IntelePeer SIP Trunking with TLS:

Connecting Cisco Unified Communications Manager 11.5.1 with Cisco Unified Border Element (CUBE 11.6.0) on ISR 4321/K9 [IOS-XE 16.5.1b] using Secure SIP

November 13, 2017
Table of Contents

Introduction .................................................................................................................. 5
Network Topology ......................................................................................................... 6
System Components ...................................................................................................... 7
   Hardware Requirements ............................................................................................. 7
   Software Requirements .............................................................................................. 7
Features ......................................................................................................................... 8
   Features Supported Over TLS .................................................................................. 8
   Features Not Supported Over TLS .......................................................................... 8
Caveats .......................................................................................................................... 8
Configuration ............................................................................................................... 9
Confignuring Cisco Unified Border Element (CUBE) .................................................... 9
   Network Interface ..................................................................................................... 9
   Global CUBE Settings ............................................................................................. 10
   Codecs ...................................................................................................................... 11
   Dial Peer .................................................................................................................. 11
   Call Flow .................................................................................................................. 14
   Configuration Example ............................................................................................ 16
Configuring Cisco Unified Communications Manager ................................................ 29
   Cisco UCM Version .................................................................................................. 29
   Cisco Call Manager Service Parameters .............................................................. 29
   Offnet Calls via IntelePeer SIP Trunk ...................................................................... 30
   Dial Plan ................................................................................................................... 38
Secure Conference Bridge Configuration ..................................................................... 42
   Generate an RSA KeyPair for the Gateway ............................................................ 42
   Create a Trustpoint ................................................................................................. 42
   Install the Root CA Certificate to the Local Trustpoint .......................................... 42
   Enroll with the CA Root and install the Local Identity Certificate ........................... 42
   Configure Media Resources on CUCM .................................................................. 42
   Configure Cisco IOS Media Resources .................................................................. 43
Secure Voicemail Integration ....................................................................................... 48
   Configure CUC ......................................................................................................... 48
Fax Gateway Configuration.................................................................................................................. 58
  Generate RSA Key-Pair for Fax Gateway ....................................................................................... 58
  Create a Trustpoint .......................................................................................................................... 58
  Install the Root CA Certificate to the Local Trustpoint ............................................................... 58
  Enroll with the CA Root and Install the Local Identity Certificate ............................................ 58
  Voice Port Configuration .................................................................................................................. 58
  Global Configuration ....................................................................................................................... 58
  POTS Dial-Peer ................................................................................................................................ 59
  VoIP Dial-Peers ............................................................................................................................... 59
  Acronyms............................................................................................................................................... 60
  Important Information....................................................................................................................... 61
Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Network Topology</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2</td>
<td>CUBE High Availability</td>
<td>6</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Outbound Voice Call</td>
<td>14</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Inbound Voice Call</td>
<td>14</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Outbound Fax Call</td>
<td>15</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Inbound Fax Call</td>
<td>15</td>
</tr>
<tr>
<td>Figure 7</td>
<td>PBX to PBX via Spectrum Call</td>
<td>15</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Cisco UCM Version</td>
<td>29</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Service Parameters</td>
<td>29</td>
</tr>
<tr>
<td>Figure 10</td>
<td>SIP Trunk Security Profile</td>
<td>30</td>
</tr>
<tr>
<td>Figure 11</td>
<td>SIP Profile</td>
<td>32</td>
</tr>
<tr>
<td>Figure 12</td>
<td>SIP Profile (Cont.)</td>
<td>33</td>
</tr>
<tr>
<td>Figure 13</td>
<td>SIP Profile (Cont.)</td>
<td>34</td>
</tr>
<tr>
<td>Figure 14</td>
<td>SIP Trunks List</td>
<td>35</td>
</tr>
<tr>
<td>Figure 15</td>
<td>SIP Trunk to CUBE</td>
<td>35</td>
</tr>
<tr>
<td>Figure 16</td>
<td>SIP Trunk to CUBE (Cont.)</td>
<td>36</td>
</tr>
<tr>
<td>Figure 17</td>
<td>SIP Trunk to CUBE (Cont.)</td>
<td>37</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Route Patterns List</td>
<td>38</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Route Pattern for Voice</td>
<td>39</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Route Pattern for Fax</td>
<td>40</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Conference Bridge</td>
<td>42</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Voicemail SIP Certificate</td>
<td>48</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Phone System</td>
<td>49</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Port Group</td>
<td>50</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Port Group (Cont.)</td>
<td>50</td>
</tr>
<tr>
<td>Figure 26</td>
<td>Port Configuration</td>
<td>51</td>
</tr>
<tr>
<td>Figure 27</td>
<td>Server Configuration in Port Group</td>
<td>52</td>
</tr>
<tr>
<td>Figure 28</td>
<td>CUC Root Certificate</td>
<td>53</td>
</tr>
<tr>
<td>Figure 29</td>
<td>SIP Trunk Security Profile for Voicemail Trunk</td>
<td>54</td>
</tr>
<tr>
<td>Figure 30</td>
<td>SIP Trunk For Unity Connection</td>
<td>55</td>
</tr>
<tr>
<td>Figure 31</td>
<td>SIP Trunk For Unity Connection (Cont.)</td>
<td>56</td>
</tr>
<tr>
<td>Figure 32</td>
<td>SIP Trunk For Unity Connection (Cont.)</td>
<td>57</td>
</tr>
</tbody>
</table>
Introduction

Service Providers today, such as IntelePeer, are offering alternative methods to connect to the PSTN via their IP networks. Most of these services utilize SIP as the primary signaling method and centralized IP to TDM POP gateways to provide on-net and off-net services.

A demarcation device between these services and customer owned services is recommended. As an intermediary device between Cisco Unified Communications Manager and IntelePeer network, Cisco Unified Border Element (CUBE) ISR 4321/K9 running IOS-XE 16.5.1b can be used. The Cisco Unified Border Element provides demarcation, security, interworking and session control services for Cisco Unified Communications Manager 11.5.1 connected to IntelePeer network.

This document assumes the reader is knowledgeable with the terminology and configuration of Cisco Unified Communications Manager (CUCM). Only configuration settings specifically required for IntelePeer interoperability are presented. Feature configuration and most importantly the dial plan are customer specific and need individual approach.

- This application note describes how to configure a Cisco Unified Communications Manager (Cisco UCM) 11.5.1 and Cisco Unified Border Element (CUBE) on ISR 4321/K9 [IOS-XE 16.5.1b] for connectivity to IntelePeer SIP Trunking service available in the former IntelePeer Business service area¹. The deployment model covered in this application note is CPE (Cisco UCM 11.5.1) to PSTN (IntelePeer).

- Testing was performed in accordance to IntelePeer generic SIP Trunking test methodology and among features verified were – basic calls, DTMF transport, Music on Hold (MOH), unattended and attended transfers, call forward, conferences and interoperability with Cisco Unity Connection (CUC).

- The Cisco UCM configuration detailed in this document is based on a lab environment with a simple dial-plan used to ensure proper interoperability between IntelePeer SIP network and Cisco Unified Communications. The configuration described in this document details the important configuration settings to have enabled for interoperability to be successful and care must be taken by the network administrator deploying CUCM to interoperate to IntelePeer SIP Trunking network.

This application note does not cover the use of Calling Search Spaces (CSS) or partitions on Cisco UCM. To understand and learn how to apply CSS and partitions refer to the cisco.com link below:

Network Topology

Figure 1: Network Topology

Figure 2: CUBE High Availability
System Components

**Hardware Requirements**
- Cisco UCSC-C240-M3S VMWare host running ESXi 5.5 Standard
- Cisco ISR4431/K9 router as CUBE
- Cisco ISR4431/K9 (1RU) processor with 1684579K/6147K bytes of memory with 4 Gigabit Ethernet interfaces
- Cisco 2851 Fax Gateway
- IP phones 9971 (SIP) and 8945 (SIP)
- Cisco 3945 router for hardware Conference Bridge

**Software Requirements**
- Cisco Unified Communications Manager 11.5.1
- Cisco Unity Connection 11.5.1
- IOS 16.05.01b for ISR 4431/K9 Cisco Unified Border Element
- Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.05.01b, RELEASE SOFTWARE (fc1)
- IOS 15.1(4)M5 for Cisco 2851 Fax Gateway
Features

Features Supported Over TLS
- Incoming and outgoing off-net calls using G711ULaw
- Call hold
- Call transfer (unattended and attended)
- Call conference
- Call forward (all, busy and no answer)
- Calling Line (number) Identification Presentation (CLIP)
- Calling Line (number) Identification Restriction (CLIR)
- DTMF relay (both directions) (RFC2833)
- Media flow-through on Cisco UBE
- Fax (G.711 pass-through and T38)

Features Not Supported Over TLS
- Cisco IP phones used in this test do not support blind transfer
- In HA redundancy mode, the primary cube will not take over the primary/active role after a reboot/network outage

Caveats
- Caller ID is not updated after attended or unattended transfers to off-net phones. This is due to a limitation on Cisco UBE and will be resolved in the next release. The issue does not impact the calls.
- CUCM Conference Bridge only supports non-secure conferencing. External Conference Bridge is required for secure conferencing.
- G.711 Pass-through fax transmitted in RTP. First call established in SRTP, when fax gateway sends Re-Invite for fax call it falls back to RTP
Configuration

Configuring Cisco Unified Border Element (CUBE)

Network Interface

Configure Ethernet IP address and sub interface. The IP address and VLAN encapsulation used are for illustration only, the actual IP address can vary. For SIP trunks two IP addresses must be configured - for LAN and WAN. An additional Virtual IP Address (VIP) is required for the LAN and WAN as defined by the redundancy group 1 ip XXX.XXX.XXX.V exclusive statement.

interface GigabitEthernet0/0/0
  ip address XXX.XXX.XXX.A 255.255.255.128
  negotiation auto
  redundancy rii 2
  redundancy group 1 ip XXX.XXX.XXX.V exclusive
!
interface GigabitEthernet0/0/1
  ip address 10.80.11.17 255.255.255.0
  negotiation auto
  redundancy rii 1
  redundancy group 1 ip 10.80.11.30 exclusive
Global CUBE Settings
In order to enable CUBE IP2IP gateway functionality, enter the following:

```
voice service voip
no ip address trusted authenticate
mode border-element
allow-connections sip to sip
redundancy-group 1
fax protocol pass-through g711ulaw
sip
   bind control source-interface GigabitEthernet0/0/0
   bind media source-interface GigabitEthernet0/0/0
session transport tcp tls
rel1xx supported "rel100"
header-passing
asserted-id pai
early-offer forced
midcall-signaling passthru
privacy-policy passthru
```

**Explanation**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-connections sip to sip</td>
<td>Allow IP2IP connections between two SIP call legs</td>
</tr>
<tr>
<td>fax protocol</td>
<td>Specifies the fax protocol</td>
</tr>
<tr>
<td>asserted-id</td>
<td>Specifies the type of privacy header in the outgoing SIP requests and response messages</td>
</tr>
<tr>
<td>early-offer forced</td>
<td>Enables SIP Delayed-Offer to Early-Offer globally</td>
</tr>
<tr>
<td>midcall-signaling passthru</td>
<td>Passes SIP messages from one IP leg to another IP leg</td>
</tr>
<tr>
<td>session transport tcp tls</td>
<td>Enable TLS</td>
</tr>
</tbody>
</table>
**Codecs**
G711Ulaw is used as the preferred codec for this testing and changed the preferences according to the test plan description

```plaintext
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
```

**Dial Peer**
Cisco UBE uses dial-peers to route the call accordingly based on the digits

```plaintext
dial-peer voice 10 voip
description Incoming from CUCM
huntstop
session protocol sipv2
session transport tcp tls
incoming called-number [0-9]T
voice-class codec 2
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/1
voice-class sip bind media source-interface GigabitEthernet0/0/1
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax-relay sg3-to-g3
fax rate disable
fax nsf 000000
fax protocol pass-through g711ulaw
no vad
!
dial-peer voice 20 voip
description Outgoing to intelepeer
huntstop
destination-pattern [0-9]T
session protocol sipv2
session target dns:user@domain.com
session transport tcp tls
voice-class codec 2
voice-class sip conn-reuse
```
voice-class sip options-ping 60
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/0
voice-class sip bind media source-interface GigabitEthernet0/0/0
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax-relay sg3-to-g3
fax rate disable
fax nsf 000000
fax protocol pass-through g711ulaw
no vad
!
dial-peer voice 30 voip
description Incoming from intelepeer
huntstop
session protocol sipv2
session transport tcp tls
incoming called-number +1980
voice-class codec 2
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/0
voice-class sip bind media source-interface GigabitEthernet0/0/0
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax-relay sg3-to-g3
fax rate disable
fax nsf 000000
fax protocol pass-through g711ulaw
no vad
!
dial-peer voice 40 voip
description Outgoing to CUCM
huntstop
destination-pattern +1980
session protocol sipv2
session target ipv4:10.80.11.2:5061
session transport tcp tls
voice-class codec 2
voice-class sip options-ping 60
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/1
voice-class sip bind media source-interface GigabitEthernet0/0/1
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax-relay sg3-to-g3
fax rate disable
fax nsf 000000
fax protocol pass-through g711ulaw
no vad
Call Flow

In the sample configuration presented here, Cisco UCM is provisioned with four-digit directory numbers corresponding to the last four DID digits. No digit manipulation is performed on the Cisco UBE.

For incoming PSTN calls, the Cisco UBE presents the full ten-digit DID number to Cisco UCM. The Cisco UCM picks up the last 4 significant Digits configured under SIP Trunk and routes the call based on those 4 digits. Voice calls are routed to IP phones; Fax calls are routed via a 4-digit route pattern over a SIP trunk that terminates on the Fax Gateway and in turn to the VentaFax client connected to the Fax Gateway.

CPE callers make outbound PSTN calls by dialing a “7” prefix followed by the destination number. For outbound fax calls from the analog fax endpoint, Cisco fax Gateway sends to Cisco UCM the DID with leading access code “7”. A “7.@” route pattern strips the prefix and routes the call with the remaining digits via a SIP trunk terminating on the Cisco UBE for Voice call or Fax. For PBX to PBX via IntelePeer, Caller dial 7 prefix followed by the target 1+10Digit DID no for that extension number, 7 was stripped and the 1+10 digits number was send to Cisco UBE, Cisco UBE sends the full 1+10 digits DID under Dial Peer 20 and send to Spectrum network which will direct back to Cisco UBE and handled same as normal incoming PSTN call. For International calls same pattern 7 followed by 011, country code and calling no is used.

![Outbound Voice Call Diagram](image1)

**Figure 3: Outbound Voice Call**

![Inbound Voice Call Diagram](image2)

**Figure 4: Inbound Voice Call**
Figure 5: Outbound Fax Call

Figure 6: Inbound Fax Call

Figure 7: PBX to PBX via Spectrum Call
Configuration Example

The following configuration snippet contains a sample configuration of CUBE with all parameters mentioned previously

**Active Cisco UBE**

```
intelPeerCube2#sh run
Building configuration...
Current configuration : 14586 bytes

Last configuration change at 11:21:44 UTC Thu Sep 7 2017 by cisco

version 16.5
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core

hostname intelPeerCube2

boot-start-marker
boot-end-marker

vrf definition Mgmt-intf

address-family ipv4
exit-address-family

address-family ipv6
exit-address-family

enable secret 5 ************

no aaa new-model

ip name-server 8.8.8.8

subscriber templating

multilink bundle-name authenticated

crypto pki trustpoint lynclabcc-DC-CA
enrollment terminal
serial-number none
ip-address 10.80.11.30
subject-name CN=intelPeerCube2
revocation-check none
rsakeypair itpcube

crypto pki trustpoint "DigiCert SHA2 Secure Server CA"
enrollment terminal
```
quit

voice service voip
no ip address trusted authenticate
mode border-element
allow-connections sip to sip
redundancy-group 1
fax protocol pass-through g711ulaw

sip
bind control source-interface GigabitEthernet0/0/0
bind media source-interface GigabitEthernet0/0/0
session transport tcp tls
rel1xx supported "rel100"
header-passing
asserted-id pai
early-offer forced
midcall-signaling passthru
privacy-policy passthru

voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8

voice class codec 2
codec preference 1 g729r8
codec preference 2 g711ulaw

voice class sip-profiles 100
request INVITE sip-header Diversion modify "<sip:(.*)@(.*)>" "<sip:9802331@2>

voice class srtp-crypto 1
crypto 1 AES_CM_128_HMAC_SHA1_32
voice translation-rule 1
  rule 1 /980233\(9116)\)/ /1/
!
voice translation-profile 10
  translate called 1
!
license udi pid ISR4321/K9 sn FDO19220MQ9
license accept end user agreement
license boot suite AdvUCSuiteK9
license boot level appxk9
license boot level uck9
license boot level securityk9
!
diagnostic bootstrap level minimal
spanning-tree extend system-id
!
username abcdef privilege 15 password 0 mnopqrst
!
redundancy
  mode none
  application redundancy
    group 1
      name voice-b2bha
      timers delay 30 reload 60
      control GigabitEthernet0/1/0 protocol 1
      data GigabitEthernet0/1/0
      track 1 shutdown
      track 2 shutdown
!
track 1 interface GigabitEthernet0/0/1 line-protocol
!
track 2 interface GigabitEthernet0/0/0 line-protocol
!
interface GigabitEthernet0/0/0
  ip address XXX.XXX.XXX.A 255.255.255.128
  negotiation auto
  redundancy rii 2
  redundancy group 1 ip XXX.XXX.XXX.V exclusive
!
interface GigabitEthernet0/0/1
  ip address 10.80.11.17 255.255.255.0
  negotiation auto
  redundancy rii 1
  redundancy group 1 ip 10.80.11.30 exclusive
!
interface GigabitEthernet0/1/0
  ip address 20.0.0.2 255.255.255.252
  negotiation auto
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
  shutdown
  negotiation auto
! threat-visibility
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 0.0.0.0 0.0.0.0 192.65.79.129
ip route 10.64.0.0 255.255.0.0 10.80.11.1
ip route 172.16.24.0 255.255.248.0 10.80.11.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
control-plane
!
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 10 voip
description Incoming from CUCM
huntstop
session protocol sipv2
session transport tcp tls
incoming called-number [0-9]T
voice-class codec 2
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/1
voice-class sip bind media source-interface GigabitEthernet0/0/1
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax-relay sg3-to-g3
fax rate disable
fax nsf 000000
fax protocol pass-through g711ulaw
no vad
!
dial-peer voice 20 voip
description Outgoing to intelepeer
huntstop
destination-pattern [0-9]T
session protocol sipv2
session target dns:user@domain.com
session transport tcp tls
voice-class codec 2
voice-class sip conn-reuse
voice-class sip options-ping 60
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/0
dtmf-relay rtp-n-te
srtp
fax-relay ecm disable
tax-relay sg3-to-g3
tax rate disable
tax nsf 000000
fax protocol pass-through g711ulaw
no vad!

dial-peer voice 30 voip
description Incoming from intelepeer
huntstop
session protocol sipv2
session transport tcp tls
incoming called-number +1980
voice-class codec 2
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/0
dtmf-relay rtp-n-te
srtp
fax-relay ecm disable
tax-relay sg3-to-g3
tax rate disable
tax nsf 000000
fax protocol pass-through g711ulaw
no vad!

dial-peer voice 40 voip
description Outgoing to CUCM
destination-pattern +1980
session protocol sipv2
session target ipv4:10.80.11.2:5061
session transport tcp tls
voice-class codec 2
voice-class sip options-ping 60
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/1
dtmf-relay rtp-n-te
srtp
fax-relay ecm disable
tax-relay sg3-to-g3
tax rate disable
tax nsf 000000
fax protocol pass-through g711ulaw
no vad!
sip-ua
crypto signaling default trustpoint lynclabcc-DC-CA
!
line con 0
  transport input none
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  logging synchronous
  login local
!
no network-clock synchronization automatic
!
end
Standby Cisco UBE

intelPeerCube1#sh run
Building configuration...
Current configuration : 14681 bytes
!
! Last configuration change at 12:35:16 UTC Thu Sep 7 2017 by cisco
!
version 16.5
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname intelPeerCube1
!
boot-start-marker
boot system flash isr4300-universalk9.16.05.01b.SPA.bin
boot-end-marker
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
enable secret 5 ************
!
no aaa new-model
!
ip name-server 8.8.8.8
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki trustpoint lynclabcc-DC-CA
enrollment terminal
serial-number none
ip-address 10.80.11.30
subject-name CN=intelPeerCube1
revocation-check none
rsakeypair itpcube
!
crypto pki trustpoint "DigiCert SHA2 Secure Server CA"
enrollment terminal
serial-number none
ip-address XXX.XXX.XXX.V
subject-name CN=intelPeerCube1
revocation-check none
rsakeypair itpcube
!
sip
bind control source-interface GigabitEthernet0/0/0
bind media source-interface GigabitEthernet0/0/0
session transport tcp tls
rel1xx supported "rel100"
header-passing
asserted-id pai
early-offer forced
midcall-signaling passthru
privacy-policy passthru
!
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
!
voice class codec 2
codec preference 1 g729r8
codec preference 2 g711ulaw
!
voice class sip-profiles 100
request INVITE sip-header Diversion modify "<sip:(.*)@(.*)>" "<sip:980233\1@\2>"
!
voice class srtp-crypto 1
crypto 1 AES_CM_128_HMAC_SHA1_32
!
voice translation-rule 1
rule 1 /980233\(9116)\// /1/
!
voice translation-profile 10
translate called 1
!
license udi pid ISR4321/K9 sn FDO19220MSQ
license accept end user agreement
license boot suite AdvUCSuiteK9
license boot level appxk9
license boot level securityk9
!
diagnostic bootup level minimal
spanning-tree extend system-id
!
username abcdef privilege 15 password 0 mnopqrstuvwxyz
!
redundancy
mode none
application redundancy
group 1
name voice-b2bha
timers delay 30 reload 60
control GigabitEthernet0/1/0 protocol 1
data GigabitEthernet0/1/0
track 1 shutdown
track 2 shutdown
!
track 1 interface GigabitEthernet0/0/1 line-protocol
track 2 interface GigabitEthernet0/0/0 line-protocol
!
interface GigabitEthernet0/0/0
 ip address XXX.XXX.XXX.S 255.255.255.128
 negotiation auto
 redundancy rii 2
 redundancy group 1 ip XXX.XXX.XXX.V exclusive
!
interface GigabitEthernet0/0/1
 ip address 10.80.11.16 255.255.255.0
 negotiation auto
 redundancy rii 1
 redundancy group 1 ip 10.80.11.30 exclusive
!
interface GigabitEthernet0/1/0
 ip address 20.0.0.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
threat-visibility
 ip forward-protocol nd
 ip http server
 ip http authentication local
 ip http secure-server
 ip route 0.0.0.0 0.0.0.0 192.65.79.129
 ip route 10.64.0.0 255.255.0.0 10.80.11.1
 ip route 172.16.24.0 255.255.248.0 10.80.11.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
 ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
control-plane
!
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 10 voip
description Incoming from CUCM huntstop
 session protocol sipv2
 session transport tcp tls
 incoming called-number [0-9]T
 voice-class codec 2
 voice-class sip profiles 100
 voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/1
voice-class sip bind media source-interface GigabitEthernet0/0/1
dtmf-relay rtp-nte
srtp
fax-relay sg3-to-g3
fax rate 14400
fax nsf 000000
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
no vad!
dial-peer voice 20 voip
description Outgoing to intelepeer
huntstop
destination-pattern [0-9]T
session protocol sipv2
session target dns:user@domain.com
session transport tcp tls
voice-class codec 2
voice-class sip conn-reuse
voice-class sip options-ping 60
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/0
voice-class sip bind media source-interface GigabitEthernet0/0/0
dtmf-relay rtp-nte
srtp
fax-relay sg3-to-g3
fax rate 14400
fax nsf 000000
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
no vad!
dial-peer voice 30 voip
description Incoming from intelepeer
huntstop
session protocol sipv2
session transport tcp tls
incoming called-number +1980
voice-class codec 2
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/0
voice-class sip bind media source-interface GigabitEthernet0/0/0
dtmf-relay rtp-nte
srtp
fax-relay sg3-to-g3
fax rate 14400
fax nsf 000000
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
no vad!
dial-peer voice 40 voip
description Outgoing to CUCM
huntstop
destination-pattern +1980
session protocol sipv2
session target ipv4:10.80.11.2:5061
session transport tcp tls
voice-class codec 2
voice-class sip options-ping 60
voice-class sip profiles 100
voice-class sip srtp-crypto 1
voice-class sip bind control source-interface GigabitEthernet0/0/1
voice-class sip bind media source-interface GigabitEthernet0/0/1
dtmf-relay rtp-nre
srtp
fax-relay sg3-to-g3
fax rate 14400
fax nsf 000000
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
no vad
!
sip-ua
crypto signaling default trustpoint lynclabcc-DC-CA
!
line con 0
exec-timeout 0 0
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login local
!
no network-clock synchronization automatic
ntp server time-pnp.cisco.com
end
Configuring Cisco Unified Communications Manager

Cisco UCM Version

![Cisco Unified CM Administration](image)

Figure 8: Cisco UCM Version

Cisco Call Manager Service Parameters

**Navigation:** System > Service Parameters

1. Select **Server***: Clus21Sub1--CUCM Voice/Video (Active)
2. Select **Service***: Cisco CallManager (Active)
3. All other fields are set to default values

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Value</th>
<th>Suggested Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Yellow Entry Latency</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Code Yellow Exit Latency Calc.</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>Code Yellow Duration</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Max Events Allowed</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>System Throttle Sample Size</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

Figure 9: Service Parameters
Offnet Calls via IntelePeer SIP Trunk
Off-net calls are served by SIP trunks configured between Cisco UCM and the IntelePeer network and calls are routed via Cisco UBE

**SIP Trunk Security Profile**

**Navigation:** System > Security > SIP Trunk Security Profile

1. **Name**: Secure Profile for intelepeer Trunk
2. **Description**: Secure Profile for intelepeer Trunk
3. **Device Security Mode**: Encrypted

![SIP Trunk Security Profile Information](image)

Figure 10: SIP Trunk Security Profile
### Explanation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Transport Type</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>Outgoing Transport Type</td>
<td>TCP</td>
<td>SIP trunks to IntelePeer SBC should use TCP as a transport protocol for SIP. This is configured using SIP Trunk Security profile, which is later assigned to the SIP trunk itself.</td>
</tr>
<tr>
<td>X.509 Subject Name</td>
<td>intelPeerCube2, intelPeerCube1</td>
<td>Subject given in CUBE</td>
</tr>
</tbody>
</table>
**SIP Profile Configuration**

SIP Profile will be later associated with the SIP trunk

**Navigation:** Device → Device Settings → SIP Profile

1. **Name**: Intelepeer SIP Profile
2. **Description**: Intelepeer SIP Profile

---

![SIP Profile Configuration](image)

**Figure 11: SIP Profile**
### SIP Profile (Cont.)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP for Audio Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for Video Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for Audio Portion of Video Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for TelePresence Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for Audio Portion of TelePresence Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>Call Pickup URI</td>
<td>x-cisco-serviceuri-pickup</td>
</tr>
<tr>
<td>Call Pickup Group Other URI</td>
<td>x-cisco-serviceuri-pickup</td>
</tr>
<tr>
<td>Call Pickup Group URI</td>
<td>x-cisco-serviceuri-pickup</td>
</tr>
<tr>
<td>Meet Me Service URI</td>
<td>x-cisco-serviceuri-meetme</td>
</tr>
<tr>
<td>User Info</td>
<td>None</td>
</tr>
<tr>
<td>DTMF DB Level</td>
<td>Nominal</td>
</tr>
<tr>
<td>Call Hold Ring Back</td>
<td>Off</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Off</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Off</td>
</tr>
<tr>
<td>Do Not Disturb Control</td>
<td>User</td>
</tr>
<tr>
<td>Telnet Level for 7940 and 7960</td>
<td>Disabled</td>
</tr>
<tr>
<td>Resource Priority Namespace</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Timer Keep Alive Expires (seconds)</td>
<td>120</td>
</tr>
<tr>
<td>Timer Subscribe Expires (seconds)</td>
<td>120</td>
</tr>
<tr>
<td>Timer Subscribe Delta (seconds)</td>
<td>5</td>
</tr>
<tr>
<td>Maximum Redirects</td>
<td>70</td>
</tr>
<tr>
<td>Off Hook To First Digit Timer (milliseconds)</td>
<td>15000</td>
</tr>
<tr>
<td>Call Forward URI</td>
<td>x-cisco-serviceuri-cfwdial</td>
</tr>
<tr>
<td>Speed Dial (Abbreviated Dial) URI</td>
<td>x-cisco-serviceuri-abbreviated</td>
</tr>
<tr>
<td>Conference Join Enabled</td>
<td>✓</td>
</tr>
<tr>
<td>RFC 2543 Hold</td>
<td>✓</td>
</tr>
<tr>
<td>Semi Attended Transfer</td>
<td>✓</td>
</tr>
<tr>
<td>Enable VAD</td>
<td>✓</td>
</tr>
<tr>
<td>Status Message Waiting</td>
<td>✓</td>
</tr>
<tr>
<td>MLPP User Authorization</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Normalization Script**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Incoming Requests FROM URI Settings**

<table>
<thead>
<tr>
<th>Caller ID DN</th>
<th>Caller Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Figure 13: SIP Profile (Cont.)

#### Explanation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default MTP Telephony Event Payload Type</td>
<td>101</td>
<td>RFC2833 DTMF payload type</td>
</tr>
<tr>
<td>SIP Rel1XX Options</td>
<td>Send PRACK for 1xx Messages</td>
<td>Enable Provisional Acknowledgements (Reliable 100 messages)</td>
</tr>
<tr>
<td>Ping Interval for In-service and Partially In-service Trunks (seconds)</td>
<td>60</td>
<td>OPTIONS message parameters- interval time</td>
</tr>
<tr>
<td>Ping Interval for Out-of-service Trunks (seconds)</td>
<td>120</td>
<td>OPTIONS message parameters- interval time</td>
</tr>
</tbody>
</table>
SIP Trunk Configuration
Create SIP trunks to CUBE

Navigation: Device → Trunk

Figure 14: SIP Trunks List

Figure 15: SIP Trunk to CUBE
**MLPP and Confidential Access Level Information**

- **MLPP Domain**: < None >
- **Confidential Access Mode**: < None >
- **Confidential Access Level**: < None >

**Call Routing Information**

- **Remote-Party-Id**: ✓
- **Asserted-Identity**: ✓
- **Asserted-Type**: Default
- **SIP Privacy**: Default

**Inbound Calls**

- **Significant Digits**: 4
- **Connected Line ID Presentation**: Default
- **Connected Name Presentation**: Default
- **Calling Search Space**: < None >
- **AAR Calling Search Space**: < None >
- **Prefix DN**: 

  - Redirecting Diversion Header Delivery - Inbound

**Incoming Calling Party Settings**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

<table>
<thead>
<tr>
<th>Number Type</th>
<th>Prefix</th>
<th>Strip Digits</th>
<th>Calling Search Space</th>
<th>Use Device Pool CSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Number</td>
<td>Default</td>
<td>0</td>
<td>&lt; None &gt;</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Incoming Called Party Settings**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

<table>
<thead>
<tr>
<th>Number Type</th>
<th>Prefix</th>
<th>Strip Digits</th>
<th>Calling Search Space</th>
<th>Use Device Pool CSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Number</td>
<td>Default</td>
<td>0</td>
<td>&lt; None &gt;</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Connected Party Settings**

- **Connected Party Transformation CSS**: < None >
- **Use Device Pool Connected Party Transformation CSS**: ✓

---

Figure 16: SIP Trunk to CUBE (Cont.)
Figure 17: SIP Trunk to CUBE (Cont.)
Explanation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Intelepeer_Trunk</td>
<td>Name for the trunk</td>
</tr>
<tr>
<td>Device Pool</td>
<td>G711pool</td>
<td>Default Device Pool is used for this trunk</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>MRGL_MTP</td>
<td>MRG with resources: ANN, CFB, MOH and MTP</td>
</tr>
<tr>
<td>SRTP allowed</td>
<td>Checked</td>
<td>Enabling secure RTP</td>
</tr>
<tr>
<td>Significant Digits</td>
<td>4</td>
<td>4 digits Extension for all CPE phones</td>
</tr>
<tr>
<td>Destination Address</td>
<td>10.80.11.30</td>
<td>IP address of the Cisco UBE Virtual LAN</td>
</tr>
<tr>
<td>Destination Port No.</td>
<td>5061</td>
<td>Destination Port for TLS</td>
</tr>
<tr>
<td>SIP Trunk Security Profile</td>
<td>Secure Profile For intelepeer Trunk</td>
<td>SIP Trunk Security Profile configured earlier</td>
</tr>
<tr>
<td>SIP Profile</td>
<td>Intelepeer SIP Profile</td>
<td>SIP Profile configured earlier</td>
</tr>
</tbody>
</table>

Dial Plan

Route Pattern Configuration

Navigation: Call Routing → Route/Hunt → Route Pattern

Route patterns are configured as below:

- Cisco IP phone dial “7”+10 digits number to access PSTN via Cisco UBE
  - “7” is removed before sending to Cisco UCM
- For FAX call, Access Code “7”+10 digits number is used at Cisco Fax gateway
  - “7” is removed at Cisco UCM
  - The rest of the number is sent to Cisco UBE to IntelePeer network
- Incoming fax call to 8021 is sent to Cisco Fax gateway

![Route Patterns List](image-url)
Figure 19: Route Pattern for Voice
**Figure 20: Route Pattern for Fax**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Pattern</td>
<td>7.@ for Voice &amp; International Calls and 8021 for Fax Call</td>
<td>Specify appropriate Route Pattern</td>
</tr>
<tr>
<td>Gateway/Route List</td>
<td>Intelepeer for Route Pattern 7.@ and 8021 for SIP Trunk To Fax Gateway.</td>
<td>SIP Trunk name configured earlier</td>
</tr>
<tr>
<td>Numbering Plan</td>
<td>NANP for Route Pattern 7.@</td>
<td>North American Numbering Plan</td>
</tr>
<tr>
<td>Call Classification</td>
<td>OffNet for Route Pattern 7.@ and 8021</td>
<td>Restrict the transferring of an external call to an external device</td>
</tr>
<tr>
<td>Discard Digits</td>
<td>PreDot for Route Pattern 7.@</td>
<td>Specifies how to modify digit before they are sent to Spectrum network</td>
</tr>
</tbody>
</table>
Secure Conference Bridge Configuration
This section explains how to configure Conference Bridge on a cisco 3900 series router with
IOS version of 15.6.3 M2. DSP card is installed to the router.

Generate an RSA KeyPair for the Gateway

```
DSPfarmRouter(config)#crypto key generate rsa general-keys label dspfarm modulus 2048
```

Create a Trustpoint

```
crypto pki trustpoint DSPfarmRouter
enrollment terminal
serial-number none
ip-address none
subject-name CN=DSPfarmRouter
revocation-check none
rsakeypair dspfarm
```

Install the Root CA Certificate to the Local Trustpoint

```
DSPfarmRouter(config)#crypto pki authenticate DSPfarmRouter
```

Enroll with the CA Root and install the Local Identity Certificate

```
DSPfarmRouter(config)#crypto pki enroll DSPfarmRouter
DSPfarmRouter(config)#crypto pki import DSPfarmRouter certificate
```

Configure Media Resources on CUCM

Create a Secure Conference Bridge

**Navigation:** CUCM Administration > Media Resources > Conference Bridge

1. Click **Add New**

![Figure 21: Conference Bridge](image-url)
Configure Cisco IOS Media Resources

*Enable dspfarm Service*

DSPfarmRouter(config)#voice-card 0
DSPfarmRouter(config-voicecard)#dsp services dspfarm

*Define SCCP Interface*

DSPfarmRouter(config)#sccp local GigabitEthernet0/0
DSPfarmRouter(config)#sccp ccm 10.80.11.2 identifier 1 version 7.0 trustpoint DSPfarmRouter
DSPfarmRouter(config)#sccp

DSPfarmRouter(config)#sccp ccm group 1
DSPfarmRouter(config-sccp-ccm)#associate ccm 1 priority 1
DSPfarmRouter(config-sccp-ccm)#associate profile 1 register DSPfarmRouter

*DSP Farm Profile Setup*

DSPfarmRouter(config)#dspfarm profile 1 conference security
DSPfarmRouter(config-dspfarm-profile)#trustpoint DSPfarmRouter
DSPfarmRouter(config-dspfarm-profile)#codec g729br8
DSPfarmRouter(config-dspfarm-profile)#codec g729r8
DSPfarmRouter(config-dspfarm-profile)#codec g729abr8
DSPfarmRouter(config-dspfarm-profile)#codec g729ar8
DSPfarmRouter(config-dspfarm-profile)#codec g711alaw
DSPfarmRouter(config-dspfarm-profile)#codec g711ulaw
DSPfarmRouter(config-dspfarm-profile)#maximum sessions 4
DSPfarmRouter(config-dspfarm-profile)#associate application SCCP
DSPfarmRouter(config-dspfarm-profile)#no shutdown
Running Configuration

DSPfarmRouter#sh run
Building configuration...
Current configuration : 7919 bytes

! version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

! hostname DSPfarmRouter

! boot-start-marker
boot system flash0 c3900-universalk9-SPA.156-3.M2.bin
boot-end-marker

! enable secret

! no aaa new-model

! crypto pki trustpoint DSPfarmRouter
enrollment terminal
serial-number none
ip-address none
subject-name CN=DSPfarmRouter
revocation-check none
rsakeypair dpsfarm

! crypto pki certificate chain DSPfarmRouter
ip cef
no ipv6 cef

multilink bundle-name authenticated

voice-card 0
dsp services dsfarm

license udi pid C3900-SPE150/K9 sn FOC14353KLH
license accept end user agreement
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
hw-module pvdm 0/0

hw-module sm 1

username cisco privilege 15 password 0

redundancy

interface Embedded-Service-Engine0/0
no ip address
shutdown

interface GigabitEthernet0/0
ip address 10.80.11.25 255.255.255.0
duplex auto
speed auto

interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface GigabitEthernet0/2
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
nocgi http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.80.11.1
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ipv6 ioam timestamp
!
nls resp-timeout 1
cpd cr-id 1
!
control-plane
!
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
!
sccp local GigabitEthernet0/0
sccp ccm 10.80.11.2 identifier 1 version 7.0 trustpoint DSPfarmRouter
sccp
!
sccp ccm group 1
  associate ccm 1 priority 1
  associate profile 1 register DSPfarmRouter
!
dspfarm profile 1 conference security
  trustpoint DSPfarmRouter
  codec g729br8
  codec g729r8
  codec g729abr8
  codec g729ar8
  codec g711alaw
  codec g711ulaw
  maximum sessions 4
  associate application SCCP
!
gatekeeper
shutdown
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
  login local
  transport input all
!
scheduler allocate 20000 1000
!
end

DSPfarmRouter#
Secure Voicemail Integration

Configure CUC

Add SIP Certificate

**Navigation:** CUC Administration > Telephony Integration > Security > SIP Certificate

1. Click **Add New**
2. **Display Name**: Secure sip integration (this name is used here. Display name can be anything)
3. **Subject Name**: SecureConnection (Subject name can be anything but it should match with X.509 Subject name in sip trunk security profile)

![SIP Certificate](image)

**Figure 22: Voicemail SIP Certificate**
Create Phone System

Navigation: Telephony Integration > Phone System

1. **Phone System Name**: clus21sip

![Phone System Basics (clus21sip)](image)

**Figure 23: Phone System**
Add Port Group

1. Click **Add Port Group** on the Phone System Page

![Port Group](image1)

**Figure 24: Port Group**

2. **SIP Security Profile**: 5061/TLS  
3. **SIP Certificate**: Secure sip integration  
4. **Security Mode**: Encrypted  
5. **Secure RTP**: Checked  
6. To add the Port, click **Add Ports**

![Port Group](image2)

**Figure 25: Port Group (Cont.)**
Add Ports

1. **Number of Ports**: 2
2. **Phone System**: clus21sip
3. **Port Group**: clus21sip-1
4. **Server**: clus28unity.lab.tekvizion.com

Figure 26: Port Configuration
Edit Servers

Navigation: Port Group > Edit > Servers

Figure 27: Server Configuration in Port Group
Download CUC Root Certificate

**Navigation:** Telephony Integration > Security > Root Certificate

1. Upload this Certificate to CUCM

---

![Image](image_url)

**Figure 28: CUC Root Certificate**
Create SIP Trunk Security Profile in CUCM

**Navigation**: System > Security > SIP Trunk Security Profile

1. Click **Add New**
2. **Name**: Unity_Connection_Trunk_Security_Profile
3. **Description**: Unity_Connection_Trunk_Security_Profile
4. **Device Security Mode**: Encrypted
5. **Incoming Transport Type**: TLS
6. **Outgoing Transport Type**: TLS
7. **X.509 Subject Name**: SecureConnection
8. **Incoming Port**: 5063

![SIP Trunk Security Profile Information](image)

**Figure 29**: SIP Trunk Security Profile for Voicemail Trunk
## SIP Trunk Configuration in CUCM

**Navigation:** Device > Trunk

1. **Click Add New**
2. **Device Name**: Unity_Connection
3. **Device Pool**: G711 pool
4. **SRTP Allowed**: Checked
5. **Consider Traffic on this Trunk Secure**: When using both SRTP and TLS

### Device Information

<table>
<thead>
<tr>
<th>Product:</th>
<th>SIP Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Protocol:</td>
<td>SIP</td>
</tr>
<tr>
<td>Trunk Service Type:</td>
<td>None (Default)</td>
</tr>
</tbody>
</table>

- **Device Name**: Unity_Connection
- **Description**: To Voicemail
- **Device Pool**: G711 Pool
- **Common Device Configuration**: < None >
- **Cell Classification**: Use System Default
- **Media Resource Group List**: MRUI_MTP
- **Location**: Hub_None
- **AAR Group**: < None >
- **Tunneled Protocol**: None
- **QSIG Variant**: No Changes
- **ASN.1 ROSE O-ID Encoding**: No Changes
- **Packet Capture Mode**: None
- **Packet Capture Duration**: 0

- **Media Termination Point Required**
- **Retry Video Call as Audio**
- **Path Replacement Support**
- **Transmit UTF-8 for Calling Party Name**
- **Transmit UTF-8 Names in QSIG APDU**
- **Unattended Port**
- **SRTP Allowed**: When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
- **Consider Traffic on This Trunk Secure**: When using both SRTP and TLS
- **Route Class Signaling Enabled**
- **Use Trusted Relay Point**: Default
- **PSTN Access**
- **Run On All Active Unified CM Nodes**

### Intercompany Media Engine (IME)

- **E.164 Transformation Profile**: < None >

### MLPP and Confidential Access Level Information

<table>
<thead>
<tr>
<th>MLPP Domain</th>
<th>&lt; None &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Access Mode</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Confidential Access Level</td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

---

Figure 30: SIP Trunk For Unity Connection
Figure 31: SIP Trunk For Unity Connection (Cont.)
6. **Destination Address**: Unity server IP address
7. **Destination Port**: 5061 for TLS
8. **SIP Trunk Security Profile**: Unity_Connection_Trunk_Security_Profile
9. **SIP Profile**: Standard SIP Profile

---

**Figure 32**: SIP Trunk For Unity Connection (Cont.)
Fax Gateway Configuration

This Section explains how to configure fax gateway on a cisco 2800 series router with Version 15.0(1)XA3

Generate RSA Key-Pair for Fax Gateway

vgw.in.tekvizion.com(config)#crypto key generate rsa general-keys label fax modulus 2048

Create a Trustpoint

crypto pki trustpoint lyncca
enrollment terminal
serial-number none
ip-address none
subject-name CN=vgw.in.tekvizion.com
revocation-check none
rsakeypair fax

Install the Root CA Certificate to the Local Trustpoint

Use the below command to install Root CA certificate to the local Trustpoint.

vgw.in.tekvizion.com (config)#crypto pki authenticate lyncca

Enroll with the CA Root and Install the Local Identity Certificate

Use below commands to enroll with CA root and install the local identity certificate.

vgw.in.tekvizion.com (config)#crypto pki enroll lyncca
vgw.in.tekvizion.com (config)#crypto pki import lyncca certificate

Voice Port Configuration

voice-port 0/3/1
no echo-cancel enable
no vad
cptone IN
description **telephone analog/fax**
station-id name fax test
station-id number 9802098021
caller-id enable

Global Configuration

voice service voip
address-hiding
allow-connections sip to sip
redirect ip2ip
fax protocol pass-through g711ulaw
no fax-relay sg3-to-g3
sip
  session transport tcp tls
  midcall-signaling passthru
  g729 annexb-all

POTS Dial-Peer
dial-peer voice 888 pots
  service session
destination-pattern 8021
  no digit-strip
  port 0/3/1
  forward-digits all

VoIP Dial-Peers
dial-peer voice 8021 voip
description Gateway to CUCM
  service session
destination-pattern 7XXXXXXXXXXX
  session protocol sipv2
  session target ipv4:10.80.11.2:5061
  session transport tcp tls
  voice-class codec 3
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax rate disable
fax nsf 000000
fax protocol pass-through g711ulaw
no vad
!
dial-peer voice 80211 voip
  service session
  session protocol sipv2
  session transport tcp tls
  incoming called-number 9115
  voice-class codec 3
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax rate disable
fax nsf 000000
fax protocol pass-through g711ulaw
no vad

## Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPE</td>
<td>Customer Premise Equipment</td>
</tr>
<tr>
<td>Cisco UBE</td>
<td>Cisco Unified Border Element</td>
</tr>
<tr>
<td>Cisco UCM</td>
<td>Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>MTP</td>
<td>Media Termination Point</td>
</tr>
<tr>
<td>POP</td>
<td>Point of Presence</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>ESBC</td>
<td>Enterprise Session Border Controller</td>
</tr>
<tr>
<td>SCCP</td>
<td>Skinny Client Control Protocol</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
</tbody>
</table>
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.
Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

© 2016 Cisco Systems, Inc. All rights reserved.

CCENT, Cisco Lumin, Cisco Nexus, the Cisco logo and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDP, CCVP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R) Printed in the USA