D45 0EAC8D6B 0B1AC98D A375DAFC CA4ED250 D2635290 D7C88B20
  14F0F872 5872FF5F EB604FA2 2F6973EB D6C74177 58A85878 2297FA3F 30407634
  756E30DB 290E3012 FD85F92F 5F5A40C7 AC67413A 193B0B15 8C079C6B 078B5923
  92792DF1 B6670203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 14246E76 31038320 19B85FB8 1246D9E5 7FDF9298
  B8301D06 03551D0E 04160414 246E7631 03832019 B85FB812 46D9E57F DF9298B8
  300D0609 2A864886 F70D0101 05050003 82010100 0723E034 EEA1B311 DADCF5F2
  DB5F2F67 3267235E CD252585 AECAE5EB 5CBF0CA3 70CBA252 85965CA4 7633DB4C
  4A4B9B28 DE4CE67F CFC8F8A9 26387BC4 1511F18B 4464FBA2 D5183354 05ED6CDD
  5921B1B8 F973DDA6 762379B9 EB85EAB4 958FF5FA A59C7F4D B923A638 53C1E4E0
  62BDB9B2 3D43F4D2 BAEF0662 4FAE9C56 D97A77AE F9BE8E42 FA9F4D75 BFD6DBCC
  5F4EC6B8 E420ADA9 22FA1266 4437511A 68622FD8 6EB828DF 1BCD05DA D8C45C35
  F2F8797A E37CD314 D22A9147 F3006DFE 8F962B31 EA8F0892 806DD770 ADCCA2CA
  7168F681 A9A1B50E 0915AF52 8246D2BF 5A6CE579 FEE96082 7C7071E1 E01E679A
  05245BF1 F3C8CDC1 19CB2CC2 D4E13C8F 79061A1E
       quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  3082031B 30820203 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  2F310E30 0C060355 040A1305 43697363 6F311D30 1B060355 04031314 4C696365
  6E73696E 6720526F 6F74202D 20444556 301E170D 31333034 32343231 35353433
  5A170D33 33303432 34323135 3534335A 302F310E 300C0603 55040A13 05436973
  636F311D 301B0603 55040313 144C6963 656E7369 6E672052 6F6F7420 2D204445
  56308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
  01009C56 7101D61E DF2EBCC3 BA7AE0DB B241B3B4 328A9B00 EB8A80D0 2AA86F5E
  F1AEBFDE B67BD6AD 7DAD7B43 F582753B FFCC1CA5 A7841A07 6934D3AF 99078EF6
  179196FA 4FB3F2ED 3942C756 BF1CA0A9 CC98A7A7 F9E43724 D9E61D47 89E9E792
  DD9F27B4 517C2BDE D0EB5B9A 787BA085 D9BBF003 F0563BE0 A4450C8F 127B5583
  3EBC1385 2D9BAD98 68D3AE07 5C27987C 6B814B99 0686B14A 5F61753C 813089E6
  AEC48C68 F6D45267 0E365F44 B4456E11 96DCB950 233C8ADB 9FEEBAF1 2B5F3BB6
  7CE521B5 F277EBF6 03B7B0A4 958C9C7D 5460C20B CF9CCFC7 14B80F58 B5268947
```

```
  6D081172 26916B41 FB07DF42 EB9B9408 EC346138 23FBD8C4 19909697 A30845F3
  01C50203 010001A3 42304030 0E060355 1D0F0101 FF040403 02010630 0F060355
  1D130101 FF040530 030101FF 301D0603 551D0E04 16041443 214521B5 FB217A1A
  4D1BB702 36E664CB EC8B6530 0D06092A 864886F7 0D01010B 05000382 01010085
  F1B1F2AE AE7D2F9C AB0351C3 29E3F1AE 982DF11F 5E3C90F6 00B3CDED 5A1491FB
  DF07E06C AA0F4325 9FB4C4AE 2080F675 8C3B7AC5 4EAAA03E C5B50A2F 670AFF87
  EDA6462F CFC43967 C024AB32 EE3CCDCF A04B9DAE 1BBABBDA C8DF5587 CF51CB1C
  005A282F 8B518A5A 8C6F9B3C AABA3446 32EF3A75 C2F45450 7A9BCFD3 0C8BE54A
  11872DE0 CF1200D0 D1018FD9 AC685968 167E421C 9BC394ED 9BC85463 83B28146
  07B2BDED DFC1605B 4D16007B 68723E25 55908512 4EEB0A70 B2A74C2A CB1EC882
  C3215B87 6FC74304 241E59D7 C7C02C6D BD3042F5 196E8133 7A4446A4 81216E70
  CF52CF22 50A7D23E FA9F6B07 FB0F6386 9DCC3BBC 65250693 38CF6BA6 CB8EFD
       quit
crypto pki certificate chain dummyTp
!
!
!
voice rtp send-recv
!
voice service voip
 ip address trusted list
 no ip address trusted authenticate
 media statistics
 media bulk-stats
 allow-connections sip to sip
 no supplementary-service sip refer
 no supplementary-service sip handle-replaces
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 trace
  shutdown
 stun
  stun flowdata agent-id 1 boot-count 12
  stun flowdata shared-secret 7 104D000A061811021F0725282D3B303A
 sip
  early-offer forced
  g729 annexb-all
!
!
voice class uri 300 sip
 pattern :8934
voice class stun-usage 1
 stun usage firewall-traversal flowdata
 stun usage ice lite
!
voice class sip-profiles 4000
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>"
"<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=tdm-ice-gw-lgw-reg-
trunk9736_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
!
!
voice class sip-profiles 5000
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>"
```

```
"<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=blr_trunk9876_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
!
voice class dpg 301
 dial-peer 301 preference 1
!
voice class dpg 200
 dial-peer 201 preference 1
!
voice class dpg 401
 dial-peer 401 preference 1
!
voice class tenant 200
 registrar dns:72436457.int10.bcld.webex.com scheme sips expires 240 refresh-ratio
50 tcp tls
  credentials number TDM-ICE-GW-LGW-Reg-Trunk3069_LGU username TDM-ICE-GW-LGW-Reg-
Trunk9736_LGU password 6 U\c^JL_[UOKFUaDVF`D]`CeMZMM_VcQFIZFK realm BroadWorks
  authentication username TDM-ICE-GW-LGW-Reg-Trunk9736_LGU password 6
`WfEMXHgcSJSF\WTfDRXT\F[IaCed[CBTWcY realm BroadWorks
 no remote-party-id
 sip-server dns:72436457.int10.bcld.webex.com
 connection-reuse
 session transport tcp tls
 url sips
 error-passthru
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/0
 bind media source-interface GigabitEthernet0/0/0
 no pass-thru content custom-sdp
 sip-profiles 4000
 outbound-proxy dns:hs2.sse.lgw.bcld.webex.com
 privacy-policy passthru
!
voice class tenant 5000
 registrar dns:47846594.cisco-bcld.com scheme sips expires 240 refresh-ratio 50
tcp tls
  credentials number BLR_Trunk8055_LGU username BLR_Trunk9876_LGU password 6
TIiH^cNiibfXNPdaJNdKUBGiTYFDhJd[V]HF realm BroadWorks
  authentication username BLR_Trunk9876_LGU password 6
UeTSM\MQO^bMdiEIUcVS^PFOXYEHiiRWaWPd realm BroadWorks
 no remote-party-id
 sip-server dns:47846594.cisco-bcld.com
 connection-reuse
 srtp-crypto 5000
 session transport tcp tls
 url sips
 error-passthru
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/0
 bind media source-interface GigabitEthernet0/0/0
 no pass-thru content custom-sdp
 sip-profiles 5000
 outbound-proxy dns:sy11.sipconnect-au.bcld.webex.com
 privacy-policy passthru
!
voice class srtp-crypto 1
 crypto 1 AES_CM_128_HMAC_SHA1_80
!
voice class srtp-crypto 5000
```

```
 crypto 1 AES_CM_128_HMAC_SHA1_80
!
voice mlpp
!
voice translation-rule 100
 rule 1 /^/ /888/
!
voice translation-rule 300
 rule 1 /^/ /777/
!
voice translation-rule 777
 rule 1 /^777/ //
!
voice translation-rule 888
 rule 1 /^888/ /+/
!
voice translation-profile 100
 translate called 100
!
voice translation-profile 300
 translate called 300
!
voice translation-profile 301
 translate called 777
!
voice translation-profile 888
 translate called 888
!
voice-card 0/1
 no watchdog
!
voice-card 0/2
 dsp services dspfarm
 no watchdog
!
voice-card 0/4
 dsp services dspfarm
 no watchdog
!
diagnostic bootup level minimal
!
no license feature hseck9
license udi pid ISR4351/K9 sn FDO2022065V
license boot suite AdvUCSuiteK9
license boot level securityk9
license smart url https://smartreceiver-stage.cisco.com/licservice/license
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
license smart transport smart
memory free low-watermark processor 66974
!
spanning-tree extend system-id
!
enable password lab
!
username lab privilege 15 password 0 lab
!
redundancy
 mode none
!
controller T1 0/2/0
 framing esf
 linecode b8zs
 cablelength long 0db
```

```
 pri-group timeslots 1-20,24
!
controller T1 0/2/1
 framing esf
 linecode b8zs
 cablelength long 0db
!
interface GigabitEthernet0/0/0
 ip address 10.64.100.179 255.255.255.128
 negotiation auto
!
interface GigabitEthernet0/0/1
 ip address 8.43.0.75 255.255.0.0
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/2
 ip address 9.45.35.101 255.255.0.0
 shutdown
 negotiation auto
!
interface Service-Engine0/1/0
!
interface Service-Engine0/2/0
!
interface Serial0/2/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 trunk-group PSTN 1
!
interface Service-Engine0/4/0
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
ip forward-protocol nd
ip tftp source-interface GigabitEthernet0/0/0
ip ftp username test
ip ftp password test123
ip dns server
ip http server
ip http authentication local
ip http secure-server
ip http client proxy-server proxy-wsa.esl.cisco.com proxy-port 80
!
ip route 0.0.0.0 0.0.0.0 10.64.100.129
ip route 72.0.0.0 255.0.0.0 10.65.86.1
ip route 202.153.0.0 255.255.0.0 8.44.22.13
ip ssh bulk-mode 131072
!
control-plane
!
!
voice-port 0/2/0:23
!
voice-port 0/1/0
!
voice-port 0/1/1
```

```
!
voice-port 0/1/2
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
dial-peer voice 301 voip
 description Outgoing dial-peer to WxC
 destination-pattern .T
 session protocol sipv2
 session target sip-server
 voice-class stun-usage 1
 no voice-class sip localhost
 voice-class sip tenant 5000
 srtp
 codec g711ulaw
 no vad
!
dial-peer voice 888 voip
 description Incoming Loopback dial-peer for PSTN to WxC
 translation-profile incoming 888
 destination dpg 301
 incoming called-number 888T
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 voice-class sip bind media source-interface GigabitEthernet0/0/0
 codec g711ulaw
 no vad
!
dial-peer voice 300 voip
 description Incoming dial-peer from WxC
 translation-profile incoming 300
 session protocol sipv2
 destination dpg 401
 incoming uri via 300
 voice-class stun-usage 1
 voice-class sip tenant 5000
 srtp
 codec g711ulaw
 no vad
!
dial-peer voice 401 voip
 description Outgoing dial-peer loopback call
 destination-pattern .T
 session protocol sipv2
 session target ipv4:10.64.100.179
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 voice-class sip bind media source-interface GigabitEthernet0/0/0
 codec g711ulaw
 no vad
!
dial-peer voice 201 pots
 description Outgoing dial-peer  PSTN
 destination-pattern .T
 port 0/2/0:23
!
dial-peer voice 777 voip
 description Incoming Loopback dial-peer for WxC  to PSTN
 translation-profile incoming 301
 session protocol sipv2
```

```
 destination dpg 200
 incoming called-number 777T
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 voice-class sip bind media source-interface GigabitEthernet0/0/0
 codec g711ulaw
 no vad
!
dial-peer voice 100 pots
 description Incoming dial-peer from PSTN
 translation-profile incoming 100
 destination dpg 401
 incoming called-number .T
 direct-inward-dial
 port 0/2/0:23
!
gateway
 media-inactivity-criteria all
 timer receive-rtcp 1000
 timer receive-rtp 86400
!
sip-ua
transport tcp tls v1.2
connection-reuse
 crypto signaling default trustpoint dummyTp
!
alias exec cl clear logg
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 privilege level 15
 password lab
 no activation-character
 login
 transport preferred telnet
 transport input telnet ssh
 stopbits 1
line vty 5 14
 login
 transport input ssh
!
network-clock synchronization automatic
ntp server 8.43.63.50
call-home
 ! If contact email address in call-home is configured as sch-smart-
licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as
contact email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  no destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
!
netconf-yang
netconf-yang ssh port 831
end
```

Acronyms

Acronym	Definitions
TDM	Time Division Multiplexing
ICE	Interactive Connectivity Establishment
GW	Gateway
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
LGW	Local Gateway
SIP	Session Initiation Protocol
SP	Service Provider

Important Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
CiscoSystems
International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134- 1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

AsiaPacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799