Implementing Cisco Unified Communications Manager, Part 1 (CIPT1)

Guide Version 1.0

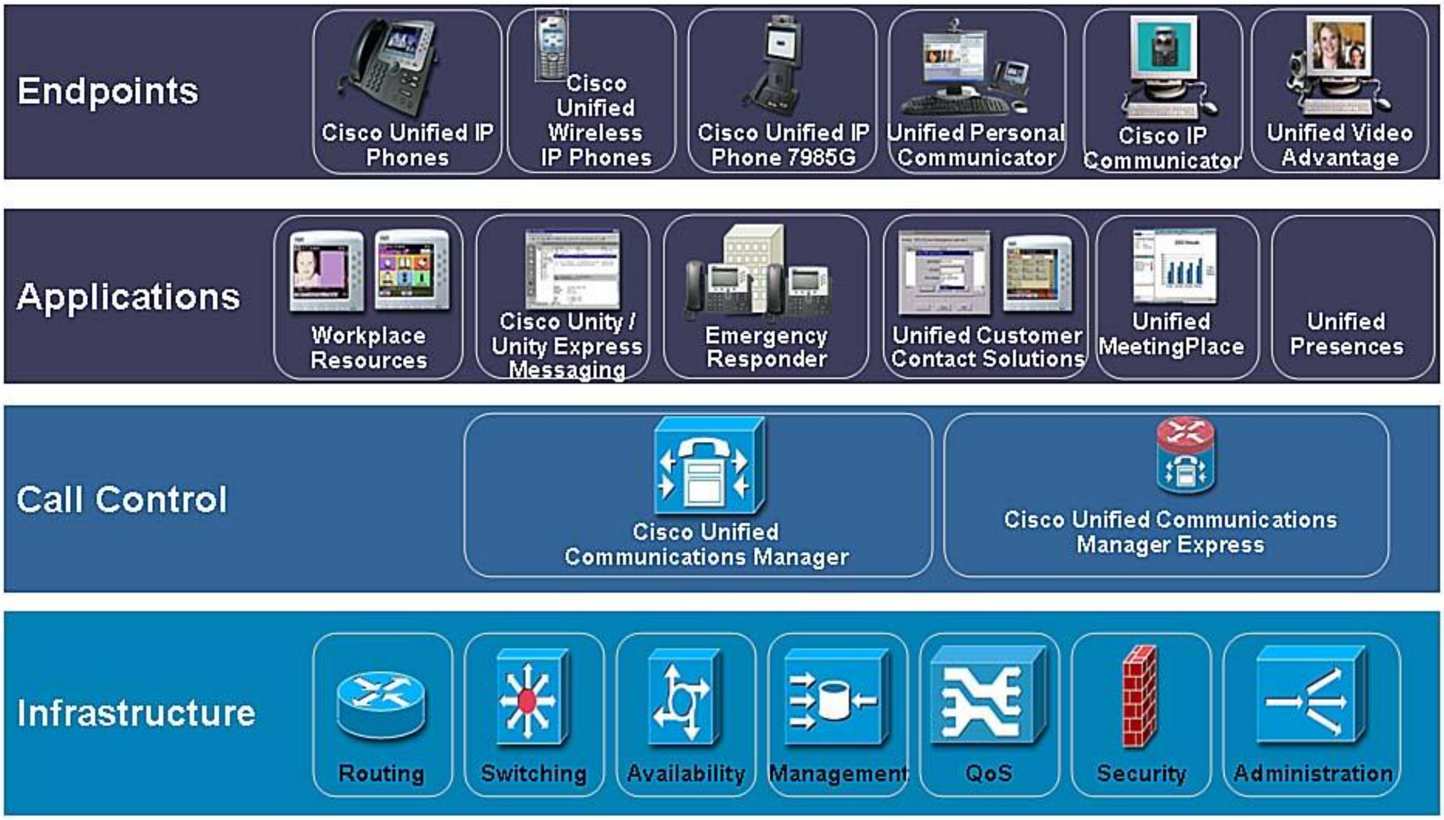
Abdul Jaseem VP

CIPT-1 Guide 1.0 (158 Pages)
(Release Date 9/Feb/2016)

CIPT 1 Syllabus

- CUCM Architecture
- Cisco Unified Network
- CUCM Software
- CUCM Clustering
- Database Replication
- Licensing
- CUCM Deployment Models
- Cisco Catalyst Switches
- H.323 Gateway
- MGCP
- SIP
- ICT
- Dial Plan Components (DNs, Call Routing, Path Selection)
- Calling Privileges (CSS, Partition)
- Time of Day Call Routing
- FAC, CMC
- Digit Manipulation in CUCM
- Call Coverage, Hunting
- Media Resources
- Annunciator
- MoH
- Conference Bridge
- Transcoder
- MTP
- Media Resource Access Control

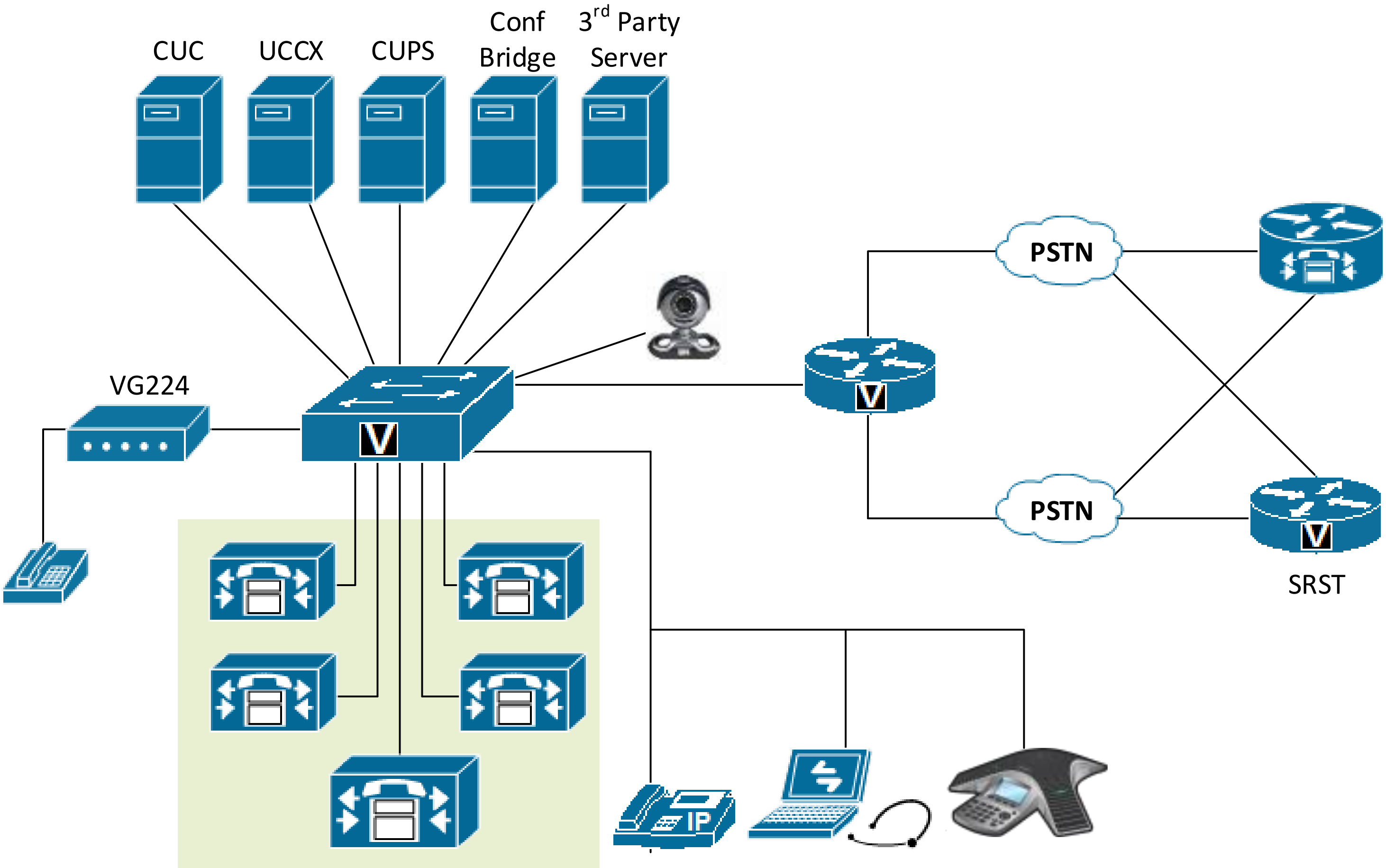
CUCM Architecture



1. ***Infrastructure Layer:*** Consists of Cisco network components (Router, Switch, Firewall, etc.)
2. ***Service/ Call Control Layer:*** Provides core vice functionalities such as Call Routing, Signaling (CUCM, CME, CUCMBE)
3. ***Application Layer:*** Offers wide variety of software which provides collection of features to the user. (Cisco Unity Express, Contact Solution, Unified Presence)
4. ***Endpoint Layer:*** Includes End user hardware & software (IP Phones, IP Communicator, Cisco Video Advantage)

Cisco Unified Network

- A cisco unified network provides fully integrated communication, covering Voice, Video & Data over single network based on standard network protocols.



- ***IP Telephony***: Transmit voice communication over IP network
- ***Customer Contact Centre***: CUCC provides architecture for call center environments. It promotes efficient and effective customer communication
- ***Video Telephony***: Provide video calling over IP network
- ***Rich media conferencing***: Cisco Unified Meeting Place, WebEx provide virtual meeting with IP based tools.
- ***Third Party Applications***: Cisco Unified network can be integrated with other third party VoIP vendors.

Benefits of Cisco Unified Communication

- ***Cost Saving:*** Traditional TDM telephone network dedicates 64Kbps for a single call, hence there unused bandwidth if no call. VoIP shares bandwidth across multiple traffic.
- ***Flexibility:*** IP network offers flexible operations to the organizations
- ***Advanced Call Routing:*** When multiple paths exist to connect a call to a particular destination, suitable and stable path selected by unified communication. Least Cost call routing, Time of Day call routing are two examples of Advanced Call routing.
- ***Unified Messaging:*** Improves communication & productivity.
- ***Long distance Toll bypass:*** VoIP calls are free of cost
- ***Voice & Video Security:*** Unified Communication offers secure communication
- ***Customer Support:*** Ability to provide customer support through various media such as Telephone, email, chat.
- ***Telepresence & Conference:*** Media rich communication

Cisco Unified Network Hardware

Cisco 7800 Series media Convergence Server

- Although it is possible for CUCM to run on most of the computers, Cisco recommends CUCM on Cisco approved hardware.
- The minimum hardware requirement of CUCM 8 is 2GHz Processor, 2GB RAM, 72GB HDD

MCS Model	Feature	Supported IP Phones
7815	80GB HDD, 1 GB RAM	1000
7825	19-23 inch Rack mount, Redundant SATA hard drive, one power supply	1500
7835	Hardware RAID, Redundant Power	2500
7845	2 CPU, Hardware RAID, Redundant Power, Backup Fan	7500

Cisco UCS (Unified Computing System)

B Series (Blade)

C Series (Rack)

UCS Model	Feature	Supported IP Phones

CUCM Software

- The operating system that CUCM application resides on Red Hat Linux Enterprise
- Root access to the system has been locked out, to avoid the use of un authorized products.
- Remote Access support has been integrated in to the CUCM service Ability to allow Cisco TAC to remotely access the server.
- Cisco Secure Agent (CSA) included with CUCM to provide protection against attacks. CSA is a host based intrusion Prevention System (HIPS)
- DHCP server is also integrated with CUCM to provide IP telephony addressing requirement. Not recommended to use if more than 1000 phones.

CUCM Clustering

- Clustering allows high availability and scalability
- CUCM Cluster can have maximum 20 servers.
- Run-Time Data (Intra Cluster Communication Signal- ICCS): Running between Servers in a cluster
- A cluster consist of 1 publisher which maintains Read/ Write copy of CUCM database IBM IDS (Informix Dynamic Server).
- There will be 8 subscriber server maximum in one cluster, publisher replicates its database as a read only data base to subscriber.
- Each cluster has a restriction of 4 active subscriber, other 4 maintained as backup.
- In smaller environment (less than 500 IP Phones) we can use publisher as call processing node. Above 500, we need dedicated subscriber
- Above 1250 IP Phone we should have dedicated TFTP server
- Other servers are TFTP, MOH, Conference, etc.

Data Base Replication

CUCM	Database
3.X	SQL 7
4.X	SQL 2000
5.X, 6.X, etc.	IBM IDS

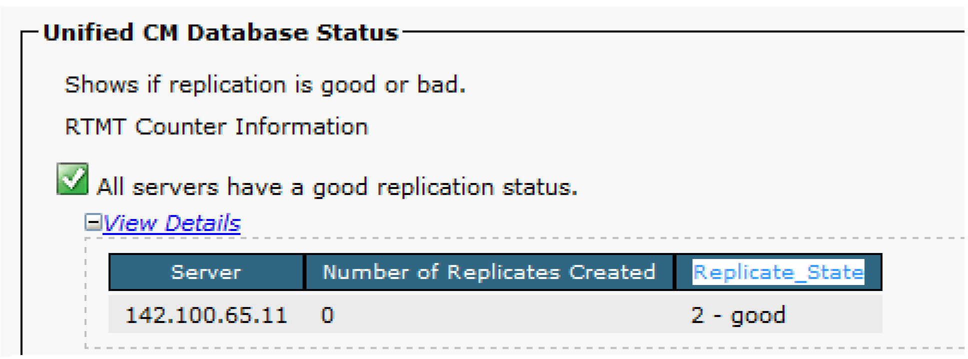
- The duty of publisher to maintain writable copy of database.
- There are three kind of data associated with CUCM cluster database.
- ***Static Configuration Data***: Publisher maintain the read/write copy of these data. Static data (administrative data) includes Adding IP Phones, Changing route pattern, Configuring MOH, etc. Subscriber has read only permission.
- Static configuration data replicates only in unidirectional (hub-and-spoke- 1 Publisher + 8 Subscriber)
- ***Dynamic Configuration Data***: Also called User facing features (UFF) Subscribers are allowed to modify certain information like Forwarding Calls, DND, Privacy Enable/ disable, extension mobility, Softkey, etc.
- User facing features are replicated to from subscribers to other subscribers eventually to Publisher.
- This methods gives high availability even when the publisher is down.
- CAR/CMR Database is stored in Subscribers and replicated to publisher.

DB Replication Status

1. From Unified Reporting CM Database Status

Cisco Unified Reporting → Unified CM Database Status

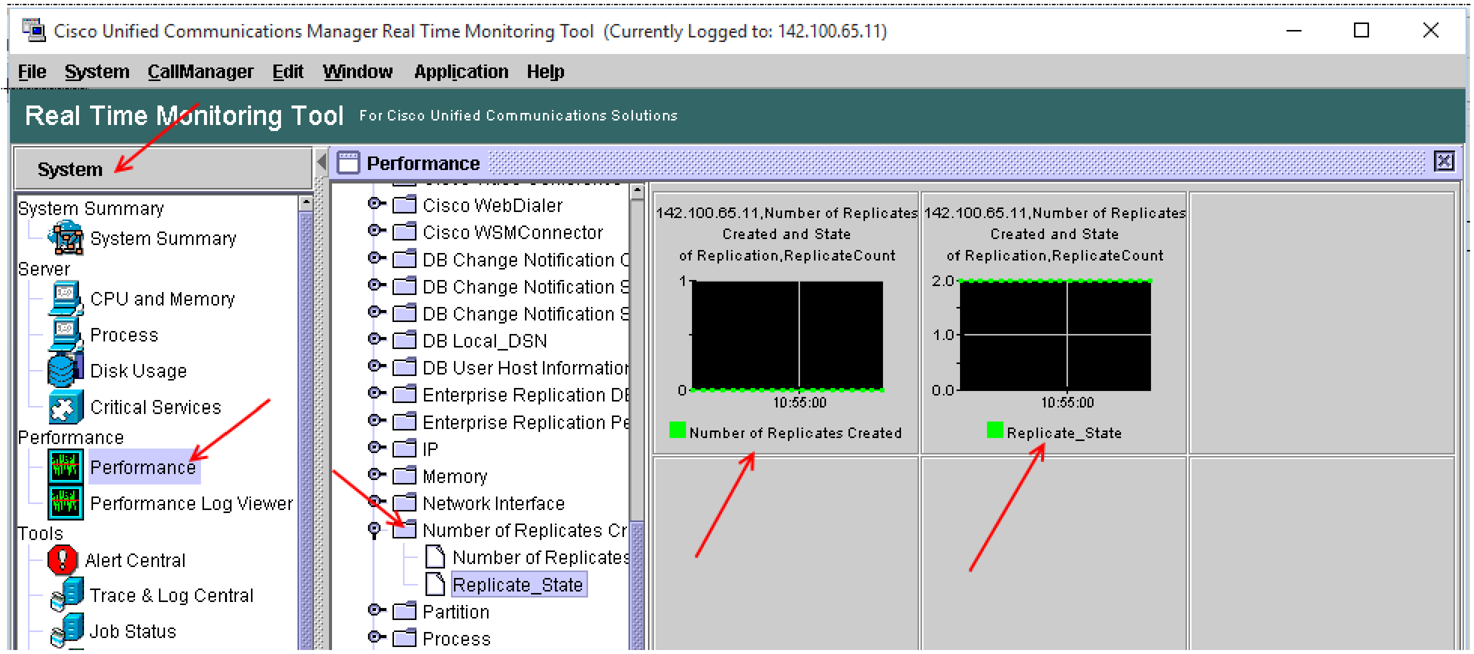
Identifier	Replicate State	
0	Not Activated	0 if server is not defined OR if server is defined but realize template is not done
1	Initiating	Replicates created but their count isn't right, not sync state
2	Good	
3	Going to Bad	When the counter shows a value of 3, it means replication is bad in the cluster. It doesn't means that replication is bad on that particular node. “utils dbreplication status”
4	Bad	Replication Setup didn't succeed. Started but not processed



2. Using RTMT

System → Performance → Number of Replicates Created and State of Replication →

Drag Number of Replicates Created & Replicate_State to right side window



3. From CUCM CLI

CLI allows you to check every single server database status. Run the command **utils dbreplication** status from publisher server

```
admin:utils dbreplication status
*********************************************************************************
This command reads and writes database information from all machines and will take
quite some time...please be patient.
*********************************************************************************

-------------------- utils dbreplication status --------------------


Status cannot be performed when replication is down on the publisher, or on a
cluster with a single active node; aborting replication status check operation


Output is in file cm/trace/dbl/sdi/ReplicationStatus.2015_11_03_23_36_55.out

admin:file view activelog
cm/trace/dbl/sdi/ReplicationStatus.2015_11_03_23_36_55.out
```

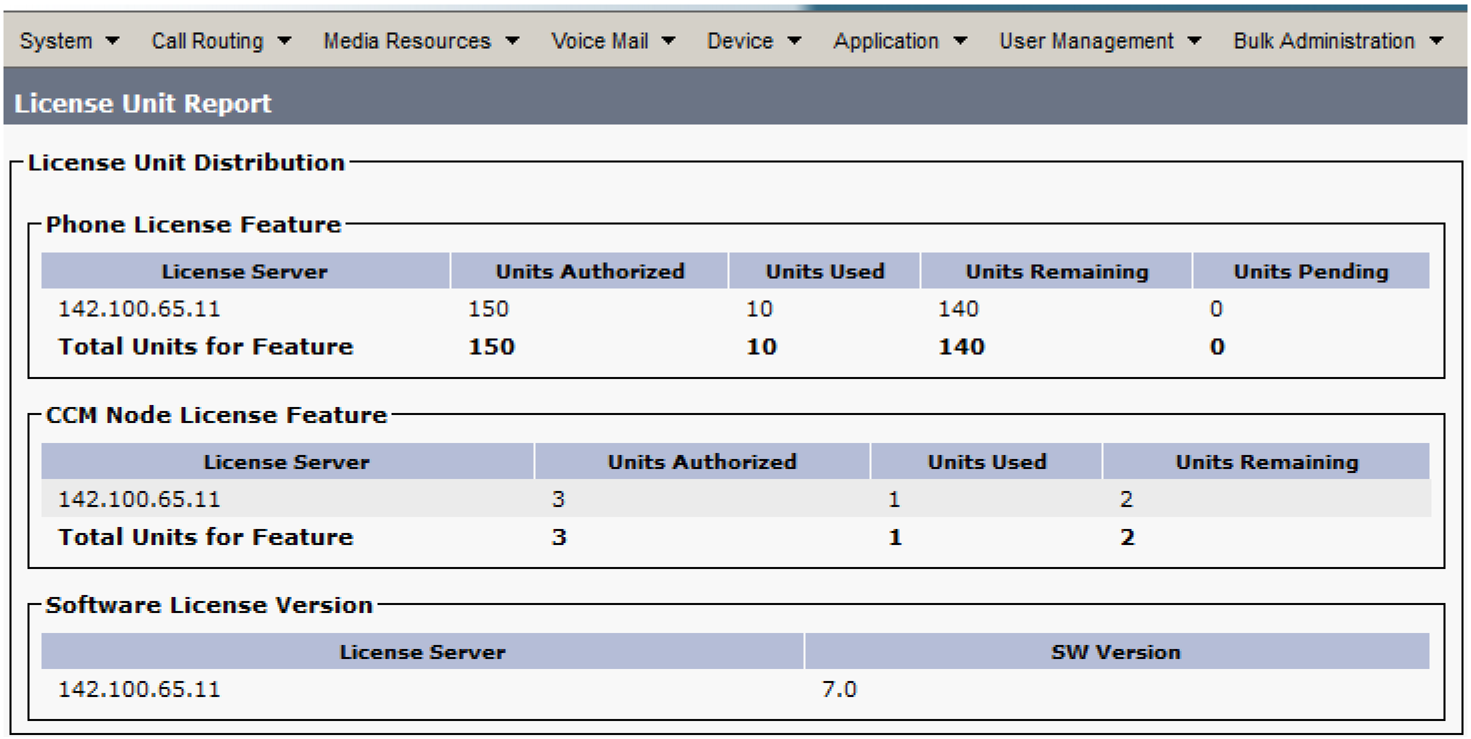
It will give the DB information of all servers

Licensing

1. ***Application or Node License*** (For Publisher, Subscriber, MOH, etc.)
2. ***Software License***: To Upgrade CUCM7 to CUCM8
3. ***Device License Unit (DLU)***: For end devices

System → Licensing → License Unit Calculator

System → Licensing → License Unit Calculator



Phone License Feature

License Server	Units Authorized	Units Used	Units Remaining	Units Pending
142.100.65.11	150	10	140	0
Total Units for Feature	**150**	**10**	**140**	**0**

CCM Node License Feature

License Server	Units Authorized	Units Used	Units Remaining
142.100.65.11	3	1	2
Total Units for Feature	**3**	**1**	**2**

Software License Version

License Server	SW Version
142.100.65.11	7.0

- Publisher is the license overload of the cluster.
- Over Draft: Cisco Provide 5% extra
- Demo: 150 DLUs

License File Request Process

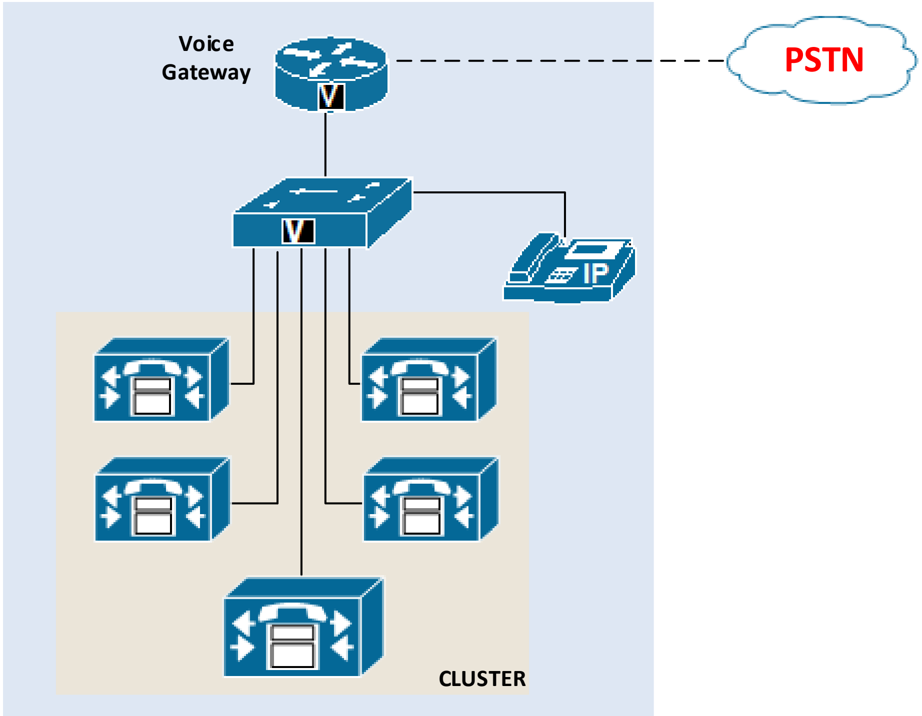
- User place order in Cisco site, and obtain Product Authorization Key (PAK)

- Manufacturing database scan PAK and record against the sales order
- PAK + MAC of Publisher and make a request in www.cisco.com/go/license
- Get license file from Cisco by email
- Install license file on publisher server.

  System → Licensing → License File Upload

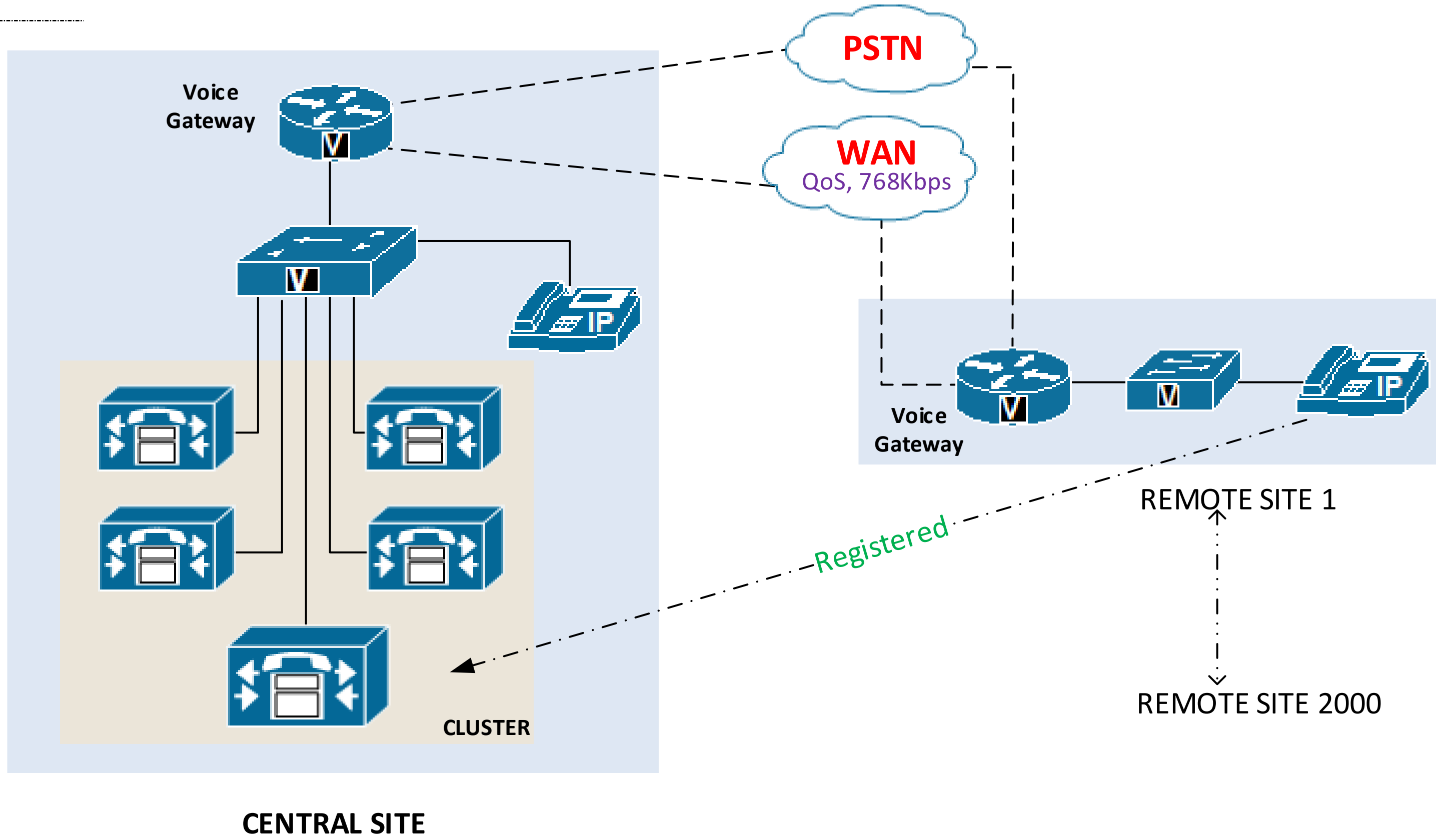
CUCM Deployment Model

1. Single Site Deployment Model



- Call processing agent, DSP resources are located on single site, no telephony service provided over IP WAN
- Maximum 30,000 IP Phone supported per cluster
- Maximum 2100 Gateway (H.323, Multi Point Conference Unit (MCU), SIP Trunk) supported per cluster
- 1100 MGCP Gateways supported per cluster
- Voice traffic occupy within the site
- Gateway or Trunks connected to PSTN handles all external calls.
- Gateway router uses T1 CAS, T1/ E1 PRI, FXO, FXS connectivity to PSTN
- High bandwidth audio & Video communication between devices within the site
- No transcoding required because only one codec used

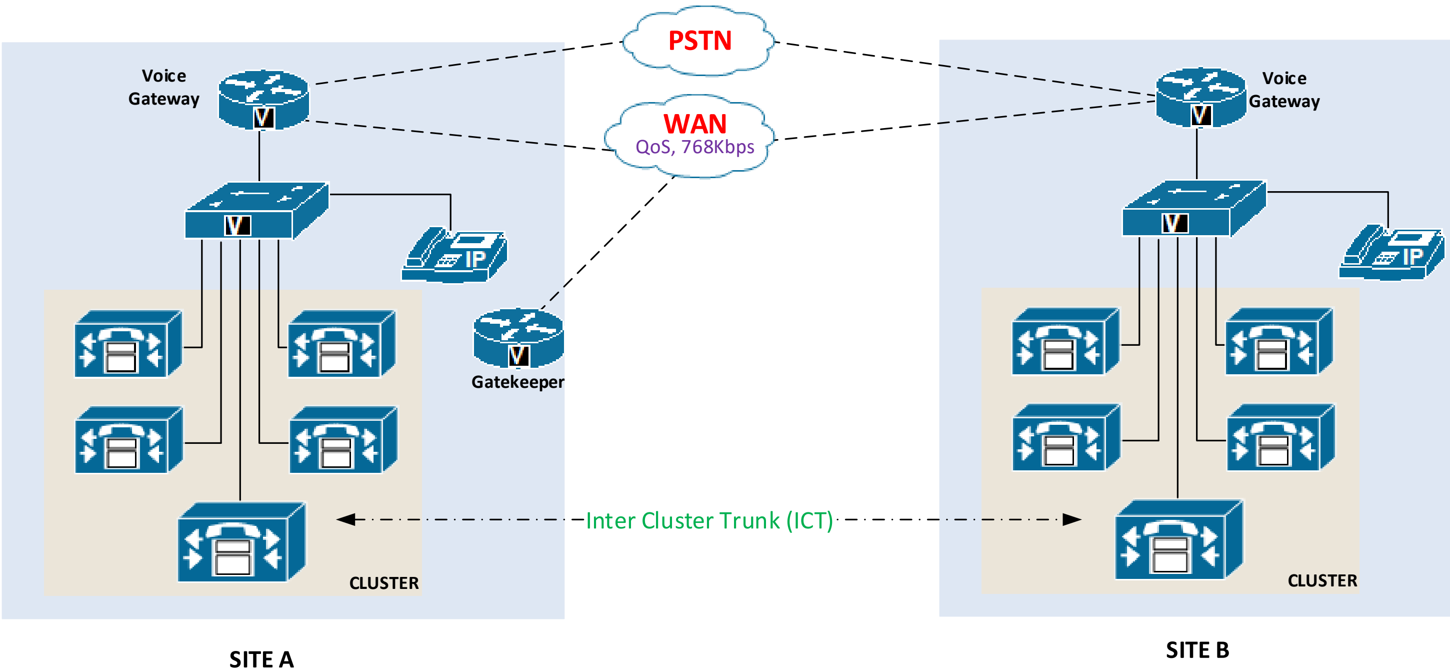
2. Multisite WAN with Centralized Call Processing Model



- Single call processing agent cluster provides telephony services to multiple remote sites over IP WAN.
- Maximum 30,000 end devices (IP Phones) supported per cluster
- Maximum 2000 remote sites are possible
- Maximum 2100 Gateway (H.323, Multi Point Conference Unit (MCU), SIP Trunk) supported per cluster
- 1100 MGCP Gateways supported per cluster
- The remote site Voice Gateway have SRST capability configuration. Cisco IOS SRST supports 1500 phones, CME SRST supports 240 phones
- We must have QoS enabled WAN to connect remote sites (768Kbps band width minimum).
- Call Admission control (use Location Mechanism) & AAR must be enabled
- WAN connectivity options are Leased Lines, Frame Relay, ATM, MPLS VPN, IPSec VPN, etc.
- DSP resources are located at central site & shared to remote sites on demand

- High bandwidth audio between devices within the site & low bandwidth audio between devices in different site
- Free call between Central site & Remote sites over IP WAN
- TEHO (tail-end hop-off) can be implemented to bypass long distance PSTN calls via IP WAN
- Easy to administrate

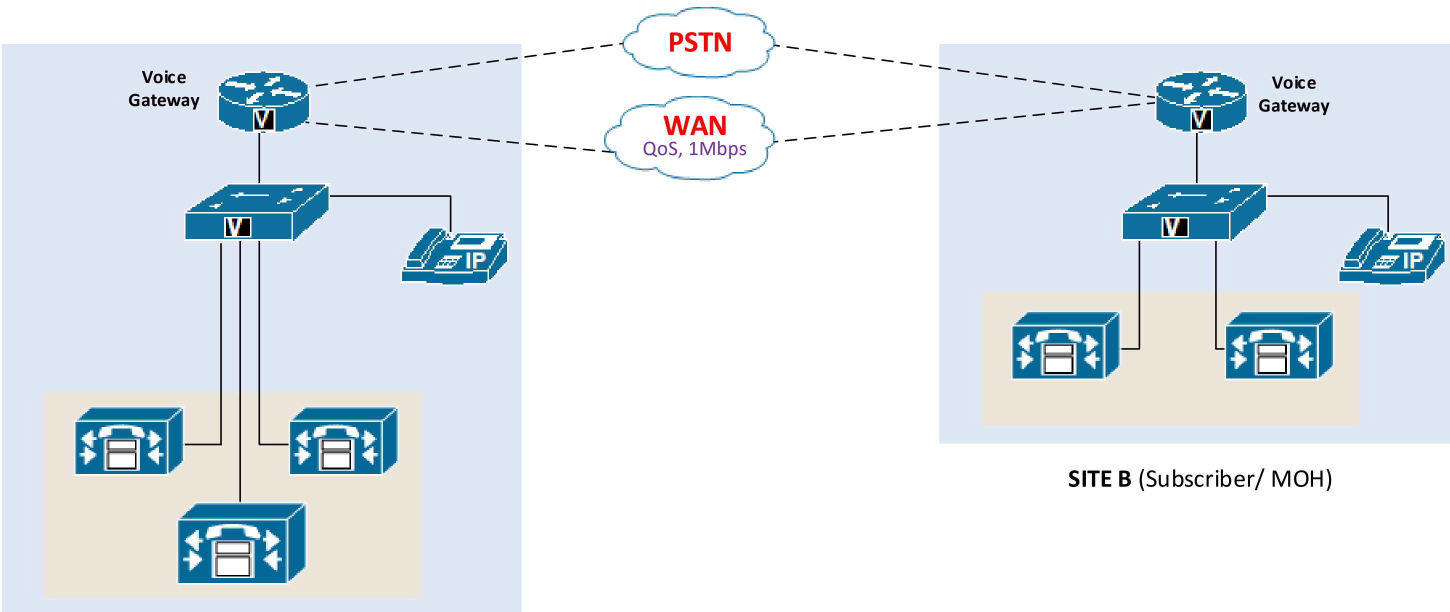
3. Multisite WAN with Distributed Call Processing Model



- Multiple independent sites each having its own call processing CUCM cluster.
- DSP resources are located on each site
- Maximum 2100 Gateway (H.323, Multi Point Conference Unit (MCU), SIP Trunk) supported per cluster
- Maximum 30,000 end devices (IP Phones) supported per cluster
- Different sites are connected via IP WAN using Inter Cluster Trunks (ICT) which carries voice traffic
- PSTN serves as a backup connection in case of WAN outage
- WAN connectivity options are Leased Lines, Frame Relay, ATM, MPLS VPN, IPSec VPN, etc.
- High bandwidth audio between devices within the site, low bandwidth audio between devices in different sites.
- Call Admission Control, AAR implemented based on the particular location

- Free call between Central site & Remote sites over IP WAN
- TEHO (tail-end hop-off) can be implemented to bypass long distance PSTN calls via IP WAN
- No loss of functionality in the case of WAN outage
- Gatekeeper or SIP Proxy servers are the key elements in Multisite with distributed call processing model. They provide dial-plan administration and Gatekeeper offers AAR

4. Clustering over IP WAN Model



SITE B (Subscriber/ MOH)

SITE A (Publisher/ TFTP, Subsriber)

- Servers in same CUCM cluster located at different sites via IP WAN (QoS enabled 1Mbps bandwidth)
- For BHCA (Busy Hour Call Attempt) needs 900Kbps bandwidth as backup
- Round trip delay less than 80msec
- Clustering over IP WAN supports two type of deployment model.
- Local Failover Deployment Model: CUCM subscriber and Backup server at the same site. Suitable for 2 or 4 sites
- Remote Failover Deployment Model: CUCM subscriber & Backup server connected across WAN. Suitable for 8 sites
- Single point of administration, Unified Dial Plan, Extension mobility

Cisco Catalyst Switches

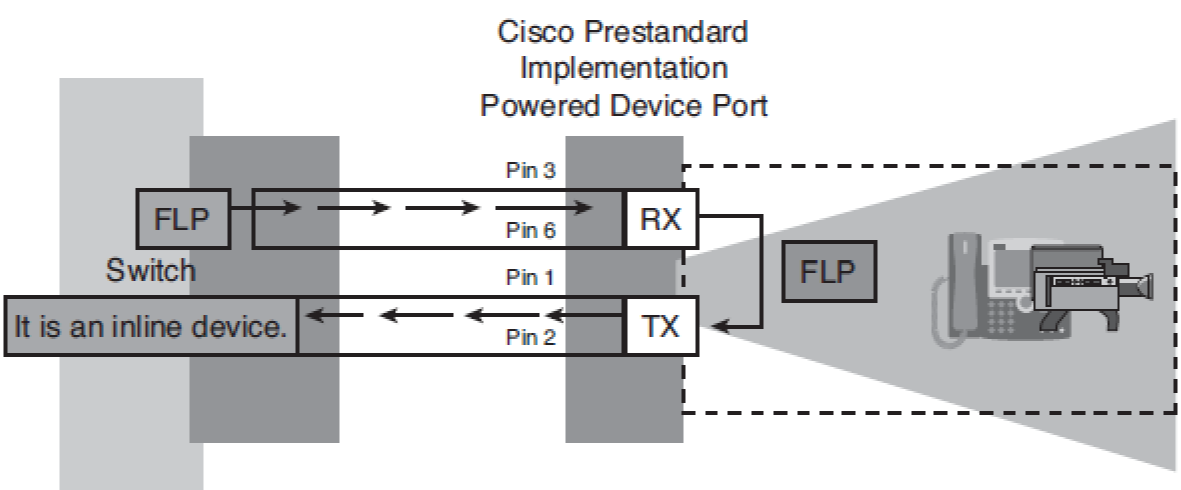
Cisco Catalyst Switch can provide three primary features to assist IP telephony features.

1. In-line power/ Power Over Ethernet (PoE): Type A Phone (7905, 7912, 7940 and 7960) supports only Cisco PoE, Type B (79x1, 79x2, 79x5, 7970) supports Cisco PoE and IEEE802.3af
2. Voice VLAN support: Additional network device can be connected to the back of IP Phone. VOICE VLAN logically separate Cisco IP phone traffic & the other network device (Desktop or Laptop).
3. Class of Service (CoS) Marking: Priorities voice packets

Cisco PoE

- Cisco developer PoE technology initially, called Cisco PoE
- Provides -48V DC/ 10Watt Power over 1, 2, 3 and 6 conductors inside the UTP (Unshielded Twisted Pair) cable
- Use Cisco proprietary method for determining whether the attached device requires power. Power is delivered only on demand

Device Detection: Switch transmit FLP (147Hz) tone to the device, and waited to hear the tone back. Cisco IP Phone loop back the FLP tone to switch. Then the switch delivers 10W power. The IP phone then sends a CDP message contains power requirement, eventually switch reduces the power to required amount. (7960 Phone requires only 6.3W power)

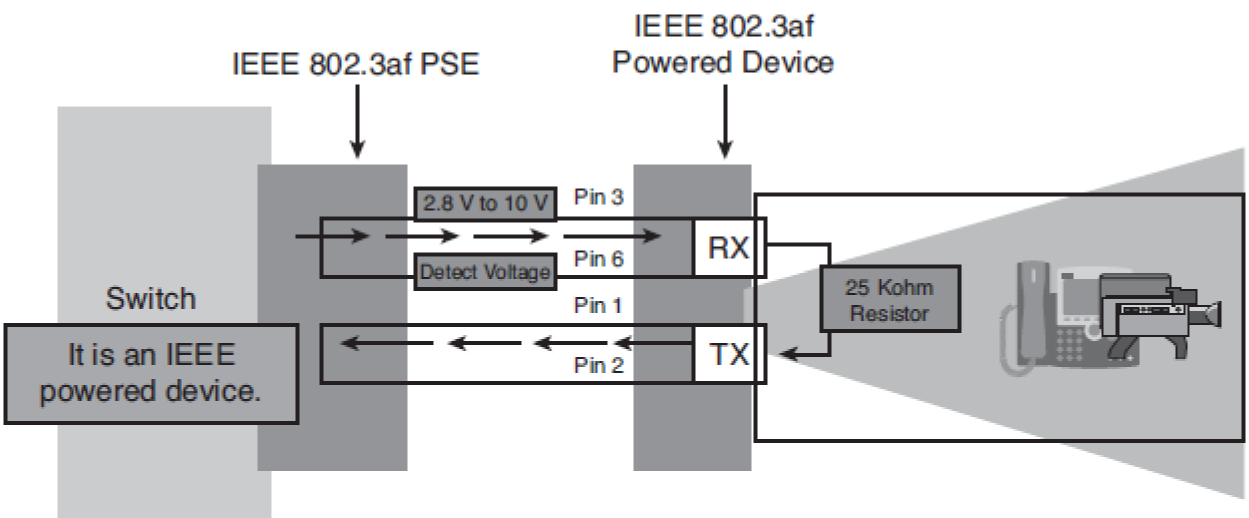


IEEE802.3af PoE

- Provides -48V DC/ 15.4 Watt Power over 1, 2, 3 and 6 conductors inside the UTP (Unshielded Twisted Pair) cable
- Use standardized method for determining whether the attached device requires power. Power is delivered only on demand
- IEEE802.3af supports power classification, which allows powered device to communicate back with how much power needed. Switch without power classification provides 15.4W through every port. It leads to over subscription of available power.

Power Classification	Power in Watts
0	15.4
1	4
2	7
3	15.4
4	30 (Future)

__Device Detection:__ Switch apply a voltage (-2.8V to -10 V) and looks for the behavior of 25KΩ resistor. If the appropriate resistance found, switch delivers the power. The device then sends LLDP (Link Layer Discovery Protocol) message contains power classification, finally switch reduces the power to required amount based on power classification.



__PoE Configuration__

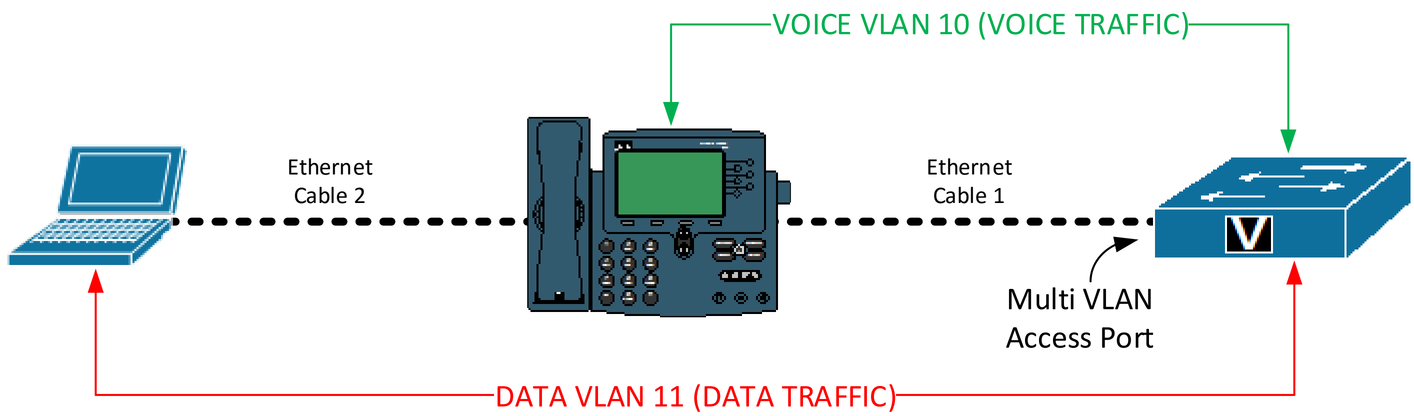
```
Switch(config)#interface fa0/1
Switch(config-if)#power inline auto/ never

Switch#show power inline
Available:360(w)   Used:18(w)   Remaining:342(w)
```

```
Interface Admin  Oper        Power   Device              Class Max
                             (Watts)
--------- ------ ----------- ------- ------------------- ----- ----
Fa0/1     auto   on          6.3     IP Phone 7961       n/a   15.4
Fa0/2     auto   off         0.0     n/a                 n/a   15.4
Fa0/3     auto   off         0.0     n/a                 n/a   15.4
Fa0/4     auto   on          6.3     IP Phone 7960       n/a   15.4
.
.
.
Fa0/13    auto   on          6.3     IP Phone 7960             15.4
```

Voice VLAN & DATA VLAN

- IP phones contain an integrated three-port switch
- Port 0: Not visible, It carry Cisco IP Phone traffic
- Port 1: PC Port, connects to co-located PC
- Port 2: Switch port, connects the phone to a network. In-line power obtained through this port
- Voice VLAN feature allows to separate Voice and Data packets separately even though the PC is connected to the phone.
- Configure VOICE VLAN ID always less than DATA VLAN ID



Multi VLAN Access Port Configuration (Recommended)

```
Switch(config)#vlan 10
Switch(config-vlan)#name VOICE

Switch(config-vlan)#vlan 11
Switch(config-vlan)#name DATA
Switch(config-vlan)#exit

Switch(config)#interface range fastEthernet 0/1-12
```

```
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 11
Switch(config-if-range)#switchport voice vlan 10
```

Verification Commands

```
Switch#show vlan brief
Switch#show vlan id 10
Switch#show vlan name DATA
Switch#show interfaces fa0/1 switchport
```

From the phone go to Network Configurations → Operational VLAN ID

PSTN VoIP Gateways

- To place external calls, CUCM deployments need a connection to PSTN. These connection provided by Gateway
- Routers that are equipped with voice interfaces and voice features
- VoIP Gateways, bridge between VoIP and traditional telephone system. Connects traditional TDM interfaces (T1, E1, ISDN, FXO) to VoIP domains
- Entry & Exit point of the system
- Provide line of security
- Provide VoIP services (Transcoding, MTP, etc.)
- Gateway can be integrated to CUCM using different protocol such as H.323, MGCP, SIP

Traditional Telephony:

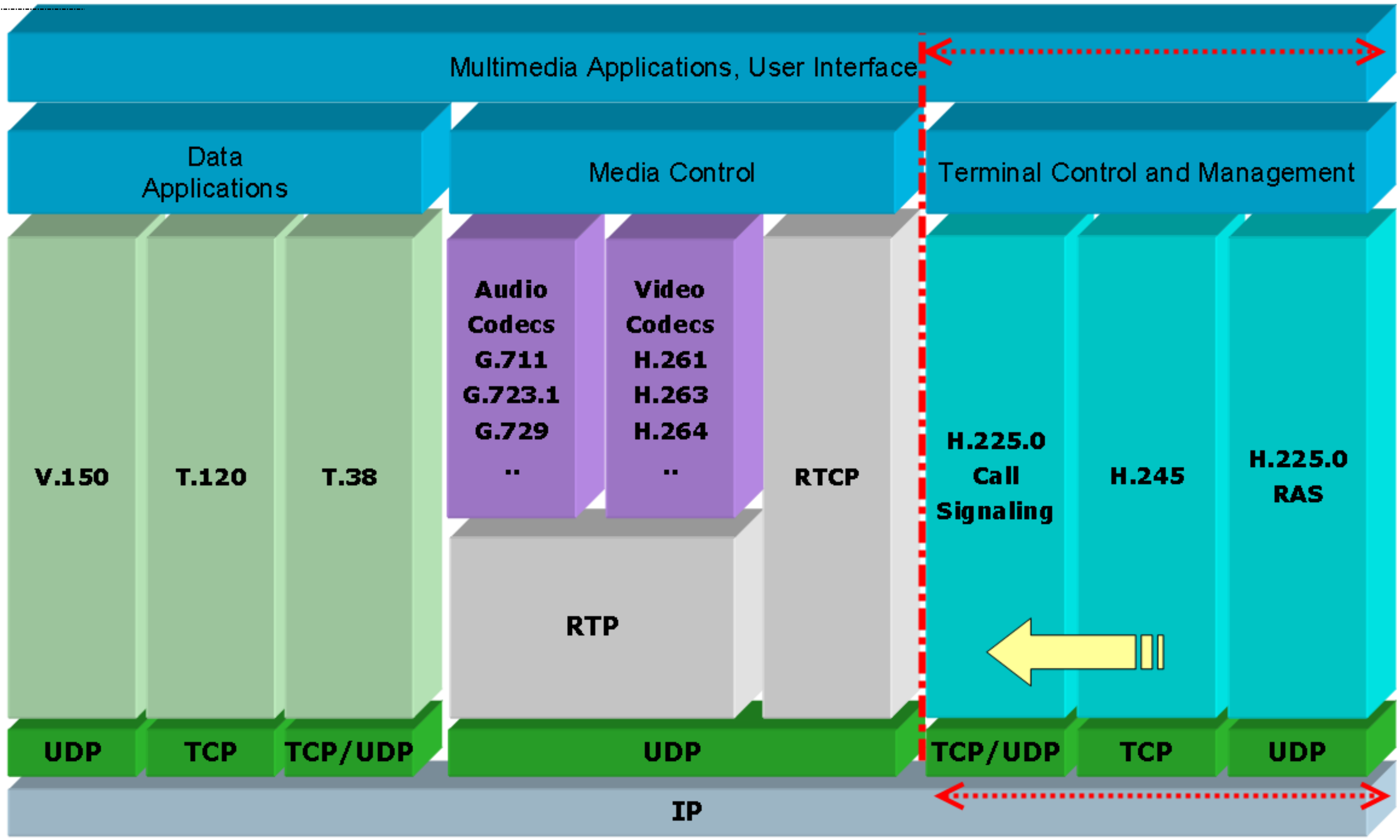
- Well known and stable
- Proprietary PBX systems (Nortel PBX – Nortel Phone)
- Central Office
- TDM & FDM

Voice Over IP:

- Open standard
- Unified network & Employees (AVVID- Architecture for Voice Video & Integrated Data)
- Internet Telephony Service Provider (ITSP)

- Toll bypass
- Phased migration steps supported

H.323 Gateway



- H.323 is Peer to peer protocol and its goal is to setup and handle Voice, Video calling between two devices.
- Most widely adapted and widely supported protocol (default protocol IOS)
- Supports fractional PRI
- H.323 Responsible for setting up the call, making sure the call remain established, Exchanging features, and tearing down the call
- H.323 was developed based on ISDN Q.931 protocol, open standard
- Each GW plays equal part in the signaling process & must maintain its own dial plan to make call forwarding
- CUCM just forward the calls to H.323 gateway and assume it will be forwarded further by the gateway using dial-peers
- H.323 gateway do not register with CUCM and will always show UNKNOWN as registration status.
- Call Preservation, When call manager down, Gateway can maintain active calls
- Wide variety of Digit Manipulation

- NFAS (Non Facility Associated Signaling) One D channel support signaling of all other PRI lines
- Industry standard umbrella protocol uses 1720 port number
- H.323 TCP by default but we can change to UDP

Terminal Control:

1. H.225 Call Signaling: Call setup/ Call tear down (like Q.931)
2. H.225 RAS (Registration Admission & Status): For Gatekeeper communication
3. H.245: Open & Close Logical Channel (RTP, RTCP); Capability Exchange (Codec); Master/Slave detection (resolve conflicts during call); Mode request (Request to change capability of media codec)
4. H.261/ H.263: Video conferencing
5. H.450: Supplementary services (Hold, Transfer, etc.)
6. T.120: Data Transfer, Application sharing

Media Control:

- Audio Codecs (G.711, G.729, G.723.1)
- Video Codecs (H.261, H.263, H.264)

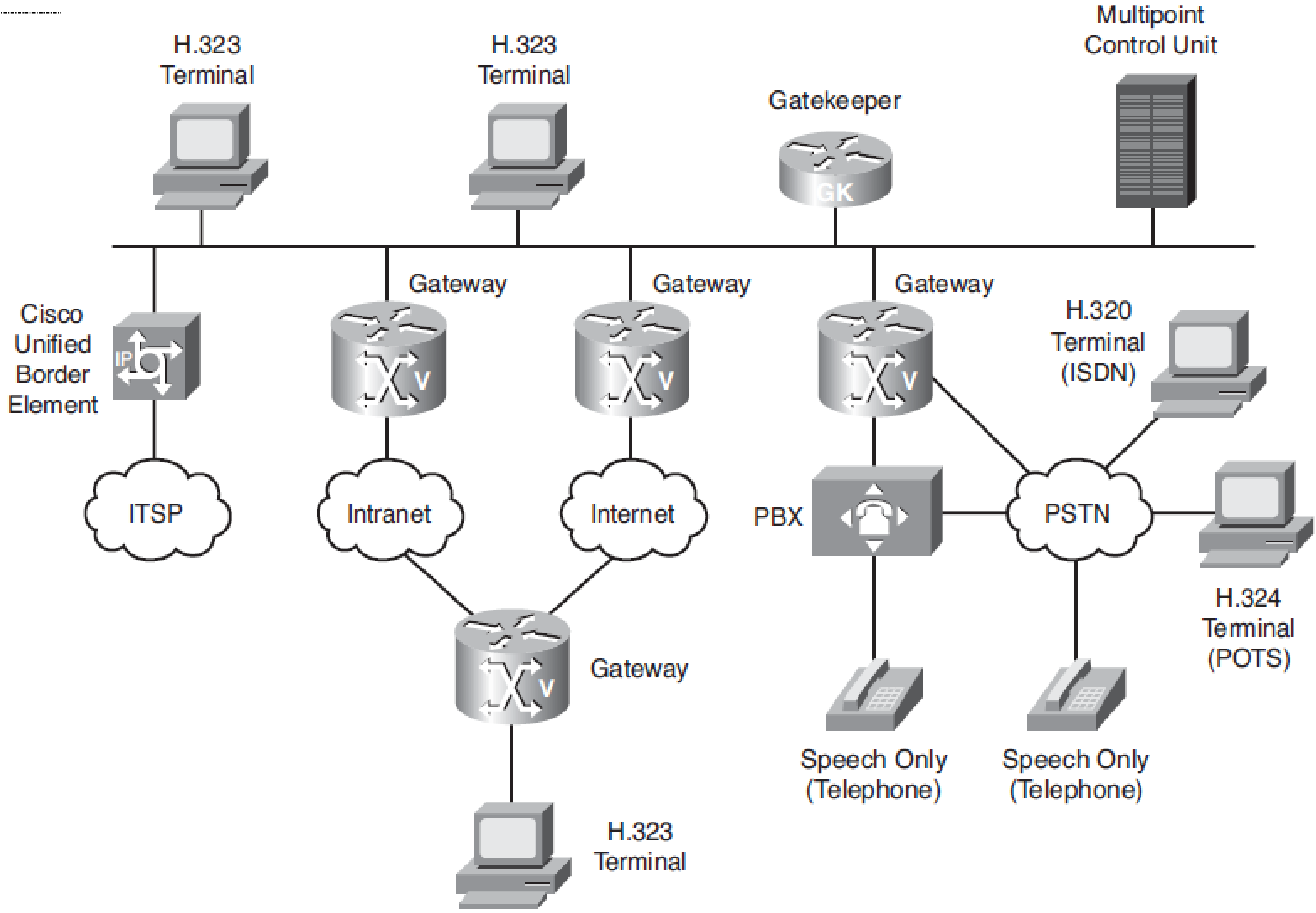
User Data Applications:

- V.150, T.120, T.38 (White board sharing)

H.323 Advantages

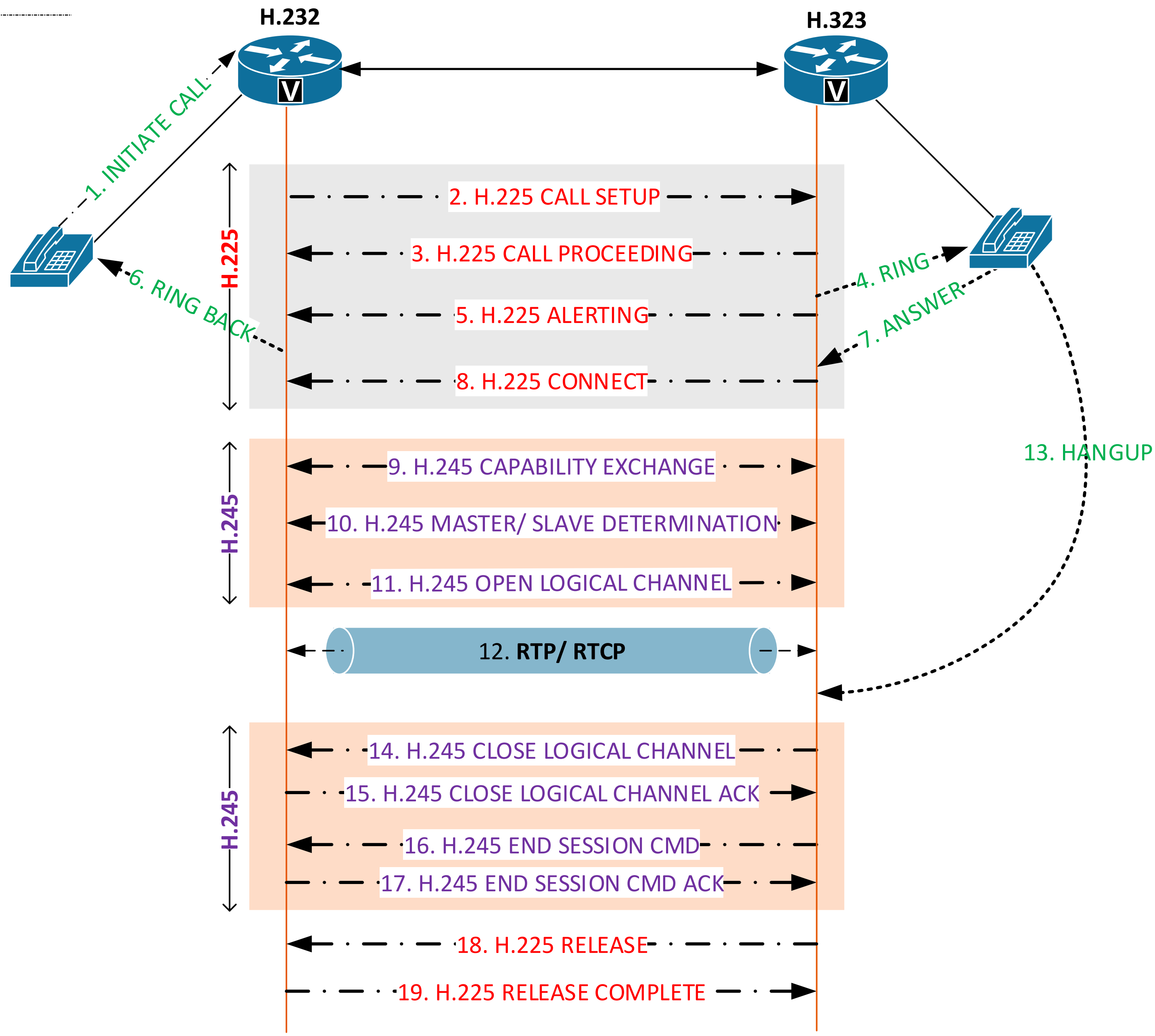
- Self-sufficient dial-plan per gateway: Enables call routing without depending Call manager
- More specific call routing than CUCM: IOS enables translating calling and called number. CUCM matches only called number
- Translation can be defined per gateway
- No need of extra call routing algorithm required for SRST
- No dependency on CUCM
- Enhanced FAX support: H.323 supports T.37, T.38 hence it can route FAX directly to an FXS port
- Enhanced Call Preservation

H.323 Components



- ***H.323 Terminals:*** Exists on a PC (Windows Net-meeting) very rare. It provide real time communication to other H.323 terminal.
- ***H.323 Gateway:*** Connects non H.323 end point to an H.323 device. Provide admission control, Address lookup, translation IP to packet switched
- ***H.323 Endpoint:*** Not a terminal, it is a device connected to H.323 gateway. Gateway doing all the work for him
- ***H.323 Gatekeeper:*** Gatekeeper is used if there is many Gateways, all these gateways are peer to peer. GK is like a centralized phonebook. It keeps a central dial plan for all the gateways. GW and GK communicate each other via RAS messages. GW asks to GK "Where do I go?" via RAS & GK replies via RAS, GW controls the bandwidth
- ***MCU:*** Multi Point Control Unit, Used for conference calling (Audio/ Video). MCU mix difference voice to a single stream

H.323 Call Flow (Slow Start) without Gatekeeper



Call Setup

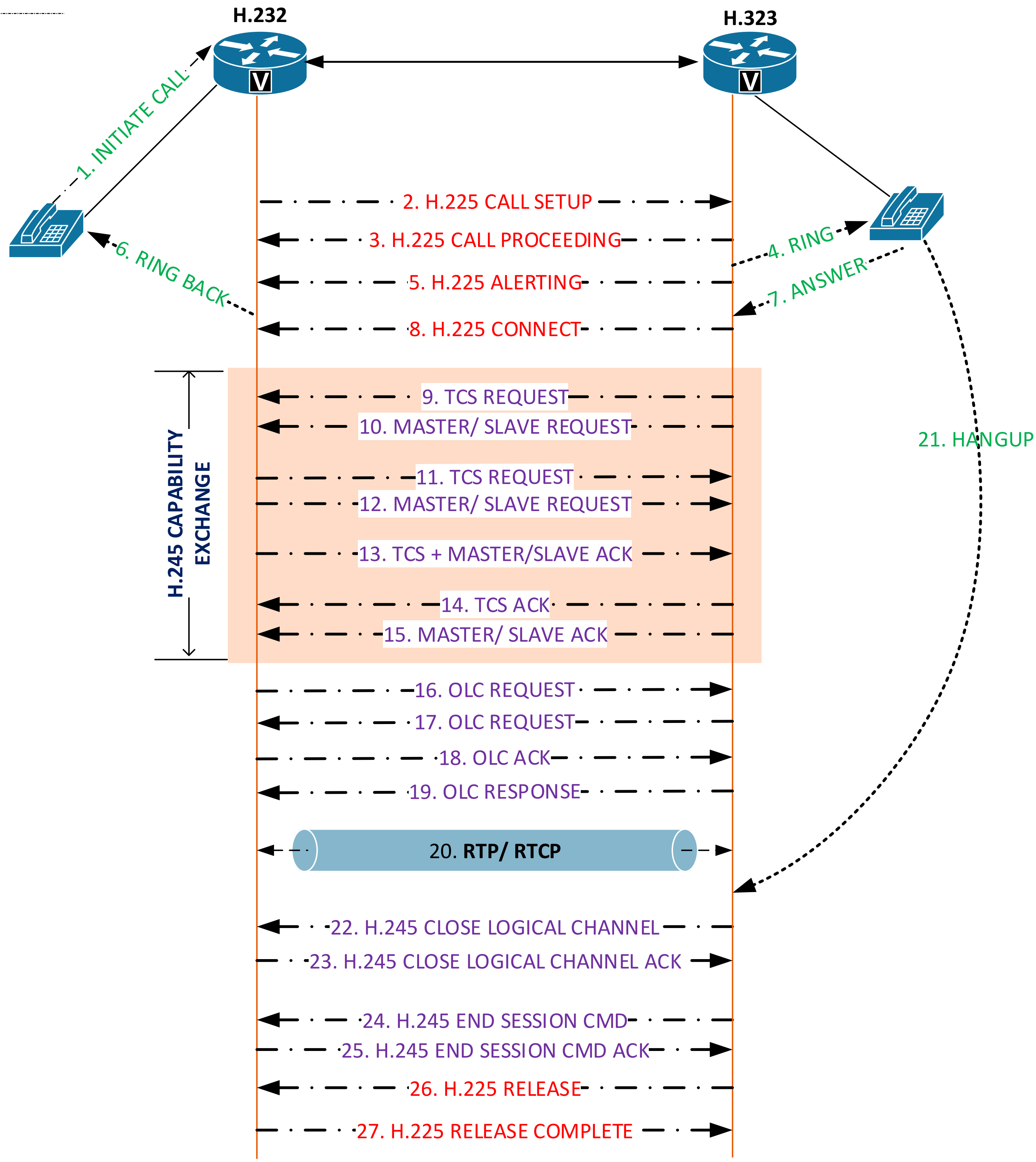
1. An end point **INITIATE** the call
2. Originating gateway initiate an H.225 session with **CALL SETUP** to terminating gateway on TCP port 1720
3. Terminating gateway acknowledge CALL SETUP with the **CALL PROCEEDING** message
4. Terminating gateway send **RING** signal to the destination end point
5. Terminating gateway notifies the originating gateway about the ringing via **ALERTING** message

6. Originating gateway send **RING BACK** to the call initiated end point
7. Destination endpoint **OFF HOOK** the phone (Answer)
8. Terminating gateway send **CONNECT** message to originating gateway
9. H.245 control function starts and exchange the **CAPABILITIES**
10. H.245 control function determines **MASTER/SLAVE** role to resolve potential conflicts while communicating
11. H.245 control function exchanges **OLC** (Open Logical Channel) messages that describes RTP port numbers
12. Both gateway start transmitting media over **RTP** channels and exchange call quality statistics using **RTCP**

Call Tear Down

13. One party **HNAGUP** the line
14. Terminating gateway sends the **CLOSE LOGICAL CHANNEL** (CLC) message to originating gateway
15. Originating gateway acknowledge with **CLC ACK**
16. Terminating gateway sends the **END SESSION COMMAND** message to originating gateway
17. Originating gateway acknowledge with **END SESSION COMMAND ACK**
18. Terminating gateway sends **RELEASE** message to originating gateway
19. Originating gateway sends **RELEASE COMPLETE** message to terminating gateway, hence the call tear down happened

H.245 Capability Exchange in H.323 Call Flow



9. H.245 exchange is triggered by terminating gateway using **TCS** (Terminal Capability Set) message to originating gateway. TCS contain information

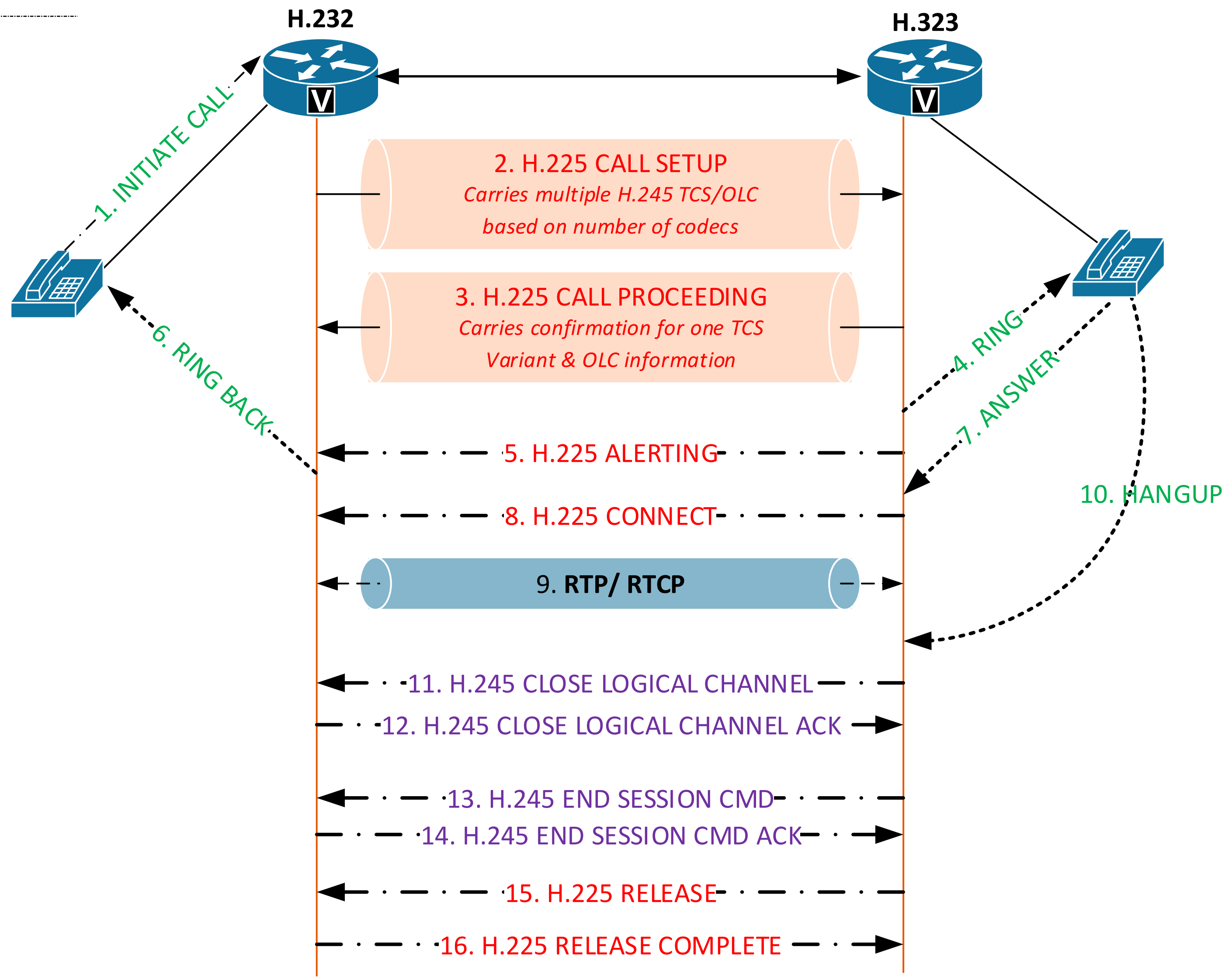
about a terminal's capability to transmit and receive multimedia stream (Codecs). Ordered list of codecs that the terminal can support

10. Terminating gateway sends **MASTER/SLAVE** request to originating gateway
11. Originating gateway sends **TCS** message to terminating gateway.
12. Originating gateway sends **MASTER/SLAVE** request to terminating gateway
13. Originating gateway send a combined **TCS + MASTER/SLAVE ACK** message to terminating gateway as a response to the previous request (9 & 10)
14. Terminating gateway sends **TCS ACK** response to originating gateway
15. Terminating gateway sends **MASTER/SLAVE ACK** response to originating gateway
16. Originating gateway starts logical channel signaling by sending **OLC** request to the terminating gateway
17. Terminating gateway request TRP port numbers to originating gateway using another **OLC** request
18. The originating gateway replies to the OLC request via **OLC ACK** by sending RTP port numbers to the terminating gateway
19. Terminating gateway replies to the initial OLC request (16) via **OLC RESPONSE** by sending RTP port number to the originating gateway
20. After confirming OLC messages, both gateways stars transmitting media stream via **RTP**

Empty Capability Set (Third Party Re-routing)

Version 2 of H.323 gives a special meaning to receipt of an empty H.245 capability set. When a node receives an empty capability set, it must close all of its channels, enter a "paused" state, and wait for a non-empty capability set to restart the H.245 session. This will effectively allow a gatekeeper to re-route connections from an endpoint that does not support Supplementary Services.

H.323 Fast Connect Call Flow



Fast connect reduces the number of round-trip exchanges & archives the capability exchange + Logical channel assignment in one round-trip. Fast connect widely supported in the industry.

Call Setup

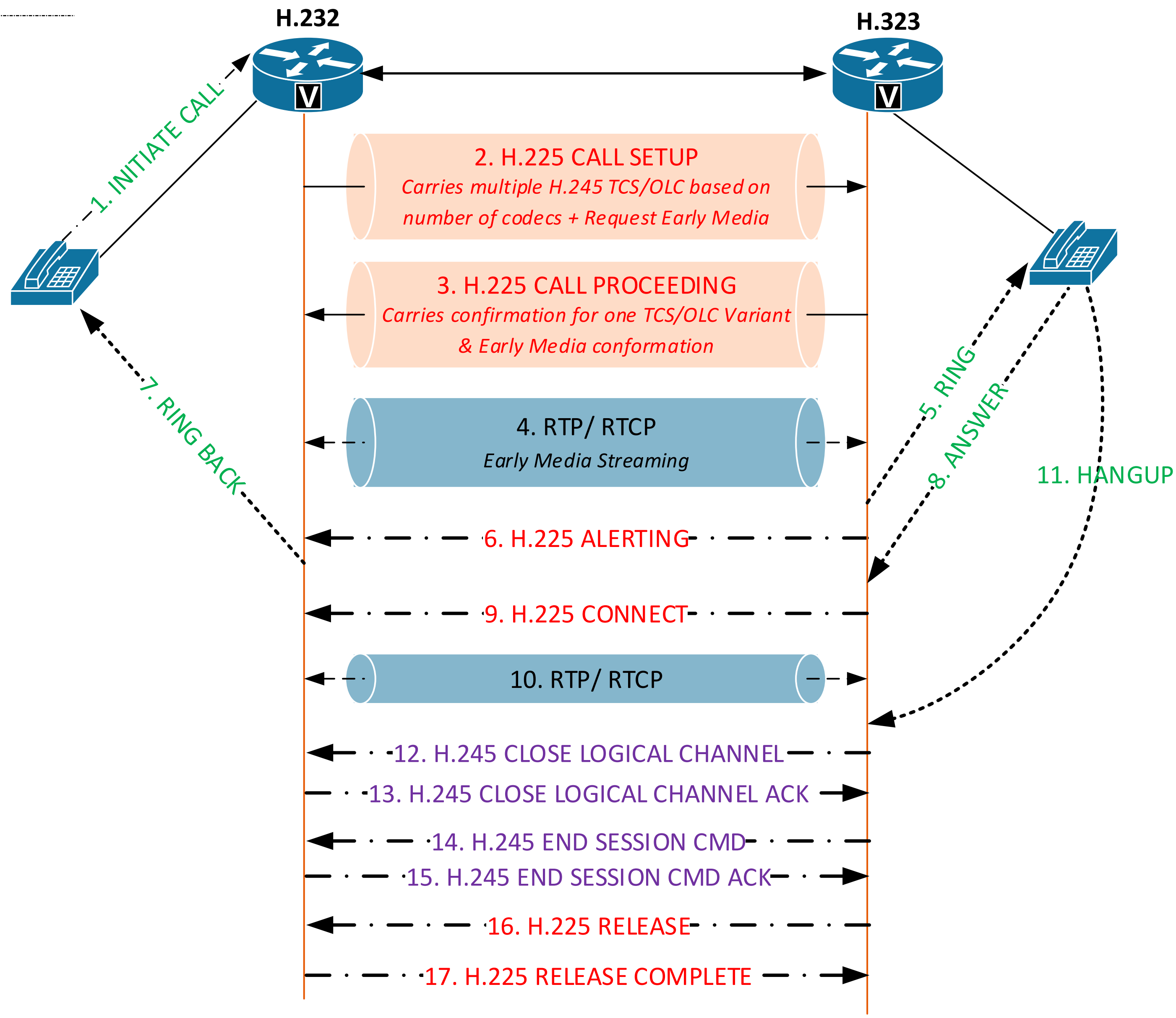
1. An end point initiates a call
2. Originating gateway initiates an H.225 session with a **CALL SETUP** message to terminating gateway on port number 1720. This H.225 CALL SETUP message combined with **H.245 control channel signals** includes set of capabilities (TCS) and logical channel descriptions
3. Terminating gateway responds using **CALL PREOCEEDING** message which combines with **confirmation** of **TCS** and **OLC** information about RTP port numbers
4. Terminating gateway send **RING** signal to the destination end point

5. Terminating gateway notifies the originating gateway about the ringing via **ALERTING** message
6. Originating gateway send **RING BACK** to the call initiated end point
7. Destination endpoint **OFF HOOK** the phone (Answering call)
8. Terminating gateway send **CONNECT** message to originating gateway
9. Both gateway start transmitting media over **RTP** channels and exchange call quality statistics using **RTCP**

Call Teardown

10. One party **HNAGUP** the line
11. Terminating gateway sends the **CLOSE LOGICAL CHANNEL** (CLC) message to originating gateway
12. Originating gateway acknowledge with **CLC ACK**
13. Terminating gateway sends the **END SESSION COMMAND** message to originating gateway
14. Originating gateway acknowledge with **END SESSION COMMAND ACK**
15. Terminating gateway sends **RELEASE COMPLETE** message to originating gateway, hence the call teardown happened

H.323 Early Media Call Flow



Early media allows sending of media from the called party or application server to the caller (calling party), prior to the call being accepted. Early media usually send PSTN and carries ringing tone, Announcement, IVR stream etc.

Call Setup

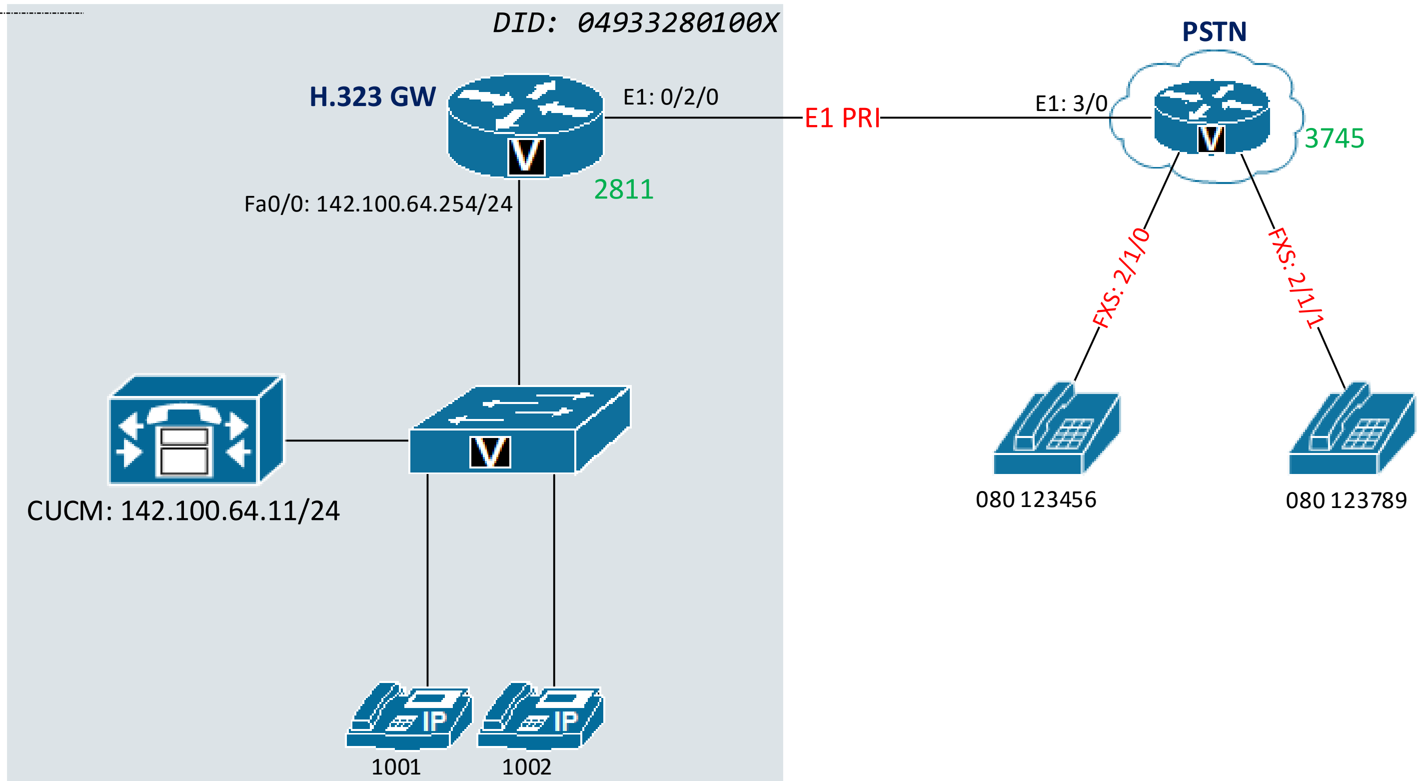
1. An end point **INITIATES** a call
2. Originating gateway initiates an H.225 session with a **CALL SETUP** message to terminating gateway on port number 1720. This H.225 CALL SETUP message combined with **H.245 control channel signals** includes set of capabilities (TCS) and logical channel descriptions + **EARLY MEDIA** request

3. Terminating gateway responds using **CALL PREOCEEDING** message which combines with **confirmation** of **TCS**, **OLC** information about RTP port numbers and **EARLY MEDIA CONFIRMATION**
4. Establish an RTP media stream between originating and terminating gateways to transmit EARLY MEDIA (Ring tone, Announcements, etc)
5. Terminating gateway send **RING** signal to the destination end point
6. Terminating gateway notifies the originating gateway about the ringing via **ALERTING** message
7. Originating gateway send **RING BACK** to the call initiated end point
8. Destination endpoint **OFF HOOK** the phone (Answering call)
9. Terminating gateway send **CONNECT** message to originating gateway
10. Both gateway start transmitting media over **RTP** channels and exchange call quality statistics using **RTCP**

Call Teardown

11. One party **HNAGUP** the line
12. Terminating gateway sends the **CLOSE LOGICAL CHANNEL** (CLC) message to originating gateway
13. Originating gateway acknowledge with **CLC ACK**
14. Terminating gateway sends the **END SESSION COMMAND** message to originating gateway
15. Originating gateway acknowledge with **END SESSION COMMAND ACK**
16. Terminating gateway sends **RELEASE COMPLETE** message to originating gateway, hence the call teardown happened

Configuration H.323 Gateway



Configure PSTN Router

```
PSTN_ROUTER(config)# dial-peer voice 1 pots
PSTN_ROUTER(config)# destination-pattern 080123456
PSTN_ROUTER(config)# port 2/1/0

PSTN_ROUTER(config)# dial-peer voice 2 pots
PSTN_ROUTER(config)# destination-pattern 080123789
PSTN_ROUTER(config)# port 2/1/0

PSTN_ROUTER(config)#isdn switch-type primary-net5

PSTN_ROUTER#show controllers E1

PSTN_ROUTER(config)#controller E1 3/0
PSTN_ROUTER(config-controller)# framing crc4
PSTN_ROUTER(config-controller)# linecoding  hdb3
PSTN_ROUTER(config-controller)# clock source internal
PSTN_ROUTER(config-controller)#pri-group timeslots 1-10
```

```
PSTN_ROUTER(config-controller)#no shutdown

PSTN_ROUTER#show voice port summary

PSTN_ROUTER(config)#interface serial 3/0:15
PSTN_ROUTER(config-if)#isdn switch-type primary-net5
PSTN_ROUTER(config-if)#isdn protocol-emulate network
PSTN_ROUTER(config-if)#isdn bchan-number-order ascending
PSTN_ROUTER(config-if)#isdn incoming-voice voice
PSTN_ROUTER(config-if)#no shutdown

PSTN_ROUTER(config)#dial-peer voice 3 pots
PSTN_ROUTER(config-dial-peer)#incoming called-number .
PSTN_ROUTER(config-dial-peer)#direct-inward-dial
PSTN_ROUTER(config-dial-peer)#port 3/0:15

PSTN_ROUTER(config)#dial-peer voice 4 pots
PSTN_ROUTER(config-dial-peer)#destination-pattern 04933280100.
PSTN_ROUTER(config-dial-peer)#no digit-strip
PSTN_ROUTER(config-dial-peer)#port 3/0:15
```

Step 1: Configure E1 PRI in H.323 Gateway

```
H323_GW(config)#isdn switch-type primary-net5

H323_GW#show controllers E1

H323_GW(config)#controller E1 0/2/0
H323_GW(config-controller)# framing crc4
H323_GW(config-controller)# linecode hdb3
H323_GW(config-controller)# clock source line
H323_GW(config-controller)#pri-group timeslots 1-10
H323_GW(config-controller)#no shutdown
```

```
H323_GW#show voice port summary
```

```
H323_GW(config)#interface serial 0/2/0:15
H323_GW(config-if)#isdn switch-type primary-net5
H323_GW(config-if)#isdn protocol-emulate user
H323_GW(config-if)#isdn bchan-number-order descending
H323_GW(config-if)#isdn incoming-voice voice
H323_GW(config-if)#no shutdown

H323_GW(config)#dial-peer voice 1 pots
H323_GW(config-dial-peer)#incoming called-number .
H323_GW(config-dial-peer)#direct-inward-dial
H323_GW(config-dial-peer)#port 0/2/0:15

H323_GW(config)#dial-peer voice 2 pots
H323_GW(config-dial-peer)#destination-pattern 080123...
H323_GW(config-dial-peer)#no digit-strip
H323_GW(config-dial-peer)#port 0/2/0:15
```

Step 2: Configure dial-peer to CUCM

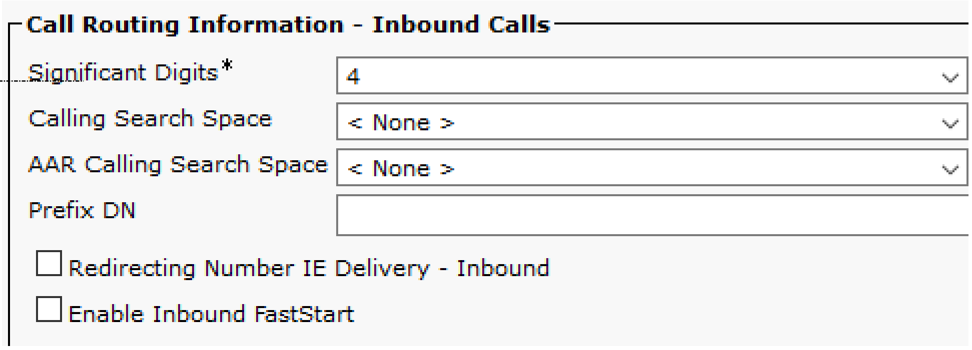
```
H323_GW(config)#dial-peer voice 3 voip
H323_GW(config-dial-peer)#destination-pattern 100.
H323_GW(config-dial-peer)# session target ipv4:142.100.64.11
```

[All of the above dial-peers serves as H.323 Protocol]

Step 3: Apply Digit Manipulation in H.323 Gateway

```
H323_GW(config)#num-exp 04933280100. 100.
```

[Digit manipulations can be also applied in CUCM (Significant Digits), but the above dial-peer should be destination-pattern 04933280100.]



Step 4: Add Gateway in CUCM

Cisco Unified CM Administration → Device → Gateway → Add New → Type : H.323

Device Name: IP Address of Gateway <142.100.64.254>

Description: H.323_GATEWAY

Device Pool: <SELECT>

Step 5: Create route Pattern to Call External (9 is the access code)

Call Routing → Route/Hunt → Route Pattern → Add new

Route Pattern : 9.080123XXX

Description : H323_GATEWAY_ROUTE_PATTERN

Gateway : 142.100.64.254

Discard Digit : Pre dot

Provide Outside Dial tone → Check

H.323 Optional Commands

Router(config)# voice class h323 1

Router(config-class)# h225 timeout tcp establish 3 [Set TCP timer]

Router(config-class)# h225 timeout setup 2 [Set H.225 SETUP Timer]

Router(config-class)# h225 timeout connect 2 [Set H.225 CONNECT Timer]

Router(config-class)# call preserve [Survivability: CUCM loss connection to H.323]

Apply Voice Class In dial-peer

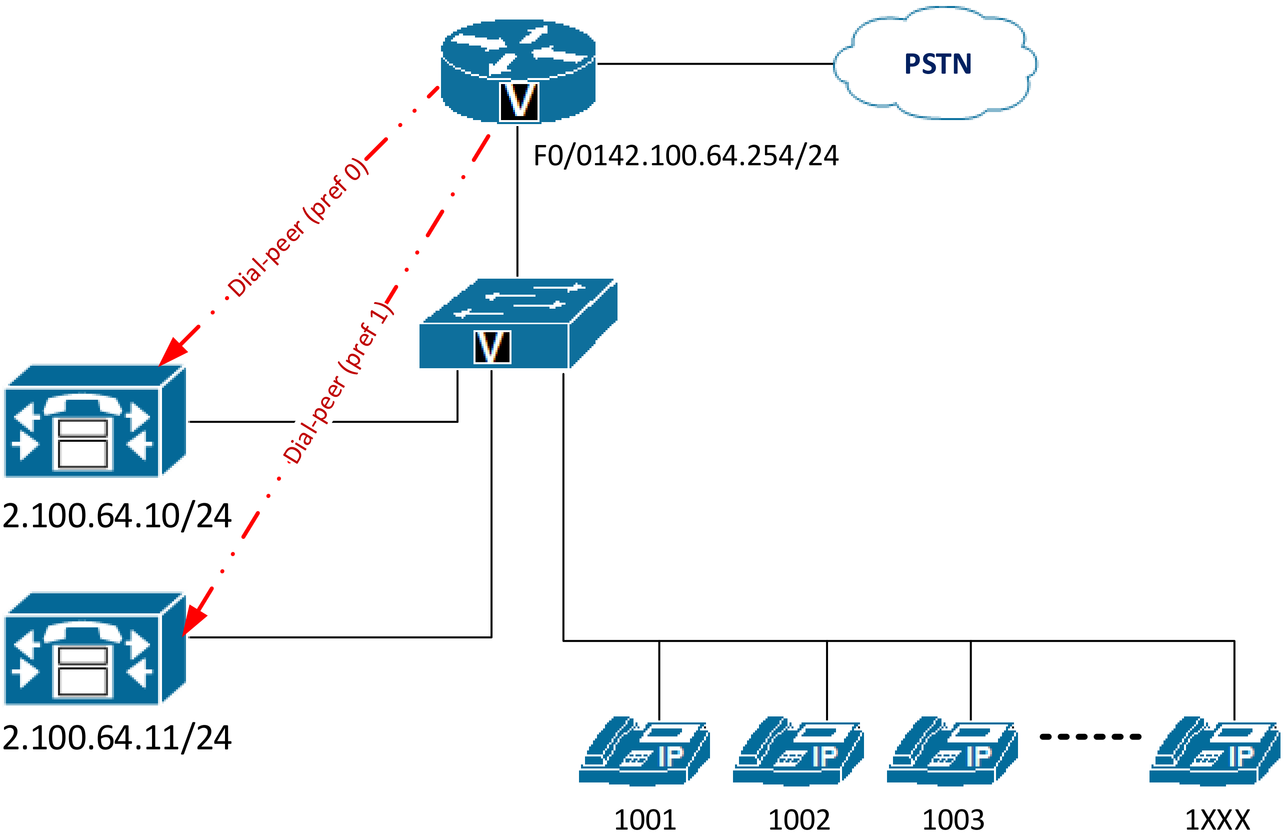
H323_GW(config)#dial-peer voice 3 voip

```
H323_GW(config-dial-peer)# voice class h323 1
```

H.323 Customizations & More on Configuration

- Every dial peer by default uses H.323 protocol unless you specify other

Scenario 1: Redundant Dial-peer and TCP Timer



Step 1: Dial-Peers

```
Router(config)#dial-peer voice 1 voip
Router(config-dialpeer)#destination-pattern 1...
Router(config-dialpeer)#session target ipv4:142.100.64.10
Router(config-dialpeer)#preference 0

Router(config)#dial-peer voice 2 voip
Router(config-dialpeer)#destination-pattern 1...
Router(config-dialpeer)#session target ipv4:142.100.64.11
Router(config-dialpeer)#preference 1
```

Step 2: Setup TCP timer (Fall Back Timer)

```
Router(config)# voice class h323 1                    [1 is a tag number only]
```

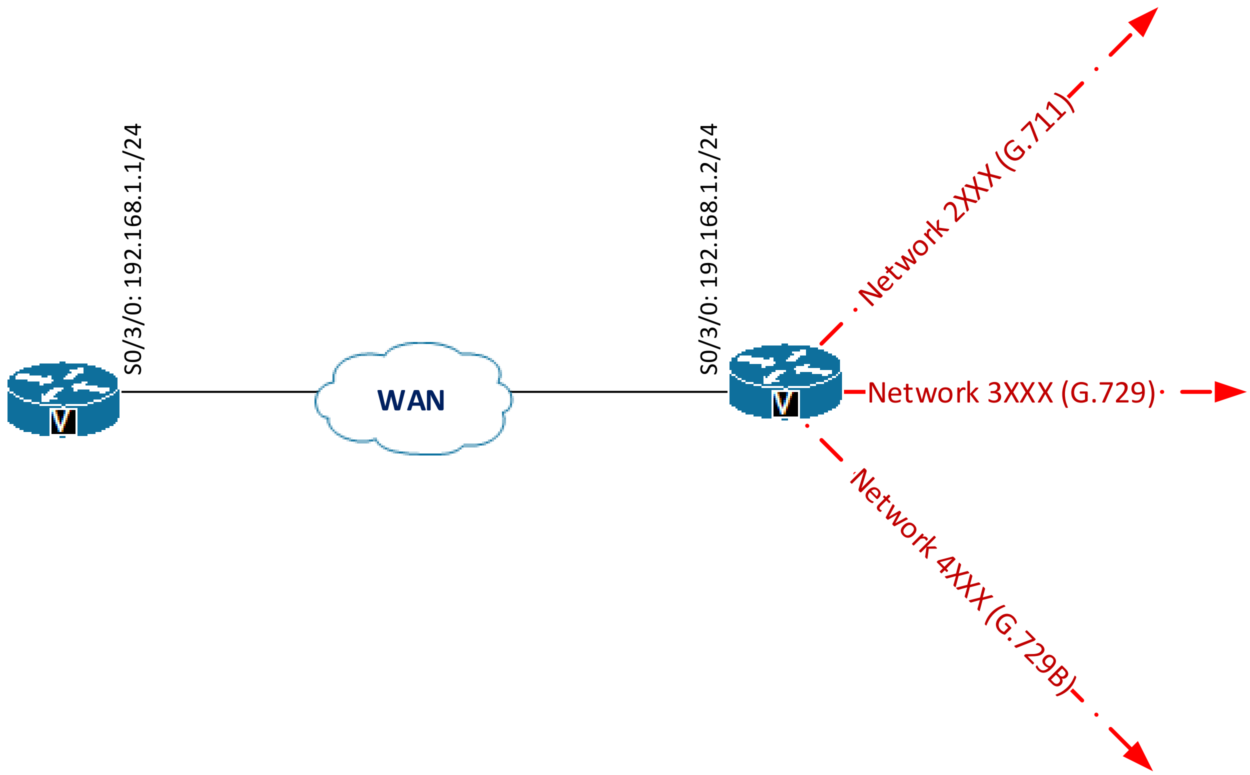
```
Router(config-class)# h225 timeout tcp establish 3     [Value in seconds, default 30]
Router(config-class)# h225 timeout setup 2             {H.225 Message timers}
Router(config-class)# h225 timeout connect 2
```

Step 3: Apply this voice class h323 <TAG> under dial-peers

```
Router(config)#dial-peer voice 1
Router(config-class)#voice-class h323 1
```

[Note: No need to apply voice class under dial-peer 2, because there is no further call manager for redundancy]

Scenario 2: Multiple Codecs per Dial-Peer



Step 1: Dial-Peer

```
Router(config)#dial-peer voice 1 voip
Router(config-dialpeer)#destination-pattern [2-4]...
Router(config-dialpeer)#session target ipv4:192.168.1.2
```

[Note: Using codec command we can specify only one under a dial-peer]

Step 2: Codec Set (Voice Class Codec)

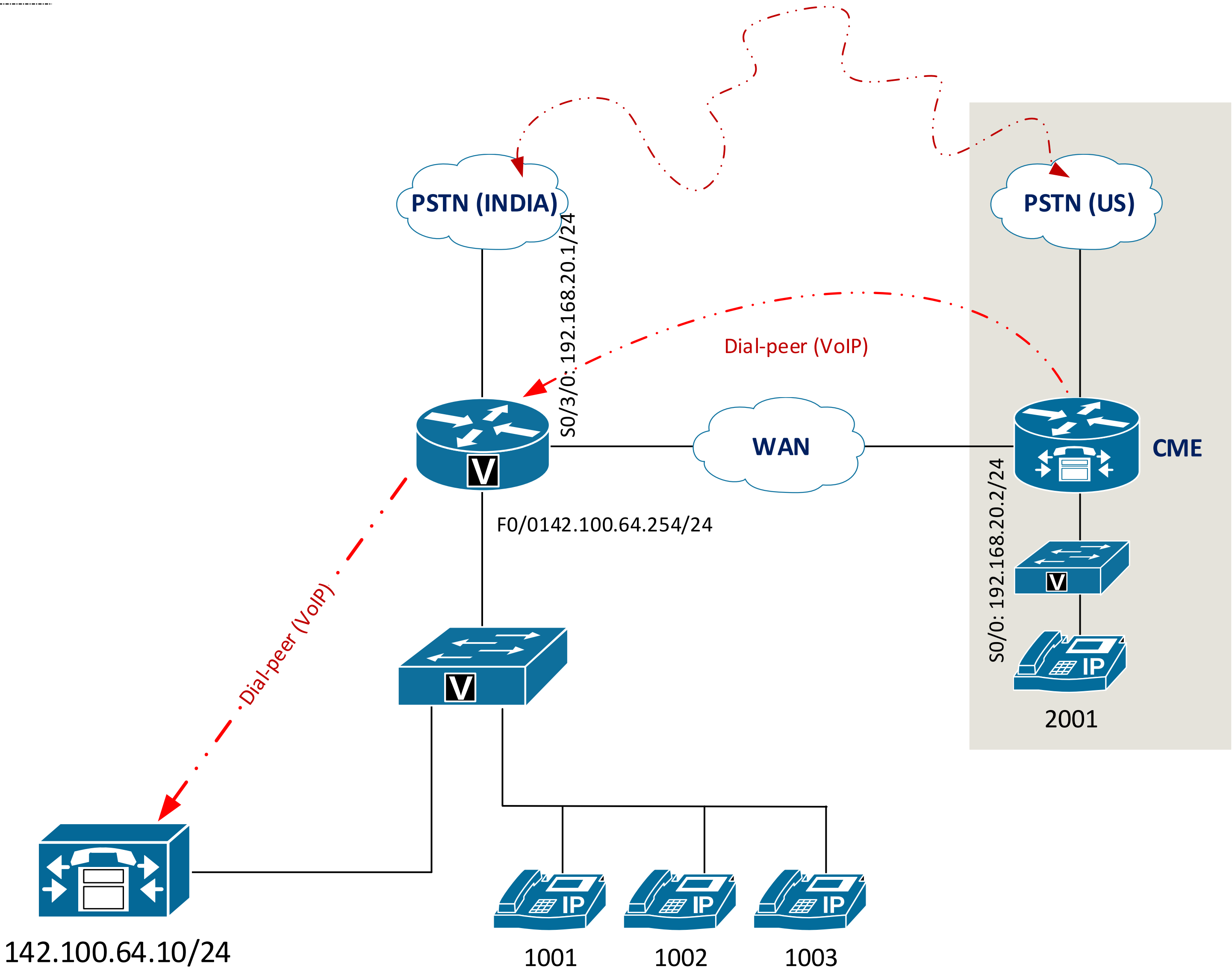
```
Router(config)# voice class codec 1                  [1 is a tag number]
Router(config-class)# codec preference 1 G711
Router(config-class)# codec preference 2 G729
Router(config-class)# codec preference 2 G729B
```

Step 3: Apply this voice class codec 1 under dial-peers

```
Router(config)#dial-peer voice 1
Router(config-dailpeer)#voice-class codec 1
```

[Note: Codec negotiation will be rotated]

Scenario 3: Allow Connections (CUBE)



If there is more than 1 VoIP Dial-Peer terminates on a Voice Gateway use CUBE command. Configure HO Router as follows

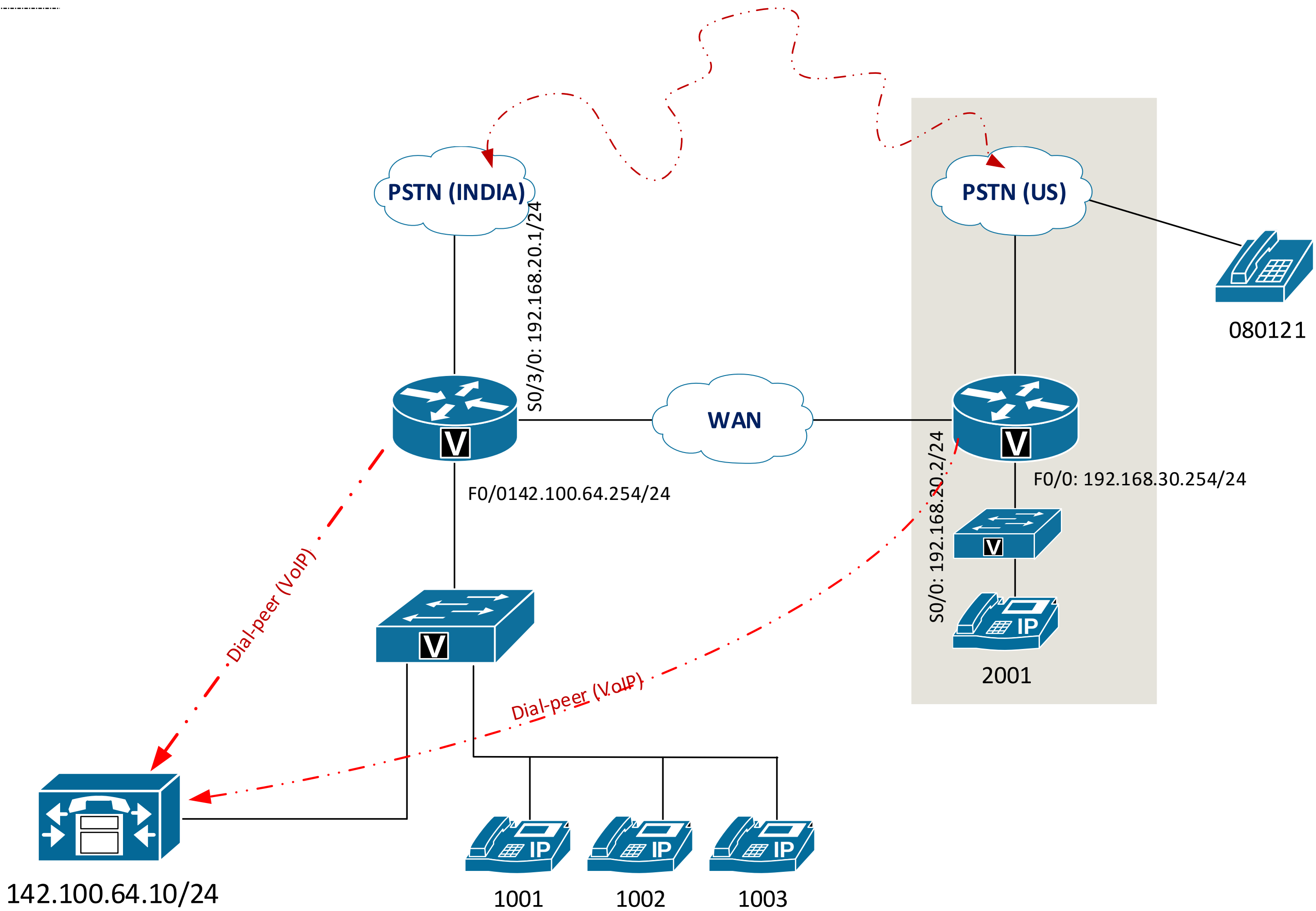
```
Router(config)# voice service voip
Router(conf-voi-serv)# allow connections h323 to h323
```

Convert H.323 to UDP (Optional)

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# session transport udp
Router(conf-serv-h323)# exit
```

- UDP is OK because our network is reliable today, hence we don’t want SYN, SYN ACK messages as in TCP
- Above command provides more efficiency
- Configure the command in both side

Scenario 3: Bind H.323 Communication to an IP or (Loopback)



- The call coming from Remote PSTN phone won't be accepted by CUCM, because CUCM only knows the IP 192.168.30.254/24 as the gateway and accept calls from that IP only
- PSTN calls having source IP address 192.168.20.2
- Hence we bind all the H.323 communications to an IP.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# h323-gateway voip interface
Router(config-if)# h323-gateway voip bind src address 142.100.64.254
```

- If the Fast Ethernet 0/0 is down, PSTN phone can't reach CUCM, so create a loopback IP and bind the H.323 communication to it.

```
Router(config)# interface loopback 1
```

```
Router(config-if)#ip address 192.168.40.254 255.255.255.0
Router(config-if)# h323-gateway voip interface
Router(config-if)# h323-gateway voip bind src address 192.168.40.254
```

Now add this loopback as H.323 Gateway in CUCM instead of 192.168.30.254

[Note: Add loopback IP in routing table]

H.323 Defaults

VoIP Dial-Peer

G.729 Codec (G.729R8)

VAD Enabled (Click voice)

DTMF Relay Disabled

Preference 0

Huntstop disabled

Play out Delay is 40ms (De-Jitter buffer)

POTS Dial-Peer

DID is disabled

Digit Strip Enabled

Automatically register with Gate Keeper

Huntstop disabled

H.323 Troubleshooting Commands

```
HO#debug h225 events
HO#debug cch323 all
HO#debug cch323 error
HO#debug cch323 h225
HO#debug cch323 h245
HO#debug cch323 session
HO#show gateway
HO#show call active/ summery/ history
---------
Router#show voice call ?
  <3-3>    Voice interface slot #
  status   Show status for active calls
```

```
  summary  Summary of all voice calls
  |        Output modifiers
  <cr>

Router#show voice call
```

MGCP (Media Gateway Control Protocol)

- Second generation protocol [SGCP- Simple Gateway Control Protocol was the 1st]
- It is defined by RFC3435
- Industry standard Plain text protocol, Cisco developed and engineered more in deeper to MGCP as compared to other vendors
- Version 0.1 (Default, all Cisco Routers running now), supported by most version of CUCM
- Version 1.0 (RFC3435), Industry standard
- MGCP is a plaintext protocol that is plaintext commands are send between call agent & gateway.
- MGCP gateway handles translation between audio signal and packet networok
- Port number 2427 is used receive commands from CUCM. 2727 used to send command acknowledgement to CUCM
- Centralize all the configuration & Centralized dial-plan on CUCM. (Survivable dial-plan configured on GW)
- Centralized management, Simple IOS configuration, MGCP BACKHAUL QSIG
- MGCP allows central control component (CUCM) to remotely control various devices
- Works as a Server/Client (Master/Slave) protocol.
- Function 1 Call Control, handled by CUCM
- Function 2: Media Translation (converting audio to packets), handled by GW itself
- Supports QSIG for working with PBX systems. No voice gateway supports QSIG, but here the CUCM processes the QSIG
- All configurations done in CUCM and gateway downloads the configuration from CUCM
- Used in hosted VoIP data centers
- When call agent goes down, MGCP loose its mind. Hence we put some backup configuration (H.323 or SIP) to the gateway called SRST MGCP Fall-back
- Call agent send a cached dial plan to the gateway to reduce over warming of messages while dialing digits

MGCP Advantages

- Simplified configuration: No need to configure static dial-peers in gateway
- Central dial plan: It simplify the management and troubleshooting of VoIP network
- Central Managements of gateway: All the gateways can be managed from a single page of CUCM
- Supports QISG: PBX integration

QSIG: All Layer 2 communication handled by router (Framing, Clock, Sync) and Layer 3 communication handled by CUCM (Call setup, Signaling)

MGCP Components

- ***End Points:*** Represent the point of interconnection between packet network and traditional telephone network
- ***Gateway:*** Handle translation between Circuit Switched network and Packet switched network
- ***Call Agent:*** Central commander for the gateway. It tell the gateway what should be reported to call agent, how end points should be connected, What signal should be implemented on end points.

MGCP Control Commands or MGCP Plaintext Messages

1. ***AUDIT ENDPOINT (AUEP):*** Request the status of endpoint. CA issues this command. Used to register the endpoint in CA.
2. ***AUDIT CONNECTION (AUCX):*** Request the status of connection. Call agent issues this command. It specify the signaling in the endpoints.
3. ***REQUEST NOTIFICATION (RQNT):*** CA instructs the gateway to watch the events on an end point and specifies the action to take when they occur. If anything happened in the MGCP Endpoint, tell me about it. CA tells to the router to do something. Call agent issues this command
4. ***NOTIFY (NTFY):*** Notify the changes in the MGCP endpoint to the CA. It is a response for RQNT. Gateway issues this command
5. ***CREATE CONNECTION (CRCX)***: CA instructs the gateway to establish connection with an end point. Call agent issues this command
6. ***MODIFY CONNECTION (MDCX):*** CA instructs the gateway to update connection parameters for previously established connection (CRCX). CA issues this command.

7. ***DELETE CONNECTION (DLCX):*** To terminate calls. CA issues this command for tear down the call. GW also issues this command if there is no resources to sustain the call
8. ***RESTART IN PROGRESS (RSIP):*** GW notifies the CA that the gateway and its endpoints are removed from service and are being placed back in service. GW issues this command

MGCP Registration Process

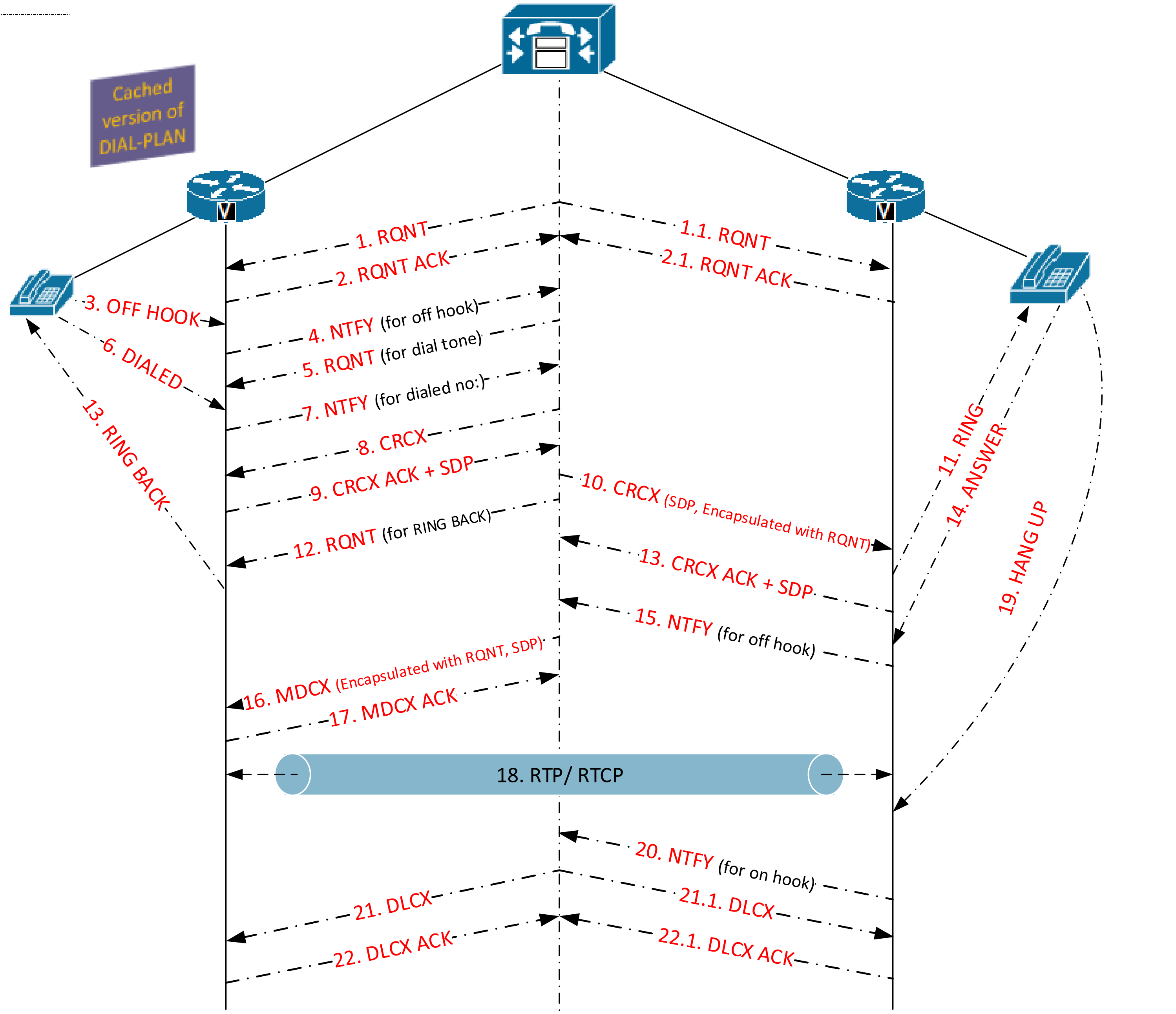
CUCM treat the Gateway not as a real gateway but as individual end points in that Gateway. E.g. FXS, FXO, T1, E1 ports in the gateway registered individually with CUCM.

Stimulus Response protocol (Soldier-Commander)

GW establish TCP session with 2427 port of CUCM based on the domain name

CUCM looks its database, and Audits (AUEP) and Register configured endpoint (we should specify endpoints to be controlled by MGCP in the GW)

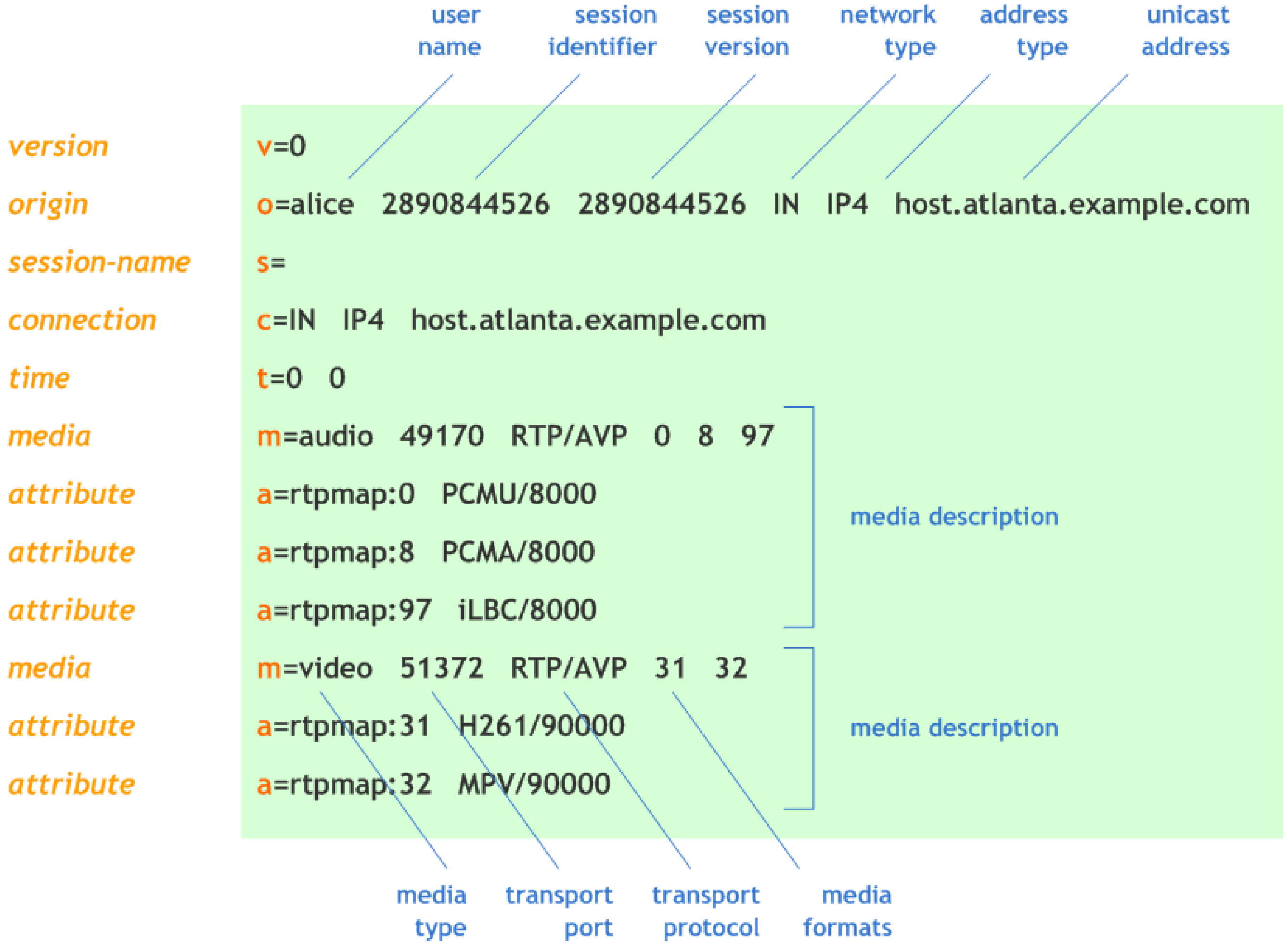
MGCP Call Flow



1. The call agent sends RQNT to each to each gateway. It instruct the gateway to wait for an event off hook.
2. In response to the RQNT, the gateway issues RQNR ACK. It defines that the gateway is ready to report all events that is going to be occur in future.
3. User off hook
4. When off hook detected, gateway report the off hook signal via NTFY
5. The call agent instruct the gateway to supply dial tone via RQNT
6. User dialed a number (There is a digit map, cached version of dial-plan, locally in the gateway)

7. The dialed digits are collected and forwarded to CA using NTFY message
8. After confirming the call is possible, the CA instruct the gateway to create a connection to the end point (FXO, FXS, E1, T1) by CRCX message
9. The gateway responds with CRCX ACK and Session Description (SDP) if it is ready to accommodate the connection. SDP identifies at least IP Address & UDP port for upcoming RTP session. Now the connection enters to a wait state.
10. The CA send CRCX to remote gateway for creating connection to its end point, along with the SDP obtained from originating gateway. This message also includes RQNT to RING the remote phone
11. CA sends a RING BACK signal via RQNT to the originating gateway
12. Originating phone get RING BACK from its gateway
13. Remote gateway sends CRCX ACK and SDP to CA
14. Remote user off hook (Answered the call)
15. When the remote user off hook, the remote gateway sends off hook event via NTFY message
16. CA sends modify connection (MDXC) to originating gateway. It contains SDP from remote gateway, and instruction to do some modification if required.
17. Initial gateway replies to CA via MDCX ACK. Now both gateway have required session information to establish RTP
18. End to end RTP streaming between two gateway
19. Remote party Hang-up
20. Remote gateway reports the hang-up (on hook event) to CA via NTFY message
21. CA sends DLCX to both gateway to terminate the connections
22. Gateways delete the connection and responds via DLCX ACK

SDP (Session Description Protocol)

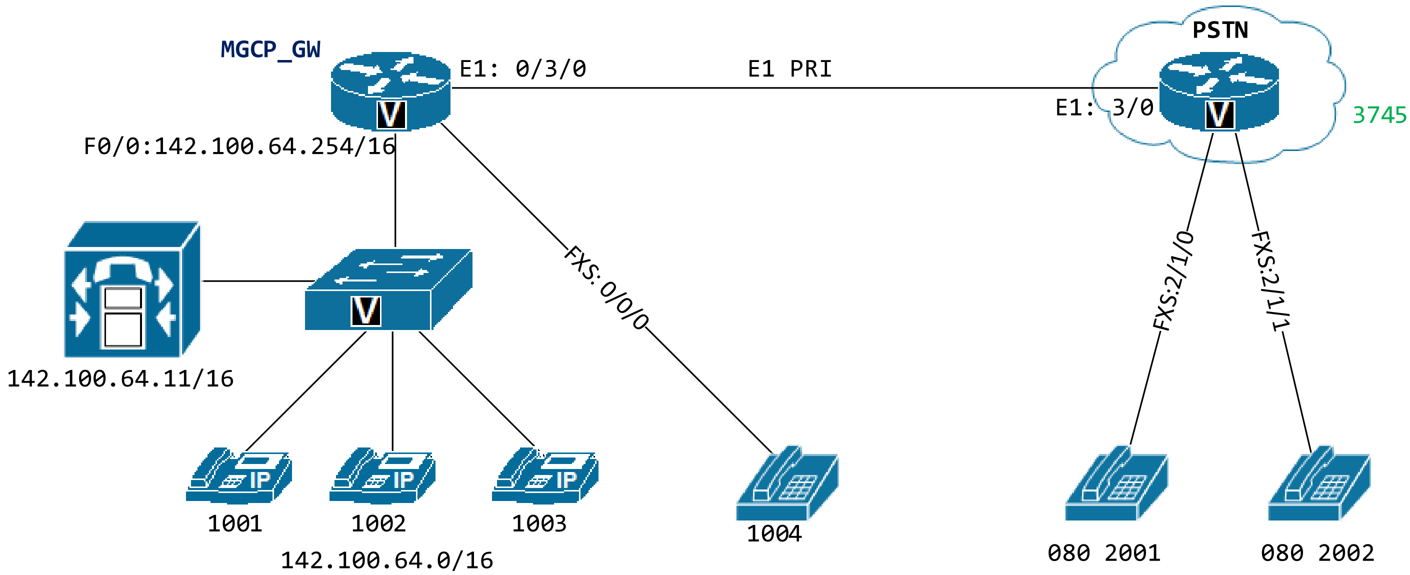


MGCP Configuration

There are three kinds of configuration in MGCP.

- ***Auto Configuration:*** Here we configure everything on the CUCM and download it to the gateway using **ccm-manager config command**
- ***Residential Gateway (RGW):*** Provide interface between analog (RJ11) call and VoIP network. FXO, FXS, Dial-peers
- ***Trunking Gateway (TGW):*** Provide interface between PSTN trunk and VoIP network. T1, E1, ISDN

Auto Configuration



PSTN Router Configuration

```
PSTN_ROUTER(config)#dial-peer voice 1 pots
PSTN_ROUTER(config-dial-peer)#destination-pattern 0802001
PSTN_ROUTER(config-dial-peer)#port 2/1/0

PSTN_ROUTER(config)#dial-peer voice 2 pots
PSTN_ROUTER(config-dial-peer)#destination-pattern 0802002
PSTN_ROUTER(config-dial-peer)#port 2/1/1

PSTN_ROUTER(config)#isdn switch-type primary-net5
PSTN_ROUTER(config)#controller E1 3/0
PSTN_ROUTER(config-controller)#framing crc4
PSTN_ROUTER(config-controller)#linecode hdb3
```

```
PSTN_ROUTER(config-controller)#clock source internal
PSTN_ROUTER(config-controller)#pri-group timeslots 1-10,16
PSTN_ROUTER(config-controller)#no shutdown

PSTN_ROUTER(config)#interface serial 3/0:15
PSTN_ROUTER(config-if)#isdn switch-type primary-net5
PSTN_ROUTER(config-if)#isdn protocol-emulate network
PSTN_ROUTER(config-if)#isdn bchan-number-order ascending
PSTN_ROUTER(config-if)#isdn incoming-voice voice
PSTN_ROUTER(config-if)#no shutdown

PSTN_ROUTER(config)#dial-peer voice 3 pots
PSTN_ROUTER(config-dial-peer)#incoming called-number .
PSTN_ROUTER(config-dial-peer)#direct-inward-dial
PSTN_ROUTER(config-dial-peer)#port 3/0:15

PSTN_ROUTER(config)#dial-peer voice 4 pots
PSTN_ROUTER(config-dial-peer)# description E1_OUTBOUND_DIAL-PEER
PSTN_ROUTER(config-dial-peer)#destination-pattern 100.
PSTN_ROUTER(config-dial-peer)#no digit-strip
PSTN_ROUTER(config-dial-peer)#port 3/0:15
```

CUCM Side Configuration

Cisco Unified CM Administration → Device → Gateway → Find → Add New →

Type : Cisco 2811 <SELECT_MODEL>

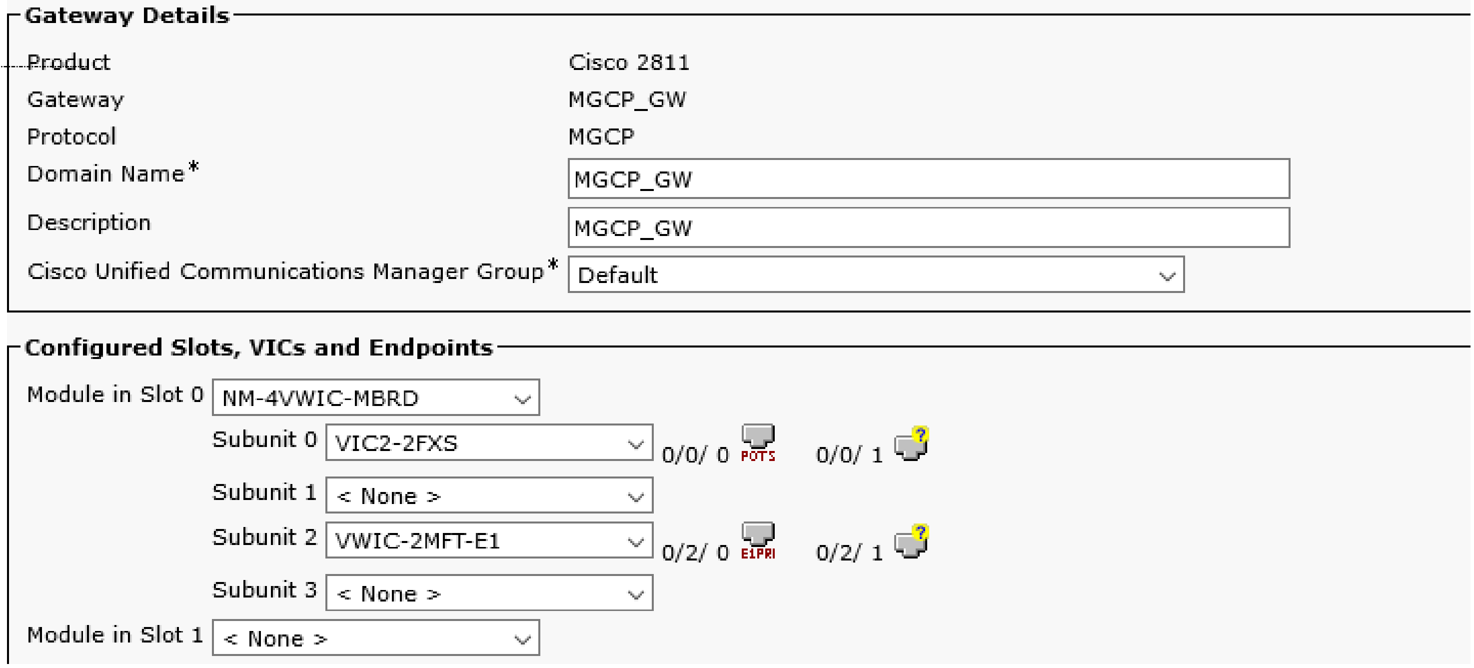
Protocol : MGCP → Next

Domain Name : MGW_GW <HOST_NAME_OF_GATEWAY_ROUTER or Domain Name>

Description : MGCP_GW_INDIA

Cisco Unified Communications Manager Group : Default

Configured Slots, VICs and Endpoints



Module in Slot 0 : NM-4VWIC-MBRD

→ Save

Subunit 0: VIC2-2FXS

Subunit 1: - - - - - -

Subunit 2: VIC2-2MFT-E1

→ Save

FXS Configuration

Click 0/0/ 0 in the subunit 0 section → Port Type: POTS

End-Point Name : AALN/S0/SU0/0@MGCP_GW

Description : Analog Phone 1004

Device Pool : Default

→ Save

Line [1] - Add a new DN → 1004 → Save

E1 PRI Trunk Configuration

End-Point Name : S0/SU2/DS1-0@MGCP_GW

Description : E1 PRI CIRCUIT

Device Pool : Default

Interface Information:

PRI Protocol Type* : PRI-EURO

Protocol Side* : User

Channel Selection Order : Bottom Up (Descending)

PCM Type : A-law

[For Fractional PRI, Enable status poll : Check]

Product Specific Configuration Layout:

Line Coding* : HDB3

Framing* : CRC4

Clock* : External

Gateway Side Configuration

```
MGCP_GW(config)#interface fastEthernet 0/0
MGCP_GW(config-if)#ip address 142.100.64.254 255.255.0.0
MGCP_GW(config-if)#no shutdown

MGCP_GW(config)#ccm-manager mgcp
MGCP_GW(config)#mgcp
MGCP_GW(config)#ccm-manager config server 142.100.64.11
MGCP_GW(config)#ccm-manager config
```

[Note: MGCP_GW.cnf.xml file will be downloaded from tftp server]

Route Pattern

To call outside number from CUCM, we must specify Route Pattern by pointing the gateway.

Call Routing → Route/Hunt → Route Pattern → Add New

Route Pattern* : 080200X

Gateway/Route List* : S0/SU2/DS1-0@MGCP_GW

→ Save

To see the status (Go to MGCP_GW and download the configuration), then

Device → Gateway → See End Points

```
AALN/S0/SU2/1@MGW    FXO2/1_CONFIG   Default         Cisco    MGCP    FXO    Port
      Registered with 142.100.64.11   142.100.64.254
AALN/S0/SU3/0@MGW    FXS3/0_CONFIG   Default         Cisco    MGCP    FXS    Port
      Registered with 142.100.64.11   142.100.64.254
-----------------------------------------------------------------------------------
```

MGCP Troubleshooting Command

- ***MGCP_GW#show isdn status***: Status of ISDN layers
- ***MGCP_GW#show mgcp***: We can see Admin state, CA IP, Port,
- ***MGCP_GW#show ccm-manager:*** Shows active redundant call managers (CUCM Group), shows where the gateway registered.
- ***MGCP_GW#show mgcp endpoint:*** List all the voice ports configured for MGCP
- ***MGCP_GW#show mgcp statistics:*** Shows the successful and unsuccessful control commands
- ***MGCP_GW#debug voip ccapi inout:*** Shows every interaction with call control and progress of call
- ***MGCP_GW#debug mgcp*** ? [all, errors, events, packets, parser]: MGCP traces

MGCP Residential Gateway Configuration

<Configure CUCM Side>

Step 1: Initiate MGCP Application on gateway

```
Router(config)# mgcp
Router(config)# ccm-manager mgcp [CA is CUCM]
```

Step 2: Specify Call Agent's IP Address, Service Type

```
Router(config)# mgcp call-agent 142.100.64.11 service-type mgcp
Router(config)# ccm-manager redundant host <SECONDARY SERVER IP> <THIRTIARY IP>
```

Step 3: Setup dial-peer for voice port

```
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# application mgcpapp
Router(config-dialpeer)# port 0/0/0

Router(config)# dial-peer voice 2 pots
Router(config-dialpeer)# application mgcpapp
```

```
Router(config-dialpeer)# port 0/0/1
```

```
MGW(config)#ccm-manager config server 142.100.64.11
MGW(config)#ccm-manager config
```

MGCP Trunk Gateway Configuration

<Configure CUCM Side>

Step 1: Initiate MGCP Application on gateway

```
Router(config)# ccm-manager mgcp
Router(config)# mgcp
```

Step 2: Specify Call Agent's IP Address, Service Type

```
Router(config)# mgcp call-agent 142.100.64.11 service-type mgcp
```

Step 3: Setup Controller under MGCP

```
Router(config)# controller E1 0/3/0
Router(config-controller)# pri-group timeslots 1-30 type none service mgcp
```

Step 4: Setup Digital Voice Port under MGCP

```
Router(config)# interface serial 0/3/0:15
Router(config-if)# isdn bind-c3 ccm manager
```

```
MGW(config)#ccm-manager config server 142.100.64.11
MGW(config)#ccm-manager config
```

MGCP Backhaul

- MGCP to control ISDN line & QSIG (Gateway & Call Manager split the configuration and control an ISDN line)
- Gateway handles Q.921 signaling, but passes Q.931 to CUCM
- It is the only way to support QSIG, Router doesn't understand QSIG so it pass to CUCM (Q.931 where QSIG resides)
- MGCP Backhaul allows you to pass layer 3 signaling (or control of PRI connection) to CUCM

- Port number used is 2428

End Point Type/ Slot/ Subunit/ Port

MGCP Port Descriptions

AALN: Analog Access Line

S0: Slot 0

SU0: Subunit 0

1: Port

SIP (Session Initiation Protocol)

- SIP is an ideal VoIP protocol for interconnecting different VoIP system and networks
- 5060 port number
- The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions.
- Internet Engineering Talk Force (IETF) developed SIP as an alternative to H.323
- SIP is a peer to peer protocol where internet end points (User Agents) initiate sessions, similar to H.323
- ITSP uses SIP as their standard
- SIP is supported by most of the VoIP vendors
- Goal of SIP is creating, modifying & terminating sessions
- SIP is an open standard, still developing protocol & expandable in future
- SIP borrows many familiar internet standards (HTTP, DNS) with clear text.
- SIP uses SDP (Session Description Protocol) to exchange capabilities (Like H.245)
- Key feature: Presence (Availability of IP Phone users)
- Integrate with other VoIP network via SIP Trunk
- Multimedia Integration (IM)
- Easy troubleshooting
- Supports 3rd party phone in CUCM

Session Management Includes 4 tasks

Locating Users (Translate SIP Address (phone number, email) to IP Address)

Negotiating Capabilities & Features (similar to H.245)

Modifying session parameters during call (Hold, Conference)

Setup and teardown of all users

SIP Components

- ***User Agents (UA)***: Client- Calling Party, Server – Called Party)

- ***Proxy Server***: Initial point of contact for user agents. It receive SIP request from UAC and forward it on behalf of the client to the next SIP server in the network
- ***Redirect Server***: Finds a location of an endpoint. It provide next hope information to UAC
- ***Registrar Server***: Receive SIP registration request from SIP endpoints & register the endpoint to a database
- ***Location Server***: Database of all User agents. It implements the mechanism to resolve the address.
- ***Presence Server***: Tracks status of UAs

SIP Messages (Methods & Responses)

Methods: Are something that takes actions

- ***REGISTER***: Endpoint sends REGISTER request to the SIP server to register. The request includes the user's contact list. The SIP server provides a challenge to endpoint. User enters her/his valid user ID and password. The SIP server validates the user's credentials. It registers the user in its contact database and returns a response (200 OK)

```
REGISTER sip:registrar.athens.gr SIP/2.0
Via: SIP/2.0/UDP 201.202.203.204:5060;branch=z9hG4bK313
Max-Forwards:70
To: sip:euclid@athens.gr
From: <sip:secretary@academy.athens.gr>;tag=543131
Call-ID: 2000-July-07-23:59:59.1234@201.202.203.204
CSeq: 1 REGISTER
Contact: sip:euclid@parthenon.athens.gr
Contact: mailto:euclid@geometry.org
Content-Length: 0
```

- ***INVITE***: The INVITE method is used to establish media sessions between user agents. It is similar to a Q.931 Setup message in ISDN. Responses to INVITEs are always acknowledged with the ACK.

```
INVITE sip:411@salzburg.at;user=phone SIP/2.0
Via: SIP/2.0/UDP salzburg.edu.at:5060;branch=z9hG4bK1d32hr4
Max-Forwards:70
To: <sip:411@salzburg.at;user=phone>
From: Christian Doppler <sip:c.doppler@salzburg.edu.at>
;tag=817234
Call-ID: 12-45-A5-46-F5@salzburg.edu.at
CSeq: 1 INVITE
Subject: Train Timetables
Contact: sip:c.doppler@salzburg.edu.at
Content-Type: application/sdp
```

```
Content-Length: 151

v=0
o=doppler 2890842326 2890844532 IN IP4 salzburg.edu.at
s=Phone Call
c=IN IP4 50.61.72.83
t=0 0
SIP Request Messages 73
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- ***ACK***: The ACK method is used to acknowledge final responses to INVITE requests. Final responses to all other requests are never acknowledged. Final responses are defined as 2xx, 3xx, 4xx, 5xx, or 6xx class responses. The CSeq number is never incremented for an ACK

```
ACK sip:laplace@mathematica.org SIP/2.0
Via: SIP/2.0/TCP 128.5.2.1:5060;branch=z9hG4bK1834
Max-Forwards:70
To: Marquis de Laplace <sip:laplace@mathematica.org>;tag=90210
From: Nathaniel Bowditch <sip:n.bowditch@salem.ma.us>;tag=887865
Call-ID: 152-45-N-32-23-W@128.5.2.1
CSeq: 3 ACK
Content-Type: application/sdp
Content-Length: 143
v=0
o=bowditch 2590844326 2590944532 IN IP4 salem.ma.us
s=Bearing
c=IN IP4 salem.ma.us
t=0 0
m=audio 32852 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- ***CANCEL***: The CANCEL method is used to terminate pending searches or call attempts. It can be generated by either user agents or proxy servers provided that a 1xx response containing a tag has been received, but no final response (200 OK) has been received.

```
CANCEL sip:i.newton@cambridge.edu.gb SIP/2.0
Via: SIP/2.0/UDP 10.downing.gb:5060
;branch=z9hG4bK3134134
Max-Forwards:70
To: Isaac Newton <sip:i.newton@cambridge.edu.gb>
From: Rene Descartes <sip:visitor@10.downing.gb>;tag=034323
Call-ID: 42@10.downing.gb
CSeq: 32156 CANCEL
Content-Length: 0
```

- ***OPTIONS***: The OPTIONS method is used to query a user agent or server about its capabilities and discover its current availability. The response to the request lists the capabilities of the user agent or server.

```
OPTIONS sip:user@carrier.com SIP/2.0
Via: SIP/2.0/UDP cavendish.kings.cambridge.edu.uk
```

```
;branch=z9hG4bK1834
Max-Forwards:70
To: <sip:user@proxy.carrier.com>
From: J.C. Maxwell <sip:james.maxwell@kings.cambridge.edu.uk>
;tag=34
Call-ID: 9352812@cavendish.kings.cambridge.edu.uk
CSeq: 1 OPTIONS
Content-Length: 0
SIP/2.0 200 OK
Via: SIP/2.0/UDP cavendish.kings.cambridge.edu.uk;tag=512A6
;branch=z9hG4bK0834 ;received=192.0.0.2
To: <sip:user@proxy.carrier.com>;tag=432
From: J.C. Maxwell <sip:james.maxwell@kings.cambridge.edu.uk>
;tag=34
Call-ID: 9352812@cavendish.kings.cambridge.edu.uk
CSeq: 1 OPTIONS
Allow: INVITE, OPTIONS, ACK, BYE, CANCEL, REFER
Accept-Language: en, de, fr
Content-Length: ...
Content-Type: application/sdp
v=0
etc...
```

- ***BYE***: The BYE method is used to terminate an established media session. In ISDN, it is similar to a RELEASE message. A session is considered established if an INVITE has received a success class response (2xx) or an ACK has been sent. A BYE is sent only by user agents participating in the session, never by proxies or other third parties. It is an end-to-end method, so responses are only generated by the other user agent.

```
BYE sip:info@hypotenuse.org SIP/2.0
Via: SIP/2.0/UDP port443.hotmail.com:5060;branch=z9hG4bK312bc
Max-Forwards:70
To: <sip:info@hypotenuse.org>;tag=63104
From: <sip:pythag42@hotmail.com>;tag=9341123
Call-ID: 34283291273@port443.hotmail.com
CSeq: 47 BYE
Content-Length: 0
```

- ***PRACK***: It is an ACK for 1XX series informational message. The informational messages are no a final response for invite, hence they acknowledge by PRACK. 2XX, 3XX, 4XX, 5XX, 6XX are acknowledged by actual ACK method. The PRACK echoes the number in the RSeq and the CSeq of the response in a RAck header.

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP lucasian.trinity.cambridge.edu.uk
;branch=z9hG4bK452352
;received=1.2.3.4
To: Descartes <sip:rene.descartes@metaphysics.org>;tag=12323
From: Newton <sip:newton@kings.cambridge.edu.uk>;tag=981
Call-ID: 5@lucasian.trinity.cambridge.edu.uk
RSeq: 314
CSeq: 1 INVITE
```

```
Content-Length: 0

PRACK sip:rene.descartes@metaphysics.org SIP/2.0
Via: SIP/2.0/UDP lucasian.trinity.cambridge.edu.uk
;branch=z9hG4bKdtyw
Max-Forwards: 70
To: Descartes <sip:rene.descartes@metaphysics.org>;tag=12323
From: Newton <sip:newton@kings.cambridge.edu.uk>;tag=981
Call-ID: 5@lucasian.trinity.cambridge.edu.uk
CSeq: 2 PRACK
RAck: 314 1 INVITE
Content-Length: 0
```

Note:

CSeq *or Command Sequence contains an integer and a method name. The CSeq number is incremented for each new request within a dialog and is a traditional sequence number.*

RSeq *or Response Sequence Each provisional response is given a sequence number, carried in the RSeq header field in the response.*

Responses: Response to the methods

- ***INFORMATIONAL (1XX)***: The informational class of responses 1xx are used to indicate call progress. Informational responses are end-to-end responses.
  1. *100 TRYING*: This special case response is only a hop-by-hop request. It is never forwarded.
  2. *180 Ringing*: This response is used to indicate that the INVITE has been received by the user agent and that alerting is taken place.
  3. *182 Call Queued*: This response is used to indicate that the INVITE has been received, and will be processed in a queue.
  4. *The 183 Session Progress*: Indicates that information about the progress of the session. 183 is an end-to-end response. A typical use of this response is to allow a UAC to hear ring tone, busy tone, or a recorded announcement. This is because call progress information is carried in the media stream in the PSTN. A one-way media connection or trunk is established from the calling party’s telephone switch to the called party’s telephone switch in the PSTN prior to the call being answered.
- ***SUCCESS (2XX)***: Success class responses indicate that the request has succeeded or has been accepted.

1. *200 OK*: 200 OK response has two uses in SIP. When used to accept a session invitation, it will contain a message body containing the media properties of the UAS (called party).

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
 ;received=192.0.2.101
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:bob@client.biloxi.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 147

v=0
o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com
s=-
c=IN IP4 192.0.2.201
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

2. *202 Accepted*: Response indicates that the UAS has received and understood the request, but that the request may not have been authorized or processed by the server

- ***REDIRECT (3XX)***: Server has returned possible locations. The client should retry request at another server. generally sent by a SIP server acting as a redirect server in response to an INVITE
  1. *300 Multiple Choices*: multiple Contact header fields, which indicate that the location service has returned multiple possible locations. They should be tried in the order in which they were listed in the response
  2. *301 Moved Permanently*: This redirection response contains a Contact header field with the new permanent URI of the called party. The address can be saved and used in future INVITE requests.
  3. *302 Moved Temporarily*: This redirection response contains a URI that is currently valid but that is not permanent.
  4. *305 Use Proxy*: This redirection response contains a URI that points to a proxy server
  5. *380 Alternative Service*: This response returns a URI that indicates the type of service that the called party would like. An example might be a redirect to a voicemail server

- ***CLIENT ERROR (4XX)***: The request has failed due to an error by the client. The client may retry the request if reformulated according to response

1. *__400 Bad Request__*: This response indicates that the request was not understood by the server
2. *__401 Unauthorized__*: This response indicates that the request requires the user to perform authentication & the authentication may fail.
3. *__402 Payment Required__*: This response is a placeholder for future definition in the SIP protocol. It could be used to negotiate call completion charges
4. *__403 Forbidden__*: This response is used to deny a request
5. *__404 Not Found__*: This response indicates that the user identified by the sip or sips URI in the Request-URI cannot be located by the server
6. *__405 Method Not Allowed__*: This response indicates that the server or user agent has received and understood a request but is not willing to fulfill the request. An example might be a REGISTER request sent to a user agent.
7. *__406 Not Acceptable__*: This response indicates that the request cannot be processed due to a requirement in the request message.
8. *__407 Proxy Authentication Required__*: This request sent by a proxy indicates that the UAC must first authenticate itself with the proxy before the request can be processed
9. *__408 Request Timeout__*: This response is sent when an Expires header field is present in an INVITE request, and the specified time period has passed.
10. *__410 Gone__*: This response is similar to the 404 Not Found response but contains the hint that the requested user will not be available at this location in the future. This response could be used by a service provider when a user cancels their service
11. *__415 Unsupported Media Type__*: This response sent by a user agent indicates that the media type contained in the INVITE request is not supported. For example, a request for a video conference to a PSTN gateway that only handles telephone calls will result in this response
12. *__480 Temporarily Unavailable__*: This response indicates that the request has reached the correct destination, but the called party is not available for some reason. The reason phrase should be modified for this response to give the caller a better understanding of the situation. The response should

contain a Retry-After header indicating when the request may be able to be fulfilled.

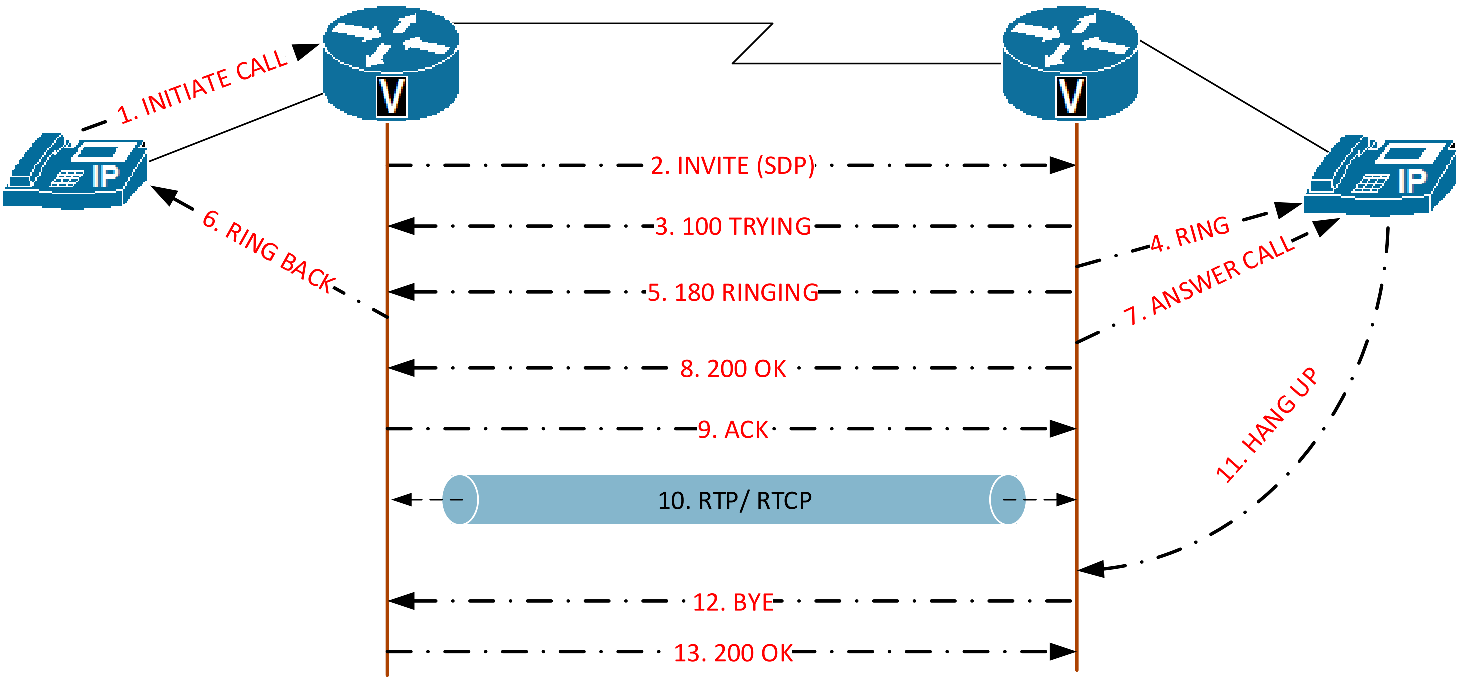
13. *483 Too Many Hops*: This response indicates that the request has been forwarded the maximum number of times as set by the Max-Forwards header in the request.
14. *486 Busy Here*: This response is used to indicate that the user agent is busy. This response is equivalent to the busy tone in the PSTN.
15. *487 Request Terminated*: For pending invites to terminate

- ***SERVER ERROR (5XX)***: The request has failed due to an error by the server. The request may be retried at another server.
    1. *501 Not Implemented*: This response indicates that the server is unable to process the request because it is not supported. This response can be used to decline a request containing an unknown method
    2. *502 Bad Gateway*: This response is sent by a proxy that is acting as a gateway to another network, and indicates that some problem in the other network is preventing the request from being processed
    3. *503 Service Unavailable*: This response indicates that the requested service is temporarily unavailable. The request can be retried after a few seconds, or after the expiration of the Retry-After header field
    4. *504 Gateway Timeout*: This response indicates that the request failed due to a timeout encountered in the other network to which that the gateway connects
    5. *505 Version Not Supported*: This response indicates that the request has been refused by the server because of the SIP version number of the request. There is only one version of SIP (version 2.0) currently implemented
- ***GLOBAL FAILURE (6XX)***: The request has failed. The request should not be tried again at this or other servers
    1. *600 Busy Everywhere*: If there is a possibility that the could be answered in other locations, this response should not be sent
    2. *604 Does Not Exist Anywhere*: This response is similar to the 404 Not Found response but indicates that the user in the Request-URI cannot be found anywhere

3. *606 Not Acceptable*: This response can be used to implement some session negotiation capability in SIP. This response indicates that some aspect of the desired session is not acceptable to the UAS, and as a result, the session cannot be established. The response may contain a Warning header field with a numerical code describing exactly what was not acceptable

SIP Call Flow

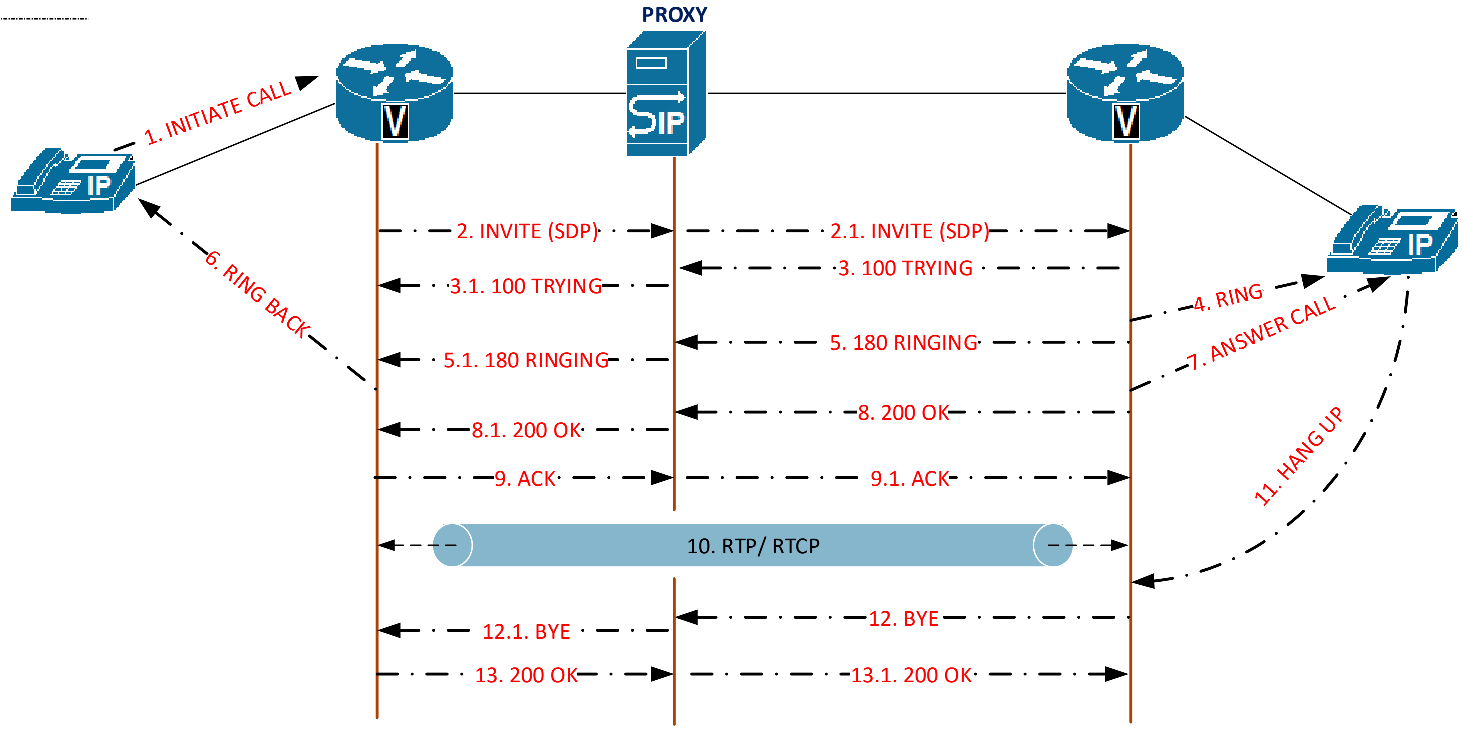
Direct Call Flow



1. Endpoint initiates a call
2. The originating User Agent Client (UAC) sends an INVITE message to the User Agent Server in the remote location. This INVITE message includes SDP (supported media parameters, IP, Port) of UAC
3. UAS responds with 100 TRYING message, hence the originating gateway enter in to a wait state
4. Remote gateway send RINGING signal to destination phone
5. UAS informs UAC about the RINGING via 180 RINGING response message
6. Originating gateway sends RING BACK signal to originating phone
7. Called party off-hook (Answered the call)
8. UAS determines the call parameters are acceptable, and responds positively to UAC by 200 OK message

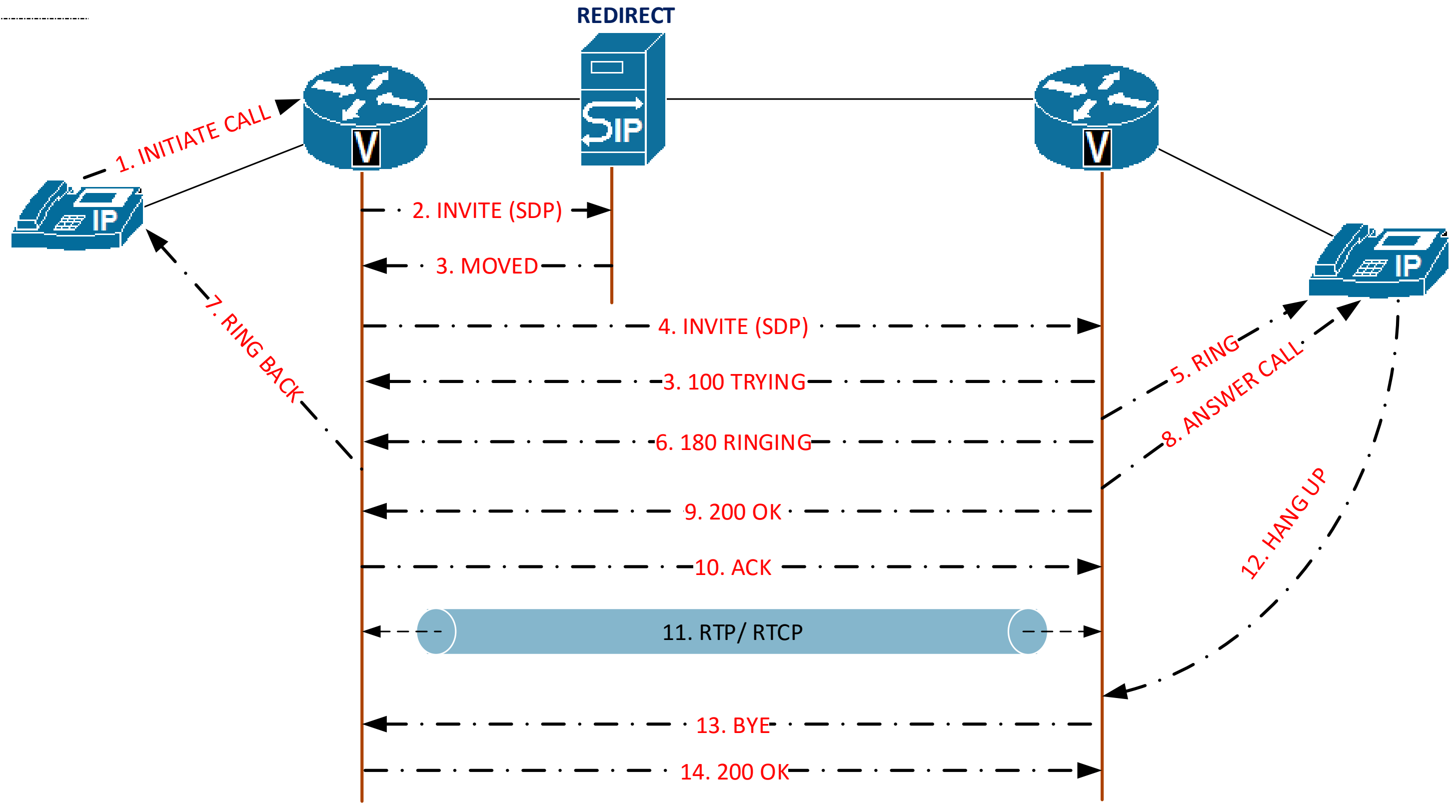
9. UAC issues ACK to confirm the previous 200 OK message from UAS. At this point UAC & UAS have all the information to establish RTP
10. RTP + RTCP Establishment
11. Remote party Hang up (on hook- disconnected the call)
12. UAS sends BYE message to UAC
13. BYE message confirmed by 200 OK by the UAC

SIP Call Flow Using PROXY Server



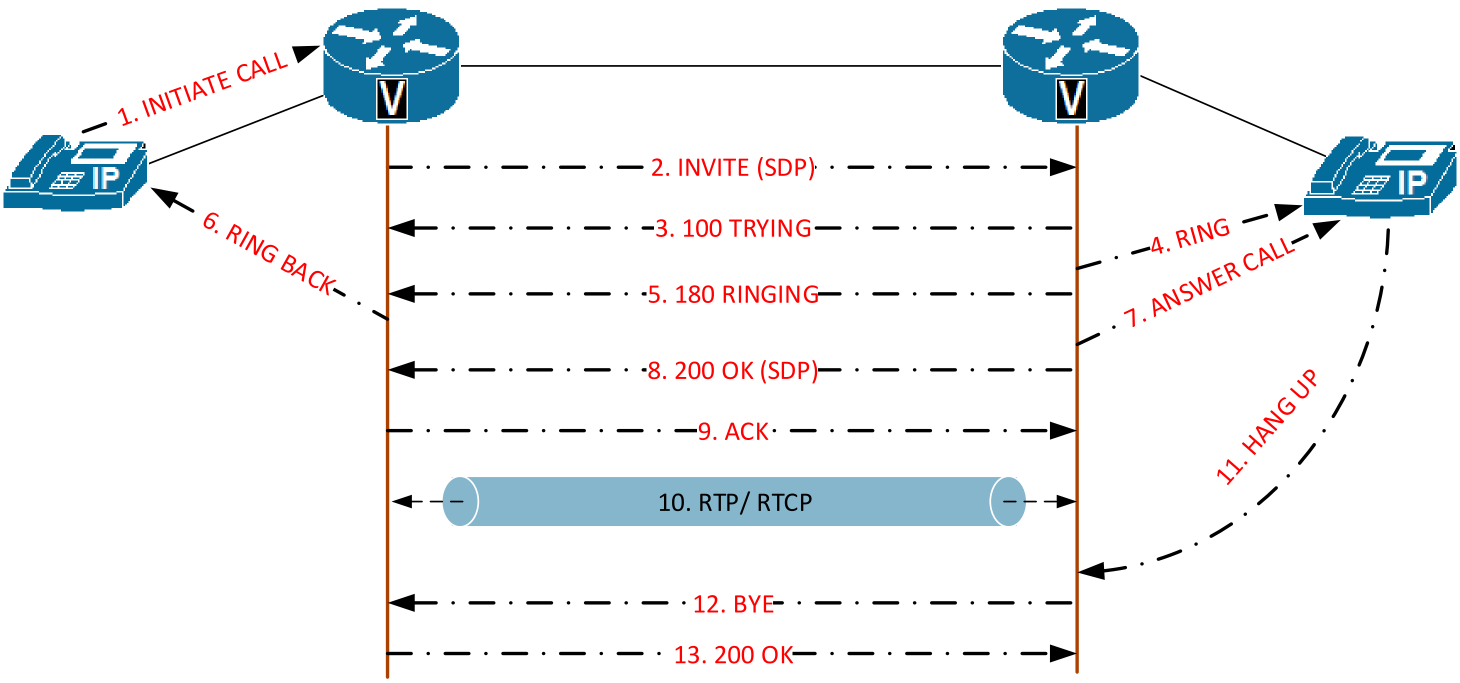
- PROXY server intercepts & forwards SIP invitation to destination UAS on behalf of the originator.
- Advantage is that UAC doesn't need to learn coordinates of destination UAS.
- Disadvantage is more signaling

SIP Call Flow Using REDIRECT Server



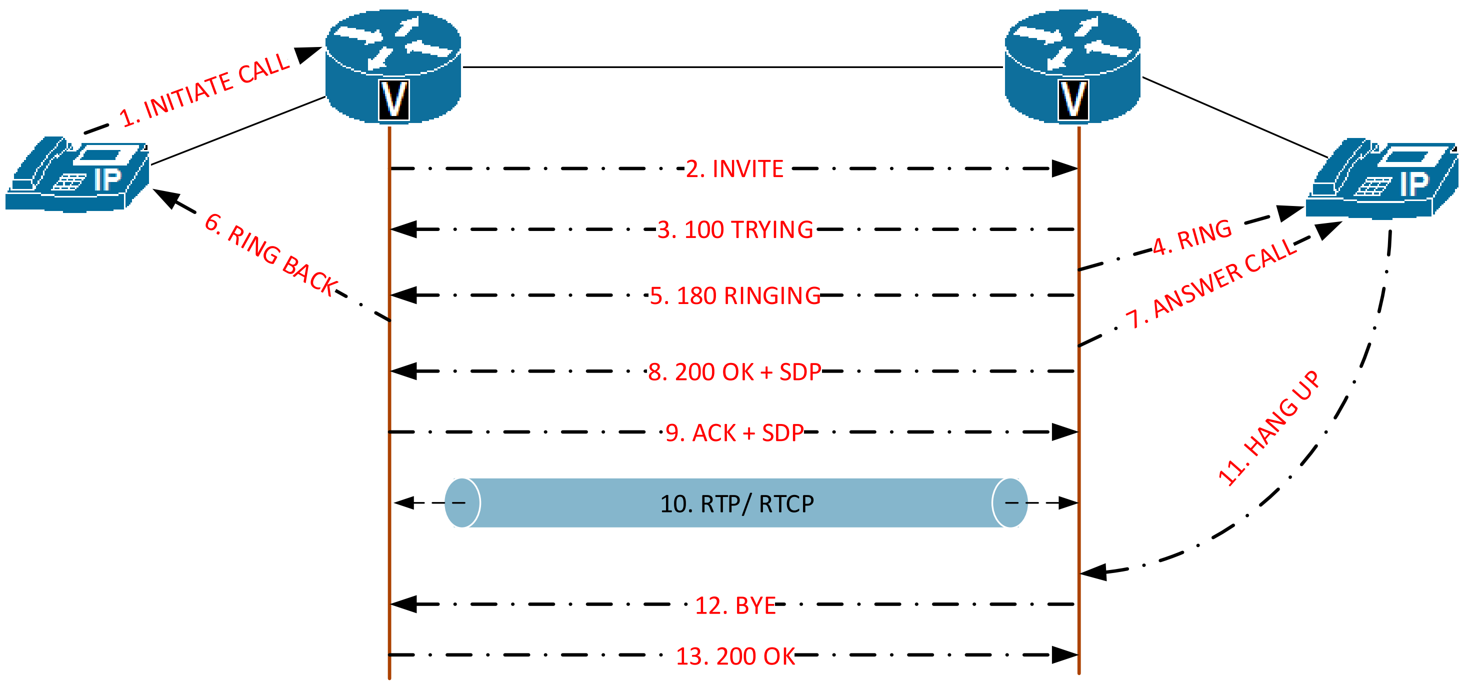
- A redirect server is programmed to discover the path to the destination.
- Instead of forwarding the INVITE message, redirect server reports back to UAC with the destination coordinates that the UAC should try next.

Early Offer SIP Call Flow



- Based on SDP offer and reply, the SIP call set up ide divided in to two.
- It is the default method used in Cisco. What we have learned before is Early offer Call setup. Here the INVITE message consists of SDP.
- The session initiator (UAC) sends its capabilities (including supported codec) along with INVITE.
- The 200 OK composed of destination party SDP parameters.

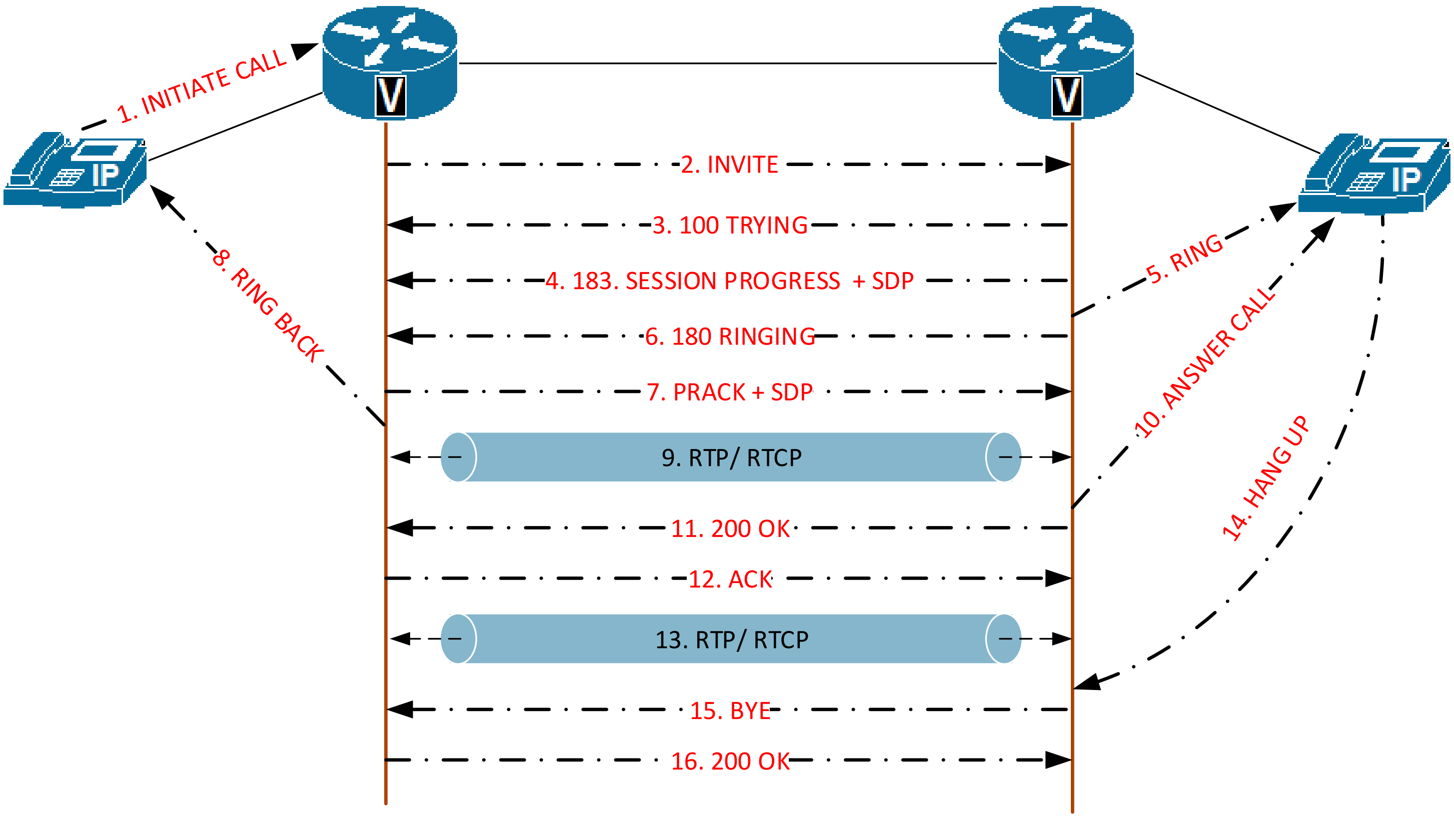
Delayed offer SIP Call Flow



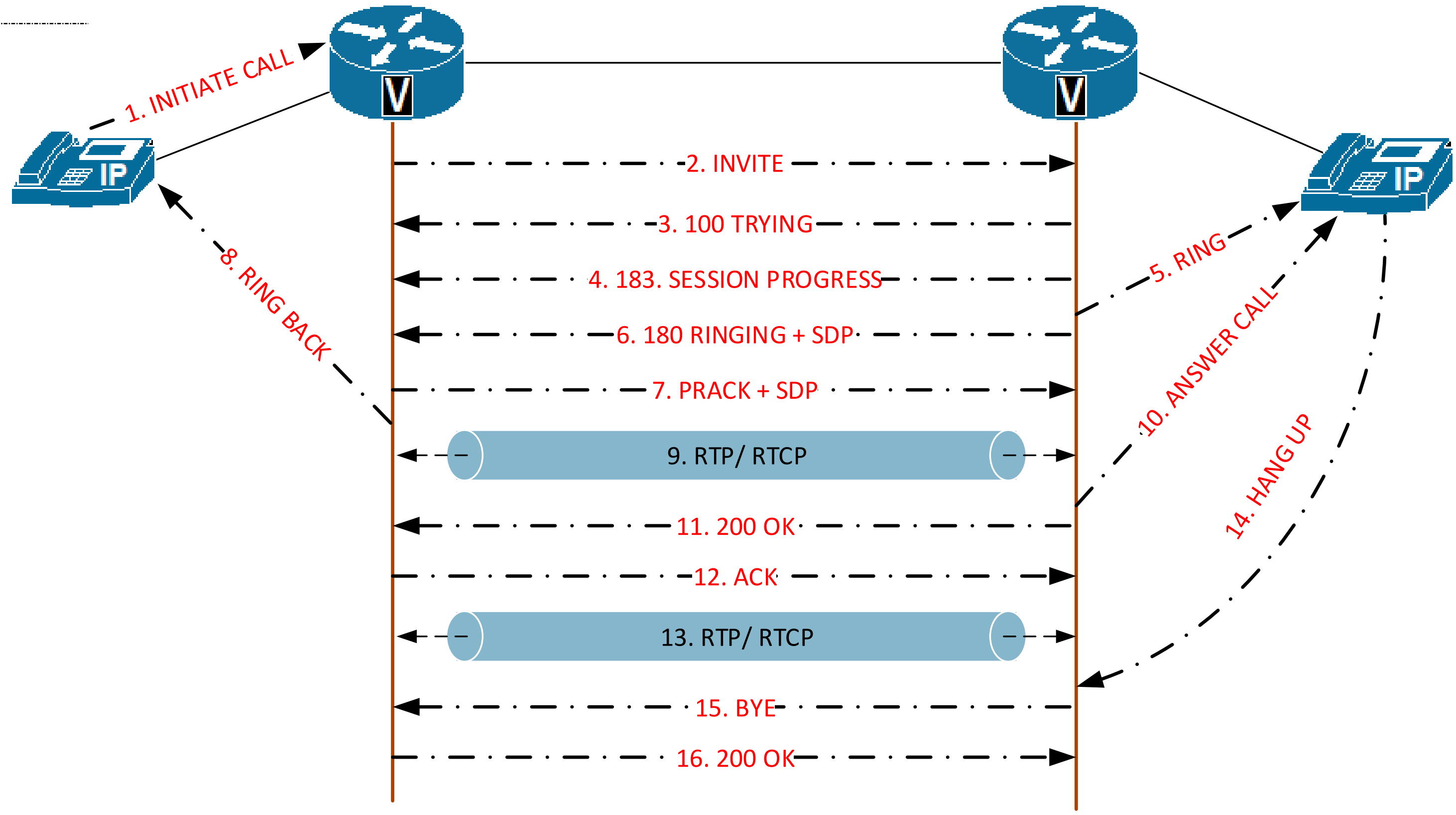
- Based on SDP offer & Answer message
- SIP INVITE message without SDP, The session initiator doesn't sent its capabilities in the initial invite message.
- Calling party wait for destination device to send SDP first along with 200 OK message.
- After getting destination SDP, UAC sends its SDP together with 200 OK ACK message
- Delayed offer is recommended method for SIP trunks, because it enables the ITSPs to provide their capabilities first.
- CUCM allows administrator to select delayed offer or early offer.

Early Media SIP Call Flow 183 Session Progress Option

- Early media allows sending of media from the called party or application to the caller, even before the call is connected. (IVR, Caller Tone, etc.)
- Cisco gateways support Early Media for both Early Offer and Delayed Offer calls



Early Media SIP Call Flow 180 Ringing Option



SIP Configurations

- SIP trunk is basically of two types; Registered and peer to peer.
- Mostly we need registered SIP trunk while interfacing with ITSP which forces SIP registration (configure sip-ua).
- Peer to Peer trunks are which can work without SIP registration

Peer to peer SIP Trunk (VoIP Dial-Peer that selects SIP protocol)

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern 100.
Router(config-dial-peer)#session target ipv4:192.168.1.2         {Next Hop IP}
Router(config-dial-peer)#session protocol sipv2
```

[Note: protocol sipv2 enables dial-peer to use SIPV2 as the signaling protocol. Default protocol is H.323]

SIP Trunk with Registrar & Proxy Server (SIP User Agent (UA) Configuration)

- All the user agents sent Registration request to Registrar server (registrar 142.100.64.11)
- There will be a central point of contact to the Proxy server (sip-server ipv4:142.100.64.11).
- Server- Client mode of operation
- Registrar server acts as a central phone book

```
Router(config)#sip-ua
Router(config-sip-ua)#registrar ipv4:142.100.64.11
Router(config-sip-ua)#sip-server ipv4:142.100.64.11
Router(config-sip-ua)#authentication username user password 1234

Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern 100.
Router(config-dial-peer)#session target sip-server
Router(config-dial-peer)#session protocol sipv2
```

[Note: Authentication command is optional it provide security]

SIPS (SIP Secure) & SRTP (Secure RTP)

SIP offers two methods to secure voice communication SIPS & SRTP

SIPS- SIP Secure: Offers signaling authentication & encryption using Transport Layer Security (TLS) protocol.

SIPS Configuration in Globally

```
Router(config)#voice service voip
Router(conf-voi-serv)#sip
Router(conf-voi-serv)#url sips
```

SIPS Configuration in dial-peer

```
Router(config)#dial-peer voice 1 voip
Router(conf-dialpeer)#voice-class sip url sips
```

[Note: dial-peer settings overwrites global settings]

SRTP: Media stream encrypted between two SIP end points. Typically SRTP is used in combination with SIPS.

SRTP Configuration in Globally

```
Router(config)#voice service voip
Router(conf-voi-serv)#securertp
Router(conf-voi-serv)#securertp fallback
```

SRTP Configuration in dial-peer

```
Router(config)#dial-peer voice 1 voip
Router(conf-dialpeer)#voice-class sip
Router(conf-dialpeer)#securertp
Router(conf-dialpeer)#securertp fallback
```

[Note: dial-peer settings overwrites global settings]

SIP Transport Protocol

Outbound Signaling Transport: Protocol for outgoing SIP messages. Default is UDP. We can configure globally as well as under dial-peer

Transport Configuration in Globally

```
Router(config)#voice service voip
Router(config-voi-serv)#sip
Router(conf-voi-serv)#session transport ?
                              system: selects what is configured in dial-peer
                              tcp tls: Uses TCP for SIP messages
                              udp: Uses UDP for SIP messages
```

Transport Configuration in dial-peer

```
Router(config)#dial-peer voice 1 voip
Router(conf-dialpeer)#session transport udp
```

Inbound Signaling Transport: It specifies transport method accepted for receiving inbound calls. It is configured under sip-ua mode. Default will accept all.

```
Router(config)#sip ua
Router(config-sip-ua)#transport ?
                                tcp  Enable SIP User Agent in TCP Mode
                                udp  Enable SIP User Agent in UDP Mode
```

SIP Source IP Address

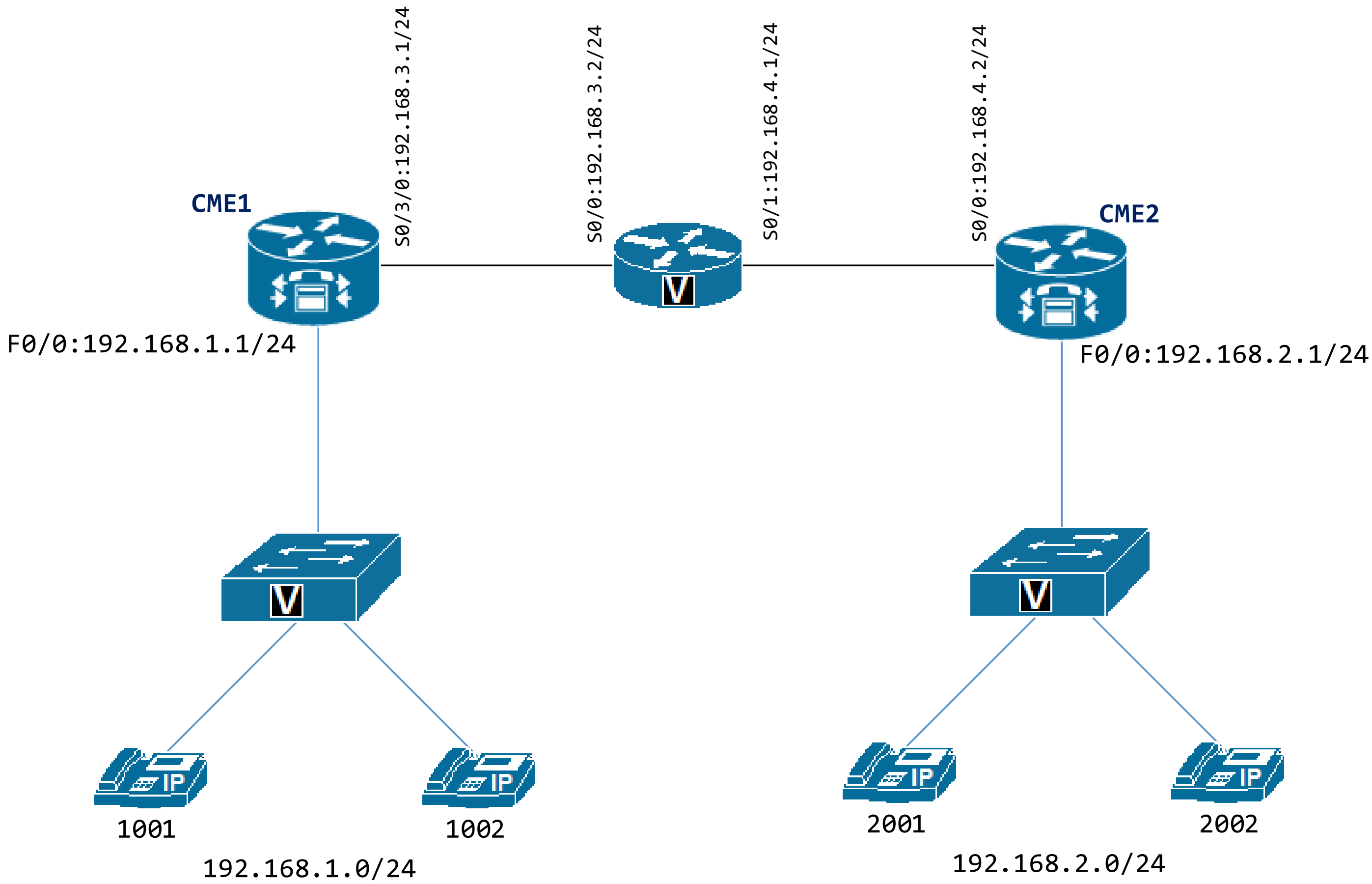
Interface binding feature sets the IP address for outgoing SIP-related traffic.

```
Router(config)#voice service voip
Router(conf-serv-sip)#bind ?
                                 all      bind both SIP control and media packets
                                 control  bind only SIP control packets
                                 media    bind only SIP media packets
Router(conf-serv-sip)#bind all source-interface fastEthernet 0/0
```

SIP Trunk Configuration Labs

SIP trunk usually configured between a VoIP network & ITSP

1. CME to CME SIP Peer to Peer Configuration



Step 1: Configure EIGRP between routers (Cisco R&S)

Step 2: Configure CME1 (CVOICE)

Step 3: Configure CME2 (CVOICE)

Step 4: SIP Peer to Peer Trunk in CME1

```
CME1(config)#dial-peer voice 1 voip
CME1(config-dial-peer)#destination-pattern 200.
CME1(config-dial-peer)#session target ipv4:192.168.4.2
CME1(config-dial-peer)#session protocol sipv2
```

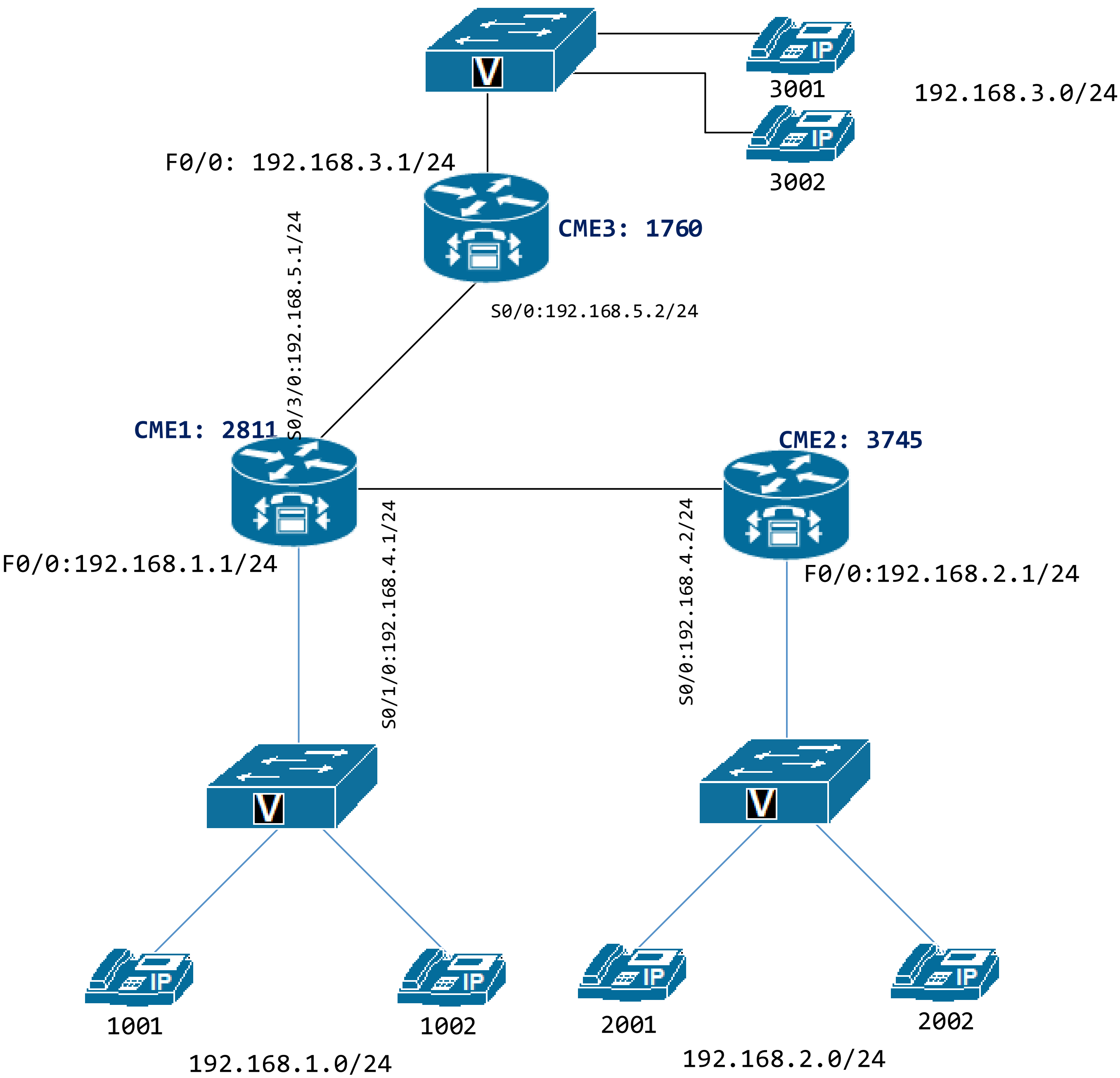
Step 5: SIP Peer to Peer Trunk in CME2

```
CME2(config)#dial-peer voice 1 voip
CME2(config-dial-peer)#destination-pattern 100.
```

CME2(config-dial-peer)#session target ipv4:192.168.3.1

CME2(config-dial-peer)#session protocol sipv2

2. Three CME based UAS Configuration



Step 1: Configure 3 CME (CCNA VOICE)

Step 2: Enable EIGRP Routing (CCNA R&S)

Step 3: Central CME Dial-Peers

CME1(config)#dial-peer voice 1 voip

CME1(config-dial-peer)#destination-pattern 200.

CME1(config-dial-peer)#session target ipv4:192.168.4.2

CME1(config-dial-peer)#session protocol sipv2

```
CME1(config)#dial-peer voice 2 voip
CME1(config-dial-peer)#destination-pattern 300.
CME1(config-dial-peer)#session target ipv4:192.168.5.2
CME1(config-dial-peer)#session protocol sipv2
```

SIP User Agent Config in CME2

```
CME2(config)#sip-ua
CME2(config-sip-ua)#registrar ipv4:192.168.1.1
CME2(config-sip-ua)#sip-server ipv4:192.168.1.1
CME2(config-sip-ua)#authentication username user password 1234
```

Dial-Peer to Central CME from CME2

```
CME2(config)#dial-peer voice 1 voip
CME2(config-dial-peer)destination-pattern [13]00.
CME2(config-dial-peer)session protocol sipv2
CME2(config-dial-peer)session target ipv4:192.168.4.1
```

SIP User Agent Config in CME3

```
CME3(config)#sip-ua
CME3(config-sip-ua)#registrar ipv4:192.168.5.1
CME3(config-sip-ua)#sip-server ipv4:192.168.5.1
CME3(config-sip-ua)#authentication username user password 1234
```

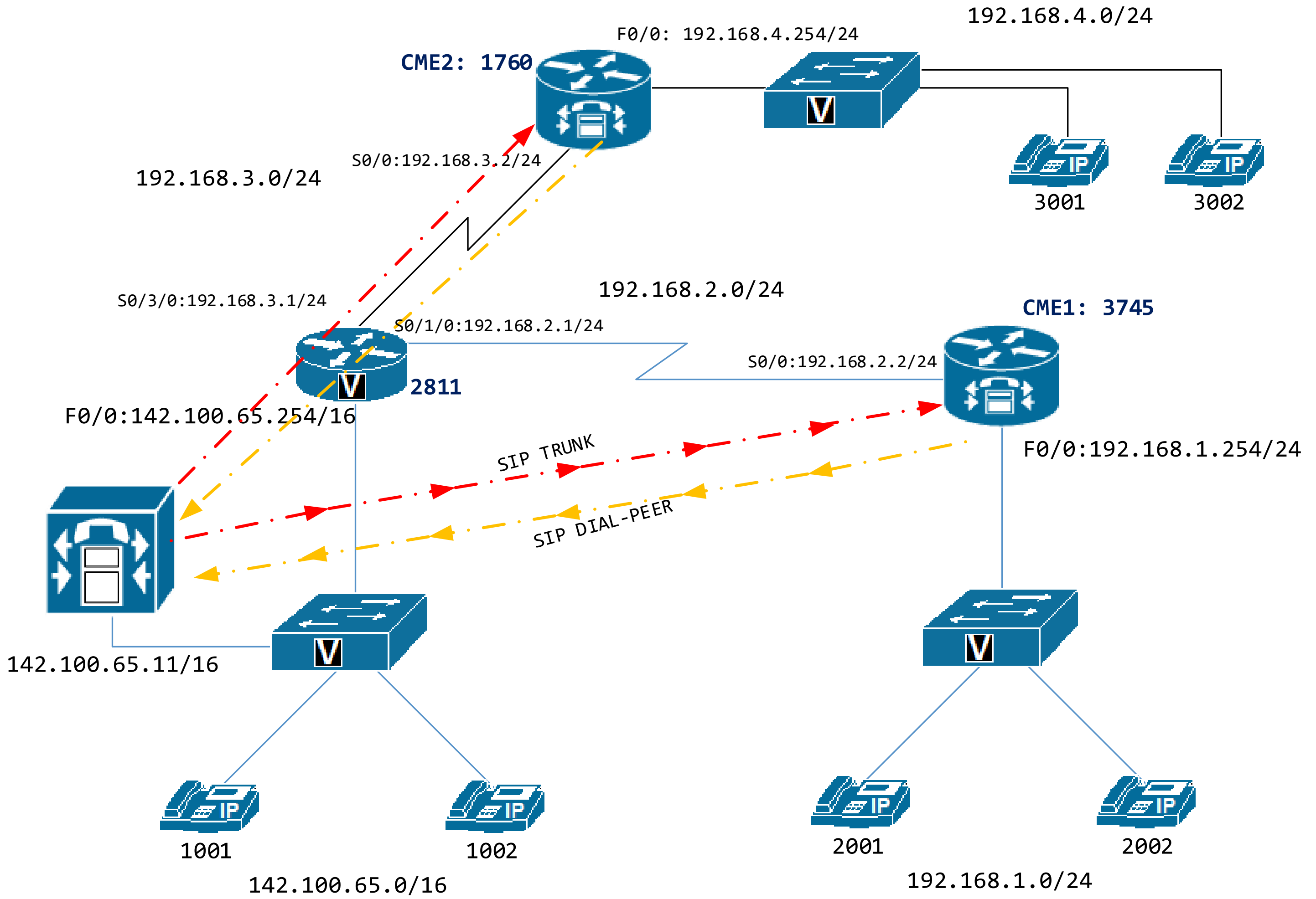
Dial-Peer to Central CME from CME3

```
CME3(config)#dial-peer voice 1 voip
CME3(config-dial-peer)destination-pattern [12]00.
CME3(config-dial-peer)session protocol sipv2
CME3(config-dial-peer)session target ipv4:192.168.5.1
```

Cube Command in Central CME1

```
CME1(config)#voice service voip
CME1(conf-voi-serv)#allow-connections sip to sip
```

3. CUCM to CME SIP Configuration



Step 1: Register IP Phones in CUCM (CCNA VOICE)

Step 2: Enable Routing EIGRP (CCNA R&S)

Step 3: Configure CME1 (CVOICE)

Step 4: Configure CME2 (CVOICE)

Step 5: CUCM to CME1 SIP Trunk

Device → Trunk →

Trunk Type* : SIP Trunk

Device Protocol* : SIP

→ Next

Device Name* : SIP_TRUNK_TO_ CME1

Description : SIP_TRUNK_TO_ CME1

Device Pool* : Default

Check Run On All Active Unified CM Nodes [For redundancy]

SIP Information

Destination Address : 192.168.2.2

SIP Trunk Security Profile* : Non Secure SIP Trunk Profile

SIP Profile* : Standard SIP Profile

→ Save

Route Pattern to Call CME1 (Outside Number)

Call Routing → Route/Hunt → Route Pattern → Add new

Route Pattern : 200X <CME1_PATTERN>

Description : SIP_TRUNK_CALL_TO_CME1

Gateway/Route list* : SIP_TRUNK_TO_ CME1 [--------↓]

→ Save

Step 6: CUCM to CME2 SIP Trunk

Device → Trunk →

Trunk Type* : SIP Trunk

Device Protocol* : SIP

→ Next

Device Name* : SIP_TRUNK_TO_CME2

Description : SIP_TRUNK_TO_CME2

Device Pool* : Default

SIP Information

Destination Address : 192.168.3.2

SIP Trunk Security Profile* : Non Secure SIP Trunk Profile

SIP Profile* : Standard SIP Profile

→ Save

Route Pattern to Call CME2 (Outside Number)

Call Routing → Route/Hunt → Route Pattern → Add new

Route Pattern : 300X <CME2_PATTERN>

Description : SIP_TRUNK_CALL_TO_CME2

Gateway/Route list* : SIP_TRUNK_TO_CME2 [--------↓]

→ Save

Step 7: SIP User Agent Configuration in CME1

```
CME1(config)#sip-ua
CME1(config-sip-ua)#registrar ipv4:142.100.64.11
CME1(config-sip-ua)#sip-server ipv4:142.100.64.11
CME1(config-sip-ua)#authentication username user password 1234
```

Step 8: SIP DIAL-PEER Configuration in CME1

```
CME1(config)#dial-peer voice 1 voip
CME1(config-dial-peer)#destination-pattern [13]00.
CME1(config-dial-peer)#session target sip-server
CME1(config-dial-peer)#session protocol sipv2
```

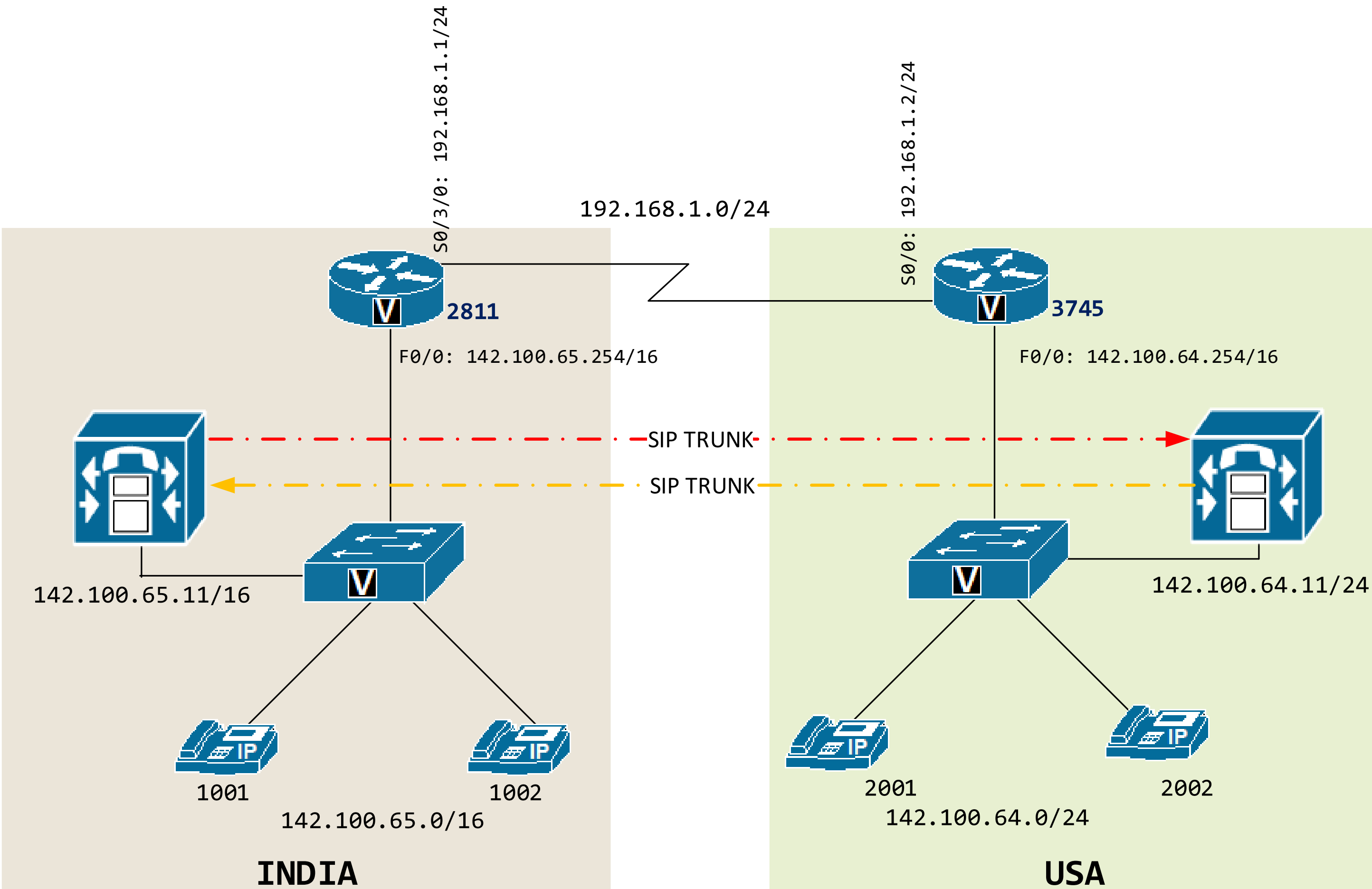
Step 9: SIP User Agent Configuration in CME2

```
CME2(config)#sip-ua
CME2(config-sip-ua)#registrar ipv4:142.100.64.11
CME2(config-sip-ua)#sip-server ipv4:142.100.64.11
CME2(config-sip-ua)#authentication username user password 1234
```

Step 10: SIP DIAL-PEER Configuration in CME2

```
CME2(config)#dial-peer voice 1 voip
CME2(config-dial-peer)#destination-pattern [12]00.
CME2(config-dial-peer)#session target sip-server
CME2(config-dial-peer)#session protocol sipv2
```

4. CUCM to CUCM SIP



Step 1: Configure INDIA CUCM

Step 2: Configure USA CUCM

Step 3: Enable Routing in Both Routers (EIGRP)

Step 4: INDIA to US SIP Trunk

Device → Trunk →

Trunk Type* : SIP Trunk

Device Protocol* : SIP

→ Next

Device Name* : SIP_TRUNK_TO_US

Description : SIP_TRUNK_TO_US

Device Pool* : Default

Check Run On All Active Unified CM Nodes [For redundancy]

SIP Information

Destination Address : 142.100.64.11

SIP Trunk Security Profile* : Non Secure SIP Trunk Profile

SIP Profile* : Standard SIP Profile

→ Save

Route Pattern to Call CME1 (Outside Number)

Call Routing → Route/Hunt → Route Pattern → Add new

Route Pattern : 200X <US_PATTERN>

Description : SIP_TRUNK_CALL_TO_US

Gateway/Route list* : SIP_TRUNK_TO_US [--------↓]

→ Save

Step 5: US to INDIA SIP Trunk

Device → Trunk →

Trunk Type* : SIP Trunk

Device Protocol* : SIP

→ Next

Device Name* : SIP_TRUNK_TO_INDIA

Description : SIP_TRUNK_TO_INDIA

Device Pool* : Default

Check Run On All Active Unified CM Nodes [For redundancy]

SIP Information

Destination Address : 142.100.65.11

SIP Trunk Security Profile* : Non Secure SIP Trunk Profile

SIP Profile* : Standard SIP Profile

→ Save

Route Pattern to Call CME2 (Outside Number)

Call Routing → Route/Hunt → Route Pattern → Add new

Route Pattern : 100X <INDIA_PATTERN>

Description : SIP_TRUNK_CALL_TO_INDIA

Gateway/Route list* : SIP_TRUNK_TO_CINDIA [--------↓]

→ Save

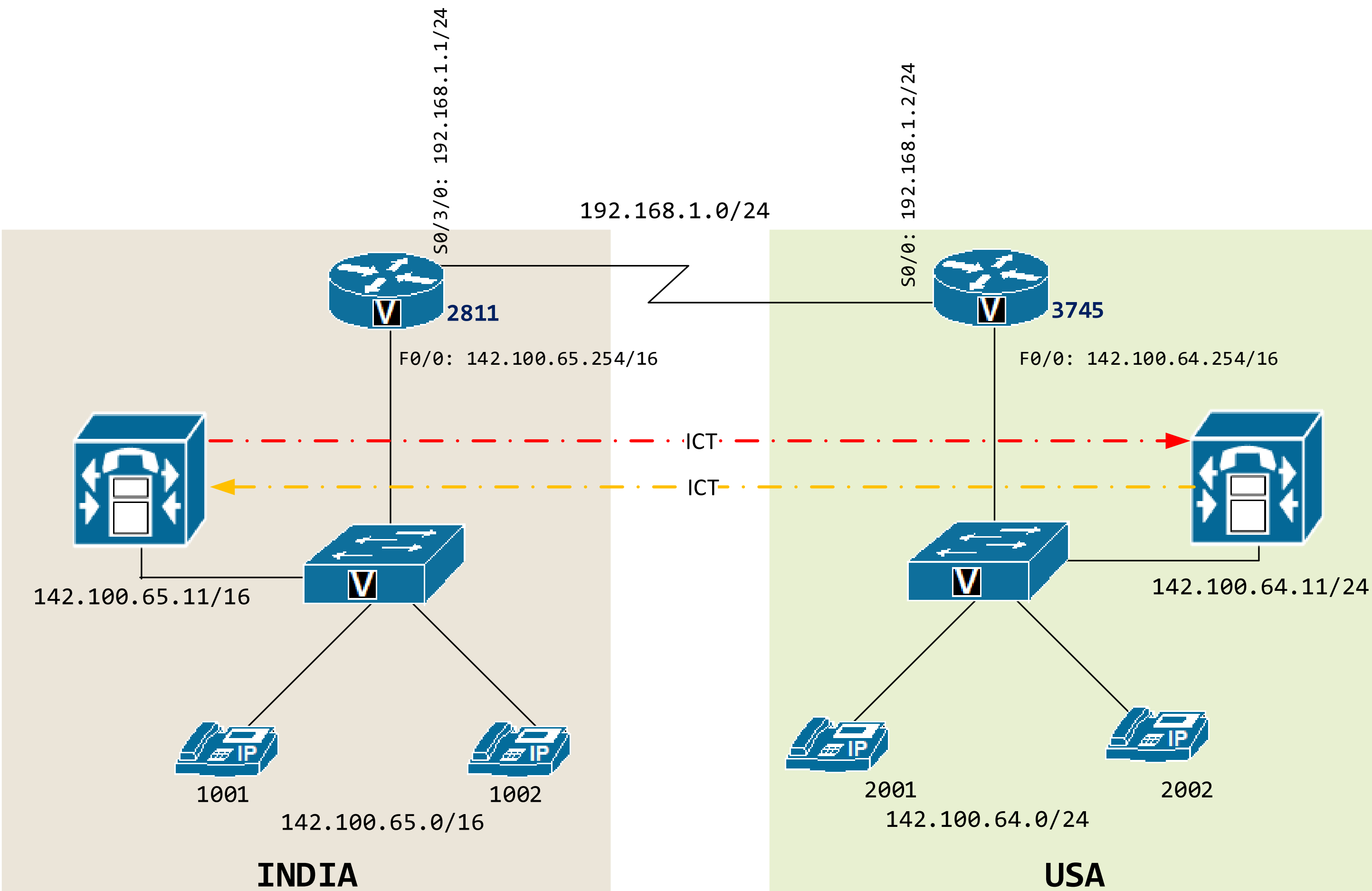
SIP Verification & Troubleshooting Commands

```
Router#show sip-ua service
Router#show sip-ua status
Router#show sip-ua registrar status
Router#show sip-ua timers
Router#show sip-ua connections
Router#show sip-ua calls
Router#show sip-ua statistics

Router#debug ccsip messages
Router#debug ccsip calls
Router#debug ccsip error
Router#debug ccsip events
Router#debug ccsip info
Router#debug ccsip states
```

ICT (Inter Cluster Trunk)

- Inter Cluster Trunk uses logical end to end connection to interconnect multiple CUCM clusters each other.
- ICT is a Cisco Proprietary method to integrate two CUCM clusters.



Step 1: Configure INDIA CUCM

Step 2: Configure USA CUCM

Step 3: Enable Routing in Both Routers (EIGRP)

Step 4: INDIA to US ICT

Device → Trunk → Add New

Trunk Type* : Inter-Cluster Trunk (Non-Gatekeeper Controlled)

Device Protocol*: Inter-Cluster Trunk

→ Next

Device Name* : ICT_TO_US_Cluster

Description : ICT to US Cluster

Device Pool*   : Default

Check Run On All Active Unified CM Nodes [For redundancy]

Remote Cisco Unified Communications Manager Information

Server 1 IP Address/Host Name*   : 142.100.64.11 <US SUB 1 IP>

Server 2 IP Address/Host Name*

Server 3 IP Address/Host Name*

→ Save

Call Routing >> Route/ Hunt >> Route Pattern >> Add New

Route Pattern*   : 200X

Gateway/Route List*   : ICT_TO_US_Cluster

→ Save

<u>Step 4: US to INDIA ICT</u>

Device >> Trunk >> Add New

Trunk Type*   : Inter-Cluster Trunk (Non-Gatekeeper Controlled)

Device Protocol*: Inter-Cluster Trunk

>> Next

Device Name*   : ICT_TO_INDIAN_Cluster

Description   : ICT to US Cluster

Device Pool*   : Default

Remote Cisco Unified Communications Manager Information

Server 1 IP Address/Host Name*   : 142.100.65.11 <INDIA SUB 1 IP>

Server 2 IP Address/Host Name*

Server 3 IP Address/Host Name*

Call Routing >> Route/ Hunt >> Route Pattern >> Add New

Route Pattern*   : 100X

Gateway/Route List*   : ICT_TO_INDIAN_Cluster

→ Save

Call Routing or Dial Plan Components

- Dial-plans are the core of Cisco Unified Communication System. It defines how a user can dial an internal or external (PSTN) number from a Unified Network.
- A dial plan is a numbering plan for voice enabled network.
- External dial-plan depends on the country and location.
- Call routing components or dial plan in CUCM includes End point Addressing, Digit Analysis, Path Selection, Digit Manipulation, Calling Privilege, Call Coverage.

Dial Plan Component	Cisco IOS Gateway	CUCM
End Point Addressing	POTS Dial-Peer, ephone-dn	Directory numbers
Call Routing & Path Selection	Dial-peers	Route pattern, Route Group, Route List
Digit Manipulation	Voice Translation Profile, Digit-strip, forward digit, num-exp	Translation Pattern, Route Pattern, Global Transformation Pattern, External Phone number mask, Calling- Called Party transformation
Calling Privileges	COR	Partition & CSS, FAC, CMC
Call Coverage	Dial-peer, Hunt	Line Group, Hunt List, Hunt Pilot

1. End Point Addressing (Internal Numbering Plan)

- Reachability of an internal destination is provided by assigning Directory Number to all the internal end points (IP Phone, Fax machine, analog phones etc.).
- Typically organizations uses 4 digit numbering patter for internal extensions.
- To avoid overlapping numbering plans we may use site codes
- Usually internal extensions never use 0, 8 and 9 starting number
- Mid-large organizations uses 5 digit extensions normally.
- DID (Direct Inward Dialing) is used in many organizations, PSTN provider maps a range of numbers to the organization. (E.g. Customer purchase DID numbers 1

80 551 XX and will be mapped to internal 99 extensions directly using digit manipulation)

- Internal users call each other using 1XX extensions and people outside the company can be able to reach via DID numbers
- Each call routed by CUCM is categorized to two types.

1. ***On-Net Call***: Call routed between devices with in the private VoIP network (between IP Phones in same CUCM cluster, between two CUCM clusters or between two VoIP vendors of same organization in different location)
2. ***Off-net Call***: Calls that are routed to outside of our private voice network (to PSTN) is referred as Off-net Call

E.164 Overview

- E.164 is an ITU-T (International Telecommunication Union) standard, defines the format of PSTN telephone number
- Maximum length is 15 digits & international phone numbers are represented with + prefix. International operator code doesn't required if we are using + prefix
- Cisco IP Phones do not have + sign in the number pad. Dialing an international number from Cisco IP phone requires dialing an access code (9), international code (00 from India, 011 from USA), and country code (966 for KSA, 91 for India) and subscriber number.

[Note: www.howtocallabroad.com]

E.g.1: Calling to Saudi Arabia from India

Local Access Code for External Number	India's International Access Code	Saudi Arabia's Country Code	Subscriber number
9	00	966	348965231

E.g.1: Calling to Saudi Arabia from USA

Local Access Code for External Number	USA's International Access Code	Saudi Arabia's Country Code	Subscriber number
9	011	966	348965231

- Cisco IP phone can able to call PSTN numbers in E.164 format with+ prefix. User cannot dial + prefix manually. But when user receive a missed call with + prefix and he can able make call back using the missed call list in the IP Phone.

- Hence to call outside we need two route pattern (one is XXX XXXX XXXX and other is \+ XXX XXX XXX)

2. Call Routing in CUCM

Call routing from CUCM is based on Call routing table. All the entries are visible in Call Routing → Route Plan Report → ----

Initially CUCM call Routing Data base consist of Directory numbers of IP Phones. We are updating the database with different configuration by adding different patterns and directions.

	Call Routing Component	Description
1	Directory Number	Numbers assigned to endpoints. Used to route call within the Cluster
2	Translation Pattern	Used to translate called party number (dialed number) to a different number
3	Route Pattern	Used to route call to a remote destination (Gateway, PSTN, another CUCM cluster)
4	Hut Pilot	Used for Call Coverage capabilities
5	Call-park, Directed Call Park Numbers	Allows user to temporarily attach a call to a Park Slot number. It is a special kind of holding and call being retrieved back from any IP phone.
6	Meet-me numbers	Allows a conference call that easily accommodate 4 or more parties

1. Directory Number (Already Discussed)

2. Translation Patter (Will be discussed in Digit Manipulation)

3. Route Pattern

- CUCM doesn't know any phone number external to the CUCM. Gateways and Trunks allows CUCM to communicate with other network.
- CUCM always uses Gateway protocol to communicate with Gateway router, but the gateway needs to convert that signal in to traditional or VoIP (CUBE)
- Route patterns are the strings of digits & wildcards configured in CUCM.
- Route Pattern route (point) calls to a prioritized list of Gateways or Trunks.
- Multiple route patterns cannot be pointed directly to same gateway. Inserting Gateway into route group allows the gateway to be used for many route patterns.
- Route Pattern uses various Wildcard parameters

Wildcard	Description

X	Single Digit from 0-9, * and #
!	One or more digit (0-9, * and #) continuously (T.302 Timer)
#	Terminates inter-digit timeout (Go now)
@	North American Numbering Plan. The @ wildcard is a special macro function that expands into a series of patterns representing the entire national numbering plan for a certain Country. A route pattern of 9.@ will load a complex 166-route-pattern North American Numbering Plan (NANP) by default
[X-Y]	Single digit from Range (E.g. [2-6]2801 = 22801, 32801, 42801, 52801, 62801)
[XYZ]	Single Digit from the group (E.g. [176]2801 = 12801, 72801, 62801)
[^X-Y]	Exclude the range (E.g. [^2-6]2801 = 02801, 12801, 72801, 82801, 92801)
.	Terminates access code
<wildcard>?	Match character to the left 0 or more time. 28? = 28, 288, 2888, 2888.....
<wildcard>+	Match character to the left 1 or more time. 28? = 288, 2888, 2888.....
\+	Match + sign as part of E.164 Number

<u>Examples</u>

12XX = 1200 to 1299, 12**, 12*#, 12##, 12#*

13[25-8]6 = 1326, 1356, 1366, 1376, 1386

13[13-59]X = 1310 – 1319, 1330 – 1339, 1340 – 1349, 1350 – 1359, 1390 – 1399, (*,# combinations also)

- @ is not usually used because we cannot perform Class of Service (CoS – Blocking some devices to access particular external number)
- International Destinations are usually configured using ! wildcard, which represents one or more digits.

USA uses 9.011! as international pattern

India uses 9.00! as international pattern

- In ! wildcard, CUCM doesn’t know when the user is done dialing so CUCM waits for 15 sec (default) to analyze the dialed digits. This delay can be reduced by two methods
- Reduce T.302 Timer in System → Service Parameter change this to 4 or 5
- Configure a 9.00!# second route pattern. Here the # serves are termination code for T.302 timer. # normally indicates the system should stop analyzing dialed digits & then route the call.
- The urgent priority check box in the route pattern is force immediate routing of certain call even if an overlapping dial-plan exist.

Example

Route Pattern 1: 9X1987 = 911987, 921987, 931987, 941987, ... , 991987

Route Pattern 2: 911 for emergency call

The user has to wait 15 sec (T.302 time) to process a 911 call. Once he check Urgent priority in Route Pattern 2, the problem will be solved. Or alternatively he can press # to stop T.302 timer

Secondary Dial Tone

- The secondary dial tone is configured by selecting the Provide Outside Dial Tone check box on the Route Pattern or Translation Pattern configuration page.
- While using access code and PreDot discard method we should check outside dial tone to get a second dial tone after dialing 9 indicating that is external PSTN access.
- The secondary dial tone typically indicates a call to the PSTN after the country-specific access code has been dialed.
- The secondary dial tone function can be enabled on route patterns and translation patterns. The dial tone will change only if all possibly matching route or translation patterns have the secondary dial tone enabled.

Example1:

Route pattern: 9.0801234 (secondary dial tone enabled)

Route pattern: 9.4933987 (secondary dial tone enabled)

After a user dials 9, the dial tone will immediately change because both matching route patterns have the secondary dial tone enabled. Or, consider

Example2:

Route pattern: 9.0801234 (secondary dial tone enabled)

Route pattern: 9.4933987 (secondary dial tone disabled)

After a user dials 9, the dial tone does not change because only one matching route pattern has the secondary dial tone enabled. If the user dials next digit as 4 the stutter (disorder) dial tone will be heard because only the route pattern that has the secondary dial tone enabled remains as a possible match.

4. Hut Pilot (Will be discussed in Digit Manipulation)

5. Call-park, Directed Call Park Numbers (Already Discussed in CCNA VOICE)

6. Meet-me numbers (Will be discussed in CIPT2)

Digit Analysis

When overlapping dial-plan exists in the form of route patterns, CUCM performs closest match routing.

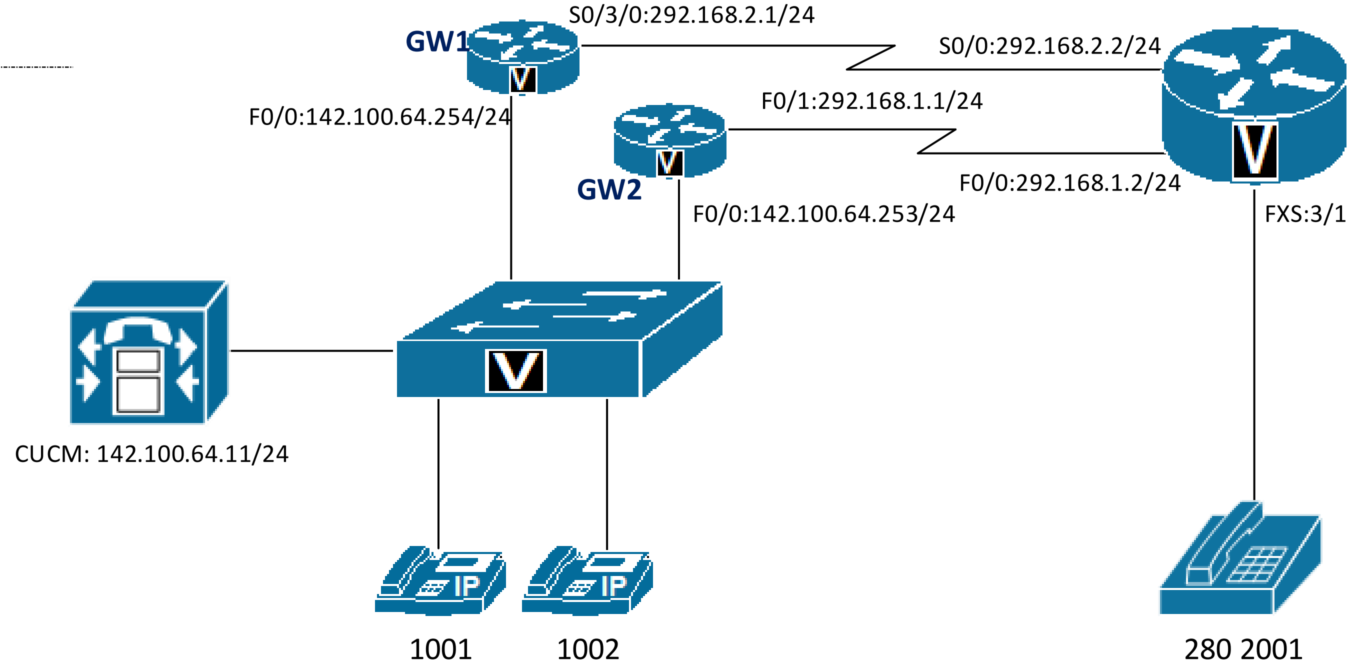
Example:

Route Pattern 1 : 280 200X Points to GW1

Route Pattern 2 : 280 20XX Points to GW2

Dialed Digit : 280 2001

Route pattern 1 will math and the call will routed based on Route pattern 1 always



Use DNA (Dialed Number Analyzer) to verify the match.

Call Classification Settings and Configurations

- ***Call forward settings***: Call forward can be configured differently for internal (On-Net) and external (Off-Net) calls. External calls are normally calls that were routed from a gateway.

(Configure under line page)

Call Forward and Call Pickup Settings

	Voice Mail	Destination	Calling Search Space
Calling Search Space Activation Policy			Use System Default
Forward All	☐ or		< None >
Secondary Calling Search Space for Forward All			< None >
Forward Busy Internal	☐ or		< None >
Forward Busy External	☐ or		< None >
Forward No Answer Internal	☐ or		< None >
Forward No Answer External	☐ or		< None >

- ***Block OffNet To OffNet Transfer***: This Call Manager service parameter toll-fraud prevention feature ensures that the UC infrastructure is not misused by an internal facilitator to connect two external parties.

(Configure System → Service Parameter → Select Server → Call Manager Active)

Clusterwide Parameters (Feature - General)

Call Park Display Timer *	10	10
Caller ID Display Priority Enabled *	True	True
Call Park Reversion Timer *	60	60
Preserve globalCallId for Parked Calls *	True	True
Maximum Call Duration Timer *	720	720
Maximum Hold Duration Timer *	360	360
Party Entrance Tone *	True	True
Message Waiting Lamp Policy *	Primary Line - Light and Prompt	Primary Line - Light and Prompt
Audible Message Waiting Indication Policy *	OFF	OFF
Message Waiting Indicator Inbound Calling Search Space	< None >	
Multiple Tenant MWI Modes *	False	False
MWI Non Message Center Signaling Call Duration *	0	0
Message Waiting Indicator APDU Digit Translation CSS	< None >	
Block OffNet To OffNet Transfer *	True	False

- ***Drop conference when no On-Net party remains***: This toll-fraud prevention feature drops a conference call when only external parties remain in the conference. If the setting is not enabled, an internal facilitator can try to connect two external parties by setting up a conference and then drop out of the call. The entire call would be billed to the company on the CUCM cluster because the conference was initiated by a Cisco IP Phone on the cluster. This service parameter would stop this toll-fraud scenario.

(Configure System → Service Parameter → Select Server → Call Manager Active)

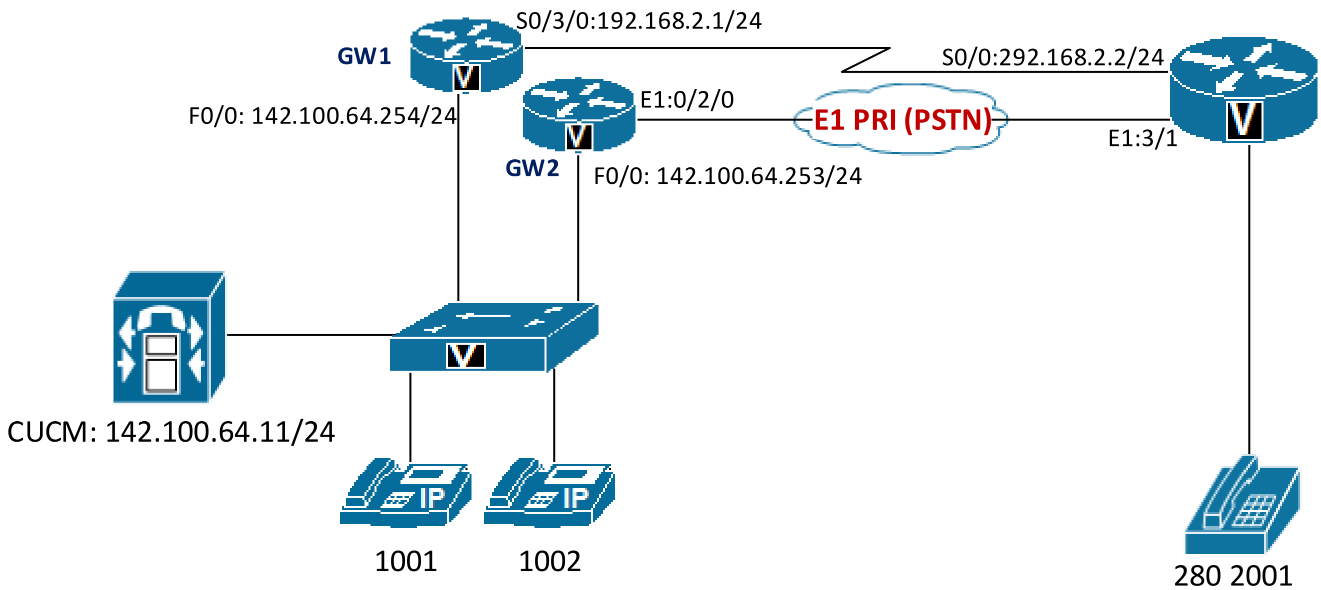
Clusterwide Parameters (Feature - Conference)

Suppress MOH to Conference Bridge *	True	True
Drop Ad Hoc Conference *	When No OnNet Parties Remain in the Conference	Never
Maximum Ad Hoc Conference *	4	4
Maximum MeetMe Conference Unicast *	4	4
Advanced Ad Hoc Conference Enabled *	False	False
Choose Encrypted Audio Conference Instead Of Video Conference *	True	True
Minimum Video Capable Participants To Allocate Video Conference *	2	2
Enable Click-to-Conference for Third-Party Applications *	False	False

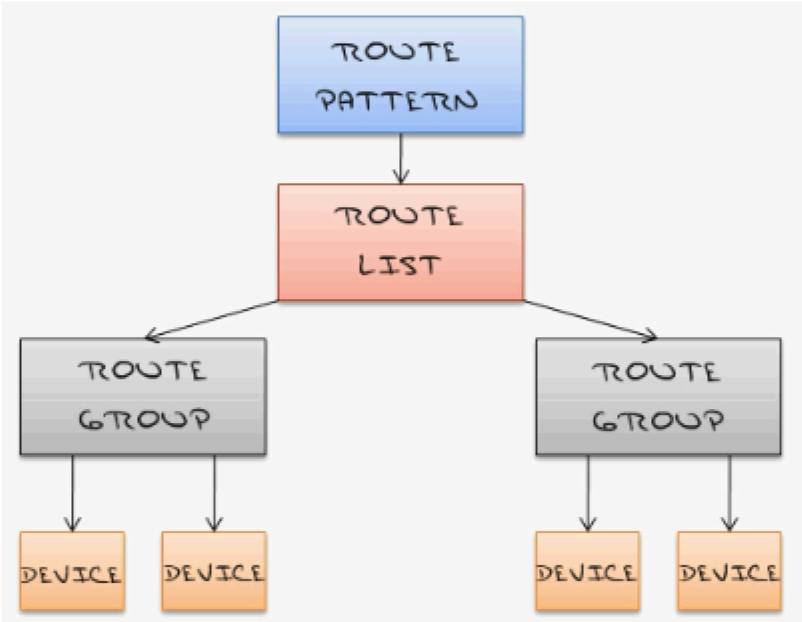
There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

3. Path Selection in CUCM

- Path selection is an essential dial plan element. CUCM selects how and where to route the call after it has matched a pattern in call-routing database (Call Routing → Route Plan Report → All Patterns).
- CUCM allows multiple paths to be configured for a ROUTE PATTERN for high-availability purpose.



- When the WAN goes down, call should be router via PSTN with 280 prefix.
- Once you point a route pattern the device (Gateway/ Trunk) would not be available for any other route pattern.
- Most CUCM administrator never point route pattern directly in to a Gateway or Trunk. Normally route patterns are pointed to a Route List
- Instead the Gateways are arranged in to prioritized group called ***Route Group***.
- These Route Group is again grouped in to ***Route List*** (It is a prioritized list of Route Group). Route List always use top-down processing of route group. (We can perform some digit manipulation under Route list Route Group)
- Route group uses top-down or circular.
- Top-down: 1st call 1st device, 2nd call 2nd device if 1st is busy only
- Circular: 1st call 1st device, 2nd call 2nd device without checking 1st device
- Route list and Route Group provides flexibility for call routing and digit manipulation.

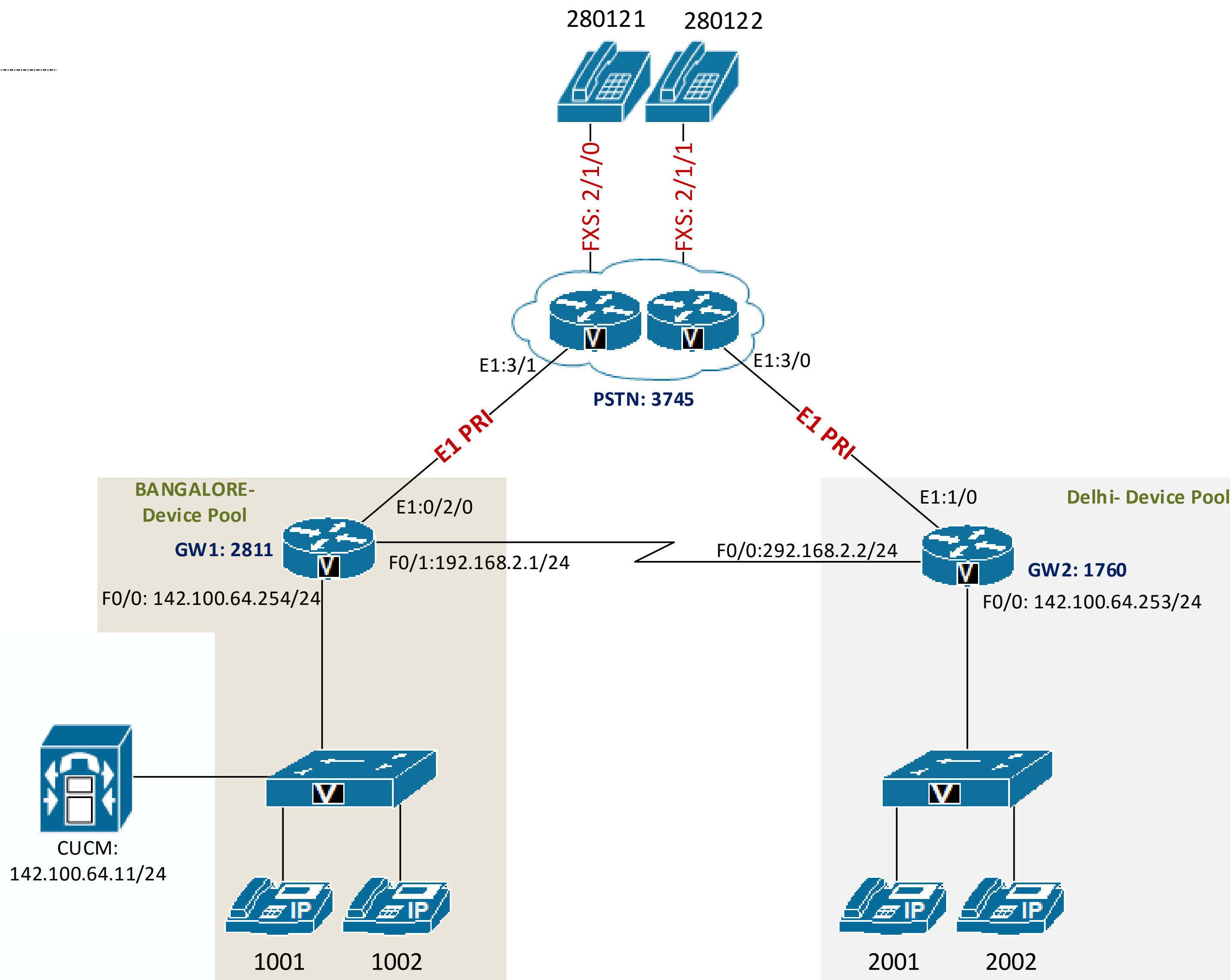


Configuration:

1. Add Gateways or Trunks to CUCM
2. Call Routing → Route/ Hunt → Route Group → Name & Put the devices in prioritized order
3. Call Routing → Route/ Hunt → Route List → Name & Add Route Groups in prioritized order
4. Create route pattern and points to Route List

<u>Local Route Group (LRG):</u>

- LRG reduces the complexity and size of Dial-plan in CUCM. LRG is a device pool parameter and introduced in CUCM 7.
- Standard Local Route Group can be added to Route List
- When a user from INDIA dials 2808001, the call will be routed via GW1 to Indian PSTN. If a user from US device pools dials 2807001, the call will be routed via GW2 to PSTN



- Create two Route Group (BANGALORE Route Group → GW1, DELHI Route Group → GW2)
- Go to BANGALORE Device Pool → Local Route Group → BANGALORE Route Group
- Go to DELHI Device Pool → Local Route Group → DELHI Route Group
- Now go to Call Routing → Route/ Hunt → Route List → Name: Route List → Add Route Group → Standard Local Route Group

4. Calling Privileges (CoS)

- Calling privileges are dial-plan components and used to implement Class of Service (CoS), which restrict calling capabilities. Calling privileges are based on calling device.
- Calling privileges control the available components of call-routing database that are accessible to an endpoint
- Primary application of Calling Privilege is to implement Calls of Service

- CoS can also be used to restrict who can call Manager, Executives, etc.
- Calling Privilege used to implement TEHO
- TEHO allows organizations to save money on PSTN toll charges by routing long distance and international call across the private IP WAN. TEHO is an application of LCR (Least Cost Routing)

Calling privilege options are

Partition & Calling Search Space (CSS):

Time Periods:

Static days or recurring time intervals

Time Schedules:

An ordered list of time periods

Client Matter Codes (CMC):

Tracks calls to certain destination

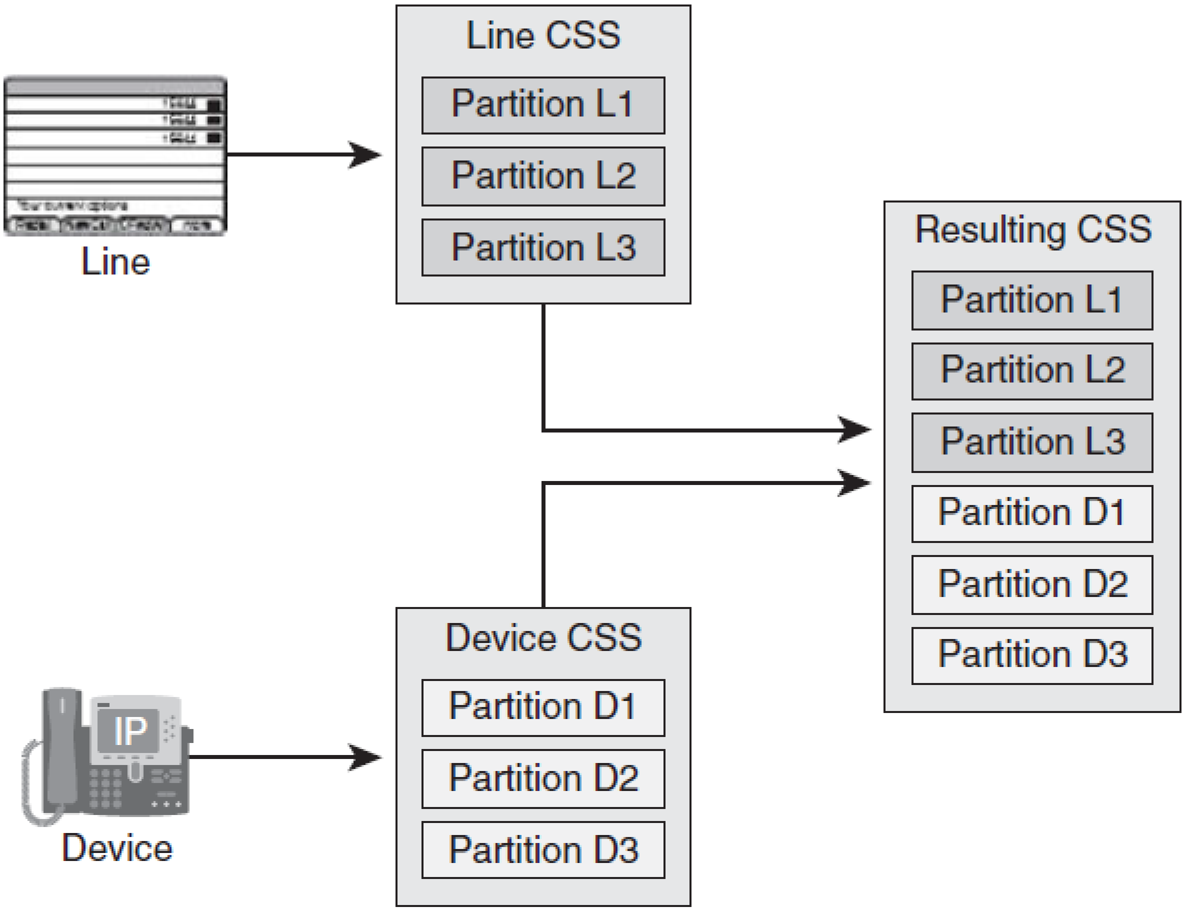
Force Authorization Codes (FAC):

Restrict outgoing calls to certain number

1. Partitions & Calling Search Space (CSS):

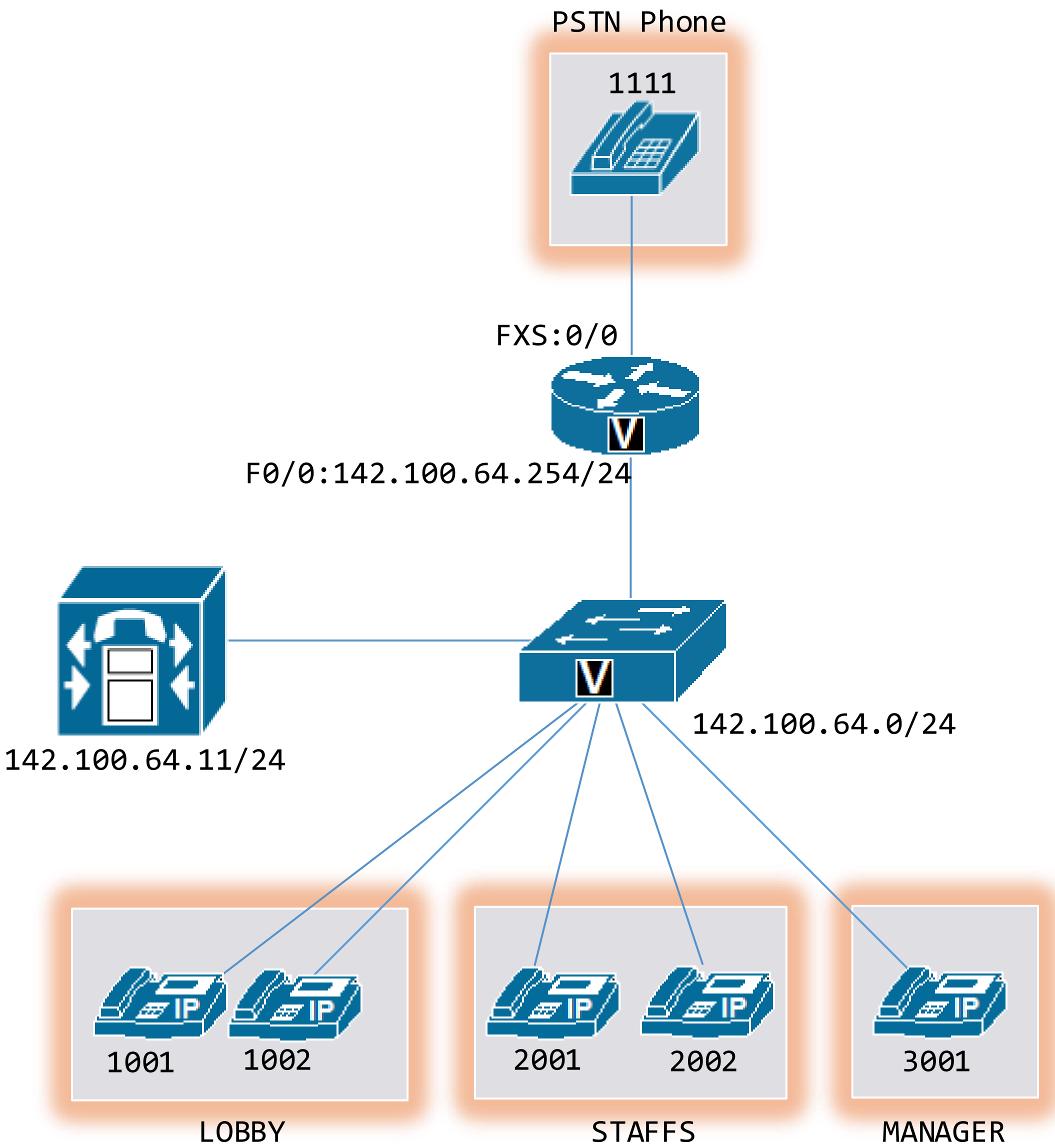
- A partition is a group of dialable pattern with similar reachability (accessibility)
- Partitions are a logical locks. All phone numbers are accessible by all devices by default. After partitions has been applied, a lock has been placed on the phone number restricting who can dial it.
- Every phone number, Route Pattern, Translation Patterns, on CUCM can be applied to a Partition
- All phone numbers are in null partition by default. All devices have access to Null Partition.
- A **CSS** defines which partitions are accessible to a particular device. CSS are assigned to device, Lines, Gateways, Trunks, Voice Mail Ports, etc.
- A CSS is like a key bunch that includes multiple keys (Partitions)
- Restriction is placed by evaluating CSS of Calling party and Partition of called party (CSS is like a Phone book & Partition is Contacts)
- The CSS of calling party must contain the partition of called party

- CSS can be applied in Device page & Line page, in such situation the resulting CSS will be a combination of both with Line CSS has highest priority.



[Note: In CTI port the device CSS has highest priority]

Scenario 1 (Simple)



Conditions

1. LOBBY can call only LOBBY PHONES
2. STAFF can call LOBBY, other STAFF
3. MANAGER can call LOBBY, STAFF, and PSTN

Step 1: Create Partitions

Cisco CM Administration → Call Routing → Class of Control → Partition → Add New

LOBBY_PT

STAFFS_PT

MANAGER_PT

PSTN_PT

→ Save

Step 2: Assign Directory Number, Route patterns to Partition

Device → Phone → Line [1] – 1001 → Route Partition: LOBBY_PT → Save

Device → Phone → Line [1] – 1002 → Route Partition: LOBBY_PT → Save

Device → Phone → Line [1] – 2001 → Route Partition: STAFFS_PT → Save

Device → Phone → Line [1] – 2002 → Route Partition: STAFFS_PT → Save

Device → Phone → Line [1] – 3001 → Route Partition: MANAGER_PT → Save

Call Routing → Route/Hunt → Route Pattern → 1111 → Route Partition → PSTN_PT

Step 3: Create Calling Search Space (CSS)

Cisco CM Administration → Call Routing → Class of Control → Calling Search Space → Add New

Name* : LOBBY_CSS

Selected Partitions : LOBBY_PT

Add New

Name* : STAFF_CSS

Selected Partitions : STAFF_PT
LOBBY_PT

Add New

Name* : MANAGER_CSS

Selected Partitions : MANAGER_PT
STAFF_PT
LOBBY_PT
PSTN_PT

Step 4: Assign CSS to Phones or DN, Route pattern

Device → Phone1 → Calling Search Space: LOBBY_CSS → Save

Device → Phone2 → Calling Search Space: LOBBY_CSS → Save

Device → Phone3 → Calling Search Space: STAFF_CSS → Save

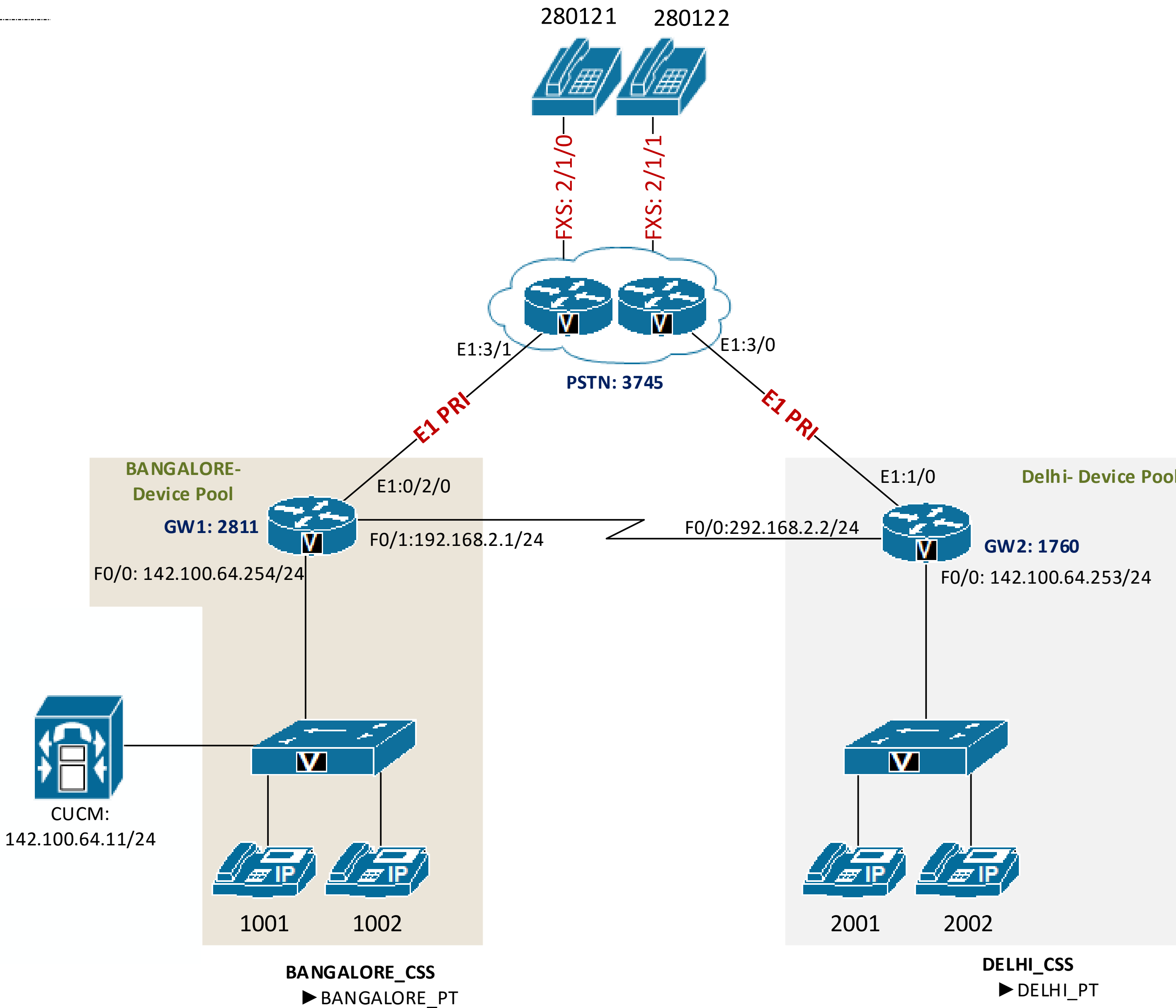
Device → Phone4 → Calling Search Space: STAFF_CSS → Save

Device → Phone5 → Calling Search Space: MANAGER_CSS → Save

Call Routing → Route/Hunt → Route Pattern → 1111 → Calling Search Space: PSTN_CSS

(If we assign under DN too, both will take in to consideration)

Scenario 2 - Gateway Selection Based on CSS- Partition



Step 1: Configure Multisite with Centralized Deployment

Step 2: Configure GW1 & GW2 (E1 PRI & Dial-peers)

Step 3: Add GW1 & GW2 to CUCM

Step 4: Create Partition BANGALORE_PT and DELHI_PT

Step 5: Create BANGALORE_PHONE_CSS with BANGALORE_PT and DELHI_PHONE_CSS with DELHI_PT

Step 6: 1001, 1002 in BANGALORE_PT and BANGALORE_PHONE_CSS, DELHI_PHONE_CSS

Step 7: 2001, 2002 in DELHI_PT and DELHI_PHONE_CSS, BANGALORE_PHONE_CSS

Step 6: Crete route Pattern 28012X with BANGALORE_PT with GW1_CSS and Point GW1

Step 7: Crete route Pattern 28012X with DELHI_PT with GW2_CSS and Point GW2

PLAR Using CSS & Partition

Call Routing → Class of Control → Partition → Add New → PLAR_PT → Save

Call Routing → Class of Control → Calling Search Space → PLAR_CSS → Save

Call Routing → Translation Pattern → Add New →

Translation Pattern :

Partition : PLAR_PT

Called Party Transform Mask : 1000 <Destination Number>

Apply PLAR_CSS to phones

[Use PLAR_CSS as Calling Search Space for Auto-registration under Device Pool. When Auto registered phones off-hook, call will go to Admin]

2. Time of Day Call Routing

- It gives you the ability to your phone system to route calls differently based on time of day.
- Different SIP trunk provides PSTN Day, PSTN Night (Low charge).
- Route calls based on time
- After working hours (8AM to 5PM) route call to Voice Mail
- Time of Day Call Routing based on Partitions &n CSS
- It is configured by applying time period & time schedule to partitions.
- A time schedule consist of one or more time periods
- Time period defines the time ranges or static dates
- The logic behind time of day call routing is that a Partition will be available in a specified time only.

Configurations

Step 0: INTERNAL PARTIOTNS & INTERNAL CSS

Assign all the internal numbers to INTERNAL_PARTION. Put the INTERNAL_PARTION to INTERNAL_CSS and apply to the phones

Step 1: Create Time Periods

Call Routing → Class of Control → Time Period → Add New →

Name* : AFTER_HOURS_TIME_PERIOD_[5PM-12AM]

Time of Day Start* : 17:00 <05PM>

Time of Day End* : 24:00 <12AM>

Repeat Every Week from : Mon through Fri

→ Save

Add New →

Name* : AFTER_HOURS_TIME_PERIOD_[12AM-8AM]

Time of Day Start* : 00:00 <12AM>

Time of Day End* : 08:00 <08AM>

Repeat Every Week from : Mon through Fri

Step 2: Create Time Schedule

Call Routing → Class of Control → Time Schedule → Add New

Name* : AFTER_HOUR_TIME_SCHEDULE

Available Time Periods ↓↓↓

Selected Time Periods

AFTER_HOURS_TIME_PERIOD_[5PM-12AM]

AFTER_HOURS_TIME_PERIOD_[12AM-8AM]

→ Save

Step 3: Create Partition

Call Routing → Class of Control → Partition → Add New

Name* : AFTER_HOURS_PARTITION

Step 4: Assign Time Schedule to a Partition

The partition should be available at specified time schedule only

Call Routing → Class of Control → Partition → Find

Select : AFTER_HOURS_PARTITION

Name* : AFTER_HOURS_PARTITION

Time Schedule* : AFTER_HOUR_TIME_SCHEDULE

Time Zone : ☼ Originating Device

◙ Specific Time Zone ↓↓↓

→ Save

Step 5: Assign the 'AFTER HOURS PARTITION' in Calling Party CSS

To manage external call routing, create a Translation pattern with same DNIS and provide Calling Party Transformation Mask.

Call Routing → Translation Pattern → Add New →

Translation Pattern : 1000

Partition : AFTER_HOURS_PARTITION

Called Party Transformation Mask: Other number to Route Call

Call Routing → Class of Control → Calling Search Space → Add New →

Name* : INCOMING_CALL_CSS

Available Partition ↓↓↓

Selected Partitions

AFTER_HOURS_PARTITION

INTERNAL_PARTITION

Go to Device → Gateway → Select Gateway →

Call Routing Information – Inbound Calls

Calling Search Space : INCOMING_CALL_CSS

3. CMC (Client Matter Code)

- Allows you to maintain your accounting correctly (Who is calling long distance, who is calling international).
- Used for department billing
- CMC detail is added to CDR to allow accounting and billing of calls based on CMC used after dialing the telephone number

Call Routing → Client Matter Code → Add New

Client Matter Code* : 1111

Description : CMC for Accounting Department

Call Routing → Route Pattern → Select Pattern

Check Require Client Matter Code.

[Note: After CMC user should press '#', otherwise 15Sec wait]

4. FAC (Forced Authorization Code)

- Way of restricting who is able to call specific numbers by assigning certain number to certain group or people.

- While trying to call, the user get a second beep for entering code
- FAC level of the code must be equal or greater than the Authorization level configured in Route Pattern
- FAC is also recorded in CDR

Call Routing → Force Authorization Code → Add New

Authorization Code Name* : EMERGENCY_LEVEL

Authorization Code* : 2222

Authorization Level : 10

Call Routing → Route Pattern → Select Pattern

Check Require Force Authorization Code

Authorization Level : 5

[FACs having 5 or more Authorization Level can be able to dial the particular pattern. Note: After FAC user should press '#', otherwise 15Sec wait]

5. Digit Manipulation.

- Digit manipulation is often used to change Calling Party number for Caller ID purposes on outgoing PSTN calls. Converting 4 digit internal extension to E.164 format.
- Digit manipulation is also used to strip PSTN access codes (9, 8, or 0) before CUCM route the call to Gateway.
- Inbound calls from PSTN can be received with many number of digits (10, 12 etc.) of called party length, but internal dial plan of CUCM follows 4 or 5 digit extensions. Digit manipulation used to route the external call to internal extensions.

Following are the Digit Manipulations in CUCM

1. External Phone Number Mask

- The external phone number mask is a DN configuration attribute. It is responsible for changing the internal 4 digit extension to full length PSTN number.
- External Phone Number Mask is configured in DN configuration page (Line Page)
- External Phone Number Mask is also used in Route List level to change the caller ID while a call routed via a particular Route List.
- Route Pattern, Translation Pattern, Calling Party Transformation Pattern, Hunt Pilot also uses External Phone Number Mask
- Automated Alternate Routing (AAR) uses External Phone Number Mask to change caller ID while routing calls via PSTN

External Phone Number Mask at first DN used for the following function,

1. Change the display of main phone number at the top IP Phone's LCD screen. Then the user can instantly identify PSTN DID number of his phone by viewing the LCD screen.

E.g. DN = 1001, External Phone Number Mask = 08012**XXXX**

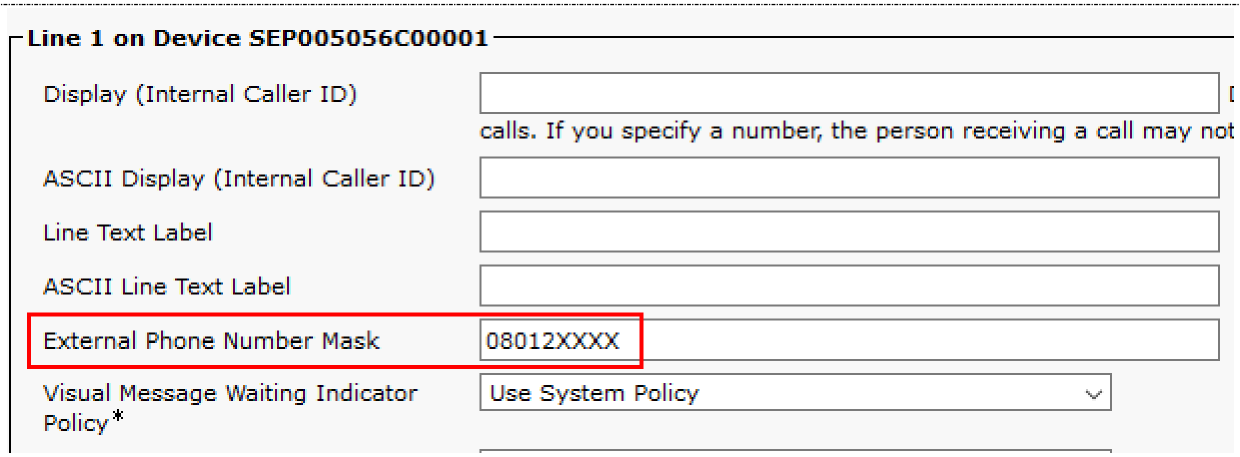
Then the display will be 08012**1001**

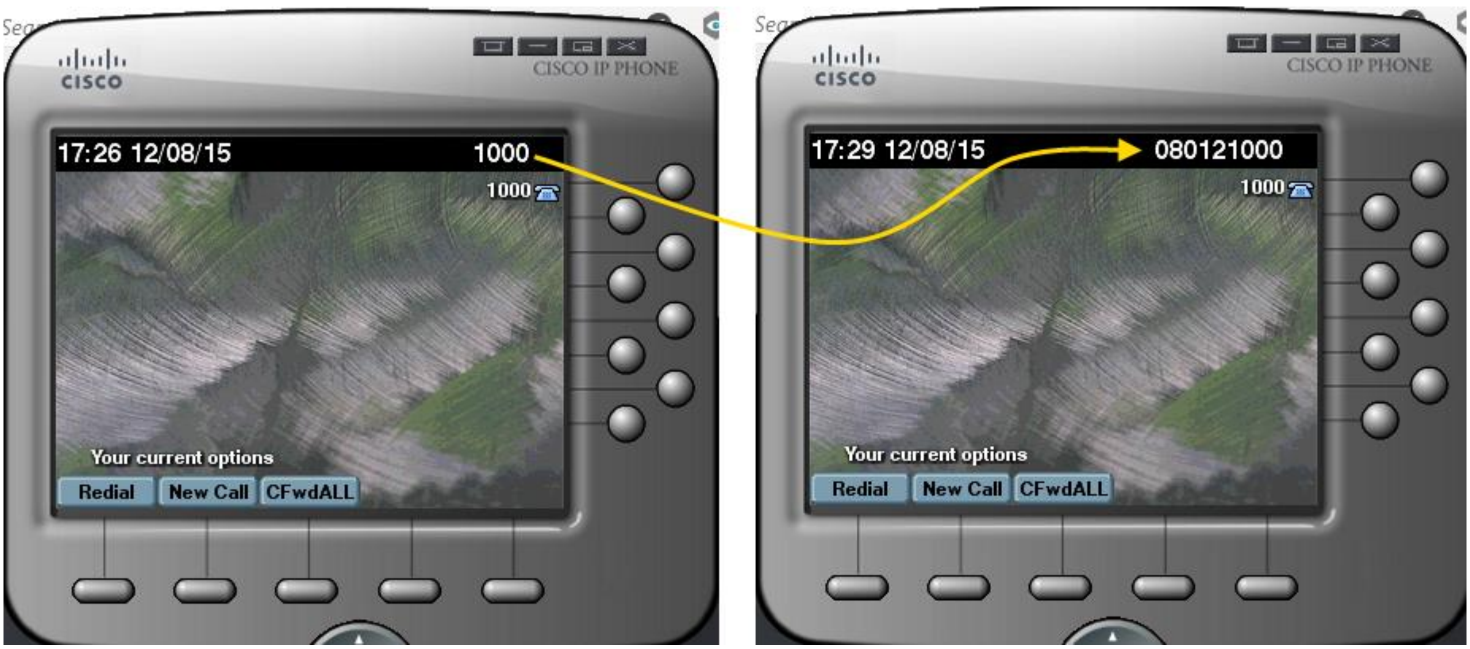
2. AAR uses External Phone Number Mask for rerouting calls via PSTN
3. Change caller ID for off-net calls (PSTN Calls)

Configuration

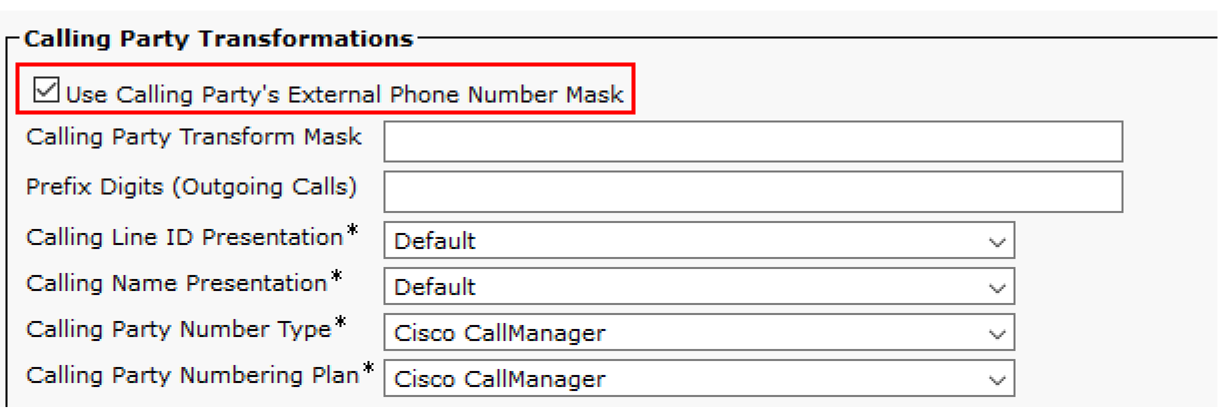
Device → Phone → Line[1] →

External Phone Number Mask: 08012XXXX





In the calling Party Transformation section under translation pattern also includes check box for External Phone Number Mask to change caller ID for PSTN calls



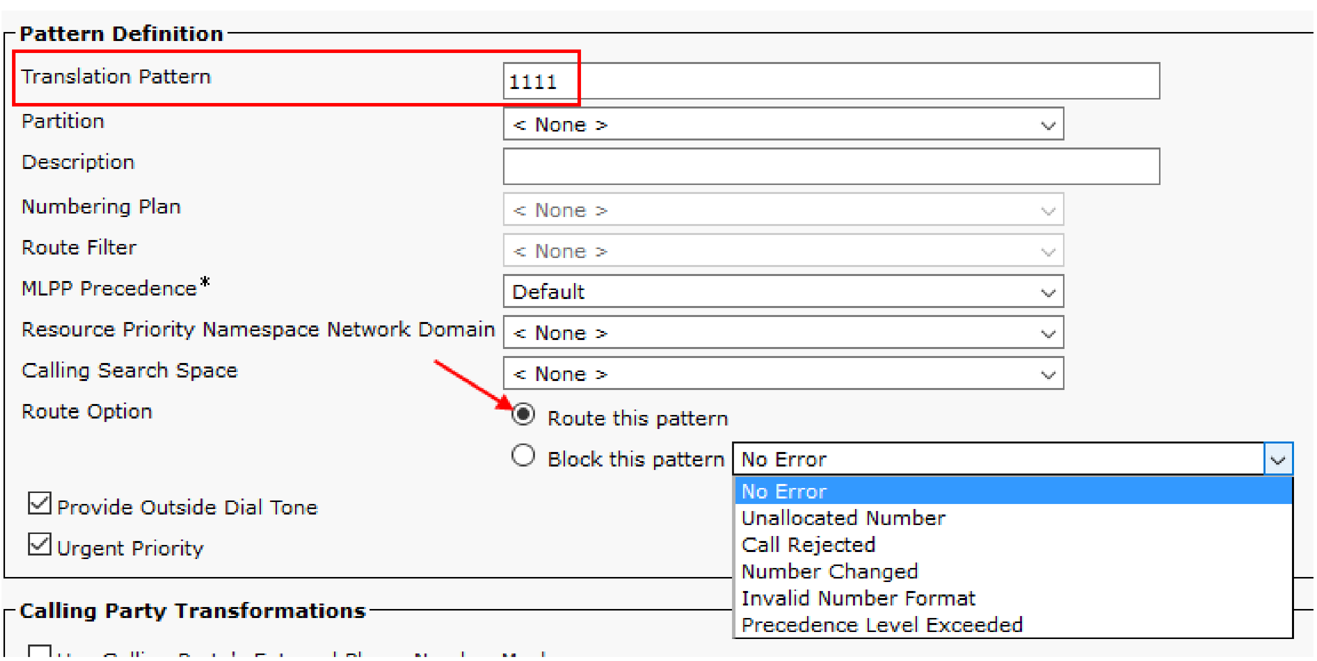
Calling Party Transformation Mask has higher priority compared to External Phone Number Mask in the Translation pattern

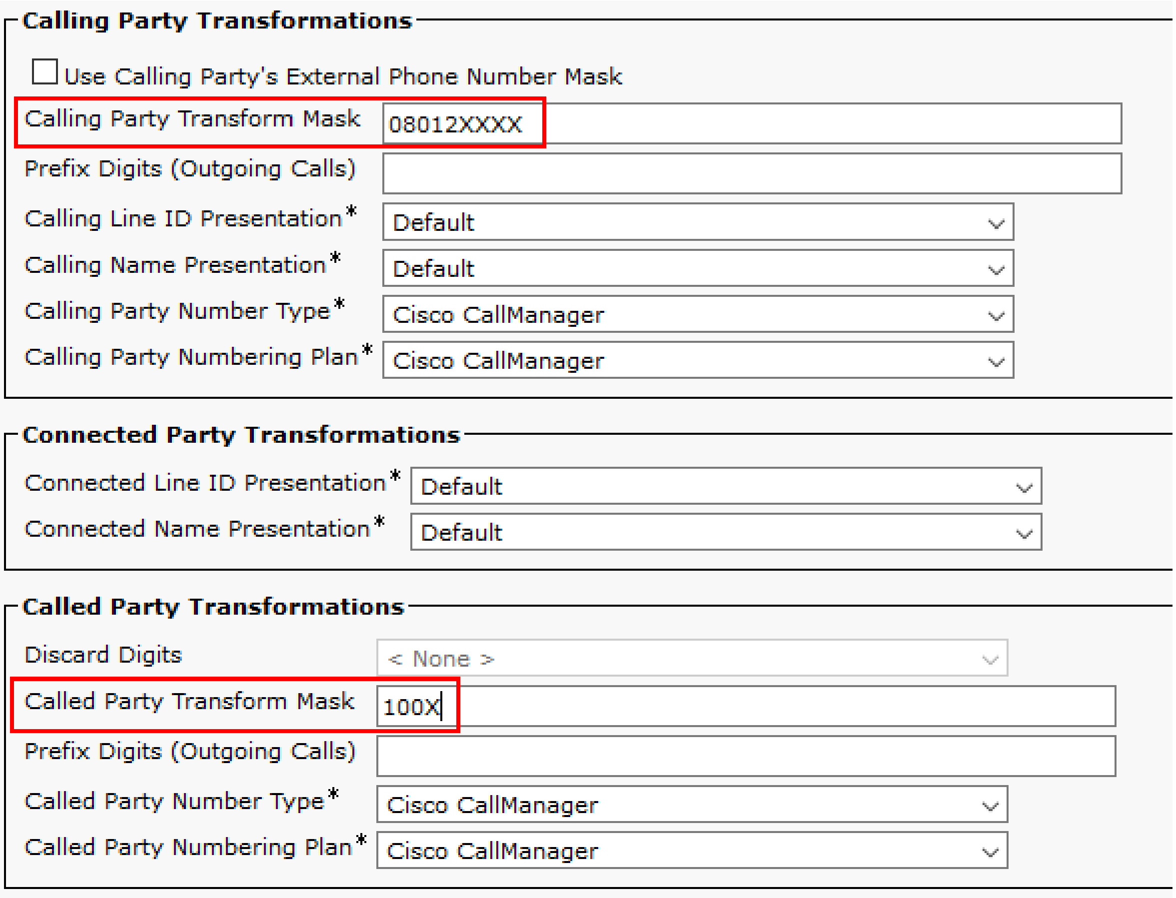
2. Translation Pattern

- CUCM uses translation pattern to manipulate digits before forwarding the call. It can also be used to block calls.
- The pattern resulting after the Translation pattern (Calling/ Called Transformed pattern) routed by the CUCM after a second digit analysis
- A translation pattern matches the called party number just like in the route pattern
- **The primary difference between Translation pattern & Route pattern is that Translation pattern do not have a final path selection. But in route pattern, there will be a path to proceed the call (Gateway, Trunk).**
- Basic use of Translation pattern is to manipulate digits (Calling & Called), they do not perform any call routing.
- First the dialed number matched with a Translation pattern, then we can change the Calling Party Number (Caller ID), Called party number using Calling Party Transformations and Called Party Transformations

<u>Configuration</u>

Call Routing → Translation Pattern → Add New





Here when user dials 1111 will be transferred to 080121000 caller ID and 1001 destination

- Translation pattern can also be used for incoming calls, when the DID from provider doesn't match the internal extensions, a translation pattern can be used to map PSTN number to internal DN

Example:

PSTN DID Range : 408 555 1XXX

Internal Extensions : 4XXX

For proper mapping create a translation pattern 408 555 1XXX and configure called party transformation to 4XXX

Transformation Mask

Transformation mask allow to modify Calling (Initiator) or Called Party (destination) digits of call.

Calling Party Transformation Mask is used to modify ANI (Caller ID)

Called Party Transformation Mask is used to modify DNIS (Dialed Number)

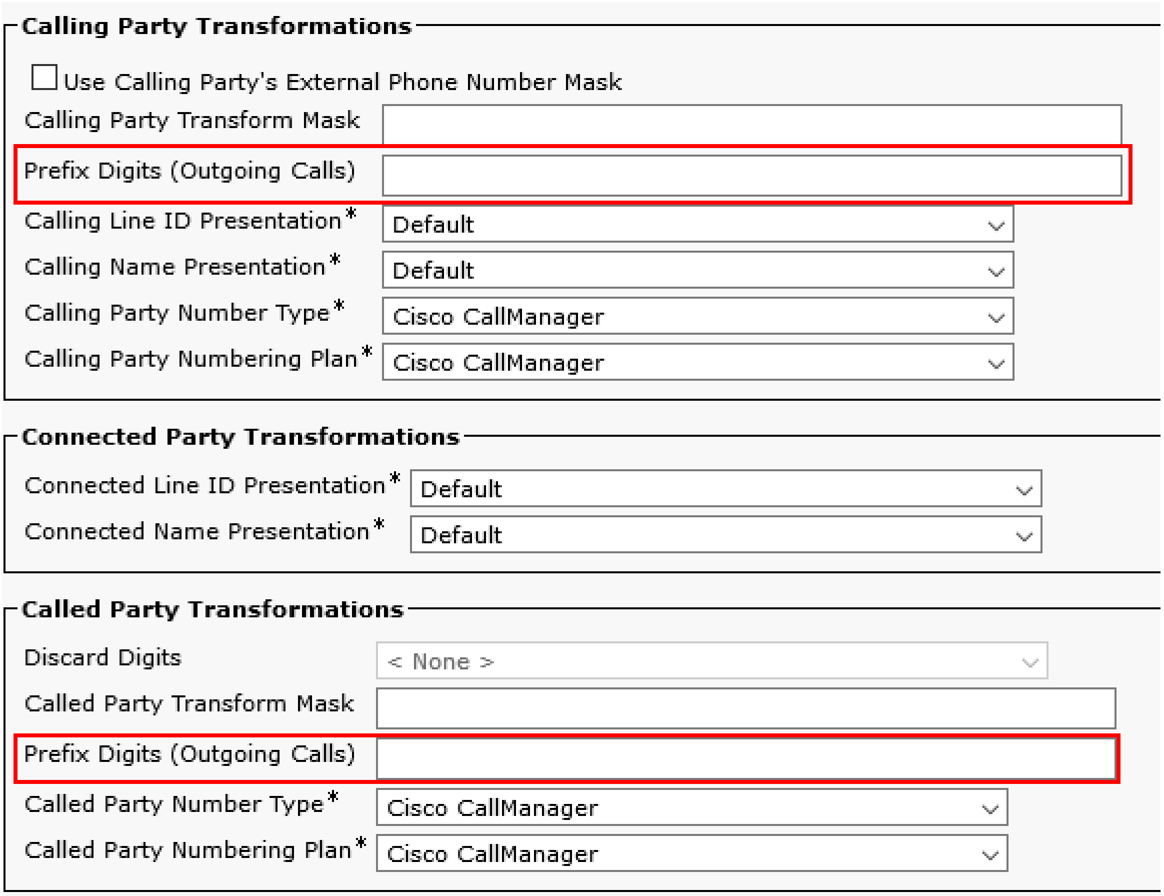
Transformation Mask can be found in various options in CUCM like Route List (assigned in the route group), Route Pattern.

Masks are always processed in right to left

Route pattern transformation can be apply when only route pattern is pointed directly to a gateway.

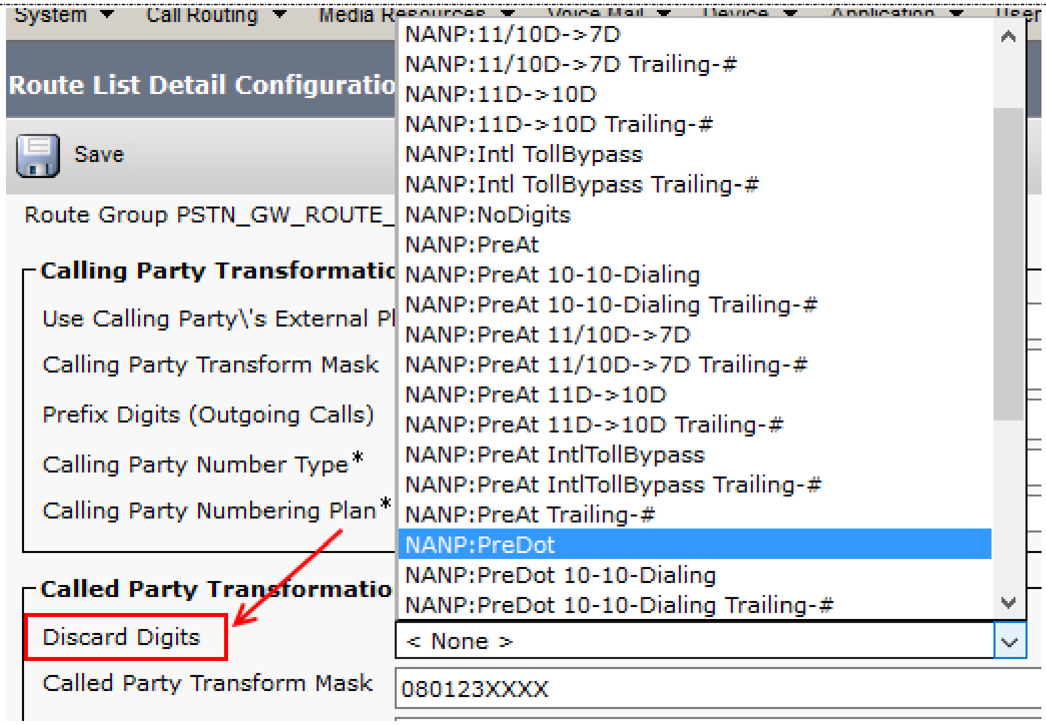
2. Digit Prefixing

- It involves prepending digits to the beginning of dialed number.
- Prefix can be added either Calling party or called party numbers in route pattern, route list, translation pattern levels



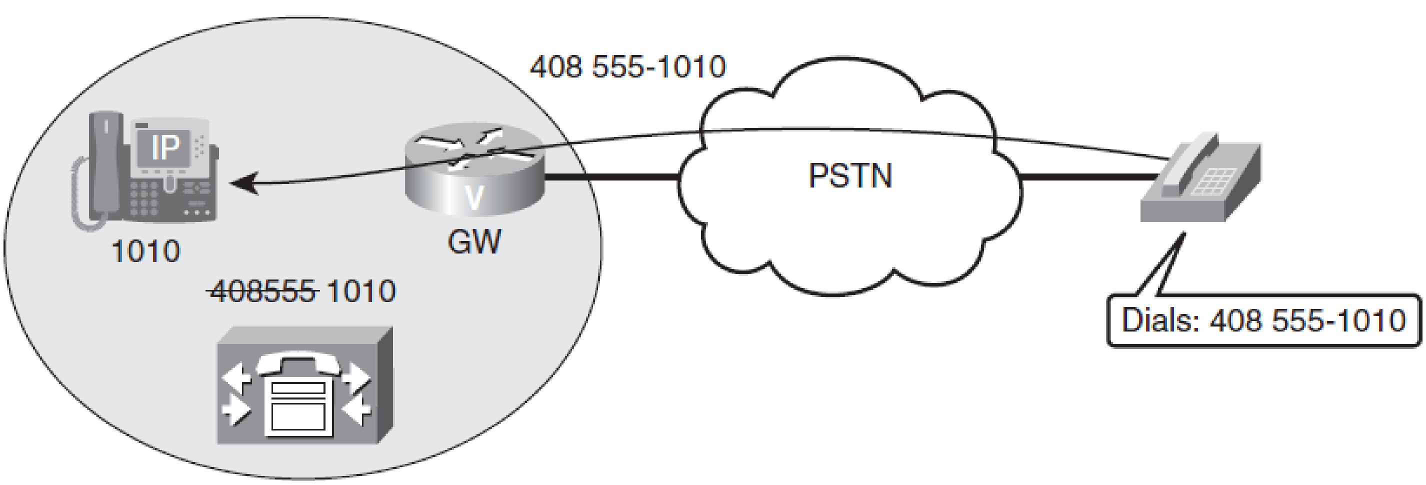
3. Digit Stripping

- Digit Discard Instruction (DDI) remove parts of dialed digits (Called Party number or dialed number)
- Access code 9 is stripped out using pre dot method under Discard Digits area in route pattern, Route group details level of route list.
- Discard Digits in the route list level will override the Discard Digits option in route pattern



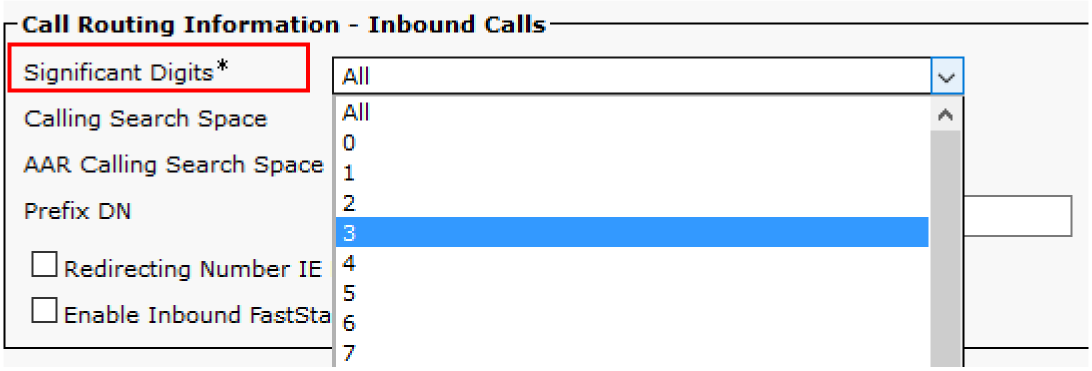
6. Significant Digits

- It instruct the CUCM to analyze the number of digits from right to left when an incoming call received by a gateway or trunk.
- It is the easiest method to convert incoming PSTN call to an internal extension. (DID mapping)
- It is more processor friendly alternative than Translation pattern to map DID to internal DNs
- Example Significant digits 4 will convert 4085551010 to 1010



Configuration

Device → Gateway or Trunk → Significant Digits*: X


Call Routing Information - Inbound Calls
Significant Digits*
Calling Search Space
AAR Calling Search Space
Prefix DN
Redirecting Number IE
Enable Inbound FastSta
All
All
0
1
2
3
4
5
6
7

6. Call Coverage

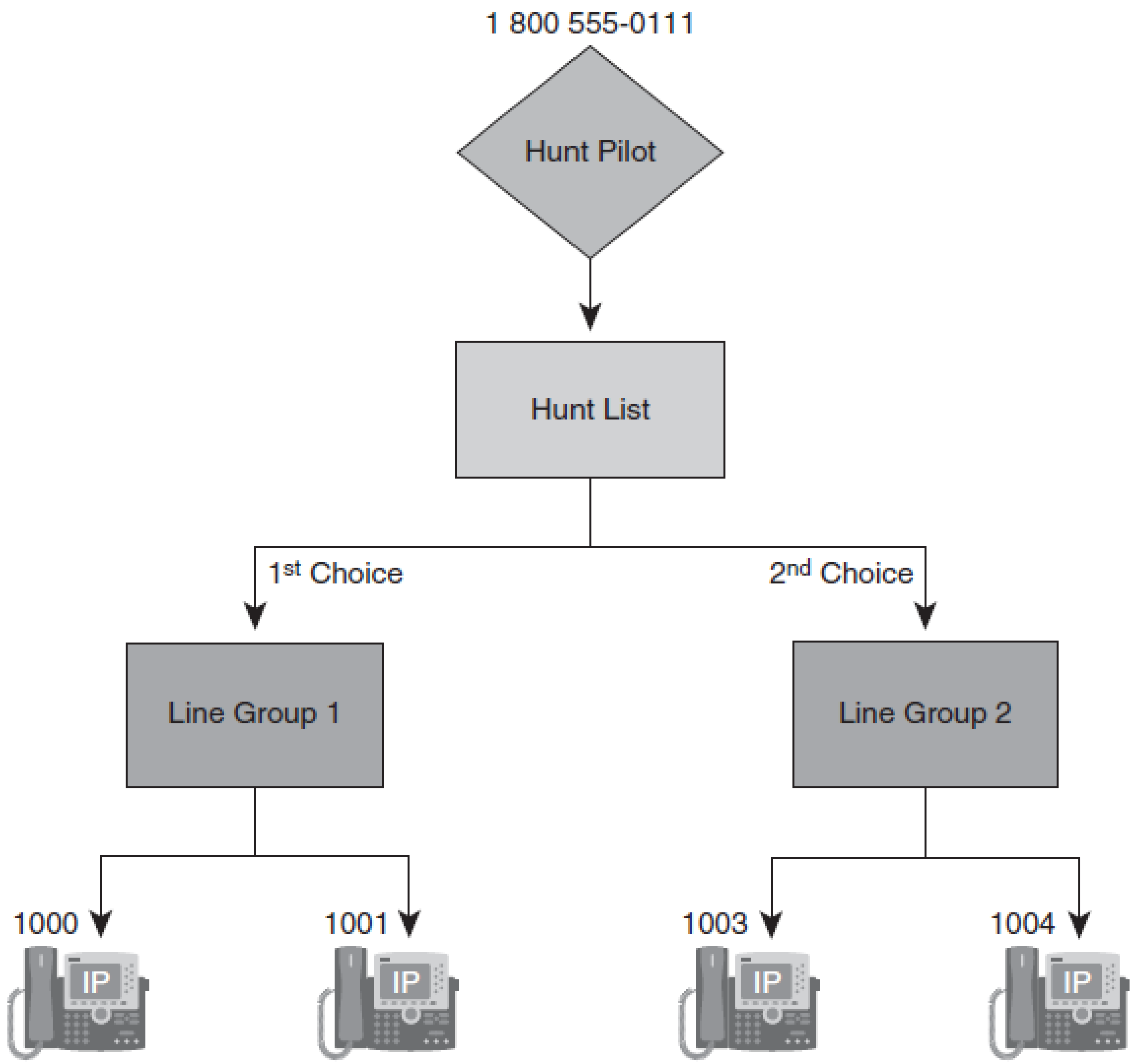
Call coverage is a part of dial-plan that ensures all incoming calls are answered. Available coverage options are,

1. Call Forwarding (CCNA VOICE)
2. Shared Line (CCNA VOICE)
3. Call Pickup (CCNA VOICE)
4. Call Hunting

- Hunt Group is a mechanism that helps business to manage inbound calls. It is a group of telephone lines that are associated with a common number. When call comes to the hunt number, the call cycles through the group of lines until available line is found.
- Call hunting is based on a pilot number which is directly called or called by a forward option to start hunting.

Call Hunting Components

- Line Number/ DNs: Number assigned to phones
- Line Group: Multiple DNs or Voice mail ports
- Hunt List: Line groups are assigned to hunt list, Hunt list is an ordered list of Line groups
- Hunt Pilot: Hunt list are assigned to Hut pilot. Hunt pilots are the numbers that will match on dialed digits to invoke the hunting process.



- While hunting the forwarding configuration of line group members is not considered. If the hunting algorithm is ringing a phone and the call is not answered, the Call Forward No answer settings of that particular phone is ignored, and hunting algorithm goes on to next line group member.
- Call Pickup option won't be applicable while hunting
- Partition of line group members won't be considered

Hunt Options

1. ***Try Next Member, Then try next group (Default)***: Sends the call to next available member, if no more members are available, go to next group
2. ***Try Next Member, Do not go next group***: Sends the call to next available member, if no more members are available, hunting stops

3. ***Skip Remaining Members, and go directly to Next group***: Sends the call to first available member, if that members are available, go to next group
4. ***Stop Hunting***: Do not proceed hunting

Hunt Distribution Algorithm

Distribution algorithm specifies the order in which group members should be used while hunting.

- ***Top Down***: 1st call always goes to 1st line member, if he is unavailable, call goes to 2nd line member
- ***Circular***: 1st call goes to 1st line, 2nd call goes to 2nd line and so on
- ***Longest idle time***: CUCM distributes the call to the line member that has been idle for the longest amount of time
- ***Broadcast***: Simultaneous distribution of calls

Configuration

Step 1: Create Line Groups

Call Routing → Route/Hunt → Line Group → Add New →

Line Group Name* : Customer_Support_Team1

RNA Reversion Timeout* : 10 <Ring No Answer time in seconds>

Distribution Algorithm* : Longest Idle Time

Hunt Options

No Answer* : Try next member; then, try next group in Hunt List

Busy** : Try next member; then, try next group in Hunt List

Not Available** : Try next member; then, try next group in Hunt List

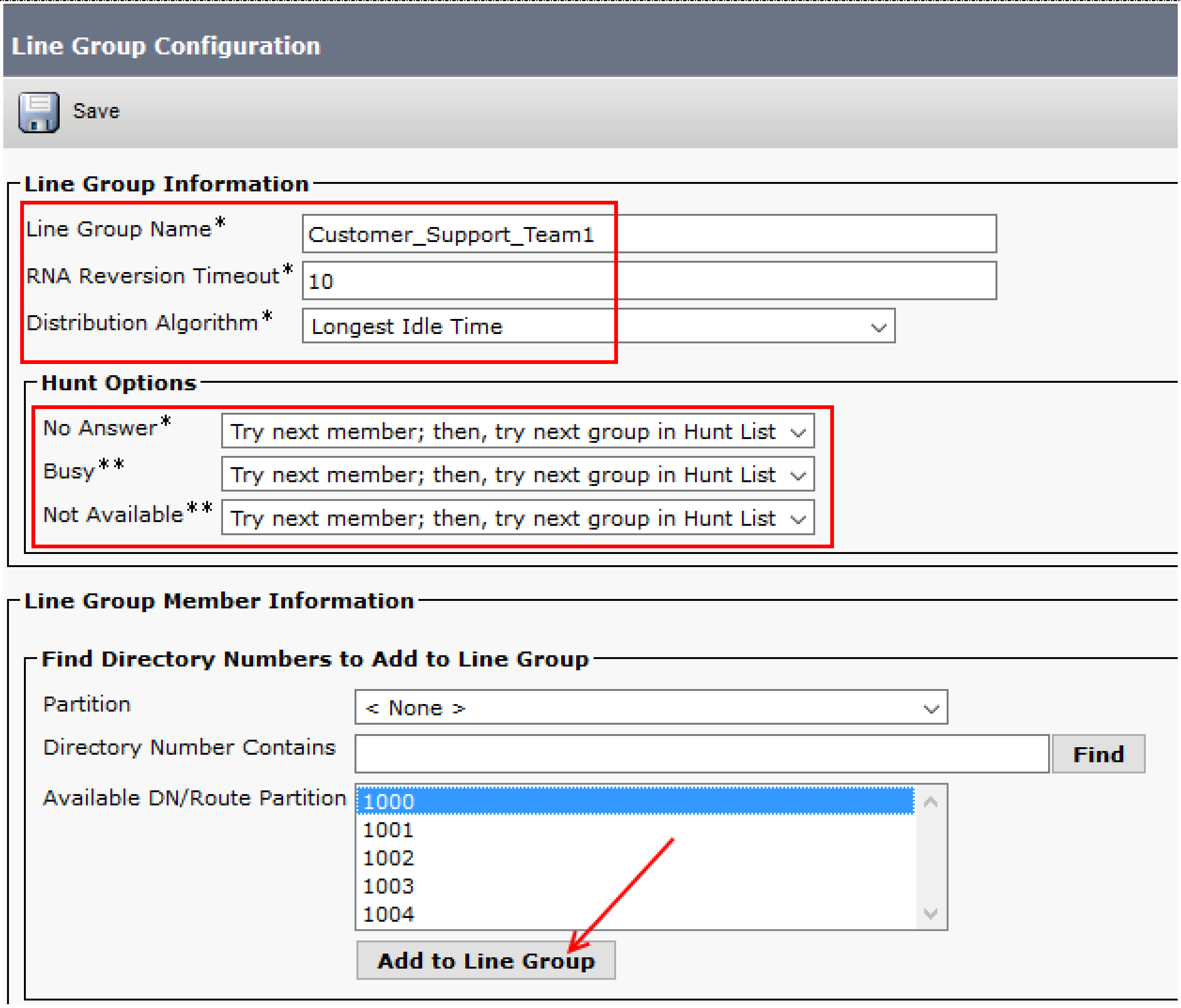
Available DN/Route Partition : ↓↓↓↓↓

Add to Line Group

Selected DN/Route Partition : ↓↓↓↓↓ <Rearrange>

→ Save

Configure additional group is needed.



__Step 2: Create Hunt List__

Call Routing → Route/Hunt → Hunt List → Add New

Name*   : Customer_Support_Hunt_List

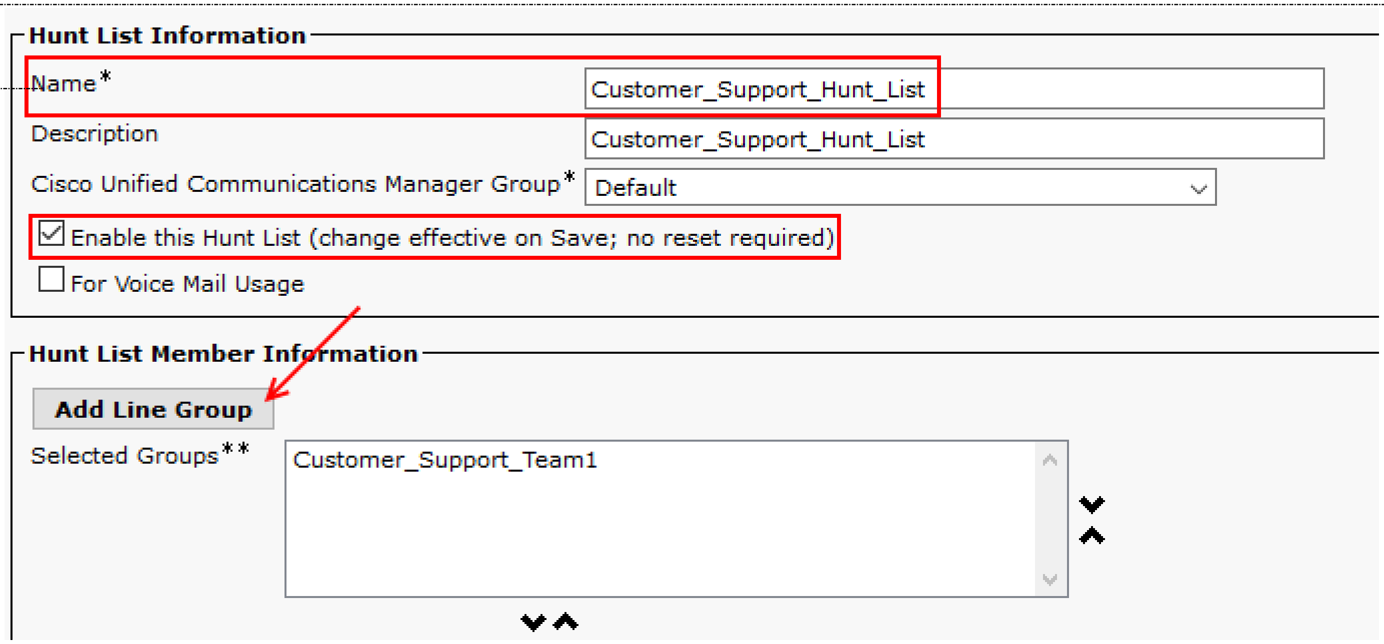
Description   : Customer_Support_Hunt_List

Cisco Unified Communications Manager Group*: Default <Select Group>

Check Enable this Hunt List

→ Save

Add Line Group → Select Line Group → Save



__Step 3: Hunt Pilot Number__

Call Routing → Route/ Hunt → Hunt Pilot → Add New

Hunt Pilot*   : 1111

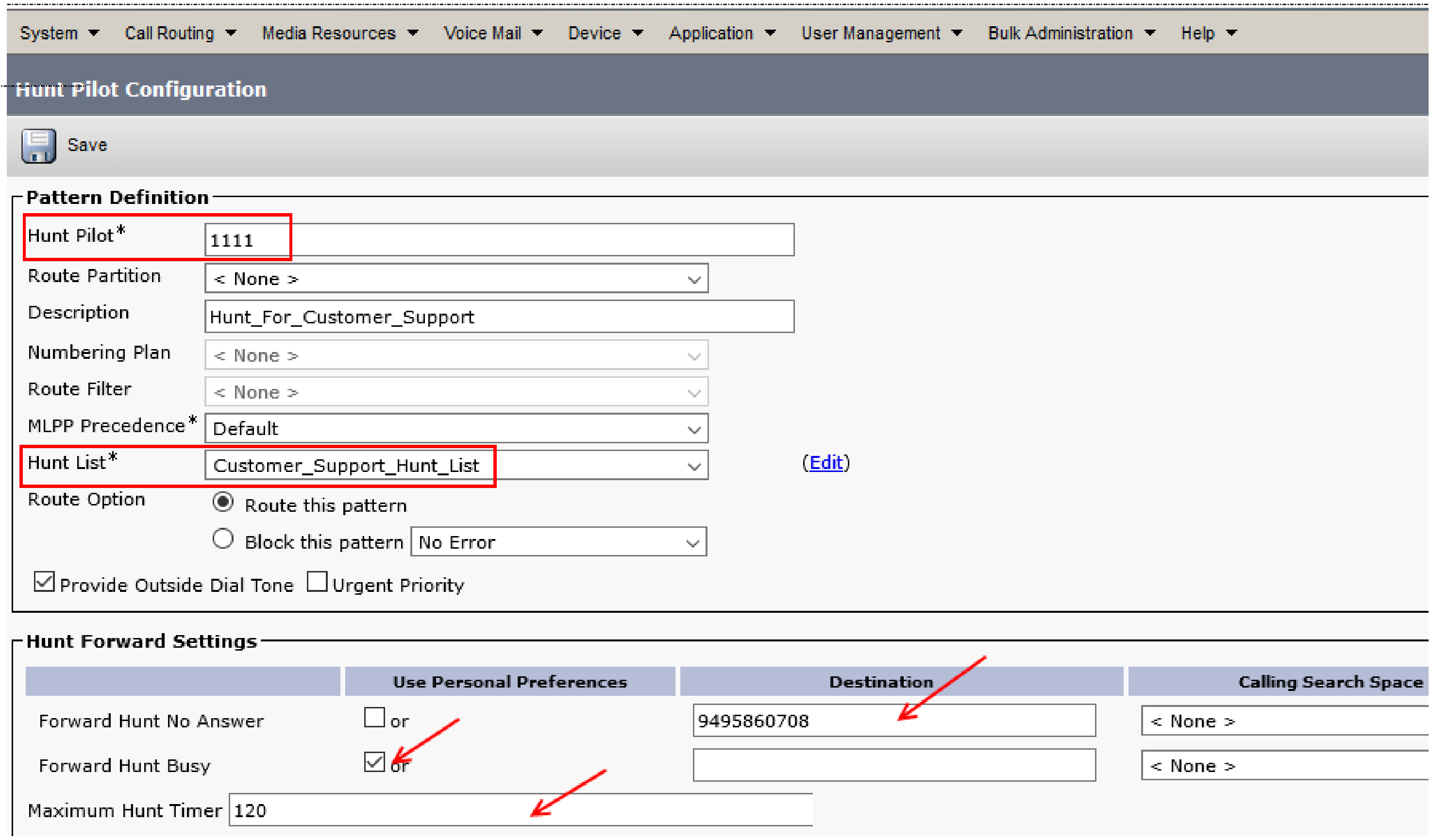
Description   : Hunt_For_Customer_Support

Hunt List*   : Customer_Support_Hunt_List   <Created in Step 2>

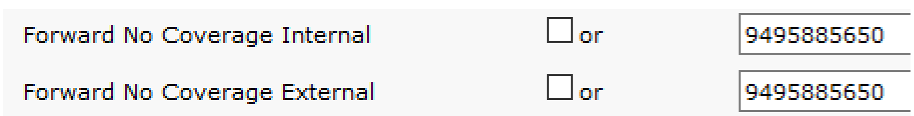
Forward Hunt No Answer: Destination- 9495860708

Forward Hunt Busy   : Check Use Personal Preferences

Maximum Hunt Timer   : 120 <Seconds>



Personal Preferences will work if only the hunt initiated via forward option. At this point Hunt algorithm finishes and forward the call based on the master phone who forwarded his call to Hunt pilot. For this you must configure ‘Forward No Coverage’.



Media Resources

- Media Resources are Hardware or Software that support the media processing functions and features of VoIP network.
- CUCM itself plays most of these roles

Media processing functions includes,

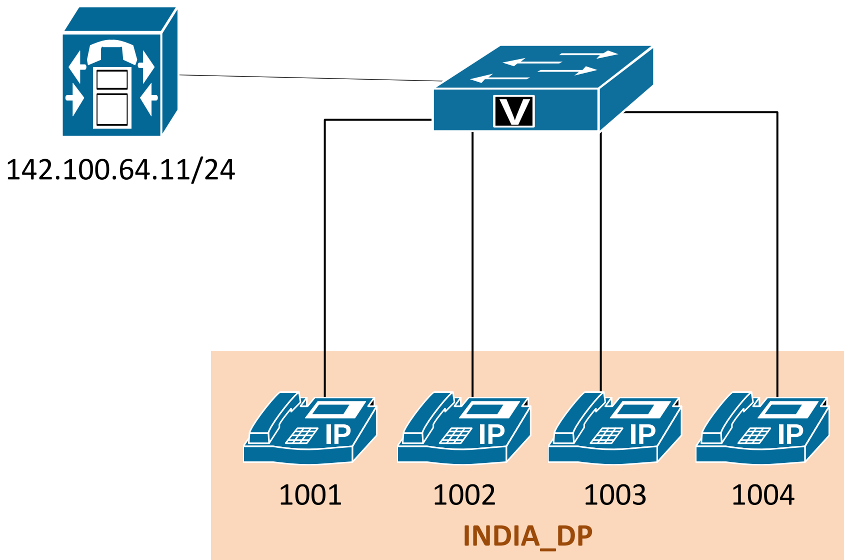
1. ***Voice Termination***: Converting an audio in to IP packet and vice versa. TDM legs must be terminated by hardware that performs coding/decoding & Packetizing of audio. This is performed by DSPs in the Gateway router
2. ***Conference***: Mixing of multiple audio stream together and provide a single stream
3. ***Transcoding***: Codec conversion
4. ***Media Termination Point (MTP)***: Bridges the media and allow them to setup and teardown properly (Holding the call while it is held by IP phone)
5. ***Annunciator***: Provides spoken messages and various tones. It uses SCCP protocols to establish one way RTP. Announcements can be customized by replacing appropriate WAW file
6. ***Music On Hold (MOH)***: Provide music to the caller when their call is placed on Hold, Parked, Transferred or added to an Ad Hoc conference.

- Software resources are provided by CUCM and IOS, hardware resources are provided by DSPs in Router or Switch
- Software resources are controlled by **Cisco IP Voice Media Streaming App** in Service ability page of CUCM
- Software resource can control **Annunciator, MOH,** Conference, MTP
- **Transcoding, Voice Termination** are available only by Hardware
- Audio Conferencing, MTP are possible by both Software & Hardware
- Signaling between CUCM and Hardware resource is controlled by SCCP

Conference Bridge

- Handles conference call. CUCM Server supports G.711 conference call because it is a software based resource.

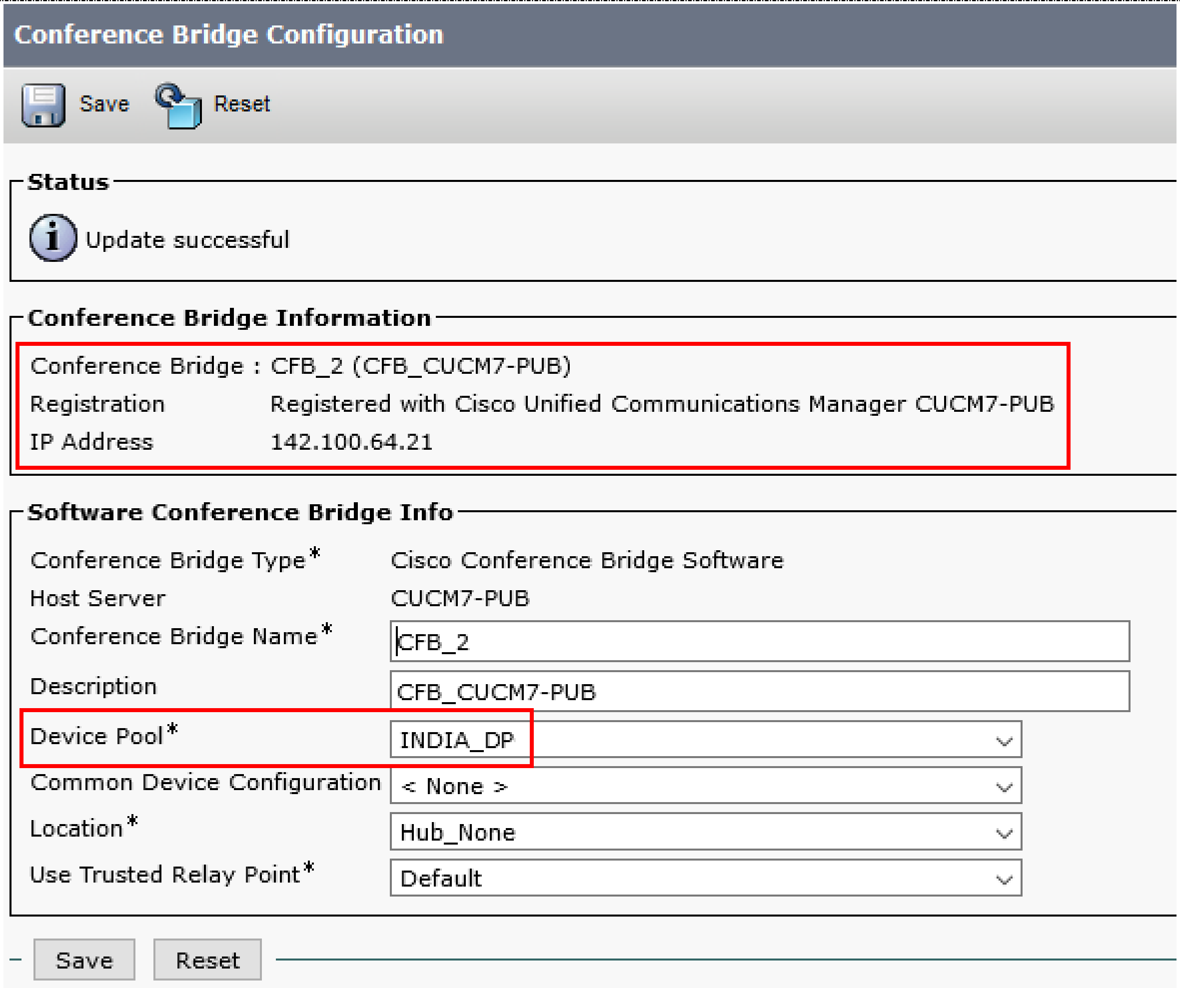
Software Conference Bridge



- Software conference is activated by default if you enable **Cisco IP Voice Media Streaming App**

Cisco Unified Service Ability → Tools → Service Activation → Cisco IP Voice Media Streaming App

Go to Media Resources → Conference Bridge



- CUCM doesn't distinguish Software and Hardware based conference bridges when it processes a conference allocation request.
- 64 ad hoc and 128 meet me conference sessions each having 4 members (by default) are supported by the software conference bridge.

Ad Hoc Conference

- Allows the conference controller to add specific participants to the conference. Here a connected user hit conference call and dial another number then consult with him and press the Conference button again to start conferencing
- The person who hit Conference soft key is called Conference controller (or Originator)

Basic Ad Hoc: Only the originator can add participants to the conference. Originator is the controller of that particular conference call. Basic ad hoc is the default conference.

Advanced Ad Hoc: Here any participant can add or remove participants. It allows linking multiple Ad Hoc conferences together.

Configurations

System → Service Parameter →

Server* : Select Server

Service* : Cisco Call manager (Active)

Drop Ad Hoc Conference* : When No OnNet Parties Remain in the Conference

Maximum Ad Hoc Conference* : 4

Advanced Ad Hoc Conference Enabled: True

Meet Me Conference

- It is a scheduled conference where users can dial in to a conference. It requires that a range of DNs to be allocated exclusively for the conference.

Step 1: Meet me number range

Call Routing → Meet Me numbers/ Pattern → Add New

Directory Number or Pattern* : 200X

Description: Meet Me

Minimum Security Level:

Authenticated: Block participants with non-secure phone profile

Encrypted:

Non Secure: Allow all

→ Save

__Step 2: Configure Meet me Soft Key__

Note: Conference is initiated by a user by Pressing Meet Me softkey followed by Meet me number or range. Then other users can join by just calling the specified meet me number

----

System → Service Parameters → Cisco IP Voice Media Streaming App (Active)

Annunciator (ANN) Parameters	
Call Count *	48
Run Flag *	True
Conference Bridge (CFB) Parameters	
Call Count *	48
Run Flag *	True
Media Termination Point (MTP) Parameters	
Call Count *	48
Run Flag *	True

Conference Bridge (CFB) Parameters:

Call Count: Specifies the maximum number of conference participants that Conference Bridge can support. The range is 0 to 256 and recommended value is 48

Multiple ad hoc conference is possible, this value is the total of all participants in multiple conference

Run Flag: It enables or disables the conference bridge feature.

System → Service Parameters → Call Manager (Active)

Clusterwide Parameters (Feature - Conference)

Suppress MOH to Conference Bridge *	True	True
Drop Ad Hoc Conference *	When No OnNet Parties Remain in the Conference	Never
Maximum Ad Hoc Conference *	4	4
Maximum MeetMe Conference Unicast *	4	4
Advanced Ad Hoc Conference Enabled *	True	False
Choose Encrypted Audio Conference Instead Of Video Conference *	True	True
Minimum Video Capable Participants To Allocate Video Conference *	2	2
Enable Click-to-Conference for Third-Party Applications *	False	False

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

Maximum Ad Hoc Conference: This parameter specifies the maximum number of participants that are allowed in a single Ad Hoc conference. (Default:4, Minimum:3, Maximum: 64. Software Conference 64; Cisco Catalyst WS-X6608: 16; Cisco Catalyst 4000: 16; and NM-HDV: 6)

Maximum MeetMe Conference Unicast: This parameter specifies the maximum number of participants that are allowed in a single Unicast Meet-Me conference. Default:4, Minimum:1, Maximum: 128

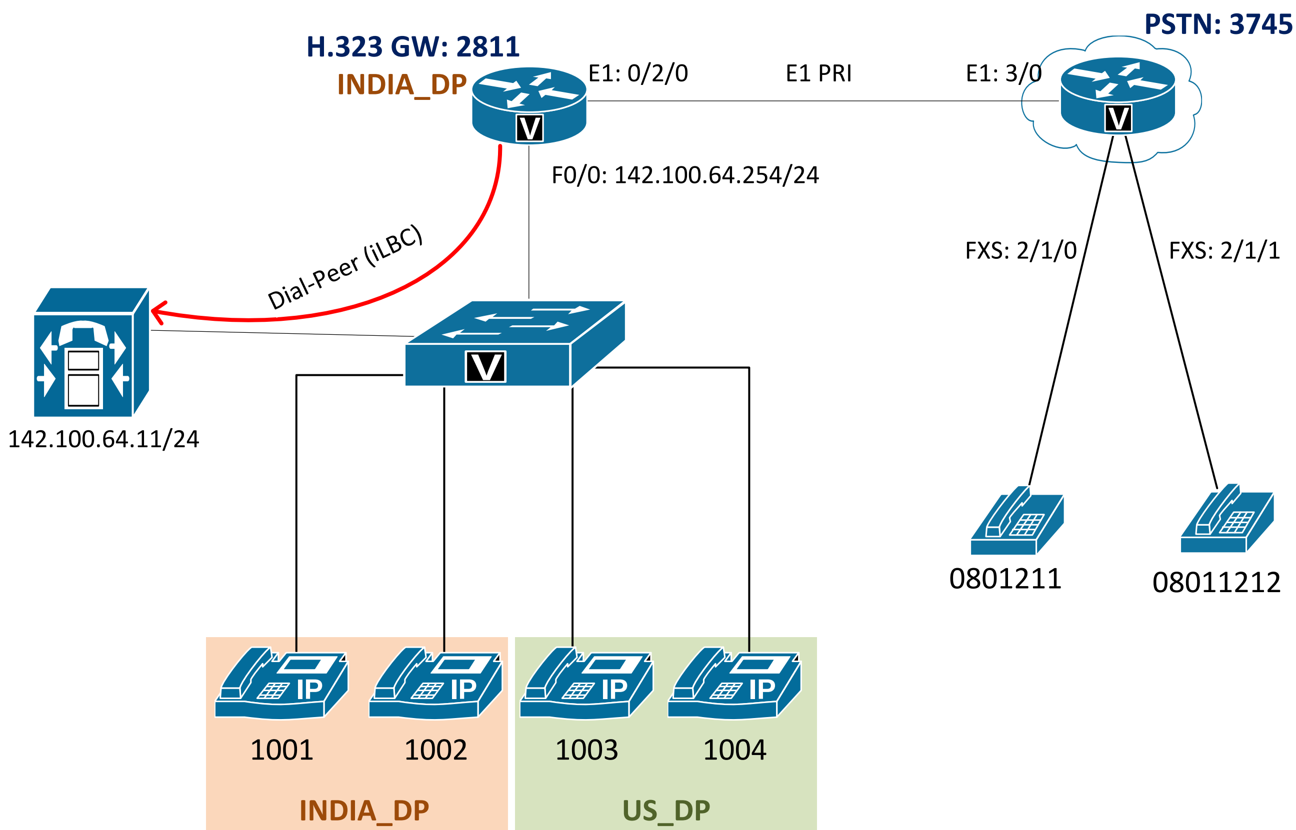
Hardware Conferencing

- For multiple codec (G.729, iLBC, GSM) conference you should go for Hardware resource (DSP)

Following hardware Conference Bridge supported by CUCM

1. Cisco Conference bridge hardware (Cisco Catalyst WS-X6608-T1, WS-X6608-E1)
2. Cisco IOS Conference Bridge (Cisco NM-HDV)
3. Cisco IOS Enhanced Conference Bridge (Cisco NM-HDV2, NM-HD-1V/2V/3VE, PVDM2). Each DSP provides a single conference bridge
4. Cisco Conference Bridge (Cisco WS-SVC-CMM, Cisco WS-SVC-CMM-ACT)
5. Cisco Video Conference Bridge (CUVC-3510, 3540)

Configuration of Hardware Conference Bridge (Cisco IOS Conference Bridge Cisco NM-HDV on 2811 Router)



- Deploy CUCM as shown in figure
- Set Inter & Intra region codecs INDIA Region to US Region iLBC
- Configure H.323 Gateway
- Configure PSTN Router with two analog phone

Router Side Configuration

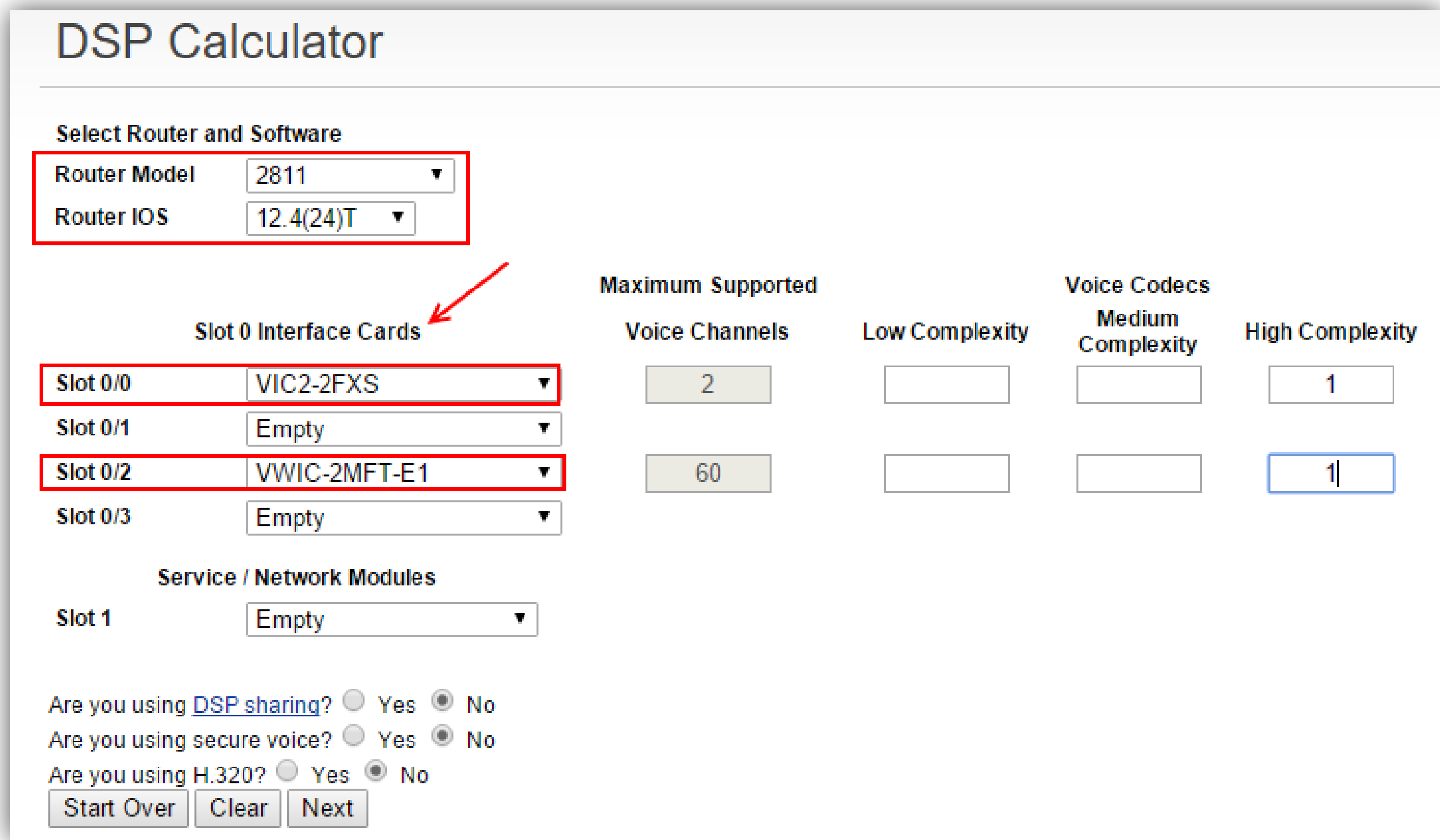
Step 1: Identification Hardware and IOS Version

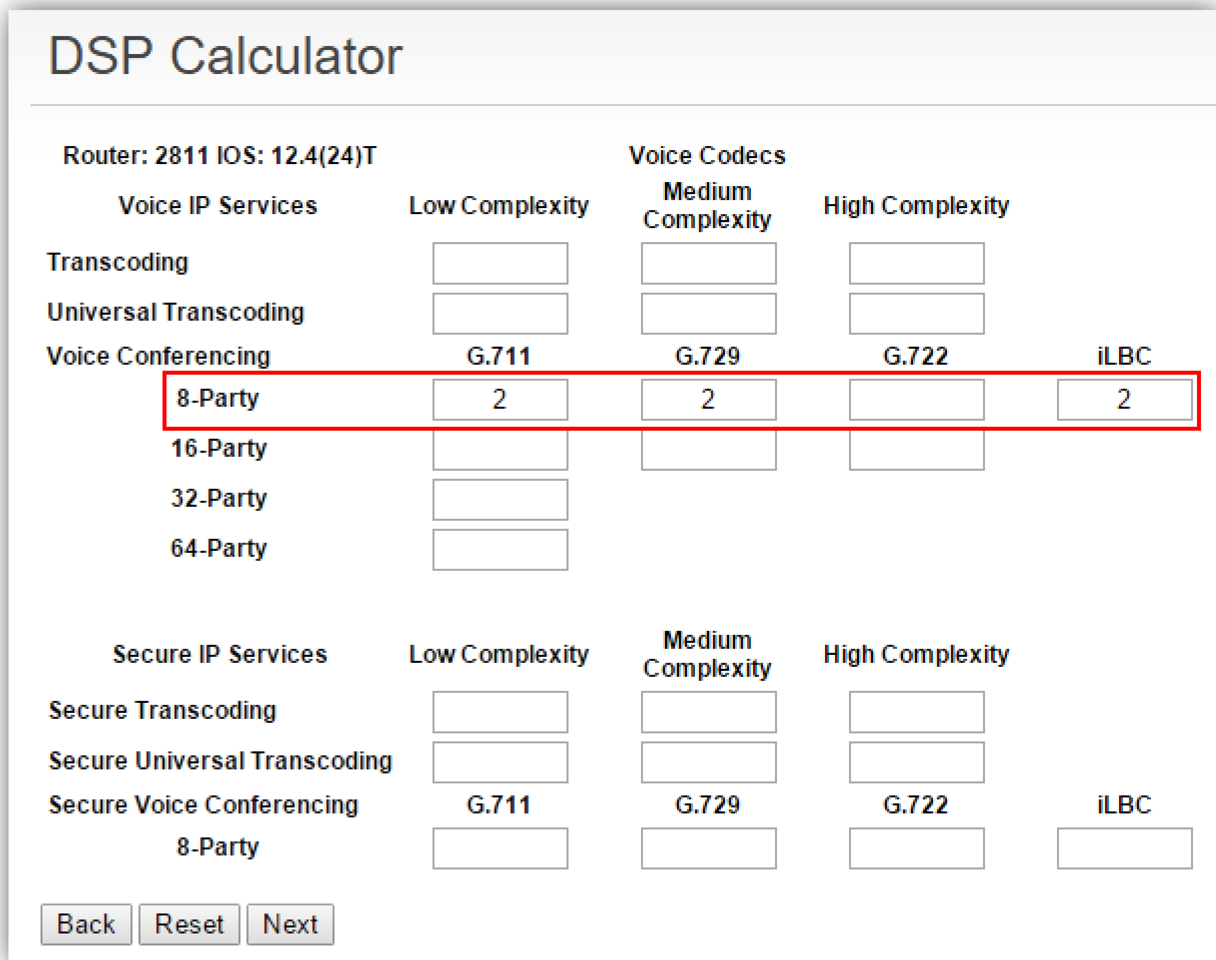
```
R1#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9_IVS_LI-M), Version
12.4(24)T6
```

Step 2: Calculate DSPs Requirement

Based on the link calculate required DSPS for conferencing

http://www.cisco.com/web/applicat/dsprecal/dsp_calc.html




DSP Calculator
Router: 2811 IOS: 12.4(24)T
Voice Codecs
Voice IP Services
Low Complexity
Medium Complexity
High Complexity
Transcoding
Universal Transcoding
Voice Conferencing
G.711
G.729
G.722
iLBC
8-Party
2
2
2
16-Party
32-Party
64-Party
Secure IP Services
Low Complexity
Medium Complexity
High Complexity
Secure Transcoding
Secure Universal Transcoding
Secure Voice Conferencing
G.711
G.729
G.722
iLBC
8-Party
Back
Reset
Next

DSP Calculator

Router: 2811
IOS: 12.4(24)T
DSP Modules Required:
PVDM2-64: 1

DSP Module Allocation:
Router Slot 0: 64 Voice (100%) 0 Available (0%)
PVDM Slot 0/0: PVDM2-64

Call Volume Allocation:

Router Slot 0	Low	Med	High
Slot 0/0: VIC2-2FXS			
Slot 0/2: VWIC-2MFT-E1			

Conference 8 Party G.711: 2
Conference 8 Party G.729: 2
Conference 8 Party iLBC: 2

Back | Start Over

Step 3: Verify DSPs & Voice Card

```
R1#show inventory
NAME: "2811 chassis", DESCR: "2811 chassis"
PID: CISCO2811         , VID: V03 , SN: FHK1038F0YB

NAME: "2nd generation two port FXS voice interface daughtercard on Slot 0 SubSlot 0",
DESCR: "2nd generation two port FXS voice interface daughtercard"
PID: VIC2-2FXS         , VID: V01 , SN: FOC1134070Q

NAME: "WAN Interface Card - Serial (1T) on Slot 0 SubSlot 1", DESCR: "WAN Interface Card -
Serial (1T)"
PID: WIC-1T=           , VID: 1.0, SN: 34086087

NAME: "Two port E1 voice interface daughtercard on Slot 0 SubSlot 2", DESCR: "Two port E1
voice interface daughtercard"
PID: VWIC-2MFT-E1=     , VID: 1.0, SN: 29238096

NAME: "WAN Interface Card - Serial 2T on Slot 0 SubSlot 3", DESCR: "WAN Interface Card -
Serial 2T"
PID: WIC-2T=           , VID: 1.0, SN: 35419506

NAME: "PVDMII DSP SIMM with Two DSPs on Slot 0 SubSlot 4", DESCR: "PVDMII DSP SIMM with Two
DSPs"
PID: PVDM2-32          , VID: V01 , SN: FOC10500XQ9



GW#show voice dsp

DSP  DSP                DSPWARE CURR  BOOT                         PAK     TX/RX
TYPE NUM CH CODEC       VERSION STATE STATE   RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ========== ===== ======= === == ========= == ===== ============
----------------------------FLEX VOICE CARD 0 ------------------------------
                           *DSP VOICE CHANNELS*
CURR STATE : (busy)inuse  (b-out)busy out  (bpend)busyout pending
LEGEND     : (bad)bad     (shut)shutdown   (dpend)download pending
DSP   DSP                 DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC        VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ========= ========== ===== ======= === == ========= == ==== ============
                           *DSP SIGNALING CHANNELS*
DSP   DSP                 DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC        VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ========= ========== ===== ======= === == ========= == ==== ============
C5510 001 01 {flex}         24.3.6 alloc idle      0  0 0/0/0     02    0         42/0
C5510 001 02 {flex}         24.3.6 alloc idle      0  0 0/0/1     02    0         15/0
------------------------END OF FLEX VOICE CARD 0 ----------------------------
```

Step 4: Configure Voice Card

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

Step 5: Point Call Manager for SCCP Operations

```
GW(config)#sccp local fastEthernet 0/0
GW(config)#sccp ccm 142.100.64.11 identifier 1 version 7.0+
GW(config)#sccp ccm 142.100.64.12 identifier 2 version 7.0+ <BACKUP SERVER>
GW(config)#sccp
```

Step 6: DSP Farm Profile for Conference

```
GW(config)#dspfarm profile 1 conference
GW(config-dspfarm-profile)#codec g711alaw
GW(config-dspfarm-profile)#codec g711ulaw
GW(config-dspfarm-profile)#codec g729r8
GW(config-dspfarm-profile)#codec ilbc
GW(config-dspfarm-profile)#maximum sessions 2
GW(config-dspfarm-profile)#associate application sccp
GW(config-dspfarm-profile)#no shutdown
```

Step 7: CUCM Group & Registration Name

```
GW(config)#sccp ccm group 1
GW(config-sccp-ccm)#associate ccm 1 priority 1
GW(config-sccp-ccm)#associate ccm 2 priority 2
GW(config-sccp-ccm)#associate profile 1 register CFB-2811-ROUTER
```

- ***dspfarm***: To enable DSP farm service. It is disabled by default.
- ***dsp services dspfarm***: To enable DSP farm service for a particular network module
- ***sccp local***: To select local interface that SCCP applications (conference bridge) use to communicate & register with CUCM
- ***sccp ccm***: To add the CUCM server to the list of available servers

- ***sccp***: To enable SCCP protocol and its related applications (Conference bridge, transcoding)
- ***sccp ccm group***: To create CUCM group
- ***associate ccm***: Associate CUCM with CUCM-Group and establish priority within the group
- ***associate profile 1 register***: Name of Conference bridge to register with CUCM

<u>CUCM Side Configuration</u>

<u>Step 8: Add Conference Bridge</u>

Media Resources → Conference Bridge → Add New →

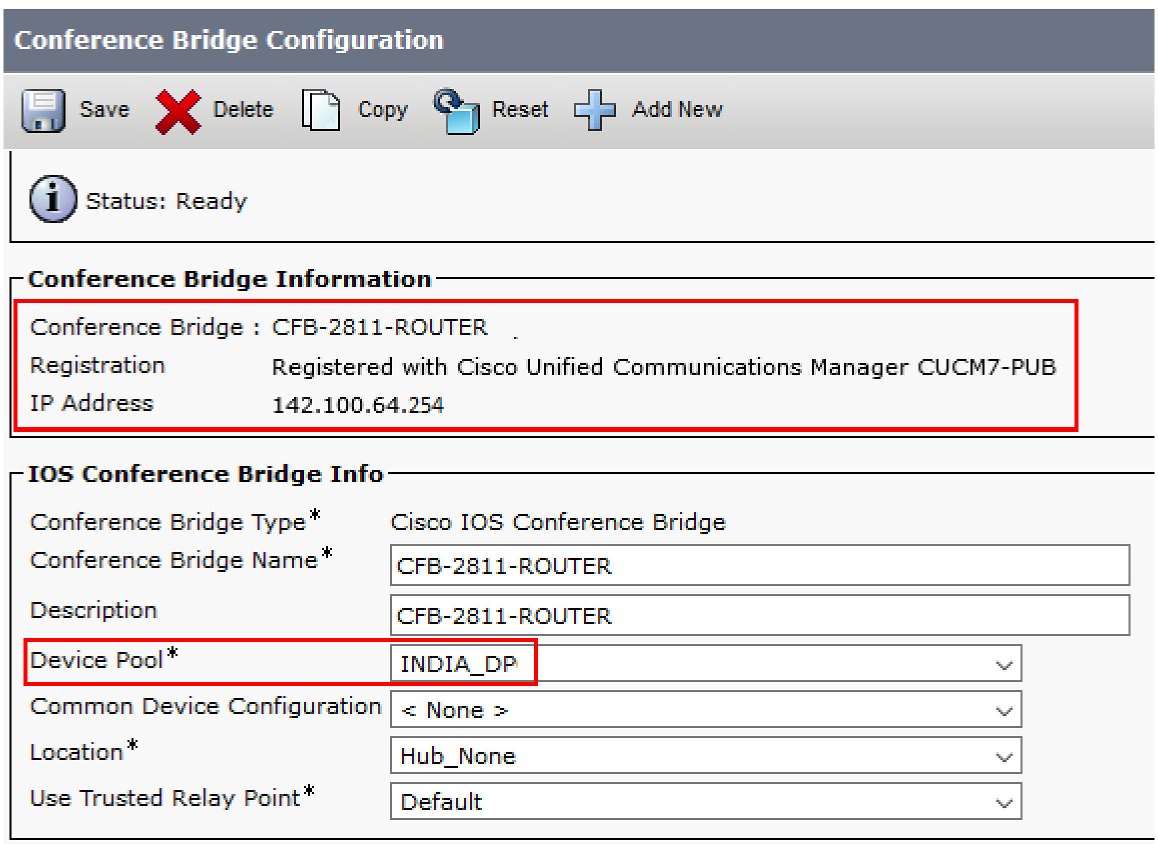
Conference Bridge Type* : Cisco IOS Conference Bridge

Conference Bridge Name* : CFB-2811-ROUTER

Description : CFB-2811-ROUTER

Device Pool* : INDIA_DP

Device Security Mode*: Non Secure Conference Bridge



Device Pool: Best practice is to configure a separate device pool dedicated to media resources. e.g. Media_Resources_DP

Step 9: Create Media Resource Group

Media Resources → Media Resource Group → Add New

Name* : MRG1

Description : Media Resource Group 1

Available Media Resources** : ↓↓↓↓↓↓

Selected Media Resources : CFB-2811-ROUTER

→ Save

Step 10: Create Media Resource Group List (MRGL)

Media Resources → Media Resource Group List → Add New

Name* : MRGL1

Description : Media Resource Group List 1

Available Media Resource Groups* : ↓↓↓↓

Selected Media Resource Groups : MRG1

Step 11: Apply MRGL under Device Page or in Device Pool

Verification Commands

GW#show sccp

```
SCCP Admin State: UP
Gateway Local Interface: FastEthernet0/0
        IPv4 Address: 142.100.64.254
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 142.100.64.11, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A

Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 142.100.64.11, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 1
Reported Max Streams: 16, Reported Max OOS Streams: 0
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
```

```
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
```

GW#show sccp ccm group

```
CCM Group Identifier: 1
 Description: None
 Binded Interface: None
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 1, Registration Name: CFB-2811-ROUTER
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: cs3, Audio DSCP value: ef
```

GW#show sccp connections

```
sess_id     conn_id      stype mode     codec   sport rport ripaddr

16781237    16777358     conf  sendrecv g729b   17700 17538 142.100.64.114
16781237    16777357     conf  sendrecv g729    17738 18000 142.100.64.254
16781237    16777355     conf  sendrecv g711u   18244 28174 142.100.64.109

Total number of active session(s) 1, and connection(s) 3
```

GW#show dspfarm profile 1

```
Dspfarm Profile Configuration

 Profile ID = 1, Service = CONFERENCING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 2
 Number of Resource Available : 2
 Codec Configuration
```

```
Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

Transcoder (XCoder)

- Transcoder used to convert between two codecs G.729 to G.711; G.711 to iLBC; etc.
- Transcoders also does Codec paketization difference (20mSec to 30mSec) conversion
- Software based transcoder not available in CUCM, we need PVDM/ Hardware resource

Role & Need of Transcoder

- If we are using single codec everywhere transcoders are not required
- Once you configure Region in CUCM and set the inter region codec, all the codec having lower bit rate are supported and we don't want to invoke transcoders
- Device who doesn't support Region-required codec is the one who checks MRGL and invokes a transcoder
- Always place transcoder local to each site where resources may need (Do not use WAN to access a transcoder in remote location). Important to consider the placement

Types of Transcoders

Traditional Transcoding

G.711 to any other codec (G.711 ↔ iLBC), requires less DSPs

Universal Transcoding

Transcoding between any non-G.711 codecs (G.729 ↔ iLBC), require more DSPs

Codec Support

G.729 μ Law/ a Law

G.722

G.729

iLBC

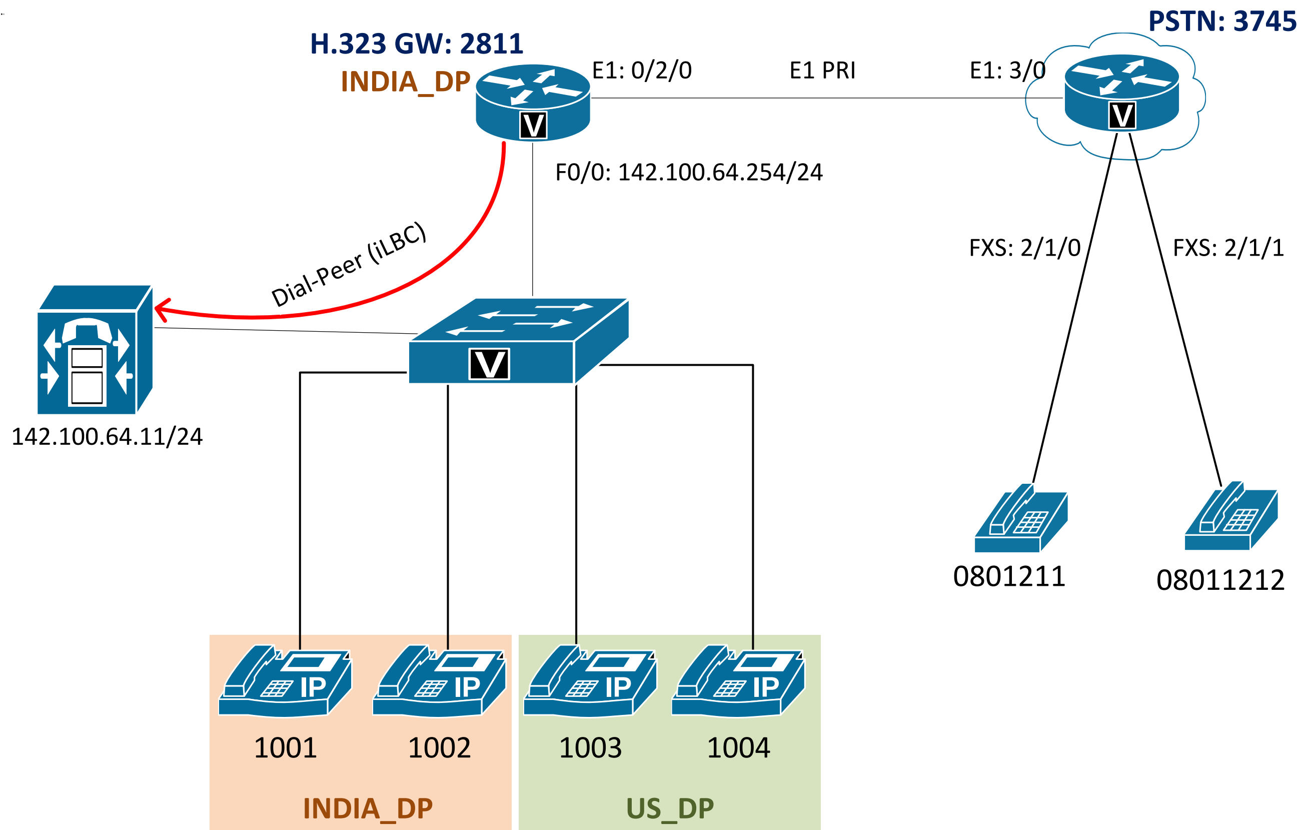
iSAC

GSMAMR (Global System for Mobile Communications Adaptive Multi-Rate)

H.263, 264 (Video codecs)

Pass through

Configuration of Transcoder (2811 Router Transcoding Configuration)



- Deploy CUCM as shown in figure
- Set Inter & Intra region codecs INDIA Region to US Region G.729
- Configure H.323 Gateway
- Configure PSTN Router with two analog phone

Router Side Configuration

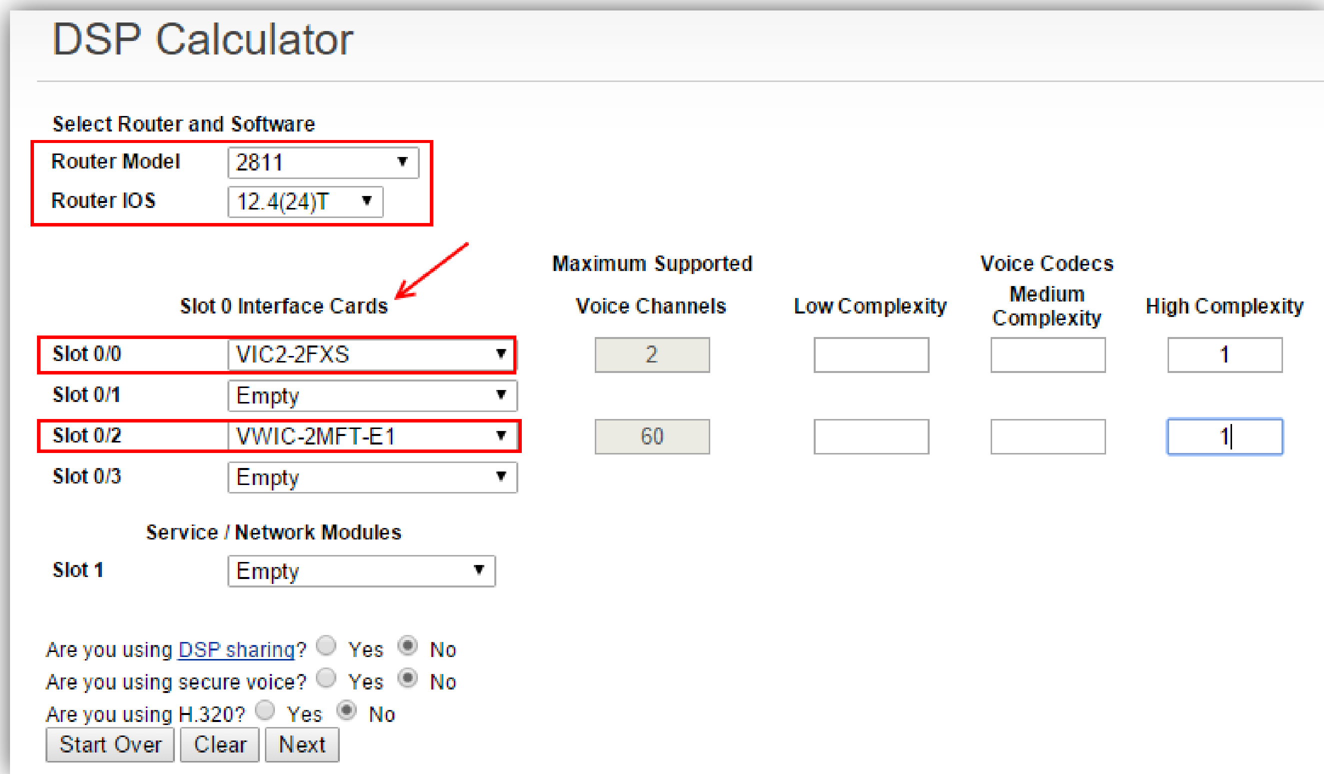
Step 1: Identification Hardware and IOS Version

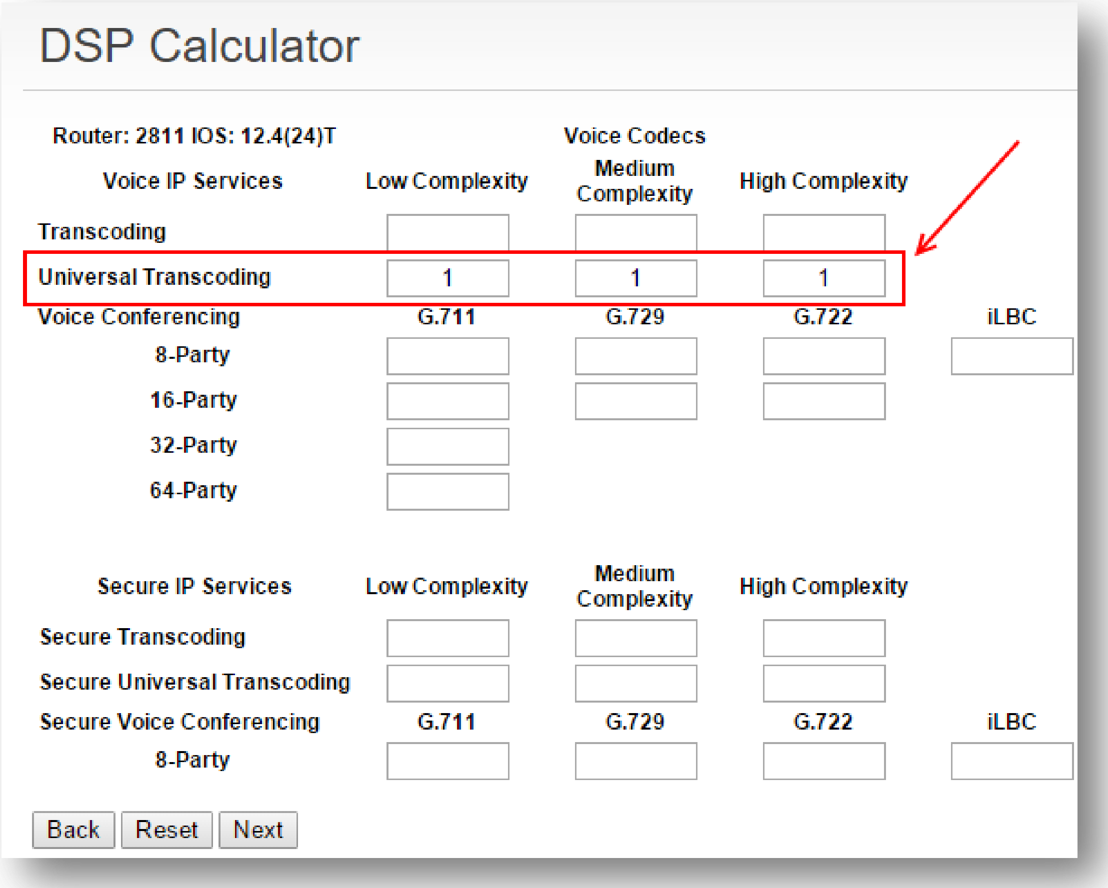
```
R1#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9_IVS_LI-M), Version
12.4(24)T6
```

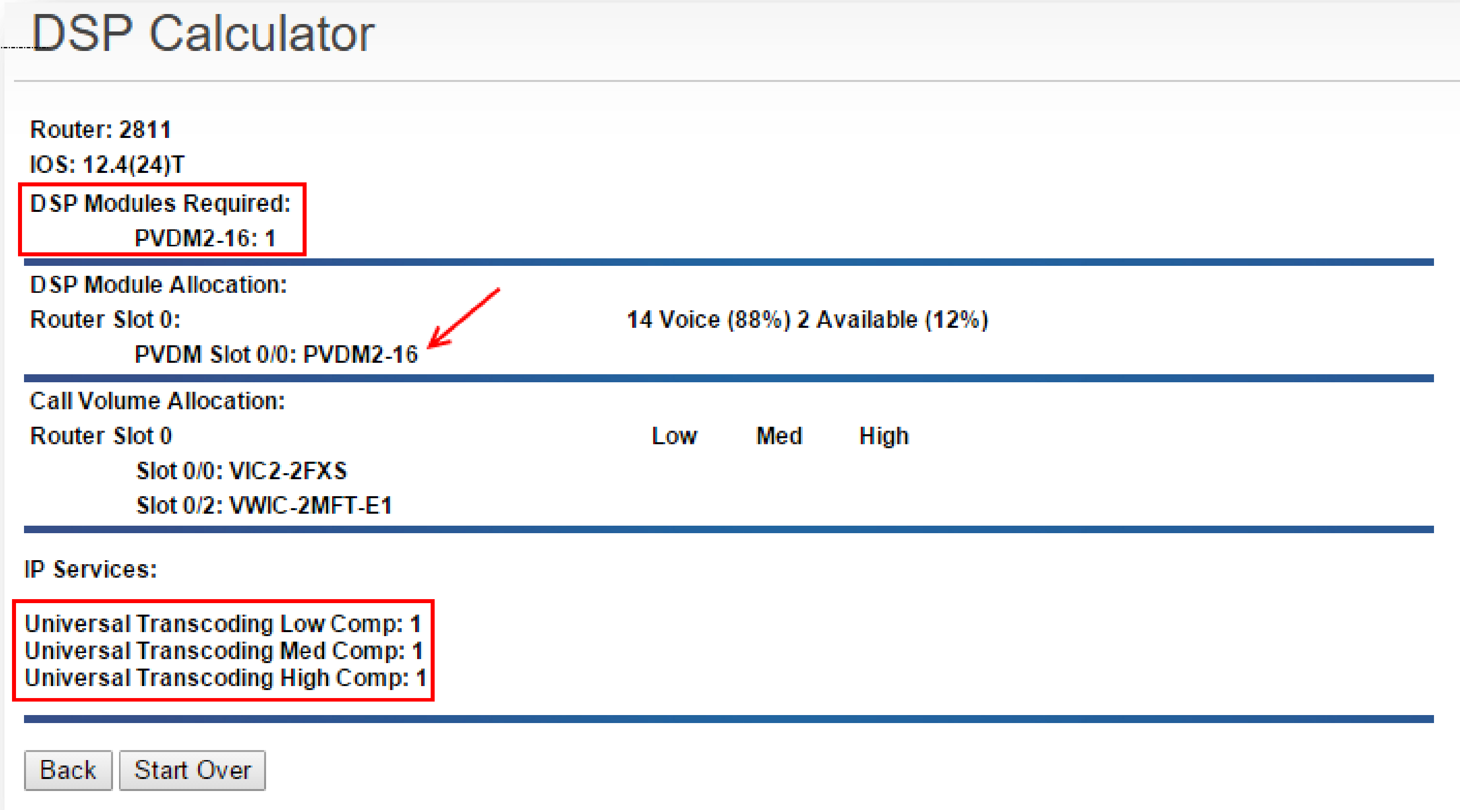
Step 2: Calculate DSPs Requirement

Based on the link calculate required DSPS for conferencing

http://www.cisco.com/web/applicat/dsprecal/dsp_calc.html




DSP Calculator
Router: 2811 IOS: 12.4(24)T
Voice Codecs
Voice IP Services
Low Complexity
Medium Complexity
High Complexity
Transcoding
Universal Transcoding
1
1
1
Voice Conferencing
G.711
G.729
G.722
iLBC
8-Party
16-Party
32-Party
64-Party
Secure IP Services
Low Complexity
Medium Complexity
High Complexity
Secure Transcoding
Secure Universal Transcoding
Secure Voice Conferencing
G.711
G.729
G.722
iLBC
8-Party
Back
Reset
Next



Step 3: Verify DSPs & Voice Card

```
------------------------------------------------------------------------------------------
R1#show inventory
NAME: "2811 chassis", DESCR: "2811 chassis"
PID: CISCO2811          , VID: V03 , SN: FHK1038F0YB

NAME: "2nd generation two port FXS voice interface daughtercard on Slot 0 SubSlot 0",
DESCR: "2nd generation two port FXS voice interface daughtercard"
PID: VIC2-2FXS          , VID: V01 , SN: FOC1134070Q

NAME: "WAN Interface Card - Serial (1T) on Slot 0 SubSlot 1", DESCR: "WAN Interface Card -
Serial (1T)"
PID: WIC-1T=            , VID: 1.0, SN: 34086087

NAME: "Two port E1 voice interface daughtercard on Slot 0 SubSlot 2", DESCR: "Two port E1
voice interface daughtercard"
PID: VWIC-2MFT-E1=      , VID: 1.0, SN: 29238096

NAME: "WAN Interface Card - Serial 2T on Slot 0 SubSlot 3", DESCR: "WAN Interface Card -
Serial 2T"
PID: WIC-2T=            , VID: 1.0, SN: 35419506

NAME: "PVDMII DSP SIMM with Two DSPs on Slot 0 SubSlot 4", DESCR: "PVDMII DSP SIMM with Two
DSPs"
PID: PVDM2-32           , VID: V01 , SN: FOC10500XQ9


GW#show voice dsp
```

```
DSP  DSP                DSPWARE CURR  BOOT                         PAK     TX/RX
TYPE NUM CH CODEC       VERSION STATE STATE   RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ========== ===== ======= === == ========= == ===== ============
----------------------------FLEX VOICE CARD 0 ------------------------------
                           *DSP VOICE CHANNELS*
CURR STATE : (busy)inuse (b-out)busy out (bpend)busyout pending
LEGEND     : (bad)bad    (shut)shutdown  (dpend)download pending
DSP   DSP                DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC       VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ========= ========== ===== ======= === == ========= == ==== ============
                           *DSP SIGNALING CHANNELS*
DSP   DSP                DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC       VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ========= ========== ===== ======= === == ========= == ==== ============
C5510 001 01 {flex}        24.3.6 alloc idle      0   0 0/0/0     02    0          42/0
C5510 001 02 {flex}        24.3.6 alloc idle      0   0 0/0/1     02    0          15/0
------------------------END OF FLEX VOICE CARD 0 ----------------------------
```

Step 4: Configure Voice Card

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

Step 5: Point Call Manager for SCCP Operations

```
GW(config)#sccp local fastEthernet 0/0
GW(config)#sccp ccm 142.100.64.11 identifier 1 version 7.0+
GW(config)#sccp ccm 142.100.64.12 identifier 2 version 7.0+ <BACKUP SERVER>
GW(config)#sccp
```

Step 6: DSP Farm Profile for Transcoding

```
GW(config)#dspfarm profile 1 transcode universal
GW(config-dspfarm-profile)#codec ilbc
GW(config-dspfarm-profile)#codec g711alaw
GW(config-dspfarm-profile)#codec g711ulaw
GW(config-dspfarm-profile)#codec g729r8
GW(config-dspfarm-profile)#maximum sessions 4
GW(config-dspfarm-profile)#associate application SCCP
GW(config-dspfarm-profile)#no shutdown
```

Step 7: CUCM Group & Registration Name

```
GW(config)#sccp ccm group 1
GW(config)#associate ccm 1 priority 1
GW(config-sccp-ccm)#associate profile 1 register XCODE-2811
```

CUCM Side Configuration

Step 8: Add Transcoder to CUCM

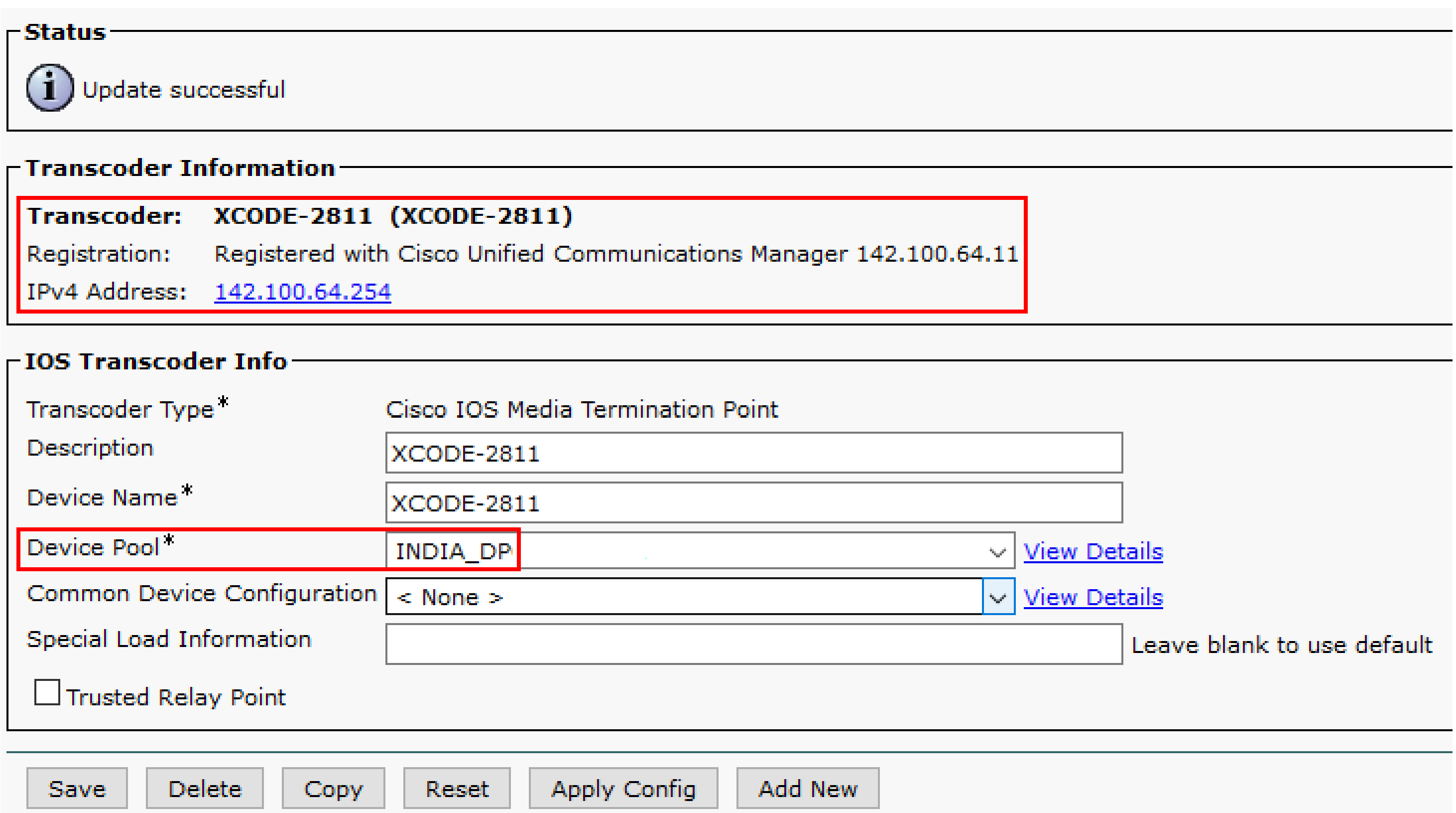
Media Resources → Transcoder → Add New

Transcoder Type* : Cisco IOS Media Termination Point

Description : XCODE-2811

Device Name* : XCODE-2811

Device Pool* : INDIA_DP



Step 9: Create Media Resource Group

Media Resources → Media Resource Group → Add New

Name* : MRG1

Description : Media Resource Group 1

Available Media Resources** : ↓↓↓↓↓↓

Selected Media Resources : XCODE-2811

→ Save

Step 10: Create Media Resource Group List (MRGL)

Media Resources → Media Resource Group List → Add New

Name* : MRGL1

Description : Media Resource Group List 1

Available Media Resource Groups* : ↓↓↓↓

Selected Media Resource Groups : MRG1

Step 11: Apply MRGL under Device Page or in Device Pool

Media Termination Point

- A MTP can bridge together two full-duplex voice stream and if necessary convert between G711 µ law and a law as well as different sample sizes.
- So as the MTP bridge is handling each stream independently, H.323 supplementary services can be supported.
- In other words, MTP will enhance H.323v1 with all these supplementary services(Call Park, Hold , Transfer , Conferencing,…).
- Pay attention also that you can use MTP in order to provide the translation between the out-of-band DTMF tones used by SCCP and SIP in-band (payload type) DTMF tones.

Role & Need of MTP

- In H.323 Gateway Fast Start requires MTP. Default is slow start it doesn't need MTP
- SIP Early Offer requires MTP (Before CUCM 8)
- For supplementary services like Call Hold, Call Transfer, MoH to PSTN calls
- SIP ICT needs MTP
- DTMF Relay in-band, out-band to communicate, we need MTP
- SCCP RSVP Agent requires MTP
- Trusted Relay Point
- Transrating: To change algorithm of Codecs (G.729ar8 to G.729r8, G.711alaw to G.711mlaw) - Need DSP, should be hardware based
- Repacketization of codecs: To change the sampling size (G.729 20msec sample size to 30msec sample size) – Need DSP, should be hardware based

Types of MTP

CUCM Based Software MTP:

- Call Manager the resource supports up to 24 MTP sessions
- Enabled by activating the Cisco IP Voice Media Streaming App service on Cisco Unified Communications Manager
- This MTP type can convert G.711 mu-law to G.711 a-law and vice versa.

- This MTP type can packetize conversion for a given codec; for example, when one call leg uses 20-ms sample size and the other call leg uses 30-ms sample size.

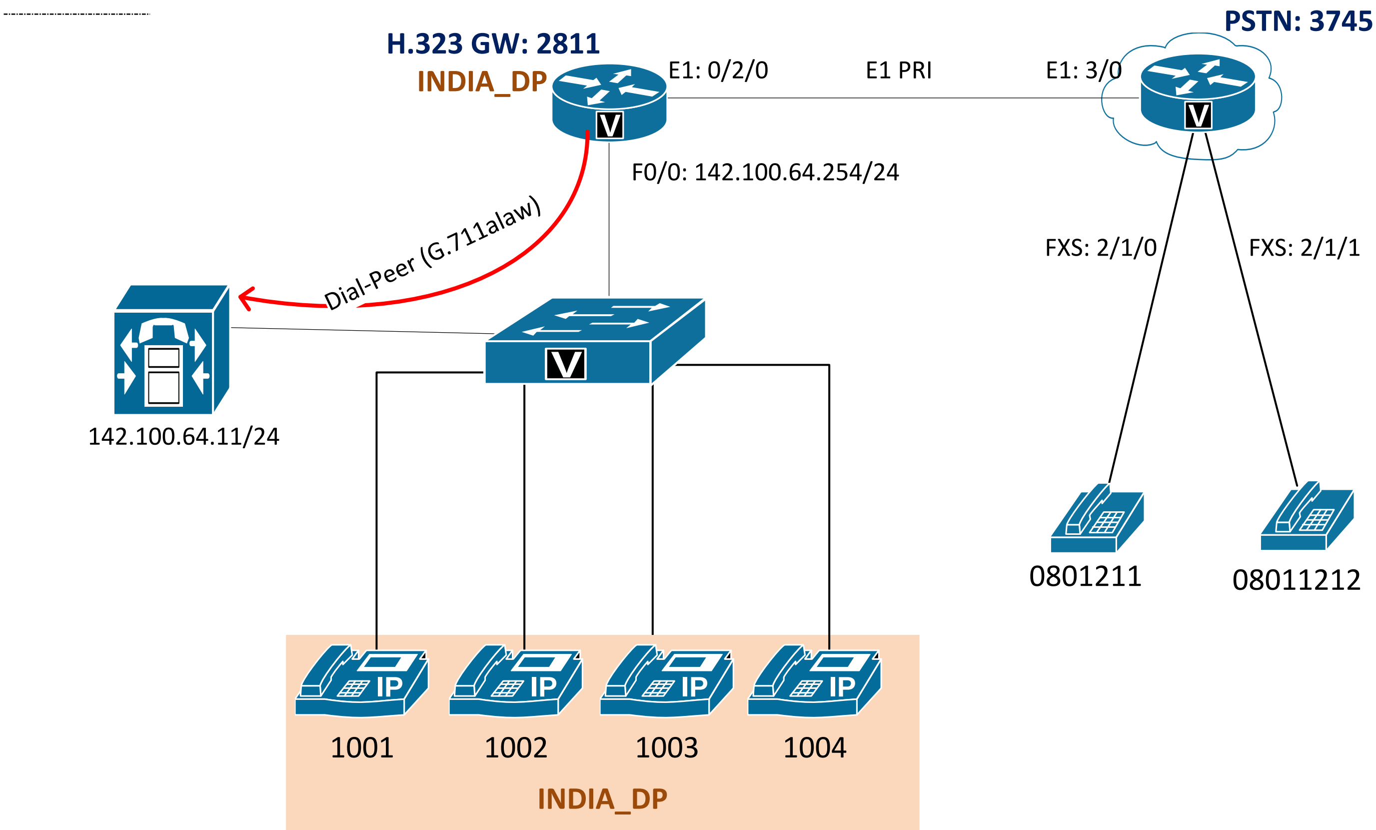
Cisco Router IOS Based Software MTP:

- Software MTP's are mostly used for DTMF internetworking, RSVP etc
- This MTP type does not require any DSP resources on the Cisco router.
- Configured by enabling Cisco IOS Software MTPs by using the **maximum session software n** command
- 500 software-based sessions can be configured.
- The codec and paketization of both call legs must be identical.
- This MTP type typically is used for Resource Reservation Protocol (RSVP) agent configurations or Cisco Unified Border Element media flow-through configurations.
- Cisco Unified Communications Manager does not differentiate between software and hardware-based Cisco IOS MTP configurations.
- Every Cisco IOS Software MTP is considered as hardware MTP in Cisco Unified Communications Manager.
- Cisco IOS Software MTPs are supported on the router only if the dsp services dspfarm command is not enabled on the voice card.

Cisco Router IOS Based Hardware MTP:

- MTP's are used for changing sampling rate, codec etc.
- DSP resources are required.
- Configure this MTP type by using the **maximum session hardware <n>** command.
- The maximum number of sessions is derived from the number of installed DSP resources on the Cisco IOS router.
- Use of the same audio codec but different paketization on both call legs is possible.

Configuration (CUCM Based Software MTP)



Step 1: Activate Cisco IP Voice Media Streaming App

Cisco Unified Service Ability → Tools → Service Activation → Cisco IP Voice Media Streaming App

Step 2: Verify MTP Registration & Device Pool

Go to Media Resources → Media Termination Point

Media Termination Point ***(1 - 1 of 1)*** ***Rows per Page*** 50

Find Media Termination Point where Name begins with [ ] Find Clear Filter

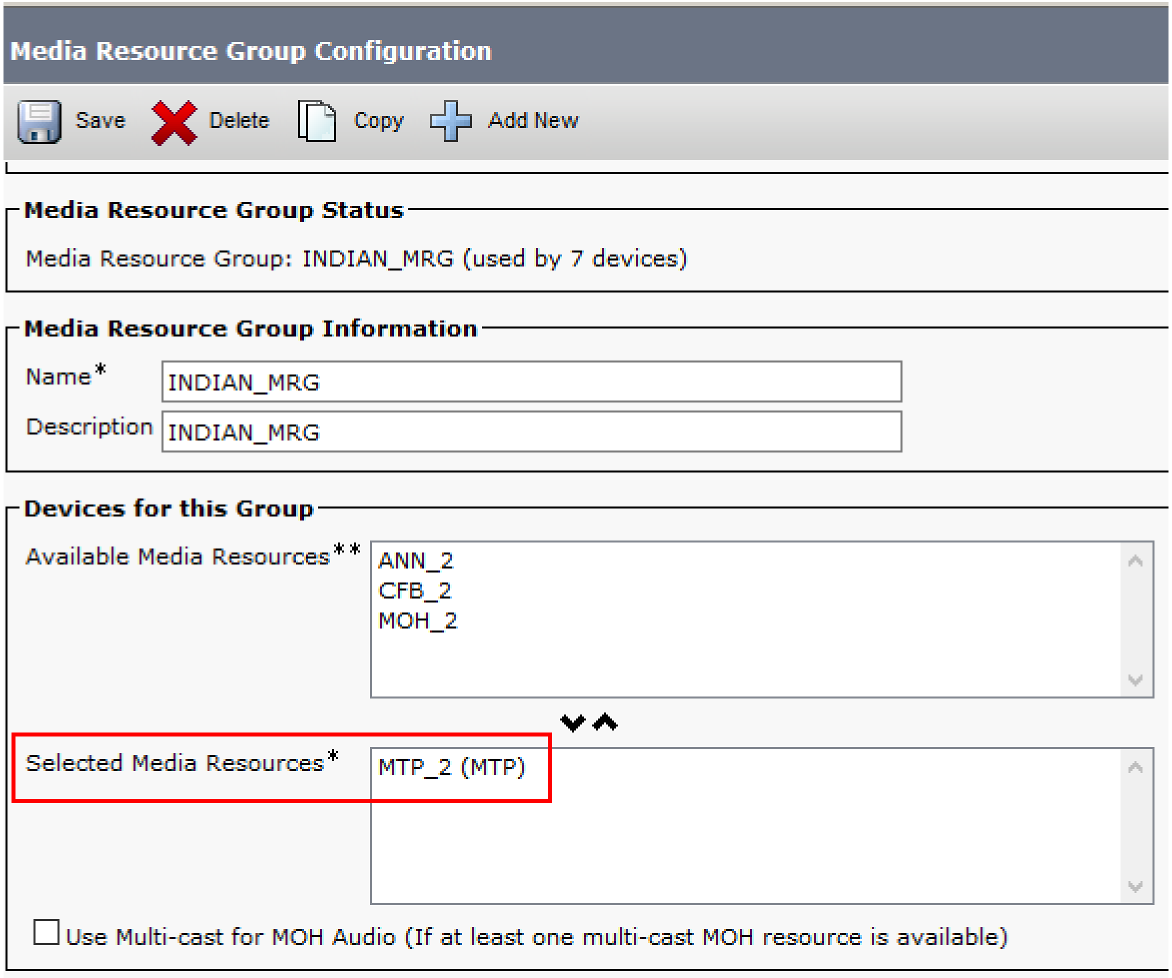
☐		Name ▲	Description	Device Pool	Status	IPv4 Address	Copy
	MTP	MTP_2	MTP_CUCM10-5-PUB	DP-INDIA	Unregistered	142.100.64.20	Not Allowed

Add New | Select All | Clear All | Delete Selected | Reset Selected | Apply Config to Selected

Change Device Pool if required.

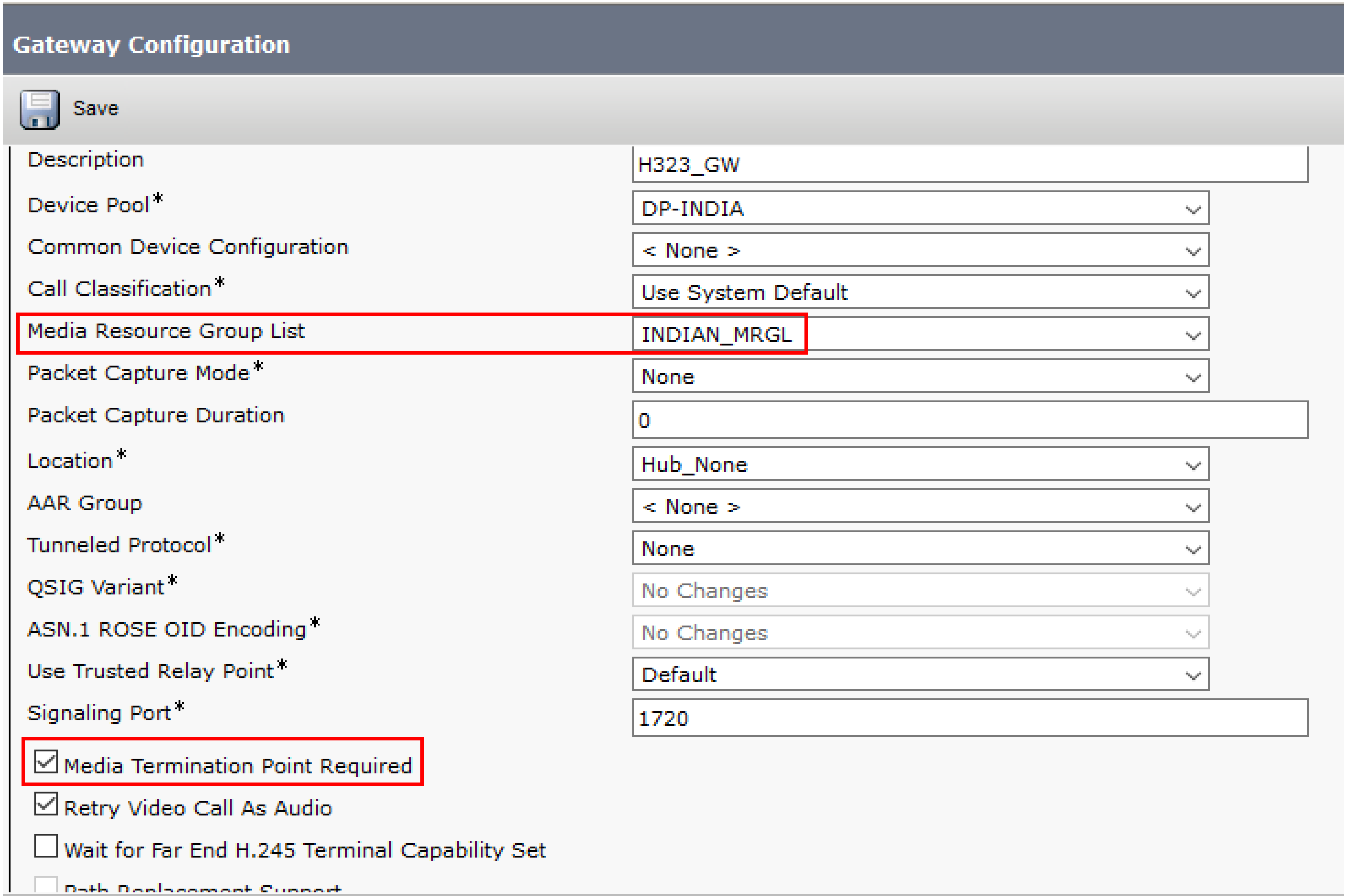
Step 3: Configure MRG & MRGL (Media Resource Access Control)

Add MTP_CUCM10-5-PUB to MRG and then configure MRGL. Apply under Device Pool



Step 4: Add H.323 Gateway

Now add an H.323 Gateway and check Media Termination Point Required box.



Create Route Pattern to call external

Step 5: Router Side

Configure dial-peers, ISDN, etc.

```
GW(config)#dial-peer voice 3 voip
GW(config-dial-peer)#destination-pattern 100.
GW(config-dial-peer)#session target ipv4:142.100.64.20
GW(config-dial-peer)#codec g711ulaw
```

Workaround: Call to analog phone and you can able to hold now. Try disabling IPVMA and see the difference.

Configuration (Cisco IOS Based Software MTP)

Step 1: Configure Voice Card

GW(config)#voice-card 0

GW(config-voicecard)#dspfarm

GW(config-voicecard)#dsp services dspfarm

Step 2: Point Call Manager for SCCP Operations

GW(config)#sccp local fastEthernet 0/0

GW(config)#sccp ccm 142.100.64.11 identifier 1 version 7.0+

GW(config)#sccp ccm 142.100.64.12 identifier 2 version 7.0+ <BACKUP SERVER>

GW(config)#sccp

Step 3: DSP Farm Profile for Transcoding

GW(config)#dspfarm profile 1 mtp

GW(config-dspfarm-profile)#codec g729r8

GW(config-dspfarm-profile)#codec g729ar8

GW(config-dspfarm-profile)#maximum sessions **software** 4

GW(config-dspfarm-profile)#associate application SCCP

GW(config-dspfarm-profile)#no shutdown

Step 4: CUCM Group & Registration Name

GW(config)#sccp ccm group 1

GW(config)#associate ccm 1 priority 1

GW(config-sccp-ccm)#associate profile 1 register MTP-2811

CUCM Side Configuration

Step 8: Add Transcoder to CUCM

Go to Media Resources → Media Termination Point → Add New

Media Termination Point Type*: Cisco IOS Enhanced Software Media Termination Point

Media Termination Point Name*: MTP-2811

Description : MTP-2811

Device Pool* : INDIA_DP

Step 9: Media Resource Access Control

Step 10: Apply MRGL under Device Page or in Device Pool

Configuration (Cisco IOS Based Hardware MTP)

Step 1: Configure Voice Card

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

Step 2: Point Call Manager for SCCP Operations

```
GW(config)#sccp local fastEthernet 0/0
GW(config)#sccp ccm 142.100.64.11 identifier 1 version 7.0+
GW(config)#sccp ccm 142.100.64.12 identifier 2 version 7.0+ <BACKUP SERVER>
GW(config)#sccp
```

Step 3: DSP Farm Profile for Transcoding

```
GW(config)#dspfarm profile 1 mtp
GW(config-dspfarm-profile)#codec g729r8
GW(config-dspfarm-profile)#codec g729ar8
GW(config-dspfarm-profile)#maximum sessions hardware 4
GW(config-dspfarm-profile)#associate application SCCP
GW(config-dspfarm-profile)#no shutdown
```

Step 4: CUCM Group & Registration Name

```
GW(config)#sccp ccm group 1
GW(config)#associate ccm 1 priority 1
GW(config-sccp-ccm)#associate profile 1 register MTP-2811
```

CUCM Side Configuration

Step 8: Add Transcoder to CUCM

Go to Media Resources → Media Termination Point → Add New

Media Termination Point Type*: Cisco IOS Enhanced Software Media Termination Point

Media Termination Point Name*: MTP-2811

Description : MTP-2811

Device Pool* : INDIA_DP

Step 9: Media Resource Access Control

Step 10: Apply MRGL under Device Page or in Device Pool

Annunciator

- An annunciator is automatically created while you activate Cisco IPVMS. A single annunciator instance can support the entire cluster.
- Annunciator registers with single CUCM in the device pool CUCM group configuration. Failover will occur automatically.
- Support 48 simultaneous streams by default (Call Manager + IPVMS).
- Supports 255 if standalone server selected

Media Resources → Annunciator

MoH (Music On Hold)

- The MoH sources makes music available to any on-net, off-net device placed on hold instead of default ‘Tone on Hold’.
- Audio codecs supported by MoH server are G.711 alaw, G.711 ulaw, G.722, G.729
- CME, SRST Gateways can be configured as MoH server also
- The CUCM integrated MoH server supports Unicast & Multicast streaming of music to the held party. Multicast method reduces the load of MoH server.
- Multicast also reduces the bandwidth because it enables multiple users to use the same audio stream. Multiple users will participate on the single audio stream.
- The recommended range of multicast IP is 239.1.1.1 to 239.255.255.255
- The MoH stream that an end point receives is determined by a combination two things. One is the source file configured in the Holding Party phone page. Other one is the MoH resource on the held party’s MRGL.

MoH Configurations

Step 0: Activate Cisco IP Voice Media Streaming App

Step 1: Plan MoH Server Capacity

- MCS7815, 7825 allows up to 250 users to be placed on hold with music. MCS7835, 7845 allows 500 users to placed on hold
- If MoH session exceeds the maximum limitations, various issues can arise like Poor MoH Quality, Unreliable MoH Operation, Loss of MoH Functionality
- To customize the capacity,

System → Service Parameters →

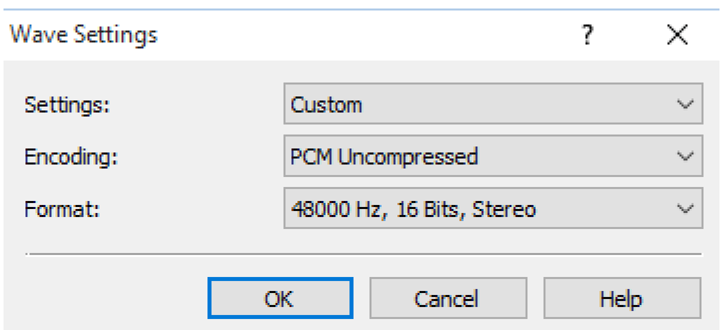
Maximum Half Duplex Streams: The number of device that can be placed on UNICAST MoH. Default value is 250

Maximum Multicast Connections: The number of device that can be placed on MULTICAST MoH. Default value is 30 that means 30,000 devices can get Multicast MoH

Step 2: Create MoH file

The format of MoH file is 16 bit PCM .WAV, Stereo or Mono. 8, 16, 32, 48 kHz sampling rate

Using any Audio converter application you can generate this file. (I have used WavePad Sound Editor)



Step 3: Upload MoH Audio Source

Media Resources → MoH Audio File Management → Upload File

Select the file and upload

(Here I'm adding two audio files for different phones)

Step 4: Configure MoH Audio Source (Assigning numbers to Audio Files)

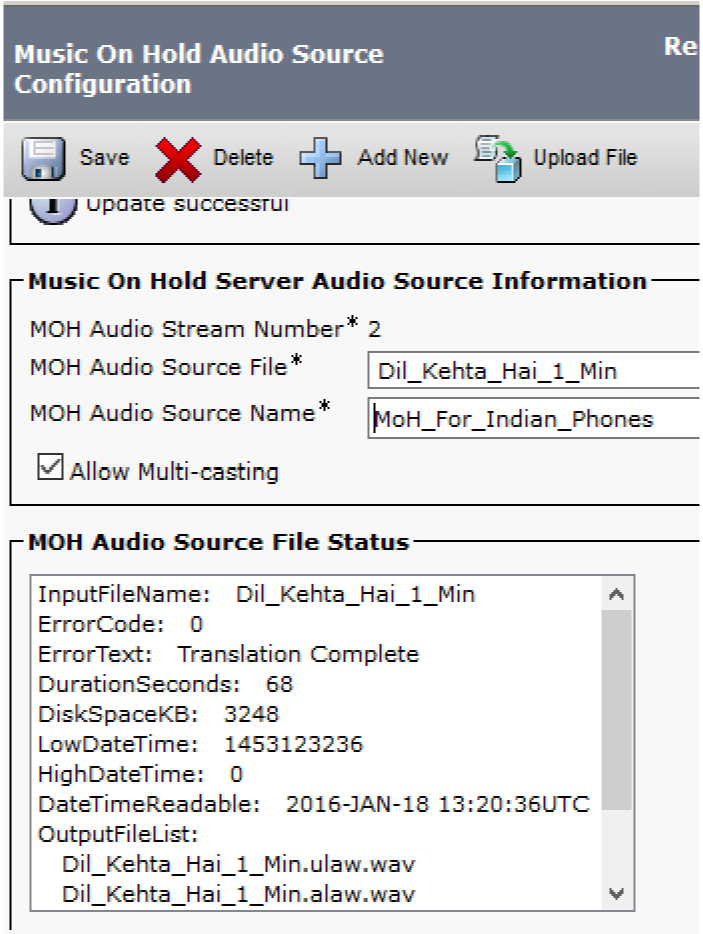
Media Resources → MoH Audio Source → Add New

MOH Audio Stream Number* : 2

MOH Audio Source File* : Dil_Kehta_Hai_1_Min

MOH Audio Source Name* : MoH_For_Indian_Phones

Check Allow Multi-casting



Media Resources → MoH Audio Source → Add New

MOH Audio Stream Number* : 3

MOH Audio Source File* : Inna_In_Your_Eyes_1_Min

MOH Audio Source Name* : MoH_For_US_Phones

Check Allow Multi-casting

Step 5: Configure MoH Server

Media Resources → Music On Hold Server → Select Server <HOH_2>

Configure Device Pool, Maximum Half Duplex Streams and Maximum Multi-cast Connections

Step 6: Customize Service Parameters

System → Service Parameters → Select Server → Service: IPVMS

Supported MOH Codecs* : Select required codec by holding Control Key

→ Save

System → Service Parameters → Select Server → Service: Call Manager (Active)

Suppress MOH to Conference Bridge: True

Default Network Hold MOH Audio Source ID: 2

Default User Hold MOH Audio Source ID: 3

Step 7: Specify MoH Files Under Device

Device → Phones → <Select Phone>

User Hold MOH Audio Source : 2-MoH_For_Indian_Phones

Network Hold MOH Audio Source : 2-MoH_For_Indian_Phones

Step 8: Configure MRGL

MoH Multicast

Media Resources → Music On Hold Server → Select Server <HOH_2>

Multi-cast Audio Source Information

Check Enable Multi-cast Audio Sources on this MOH Server

Base Multi-cast IP Address*: 239.1.1.1

Base Multi-cast Port Number*: 16384

Increment Multi-cast on* : Port

Selected Multi-cast Audio Sources:

Max Hops: 4

Media Resource Access Control

- All media resources are located in a null media resource group by default. Usage of media resources is load balanced among all existing one.
- Media Resource management controls and manages the availability of media resouces with in the cluster.

Media Resource Group (MRG): Logical grouping of all media resources

Media Resource → Media Resource Group → Add New

Name* : HW_CFB_MRG

Description: Hardware Conference Bridges MRG

Available Media Resources : ↓↓↓↓↓

Selected Media Resources : ↓↓↓↓↓-

→ Add New

Name* : XCODE_MRG

Description: Transcoders

Available Media Resources : ↓↓↓↓↓

Selected Media Resources : ↓↓↓↓↓-

→ Add New

Name* : MOH_MRG

Description: Music on Hold

Available Media Resources : ↓↓↓↓↓

Selected Media Resources : ↓↓↓↓↓-

Media Resource Group List (MRGL): Specifies a list of prioritized MRGs. MRGL is assigned to a Device or Device pool.

Media Resource → Media Resource Group List → Add New

Name* : Indian_MRGL

Available Media Resources Groups : ↓↓↓↓↓

Selected Media Resources Groups : ↓↓↓↓↓-

Assign MRGL to Device Pool,

System → Device Pool → Media Resource Group List: Indian_MRGL