Implementing Cisco Unified Communications Manager, Part 2 (CIPT2)

Guide Version 1.0

Abdul Jaseem VP

CIPT-2 Guide 1.0 (55 Pages)
(Release Date 21/Mar/2016)

Syllabus

- Cisco IP Phone Services
- Implementing Extension Mobility
- Cisco Unified Mobility (SNR, Mobile Voice Access)
- Identifying issues in multisite deployment
- Identifying multisite deployment Solutions
- Implementing Cisco Unified SRST and MGCP fallback
- Implementing CME SRST
- Implementing Bandwidth management
- Implementing Call Admission Control

IP Phone Services

- Cisco IP Phones services are applications that use the web client or server and XML capabilities of Cisco IP Phone. IP Phone firmware contains a micro web browser that enables limited web browsing capability.
- E.g. Used in hotels to order food menu, To know the temperature, weather, etc.
- Administrator or End user can subscribe these services to an IP Phone. After subscription user can access the specified services offered by the network
- Administrator can also provision service with Enterprise Subscription that applies to all devices

Following list represents some of the configuration parameters related to IP phone services and XML operations

System → Enterprise Parameter →

URL Authentication: Points to authenticate.jsp service. (Java Server Page (JSP) is a technology for controlling the content or appearance of Web pages). This URL used to validate push requests from an IP Phone.

Default value is http://<CUCM IP>:8080/ccmcip/authenticate.jsp

URL Directories: URL points xmldirectory.jsp service. It generates and return directory menu that presented when user pushes Directory button (book icon). Missed call list, dialed list etc.

Default value is http://<CUCM IP>:8080/ccmcip/xmldirectories.jsp

URL Idle: Points to a service that provides text or image to be displayed on the phone screen when the phone is idle

Default value is Blank

URL Idle Time: Parameter indicates the time in seconds that a phone waits before initiating URL idle service

URL Information: It points GetTelecasterHelpText.jsp service in CUCM. It provides help or call statistics when user pushes '?/ i' button.

Default value is http://<CUCM IP>:8080/ccmcip/GetTelecasterHelpText.jsp

URL Services: It points to getservicesmenu.jsp services. It provides list of user subscribed services for the phone when the user presses the service (Globe) button

Default value is http://<CUCM IP>:8080/ccmcip/getservicesmenu.jsp

Default IP Phone Services

Device → Device Settings → Phone Services

IP Phone Service (1 - 7 of 7)

Find IP Phone Service where IP Phone Service begins with

	IP Phone Service	Description	Ent
☐	Corporate Directory	Corporate Directory	true
☐	Intercom Calls	Intercom Calls	false
☐	Missed Calls	Missed Calls	true
☐	Personal Directory	Personal Directory	true
☐	Placed Calls	Placed Calls	true
☐	Received Calls	Received Calls	true
☐	Voicemail	Voicemail	true

IP Phone Service Subscriptions

To use Cisco IP phone service, you need to subscribe the configured service to IP phones. Subscription can be done by administrator from Admin page or by the user from user page.

Administrator Service Subscription

Go to Device → Phone → Subscribe/ Unsubscribe from related links → <Select Service> → Next → Subscribe

End User Service Subscription

Login to CUCM User page → Device → Phone Services → Add New → <Select Service> → Next → Save

Extension Mobility

- Allows roaming users to login to any device and get their personal settings such as Line number, Speed dial, Forward settings, calling privileges, Music on Hold source etc. Device specific parameter remain the same
- Instead of configuring phones for users we just are creating Device Profile. It is a virtual phone that is able to move around to whatever phones the user logs into.
- The configuration changes are triggered by a user login with a user ID & password, when the user stops using the phone, he logs out and default configuration reapplied
- It is implemented as a phone service and works on single cluster. From CUCM8 onwards Extension Mobility Cross Cluster (EMCC) can be implemented.

Parameters that are changed while evoking device profile to an IP Phone

- Line CSS Pulled from Device Profile
- Device CSS remains same

Configuration

Step 1: Enable Extension Mobility Service

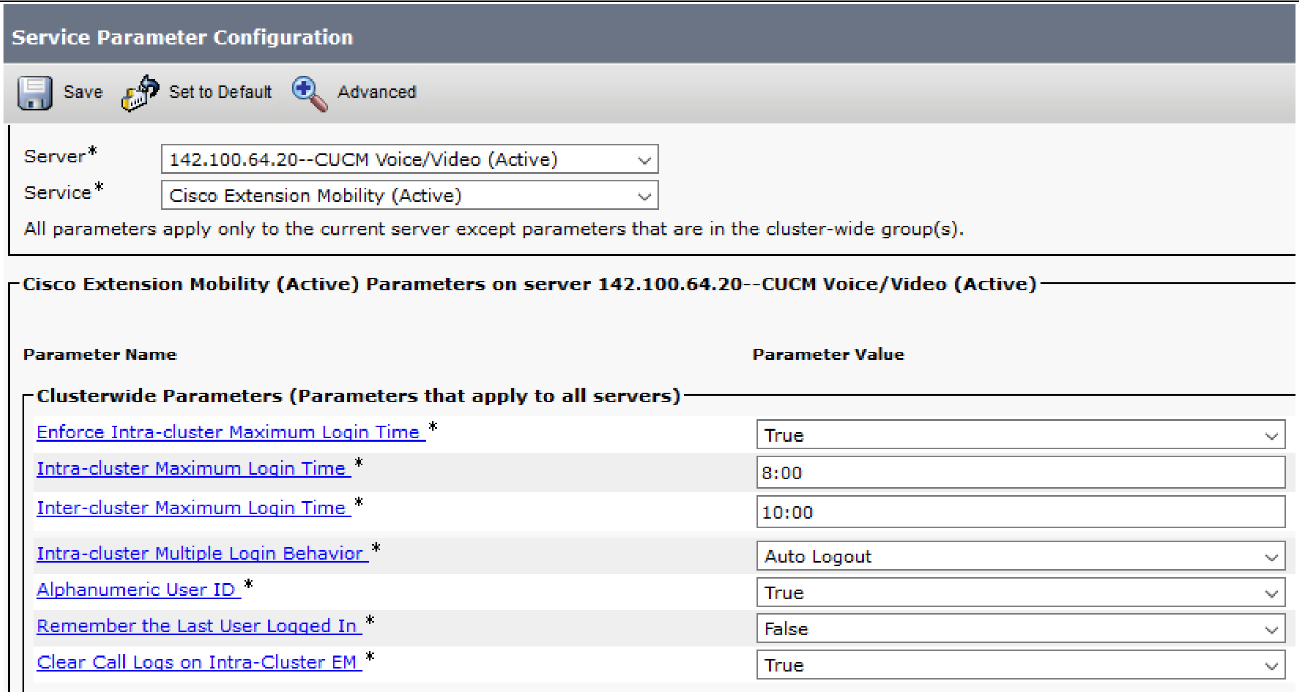
Service Ability → Tools → Service Activation → Cisco Extension Mobility

Step 2: Configure Enterprise Parameters

System → Service Parameters →

<Select Server> →

Service: Cisco Extension Mobility (Active)



Enforce Intra-cluster Maximum Login Time: This parameter determines whether a maximum login time is enforced for local login.

True: login time is enforced or

False: No time limit for logins

Intra-cluster Maximum Login Time: This parameter specifies the maximum time that a user is allowed to be locally logged in to a device. (Default 8 hours). After 8 hours the user automatically logged out. The system ignores this parameter if the Enforce Maximum Login Time parameter is set to False.

Inter-cluster Maximum Login Time This parameter specifies the maximum time that a user is allowed to be remotely logged in to a device in EMCC mode. EMCC always enforce auto logout based on this value irrespective of the value of Enforce Maximum Login Time parameter. (Default is 10 Hours)

Intra-cluster Multiple Login Behavior: This parameter specifies the behavior for multiple attempted logins by the same user on different devices within the same cluster.

1. *Multiple Logins Allowed* (the same user ID can be logged in to extension mobility on more than one device),
2. *Multiple Logins Not Allowed* – default (a user ID can only be logged into one device)

3. *Auto Logout* (if a user ID is logged into extension mobility on one device, and the same user ID attempts to login to extension mobility on a different device, the first device automatically logs out).

For EMCC, multiple login is always allowed.

Alphanumeric User ID: This parameter specifies whether the user ID to be used is alphanumeric or numeric.

True: User ID is alphanumeric

False: User ID is numeric

Remember the Last User Logged In: This parameter specifies whether the user ID of the last user logged in on a phone is remembered by the extension mobility application.

True: remember the last user ID

False: Do not remember the last user ID.

(For greater security, use the default value of False)

Clear Call Logs on Intra-Cluster EM: This parameter determines whether the call information stored on the phone directory (missed calls, placed calls, received calls) is cleared when a user manually logs in or out of a phone in the same cluster.

True: The phone deletes the call information

False: The phone does not delete the call information and subsequent phone users can review the missed, placed, and received call information.

(For Extension Mobility Cross-Cluster (EMCC), the call log is always cleared when the user logs in or out of a phone)

Step 3: Create Extension Mobility Service

Device → Device Settings → Phone Services → Add New

Service Name* : Extension_Mobility

Service Description : Extension_Mobility

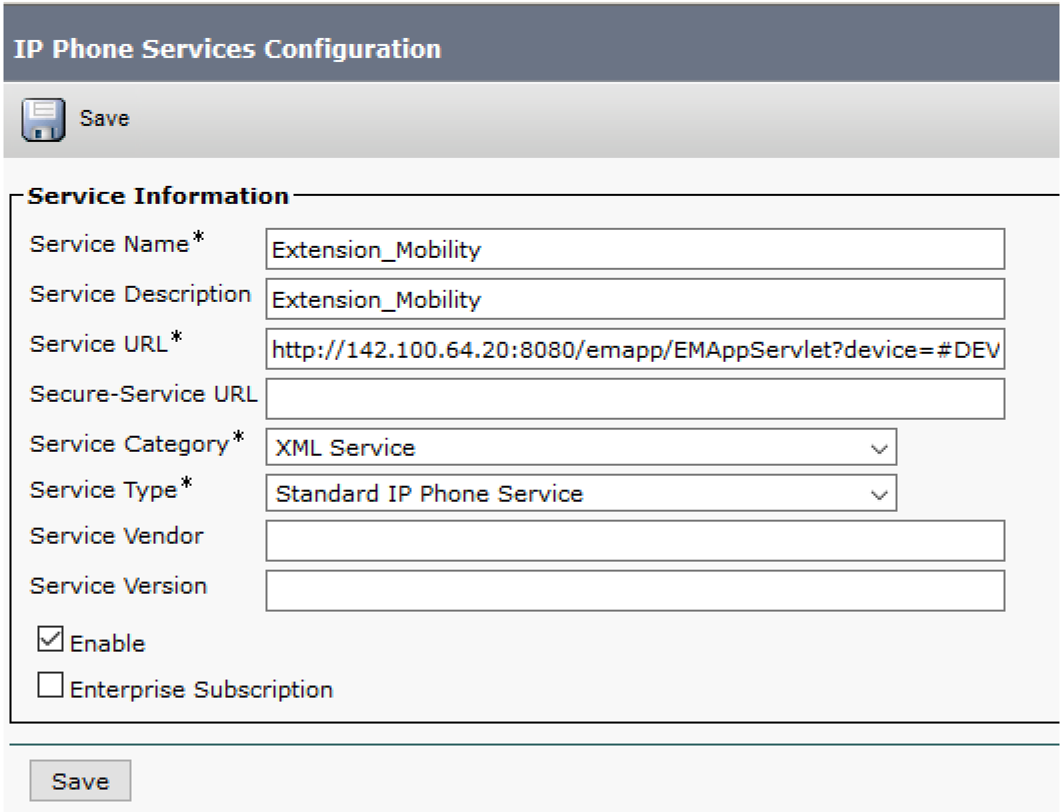
Service URL* : http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#

Service Category * : XML Service

Service Type* : Standard IP Phone Service

Check Enable Check box

(Once you check Enterprise Subscription bot, the service will be subscribed to all the phones)



Step 4: Configuring User Device Profile (User Phone is 7960)

Looks and feel like an IP Phone. User Device Profiles are created based on the model of IP Phone. It stores user specific phone configuration in logical profile.

Device → Device Settings → Device Profile → Add New

Device Profile Type* : Cisco 7960

Protocol : SCCP

Device Profile Name : JASEEM-Cisco 7960 SCCP Device Profile

Description : JASEEM-Cisco 7960 SCCP Device Profile

Phone Button Template*: Standard 7960 SCCP

Softkey Template : Standard User

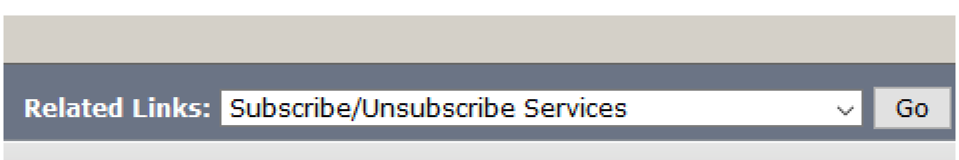
→ Save

Line [1] - Add a new DN

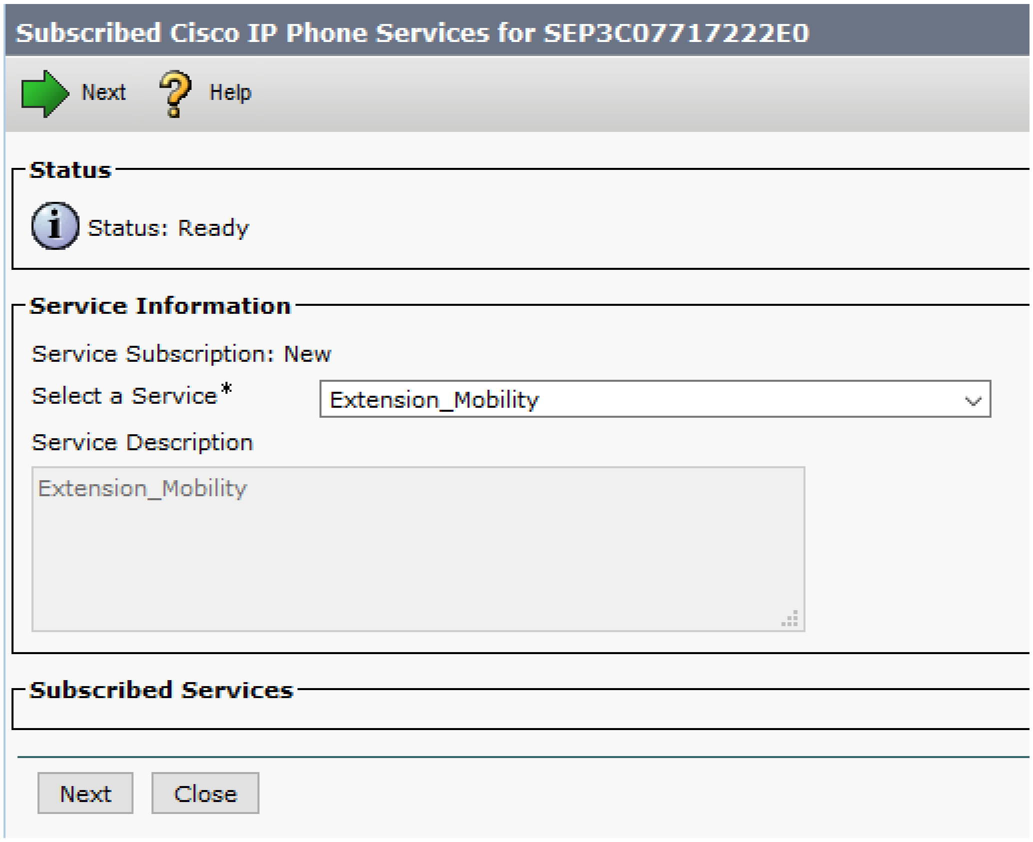
Directory Number : 2828

Step 5: Subscribe Extension Mobility Service to Device Profile

Related Links: Related Links: Subscribe/Unsubscribe Services → Go



→ Next → Subscribe



[Note: This is required to logout from a phone]

Step 6: Configuring Default Device Profile

- It's a generic profile which has the softkey template, Button template. If the user is login to another model, default device profile will be applied to the phone and merged with User Device Profile contents.
- E.g. 7961 having 6 line buttons. When the user logins to 7911, the primary line will be taken.

- For the sake of the lab environment I’m just considering 7960 (6 Line buttons) and 7940 (2 Line buttons)
- Default device profile won’t be applied if user tries to login same phone series model (e.g. 7960, 7961, 7965) instead Feature Safe function enabled by deault.
- So create default device profile for 7940 (Actually we have to create this for all the existing phones in the organization)

Device → Device Settings → Default Device Profile →

Device Profile Type* : Cisco 7940

Description : Cisco 7940 SCCP Default Device Profile

Phone Button Template*: Standard 7940 SCCP

Softkey Template : Standard User

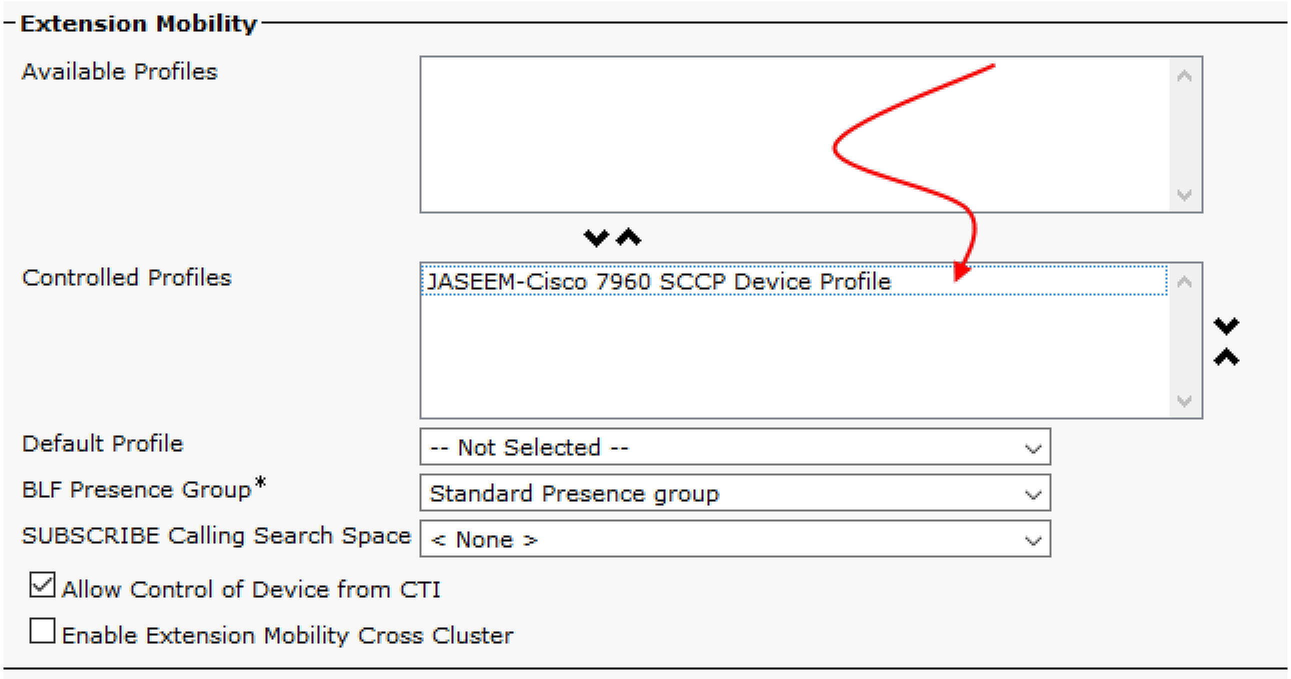
→ Save

[Note: Once you enable Extension Mobility on a phone, its default device profile will be created automatically]

Step 7: Link End User with Device Profile

User Management → End User →

Under Extension Mobility associate Device Profile that we created in step 4

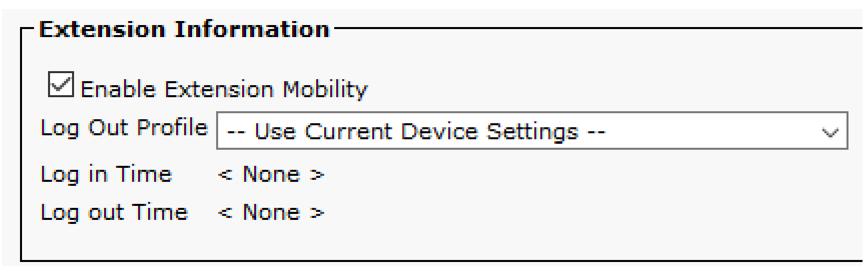


(Note: If user associated with multiple profiles, he must choose the device profile to be used)

Step 8: Enable & Subscribe Extension Mobility to Phones

Device → Phone → <Select Phone> → Under Extension Information

Check Enable Extension Mobility box



Related Links: Subscribe/Unsubscribe Services → Go

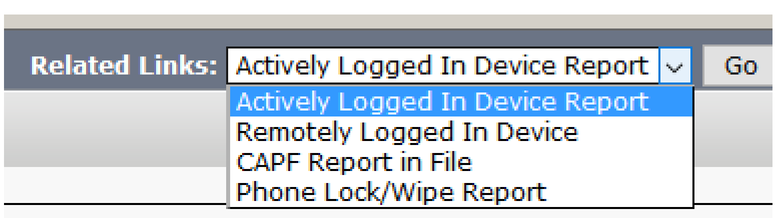
Select a Service*: Extension_Mobility (Created in Step 3)

→ Next → Subscribe

How to Login?

Push Services button → Select Extension_Mobility

To see logged in devices, go to Device → Actively Logged In Device Report → Go



Extension Mobility Issues

Error: Host not found

Resolution:-

- Check that the Cisco Tomcat service is running by choosing Cisco Unified Serviceability > Tools > Control Center—Network Services
- If you have changed the IP address on service URL then click on "Update subscriptions" (Device > Device Settings > Phone Services >IP Phone Services Configuration) and resubscribe each phone to which the wrong service was subscribed.

You can't see the EM feature after hitting the services button

Resolution:-

- Verify that you have configured the Extension Mobility service
- Verify the service URL is correct
- Start/Restart the EM services on each node you are running.

You can't log in/out of the EM feature but you can see it after pressing the services button

Resolution:-

- This error comes when you haven't enabled the extension mobility, subscribed the phones/device profiles to the service as needed and haven't associated user to a device profile.

Error: - To set up speed dials and other services from your phone, please goto https://x.x.x.x:8443/ccmuser/showHome.do

Resolution:-

- The above error comes when you haven't subscribed the phone or device profile to the EM profile. Once this is done you should be able to see the EM profile and log in correctly.

Error:-After a user logs out and the phone reverts to the default device profile, the user finds that the phone services are no longer available.

Resolution:-

- Check the Enterprise Parameters to make sure that the

Synchronization between Auto Device Profile and Phone Configuration: True

- Subscribe the phone to the Cisco Extension Mobility service.

Error:-After performing a login or logout, the user finds that the phone resets instead of restarting.

Resolution:-

- Locale change may provide the basis for reset.
- If the User Locale that is associated with the login user or profile is not the same as the locale or device, after a successful login, the phone will perform a restart that is followed by a reset.
- This occurs because the phone configuration file is being rebuilt.

Extension Mobility Error Codes

Error[201]-Authentication error

Resolution:-

- The user should check that the correct User ID and PIN were entered; the user should check with the system administrator that the User ID and PIN are correct.

Error [22]-Dev.logon disabled

Resolution:-

- Make sure that you have chosen "Enable Extension Mobility" check box on the Phone Configuration window.

Error [205]-User Profile Absent

Resolution:-

- Make sure that you have associated a Device Profile to the user.

Error [208]-EMService Conn. error

Resolution:-

- Verify that the Cisco Extension Mobility service is running by choosing Cisco Unified Serviceability > Tools > Control Center—Feature Services

Error [25]-User logged in elsewhere

Resolution:-

- Check whether the user is logged in to another phone. If multiple logins need to be allowed, ensure the Multiple Login Behavior service parameter is set to Multiple Logins Allowed

Error:- Http Error [503]

Resolution:-

- If you get this error when Services button is pressed, check that the Cisco Communications Manager Cisco IP Phone Services service.
- If you get this error when you select Extension Mobility service, check that the Cisco Extension Mobility Application service is running by choosing Cisco Unified Serviceability > Tools > Control Center—Network Services.

Error:- [202]-Blank userid or pin

Resolution:-

Enter a valid userid and PIN.

Error:- [26]- Busy, please try again

Resolution:-

- Check whether the number of concurrent login/logout requests is greater than the Maximum Concurrent requests service parameter. If so, lower the number of concurrent requests.
- To verify the number of concurrent login/logout requests, use Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool to view the Requests in Progress counter in the Extension Mobility object.

Error:-[6]-Database Error

Resolution:-

- Check whether a large number of requests exists
- If large number of requests exists, the Requests In Progress counter in the Extension Mobility object counter specifies a high value. If the requests are rejected due to large number of concurrent requests, the Requests Throttled counter also specifies a high value.

Error:- [207]-Device Name Empty OR Error:- XML Error [4] Parse Error

Resolution:-

- Check that the URL that is configured for Cisco Extension Mobility is correct and there should be no space in between.

Error:- 8945 phone does not show EM service

Resolution:-

Set service provisioning to default or internal. Refer Bug CSCtx70127

Error:-[http-8080-9]

EMX509TrustManager - checkServerTrusted: BSCUCM001.blocksolutions.local Certificate not found in the keystore : the certificate chain is not trusted, Could not validate path.

Resolution:-

- Go to Certificat managent under security
- Delete/Add Cisco Tomcat Cert
- Restart Cisco Tomcat service,Cisco Trust verification service and EM service.
- Try login to EM.

Error:- Login is unavailable(213)

Resolution:-

- This error comes when the device or phone load does not support EMCC (eg. non-supported phone models, supported phone models with older phone load).It could also be the incorrect service URL and/or secure Service URL.

Error:- Untrusted IP Error

Resolution:-

- This error comes when "Validate IP Address" service parameter is set to true and user tries to login/logout from a machine whose IP address is not trusted i.e. not listed in Trusted List of Ips service parameter)

Error:- Extension mobility fails after upgrade to 8.0.3

Resolution:-

- In the CUCM OS Administration page, re-generate the "Tomcat" certificates in all the nodes in the cluster. When the certificate is re-generated, the new certificate will be updated in the DB and CertMgr component should create the tomcat-trust.keystore file.
- Restart Tomcat in all the nodes.

Error:- 79XX phones cannot access certain SURLs when running firmware 9-0-3+

Resolution:-

- Access the service from the services button on the phone or downgrade the phone firmware to 9-0-2SR2 or earlier.

Login Server Connection Error

Resolution:-

If you are running Cisco Call Manager Extension Mobility on an IBM-340 platform, check that the system allows anonymous access to the Login Service web site.
And talso check the URL of the Login Service may not be configured properly in the LDAP directory. Check that the URL is correct.

Cisco Unified Mobility: Mobile Connect SNR (Single Number Reach)

- A user IP Phone number becomes the single number by which all the various other devices that the person uses can be reached including Mobile phone, Home phones, etc.
- Mobile Connect provides maximum flexibility and reachability.
- Somebody can call to your Cisco IP Phone in the office and the call sends out to multiple destinations outside to the CUCM network such as Mobile Number, Home landline number, etc.
- Suppose the user answered the call on his mobile phone while on the way to office, when he gets to the desk he can transfer the active call to his desk phone by pressing s soft key (Resume) after disconnecting the active call. The active call seamlessly transferred to desk phone and the user may not even realize that.
- Same way the active call on user's IP phone can be pushed to mobile phone by hitting 'Mobility Softkey'

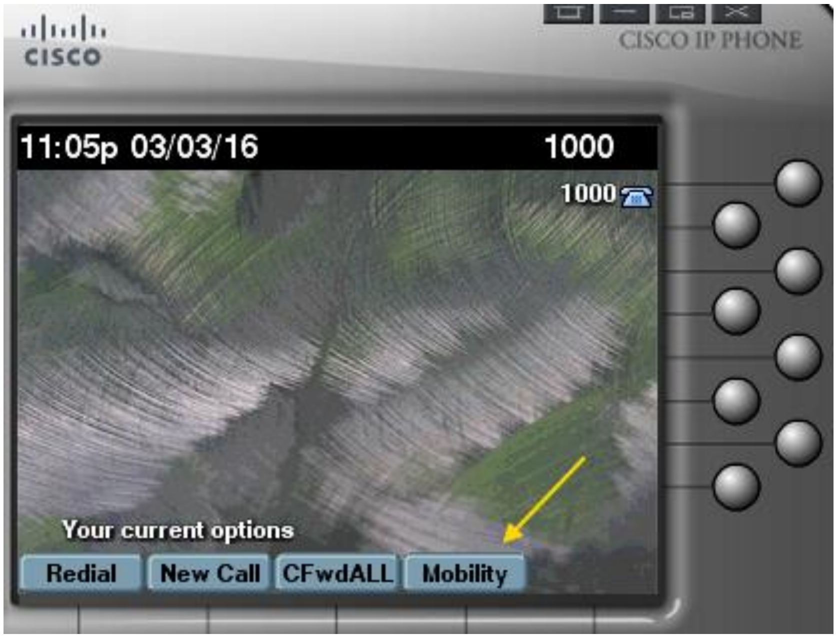
Configurations

Step 1: Add Mobility Softkey

Device → Device Settings → Softkey Template → Add New

Configure Mobility Softkey in On-Hook as well as Connected state.

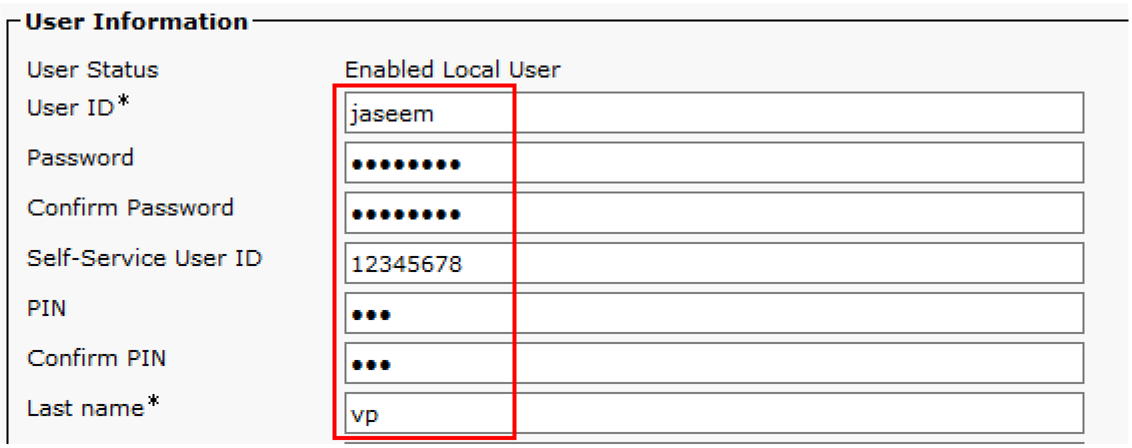
Apply to the phones.



Press Mobility Softkey and Enable and Disable the feature

Step 2: Configure End User

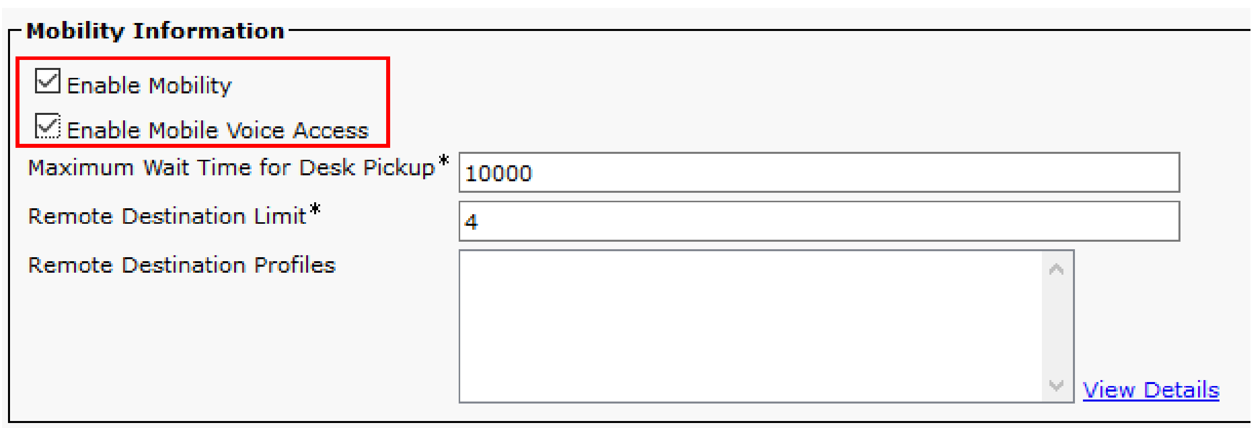
User Management → End User → Add New



Check Enable Mobility & Mobile Voice Access

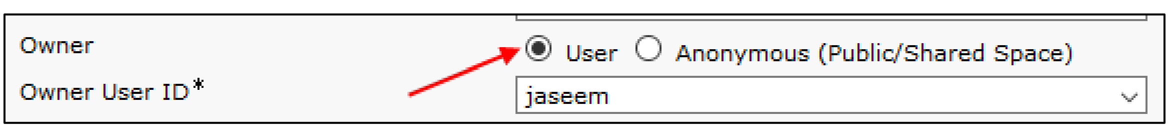
Maximum Wait Time for Desk Pickup : 10000 (Mille seconds)

Remote Destination Limit : 4



Step 3: Associate End User to IP Phone

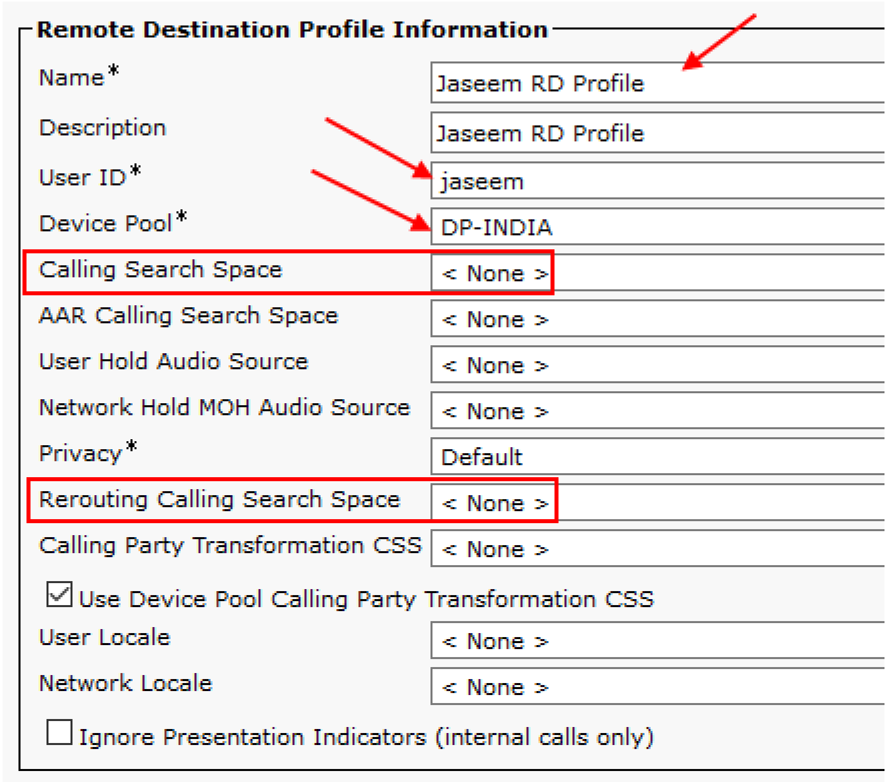
Go to device page and associate owner user ID as the new user



Step 4: Add Remote Destination Profile (Shared Lines)

Remote Destination Profile connects multiple destination number. It is shared line having the same number of your IP Phone. We can consider it like a virtual phone.

Device → Device Settings → Remote Destination Profile → Add New



Name* : Jaseem RD Profile

Description : Jaseem RD Profile

Device Pool : <Select Proper>

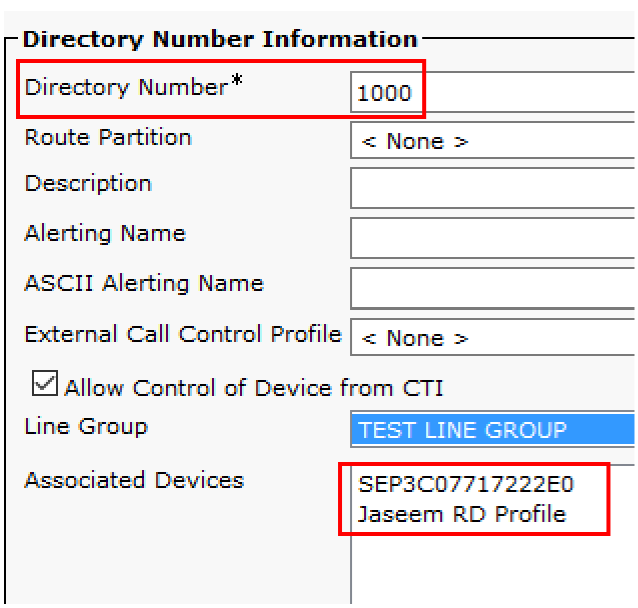
Calling Search Space : To Avoid Toll fraud

Rerouting Calling Search Space : For Single number reach reachability

→ Save

Line [1] - Add a new DN

Directory Number : 1000 [Same as Desk phone number shared line]



Associate profile with end user

Step 5: Add Remote Destinations

Device → Remote Destinations → Add New

Adding a Remote Destination do two things one is SNR and other one is MVA

Name : Jaseem's Mobile Number

Destination Number* : 9.9495860708

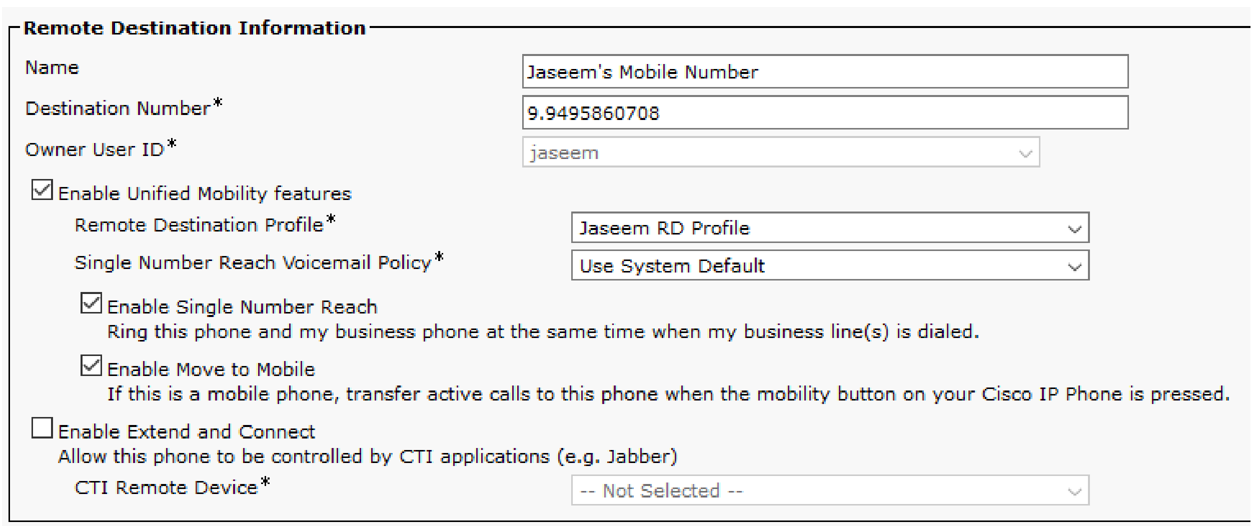
Owner User ID* : jaseem

Check Enable Unified Mobility features

Remote Destination Profile* : Jaseem RD Profile

Check Enable Single Number Reach

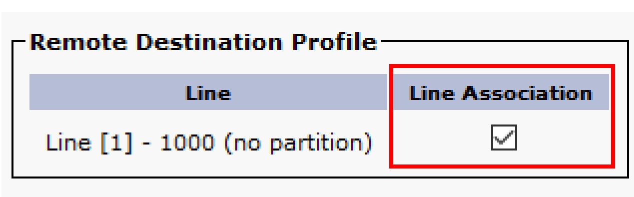
Check Enable Move to Mobile



[Note: End User can also configure this in End user page (Self Care Portal)]

→ Save

Check Line Association



Step 7: Add Access List (Optional)

Call Routing → Class Of Control → Access List → Add New

Name* : Jaseem's ACL (BLOCKED)

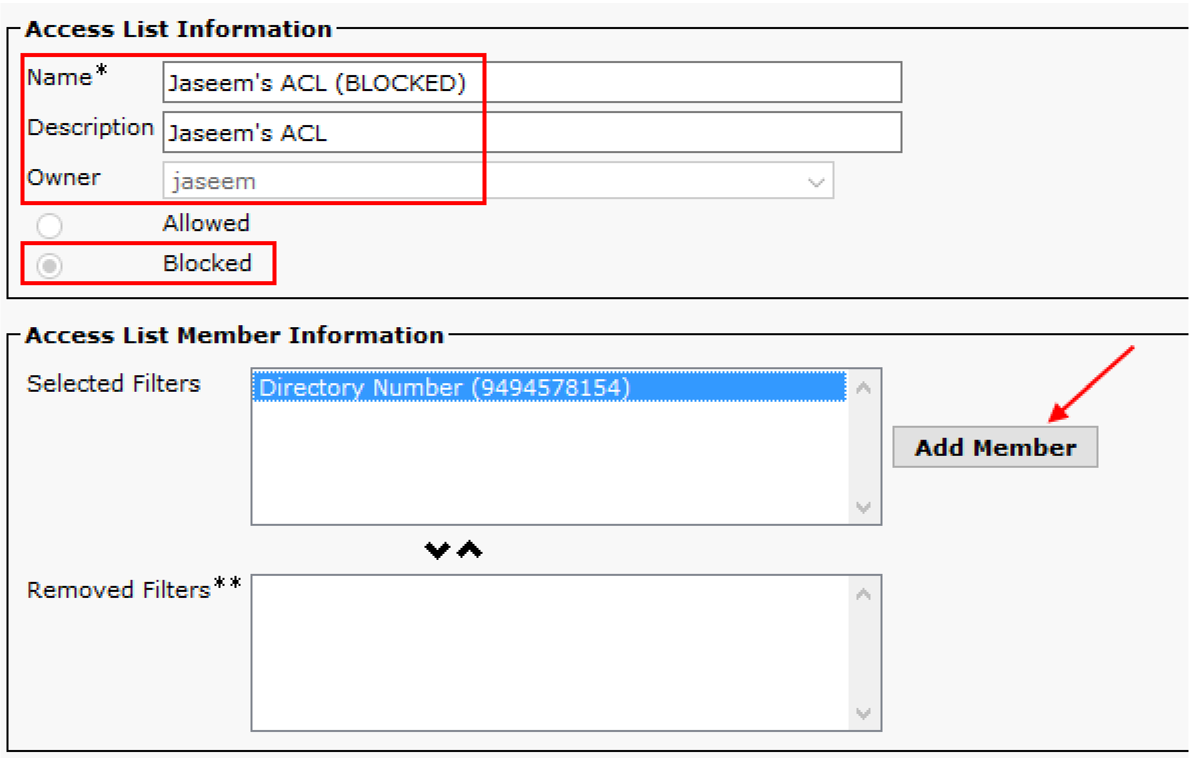
Description : Jaseem's ACL (BLOCKED)

Owner : jaseem (End User)

→ Save

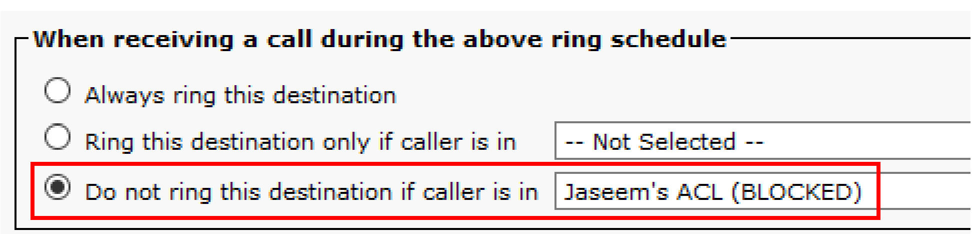
Click Add Member and add numbers to block

[This block only reaching to your remote destinations, not block calling to your desk phone]



Apply ACL under Remote Destination

Device → Remote Destinations → Jaseem's Mobile Number



Cisco Unified Mobility MVA (Mobile Voice Access)

- From your cell phone you can dial in to the corporate network by entering some passcodes and dial out from the corporate network with the caller ID information of the company.
- MVA provides access to CUCM from user's mobile phone number and make external calls from enterprise UC network.
- To use this feature user dials in to a specific PSTN DID to access MVA service. A specifically configured Voice XML gateway routes the calls to IVR application.

Configurations

Step 1: Activate Cisco Unified Mobile Voice Access

Service Ability → Tools → Service Activation →

Check Cisco Unified Mobile Voice Access Service → Save

Step 2: Service Parameter Configuration

System → Service Parameters →

Server : <Select Server>

Service : Call Manager (Active)

Enable Mobile Voice Access *	True
Mobile Voice Access Number	1005
Matching Caller ID with Remote Destination *	Partial Match
Number of Digits for Caller ID Partial Match *	10

MVA Number is the Caller ID for outside

Step 3: Enable MVA for Users

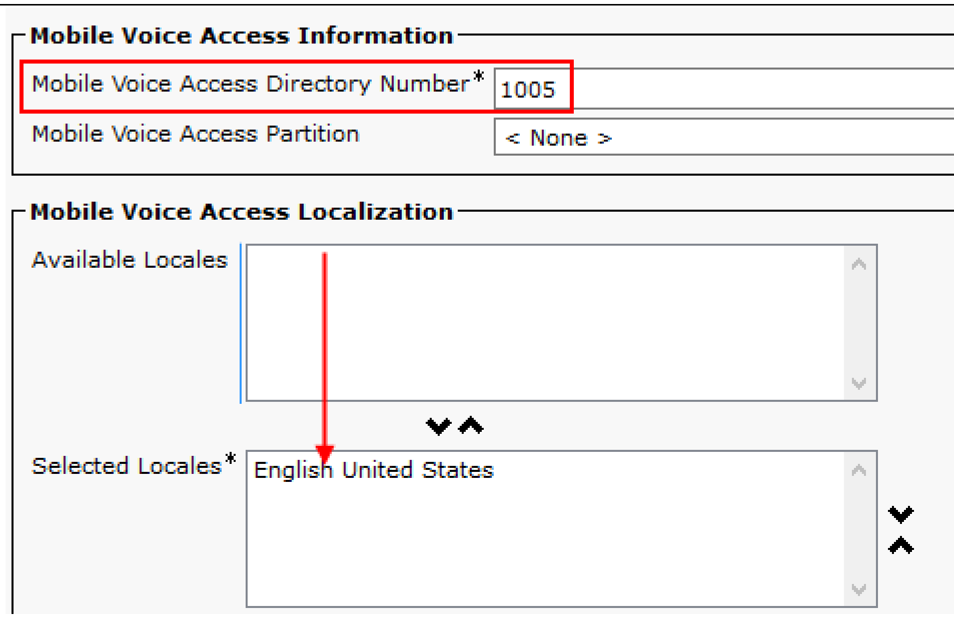
In End User page, check Enable Mobile Voice Access and associate Remote Destination Profile.

Step 4: Media Resources Configurations

Media Resources → Mobile Voice Access

Mobile Voice Access Directory Number : 1005

Select Available Locales



Step 5: Configure MVA between CUCM and Gateway

```
HQ_GW(config)#application
HQ_GW(config-app)#service mva
http://<CUCM IP ADDRESS>:8080/ccmivr/pages/IVRMainpage.vxml

HQ_GW(config)#dial-peer voice 1 pots
HQ_GW(config-dial-peer)#incoming called-number 1005
HQ_GW(config-dial-peer)#direct-inward-dial
HQ_GW(config-dial-peer)#service mva

HQ_GW(config)#dial-peer voice 2 voip
HQ_GW(config-dial-peer)#destination-pattern 1005
HQ_GW(config-dial-peer)#session target ipv4:142.100.64.11
HQ_GW(config-dial-peer)#detmf-relay h245-aphanumeric
HQ_GW(config-dial-peer)#codec g711ulaw
HQ_GW(config-dial-peer)#no vad
```

Multisite Deployment Issues & Solutions

Deploying CUCM in a multisite environment is little bit complex than a single site solution.

Quality Issue: Voice and Video traffic must be prioritized over data packets.

Bandwidth Issue: We have to ensure that the Data applications and UC applications do not overload the available band width.

- Use Low bit rate codecs (G.729)
- Deploy local annunciator, Conference bridges, MTPs and MoH
- Compressed RTP
- Multicast MoH from Branch router flash
- Call Admission Control (CAC): Limiting the number of voice calls

Availability Issue: At the time of WAN outage it is important to provide fallback solutions for MGCP Gateways, IP Phones. The fallback solution applies H.323 or SIP protocol to the gateway with the help of dial-peers

- MGCP Fallback
- SRST for IP Phones (Call forward unregistered to PSTN DID)

Dial-plan Issue: Overlapping dial plan must be solved by designing a robust multisite dial-plan

- Configure site codes for each locations

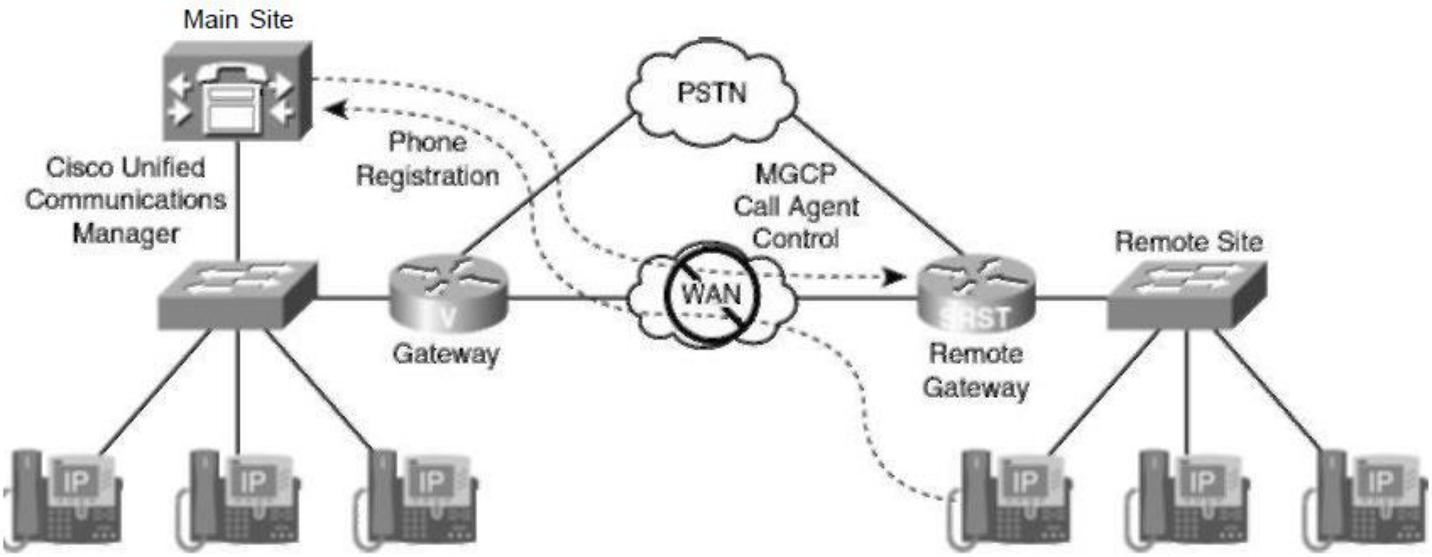
NAT & Security Issue: During public to Private mapping there will be possibility of attack.

- Solved by using CUBE

To connect two independent clusters we have multiple connectivity options are available like SIP Trunk, ICT, H.323, MGCP

Remote Site Redundancy Options

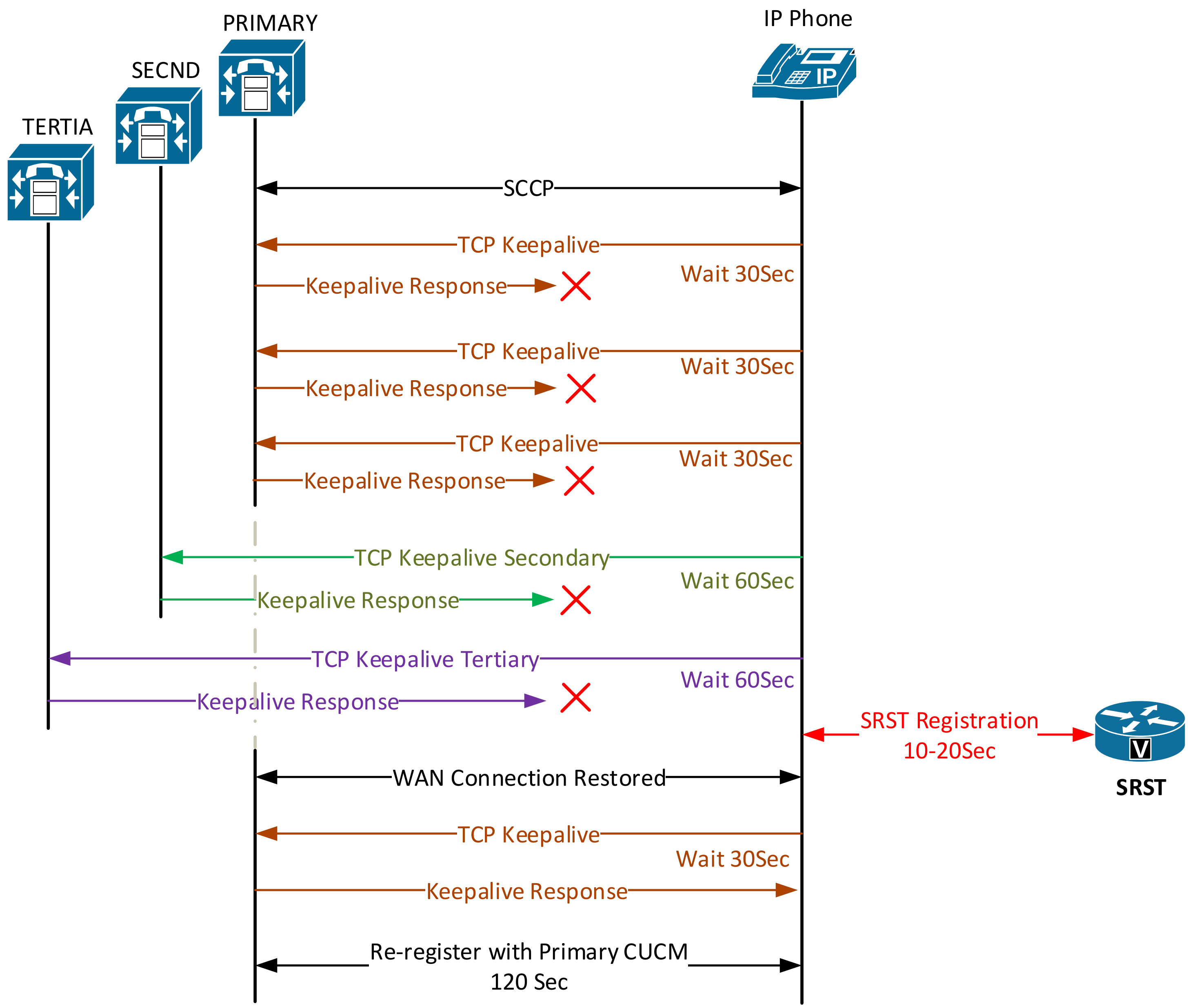
- Two technologies are used to provide remote site redundancy for remote sites Survivable Remote Site Telephony (SRST) and MGCP Fallback.
- Cisco IP Phone requires SCCP or SIP connectivity to call processing agent, in the absence of signaling connectivity the phones become fully unusable.
- Both of these technologies can be configured in single router since IOS version 12.2(11)T



SRST (Survivable Remote Site Telephony)

- Keeps your phone system running in case of WAN outage (Basic features).
- Support IP Phones (telephony service) during WAN link failure.
- Provide only core features (Hold, Transfer, Conference, etc.)
- Simple configuration, Supports SCCP & SIP phones
- Supports maximum of 1500 phones in SRST mode (Depends on the hardware. Cisco 3945E router supports 1500 IP Phones)
- When connection to CUCM restored, call handling reverts back to primary CUCM

SRST Failover Process



- Phone's Keepalive = 30 Seconds
- IP Phones listen to 3 keepalive reply before thinking about Secondary backup server. If there is no response for 3 consecutive keepalive messages phone send keepalive message to secondary Call Manager (Secondary (Backup) Server keepalive = 60 Seconds)
- If there is no response from Secondary server, IP Phone sends keepalive to Tertiary Call Manager. (Tertiary (Backup) Server keepalive = 60 Seconds)
- SRST Registration = 10-20 Seconds
- Switch back timer = 120 Seconds

SRST Platform Density

ROUTER MODEL	SUPPORTED ENDPOINTS
800 Series	4
1861	15
2801-2851	25-100
2901-2951	35-250
3825, 3845	350, 730
3925-3945E	730-1500

Configurations

Step 1: SRST Reference

SRST reference Delivered directly to the IP phone through the device pool configuration. It is the IP address of SRST Gateway.

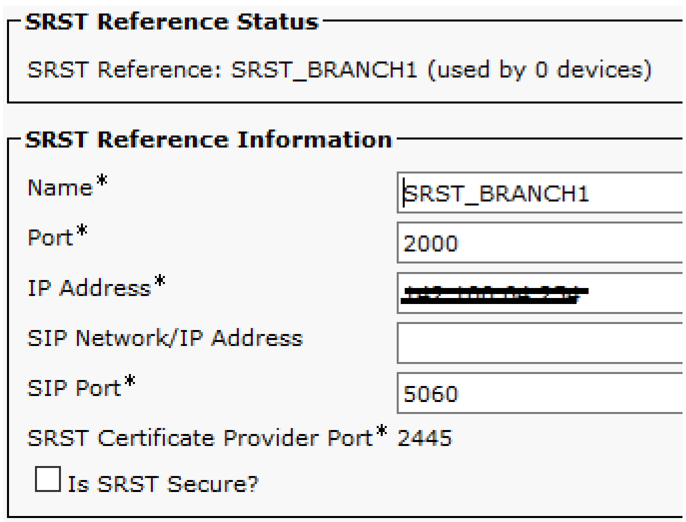
System → SRST → Add New

Name*   : SRST_BRANCH1

Port*   : 2000

IP Address*: 192.168.30.254

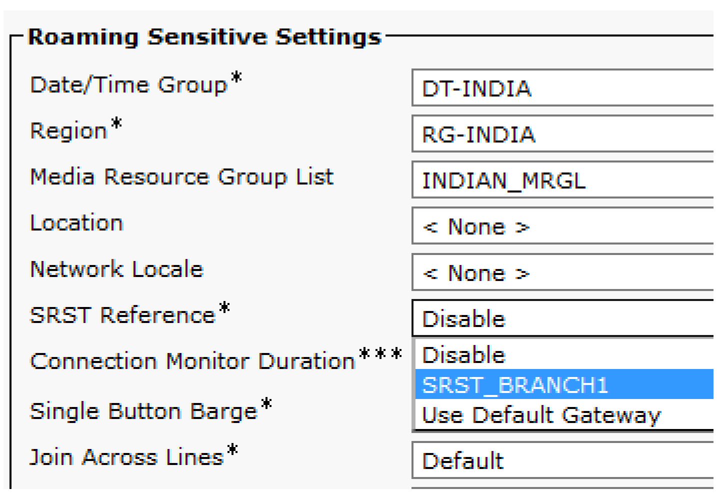
→ Save



Go to System → Device Pool →

SRST Reference* : SRST_BRANCH1

→ Save



Step 2: Router Side SRST Configuration

BRANCH1_GW(config)#call-manager-fallback

BRANCH1_GW(config-cm-fallback)#max-ephones 10

BRANCH1_GW(config-cm-fallback)#max-dn 10 dual-line

BRANCH1_GW(config-cm-fallback)#ip source-address 192.168.30.254

BRANCH1_GW(config-cm-fallback)#keepalive 30

BRANCH1_GW(config-cm-fallback)#limit-dn 7960 2

Verification

```
BRANCH1_GW#show call-manager-fallback
CONFIG (Version=3.2)
=====================
Version 3.2
For on-line documentation please see:
www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/index.htm

ip source-address 142.100.64.254 port 2000
max-ephones 10
max-dn 10 dual-line
max-conferences 4
dspfarm units 0
dspfarm transcode sessions 0
huntstop
no huntstop channel
time-format 12
date-format mm-dd-yy
timezone 0 Greenwich Standard Time
keepalive 30
timeout interdigit 10
timeout busy 10
timeout ringing 180
caller-id name-only: enable
Limit number of DNs per phone:
  7910: 34
  7935: 34
  7936: 34
  7940: 34
  7960: 2
  7970: 34
Log (table parameters):
     max-size: 150
     retain-timer: 15
local directory service: enabled.

BRANCH1_GW#show ephone
```

```
ephone-1 Mac:3C07.7172.22E0 TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:142.100.64.100 50032 CIPC   keepalive 4 max_line 8
button 1: dn 1  number 1000  CM Fallback CH1   IDLE         CH2   IDLE


ephone-2 Mac:001B.D584.E1E5 TCP socket:[2] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:142.100.64.105 51997 Telecaster 7960  keepalive 4 max_line 6
button 1: dn 2  number 1001  CM Fallback CH1   IDLE         CH2   IDLE
```

__Step 3: Call Forward Unregistered (CFUR)__

When WAN goes down, the phones become unregistered in CUCM perspective. CFUR allows forwarding the call through PSTN to the SRST Gateway router as DID number.

Device → Phone → Line Page

Call Forward Unregistered Internal   : PSTN DID Number

Call Forward Unregistered External   : PSTN DID Number

Forward Unregistered Internal	☐ or	5125552001
Forward Unregistered External	☐ or	5125552001

- [Issue: If WAN up, somebody unplug their phone, call routed via PSTN and from remote gateway it routed back to CUCM. From CUCM it is again routed to PSTN.... Call Routing Loop]

System → Service Parameter → <Select Server> → Service: Call Manager Active

Max Forward UnRegistered Hops to DN* : 2

- This parameter specifies the maximum number of forward UnRegistered hops that are allowed for a DN (directory number) at the same time. This parameter limits the number of times the call can be forwarded due to UnRegistered DN when a forwarding loop occurs.

0 = Unlimited forwarding

2 = Voice Mail to work

CME SRST Mode

- Supports only SCCP phones
- Supports maximum 450 IP Phones (Cisco 3945E Router) where as normal SRST supports 1500 IPPhones.
- Provide wide features (Hunt Group, Call Park, Extension Mobility, etc.)

Core Commands

- Telephony-service, max-ephones, max-dn, ip source-address, ephone-dn, tftp-server, mac-address, button, dial-plan-pattern
- When CME provides SRST functionality, provisioning of phone is automatic. That is when we are configuring CME in SRST mode, no phones have to be configured, they can be learned by Simple Network Auto Provisionig (SNAP) method.

Phone Provisioning in CME SRST Mode

- Manually Configured ephones with associated phone-dns: In this case the ephone fully configured exactly like CME.
- Manually configured ephone with no associated ephone-dn: Phone configurations are required but DN parameters are not required. In this case DNs are not learned via SNAP hence CME will auto assign DNs randomely.
- Manually configured ephone-dn: Ephones are learned by SNAP
- No manual configuration: In this case ephone and ephone-dn are learned via SNAP

Configuration

- CME SRST is configured by #telephony-service command. Once telephony-service is active, the command #call-manager-fallback not accepted by Router and vise versa.

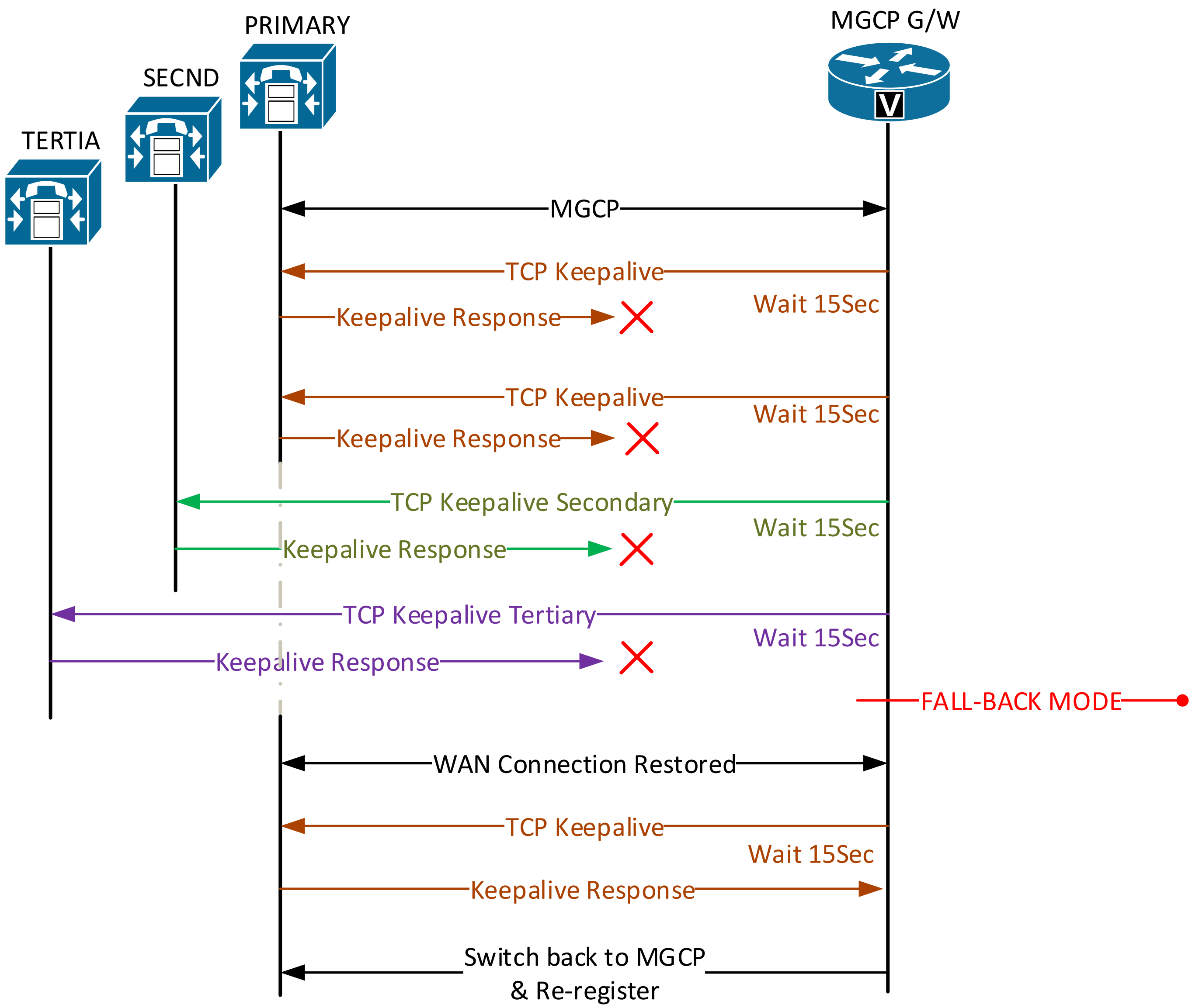
```
REMOTE_GW(config)#telephony-service
REMOTE_GW(config-telephony)#max-ephones 10
REMOTE_GW(config-telephony)#max-dn 10
REMOTE_GW(config-telephony)#ip source-address 192.168.30.254
REMOTE_GW(config-telephony)#srst mode auto-provision all
REMOTE_GW(config-telephony)#srst dn line-mode dual
```

Note: If the administrator saves the running configuration afer learning ephone and ephone-dns, the fallback IP phones are treated as locally configured phones on CME.

MGCP Fallback

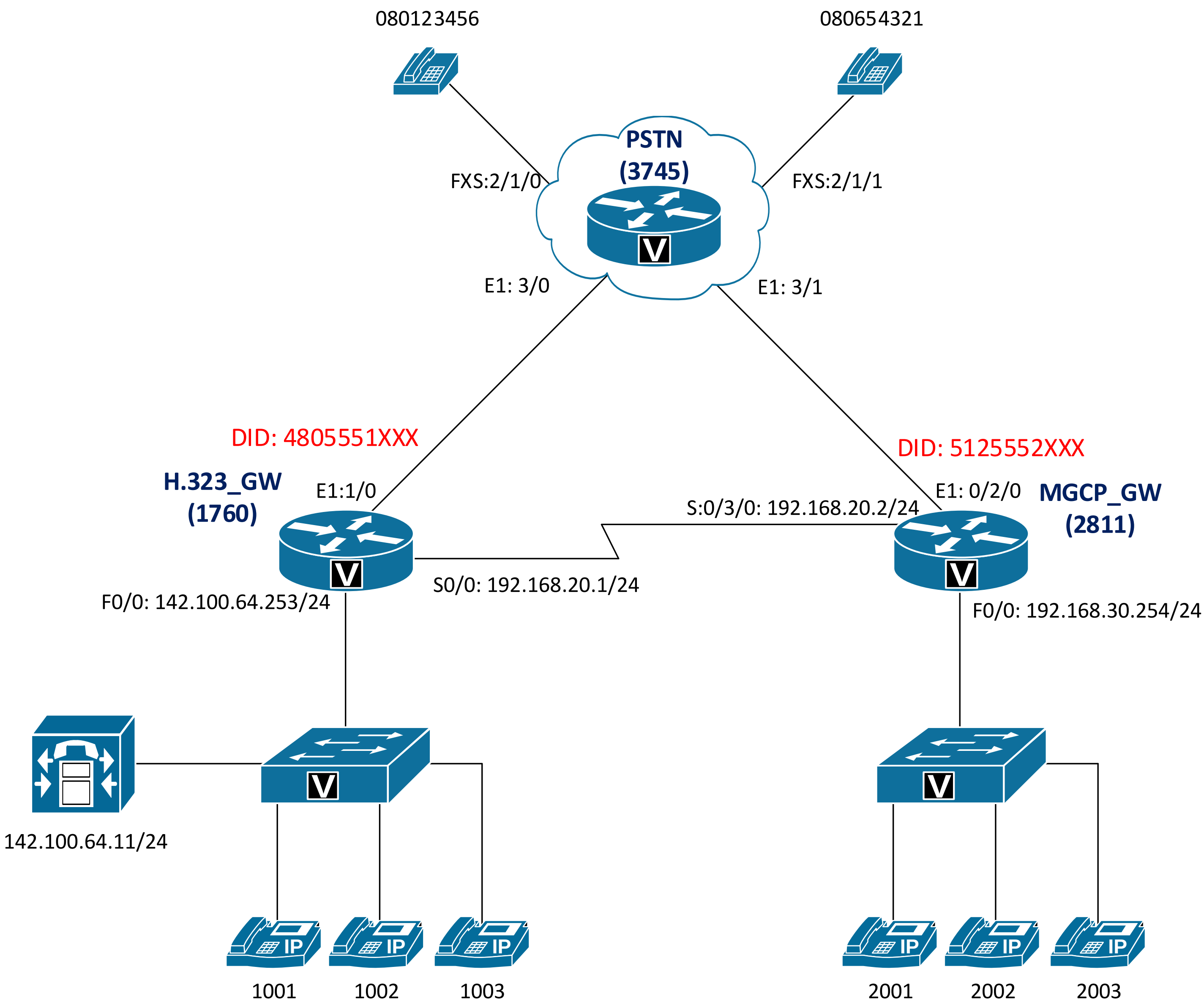
- When WAN connection to Call Manager goes down, MGCP gateway switches back to H.323 or SIP.
- We have to put some backup base (small) configuration (H.323 or SIP dial-peers) in MGCP gateway to support fallback
- Those dial-peers responsible for connecting you to PSTN
- The active calls along Analog line (FXO, FXS), E1 CAS, T1 CAS are unaffected during fall back. PRI calls will be released

MGCP Failover Process



- Keepalive = 15 Seconds,
- After missing two keep alive from primary CUCM, Gateway tries secondary Call Manager.
- If there is no keepalive reply from secondary gateway tries for tertiary Call Manager
- If no keepalive reply from tertiary gateway falls back to default application H.323 or SIP
- WAN connection restored, gateway reestablish TCP connection keepalive to CUCM and re-register with CUCM
- Gateway can switch back to CUCM immediately when active calls are finished, or after a fixed amount of time, or at a fixed time of day

Configurations



<u>Prerequisites</u>

1. Configure Multisite deployment
2. Configure PSTN Router (Two DID dial-peers)
3. Configure 1760 Router as H.323 Gateway in Head Office
4. Configure 2811 Router as MGCP Gateway in Branch office
5. Configure LRG based call routing to PSTN

<u>Step 1: MGCP Fallback Configuration</u>

<u>IOS Versions 12.3(14T)</u>

```
BR_MGCP_GW(config)#ccm-manager fallback-mgcp
BR_MGCP_GW(config)#call application alternate Default
```

Later IOS Versions

```
BR_MGCP_GW(config)#ccm-manager fallback-mgcp
BR_MGCP_GW(config)#application
BR_MGCP_GW(config-app)#global
BR_MGCP_GW(config-app-global)#service alternate Default
```

[Note: When WAN goes down PRI line loose its layer 3 capacity only (Q.931), Layer 2 will be always up (Q.921)]

Step 2: Configure Backup Dial-peers (H.323) for PSTN Calls

```
BR_MGCP_GW(config)#dial-peer voice 1 pots
BR_MGCP_GW(config-dial-peer)#description PSTN_OUTGOING
BR_MGCP_GW(config-dial-peer)#destination-pattern .T
BR_MGCP_GW(config-dial-peer)#port 0/2/0:15
BR_MGCP_GW(config-dial-peer)#no digit-strip

BR_MGCP_GW(config)#voice-port 0/2/0:15
BR_MGCP_GW(config-voiceport)#timeouts interdigits 3

BR_MGCP_GW(config)#dial-peer voice 2 pots
BR_MGCP_GW(config-dial-peer)#description PSTN_OUTGOING_TO_HEAD_OFFICE
BR_MGCP_GW(config-dial-peer)#destination-pattern 1...
BR_MGCP_GW(config-dial-peer)#prefix 4805551...
BR_MGCP_GW(config-dial-peer)#port 0/2/0:15
BR_MGCP_GW(config-dial-peer)#no digit-strip

BR_MGCP_GW(config)#dial-peer voice 3 pots
BR_MGCP_GW(config-dial-peer)#description PSTN_INCOMING
BR_MGCP_GW(config-dial-peer)#incoming called-number .
BR_MGCP_GW(config-dial-peer)#direct-inward-dial
BR_MGCP_GW(config-dial-peer)#port 0/2/0:15
```

Digit Manipulations

Method 1: Number Expansion

```
BR_MGCP_GW(config)#num-exp 5125552... 2...
```

Method 2: Voice Translation Rule

```
BR_MGCP_GW(config)#voice translation-rule 1
BR_MGCP_GW(cfg-translation-rule)#rule 1 /^5125552\(...\)$/ /2\1/
```

```
BR_MGCP_GW(config)#voice translation-profile PSTN_INCOMING
BR_MGCP_GW(cfg-translation-profile)#translate called 1
```
[Think about PSTN perpective]

OR

```
BR_MGCP_GW(config)#voice-port 0/2/0:15
BR_MGCP_GW(config-voiceport)#translation-profile incoming PSTN_INCOMING
```

Method 3: Dial-Plan Pattern

```
BR_MGCP_GW(config-cm-fallback)#dialplan-pattern 1 5125552.... extension-length 4 extension pattern 1...
```

Step 3: Configure Call Forward Unregistered in Central Site

- Central site users dial 200X to reach remote office even when WAN is down. At this point we want to forward their calls via PSTN.
- In the line page of CUCM we have one option available 'Call Forward Unregistered (CFUR)'. It is introduced in CUCM 4.2 release. Set CFUR to the remote office DID.

Go to line page of each remote office phones (2001, 2002, etc.) and configure CFUR to proper DID extensions.

Forward Unregistered Internal	☐ or	5125552001
Forward Unregistered External	☐ or	5125552001

[Note: If block of DIDs are not available set the CFUR to reception DID of remote office. The call should go via main site Gateway, to achieve this use 'Call Forward CSS']

- CFUR causes Call Routing loops whenever the remote site phone is disconnected from the network in which the remote location is not in SRST mode. Internal calls to that DN are forwarded to CFUR (PSTN DID of remote office) destination. The remote gateway treat the call as a normal PSTN call and send signaling to CUCM, CUCM again forward the calls to PSTN, causing infinite call routing loop.
- To overcome this issue, go to

Service parameter → Max Forward UnRegistered Hops to DN: 2

0 → Unlimited (Cause Loop)

1 → We can't forward to Voice Mail

MGCP Fallback Dial-Plan Consideration

- The above configured destination pattern '**.T**' allows all the users to call any number (Local, Long distance, International) during MGCP fallback mode.
- To implement restriction we have to configure COR in fallback mode.
- Also Voice Translation Rule should be configured to change incoming PSTN DID number to internal extension.

COR List (Optional)

If you have configured proper PSTN numbering plan, configure COR list also for providing restrictions.

1. Create COR Custom Member
2. Create Outgoing COR List (INTERNATIONAL-LIST, NATIONAL-LIST, LOCAL-LIST)
3. Create Incoming COR List (CEO-LIST, MANAGER-LIST, EMPLOYEE-LIST)
4. Apply Outgoing COR List Under Outgoing Dial-peers
5. Apply Incoming COR List

```
MGCP_GW(config)#call-manager-fallback
MGCP_GW(config-cm-fallback)#cor incoming CEO-LIST 1 2001
MGCP_GW(config-cm-fallback)#cor incoming MANAGER-LIST 2 2002 - 2005
MGCP_GW(config-cm-fallback)#cor incoming EMPLOYEE-LIST 3 2006 - 2020
```

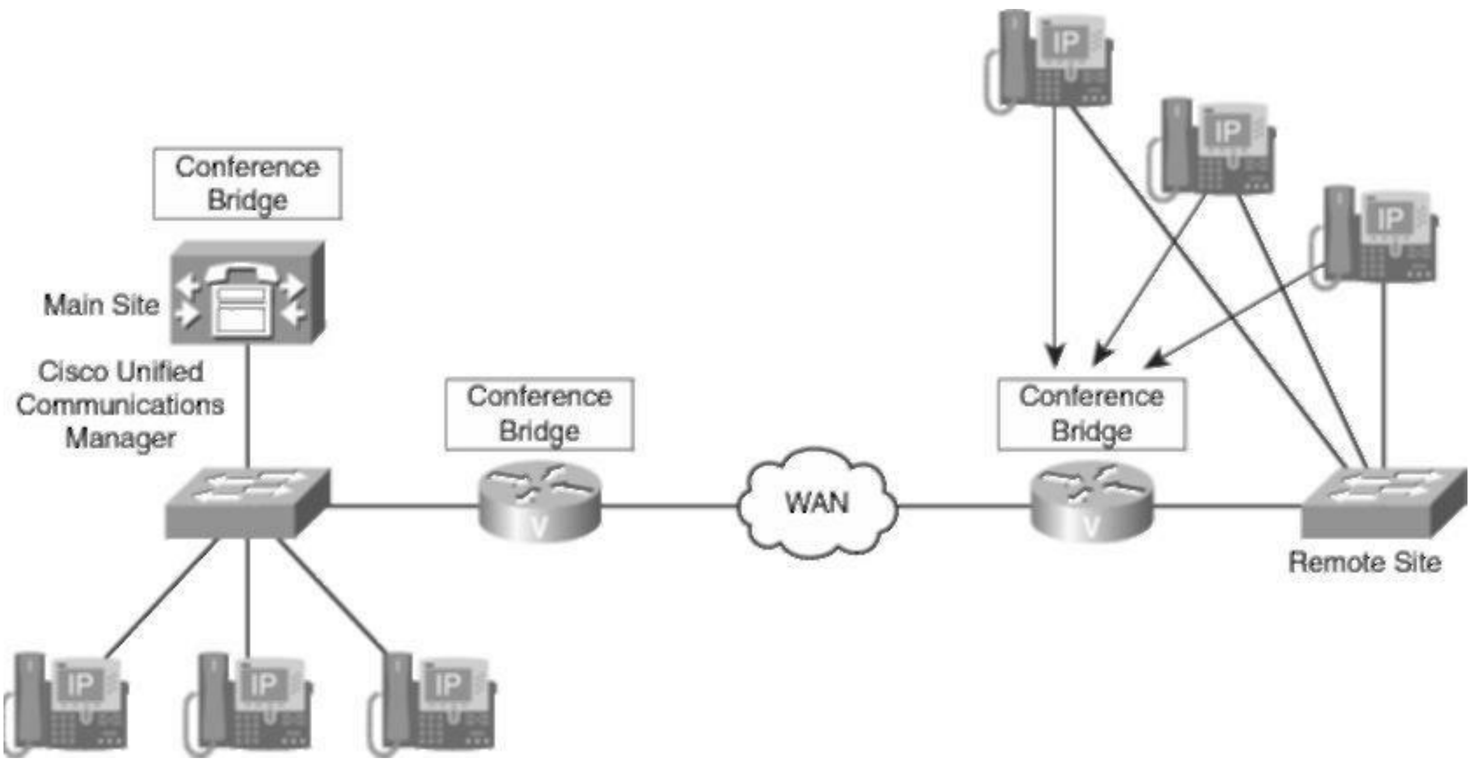
Bandwidth Management

When IP WAN connects two different sites in Cisco UC network, bandwidth consumption at IP WAN should be minimized.

Valuable IP WAN bandwidth can be conserverd by various technique.

1. RTP Header copmression
2. QoS
3. Low bandwidth Audio Codec
4. Deploying Local Conference bridges
5. Deploying Local Transcoder
6. Deploying Local MoH Servers (Multicast MoH from remote branch router flash)

Local Conference Bridge Implementation



Configuration is done in CIPT1 series.

Here we have to group the resources with MRGL

Media Resources → Media Resourse Group → Add New

Name: HO_HW_MRG

Device: Hardware Conf Bridge

→ Save

Name: HO_SW_MRG

Device: Software Conf Bridge in Head office

→ Save

Media Resources → Media Resourse Group List → Add New

Name: HO_MRGL

1. HO_HW_MRG

2. HO_SW_MRG

→ Save

Configure HO_MRGL in device pool in HO with HO_MRGL → Save

Media Resources → Media Resourse Group → Add New

Name: BR_HW_MRG

Device: Hardware Conf Bridge in Branch router

→ Save

Media Resources → Media Resourse Group List → Add New

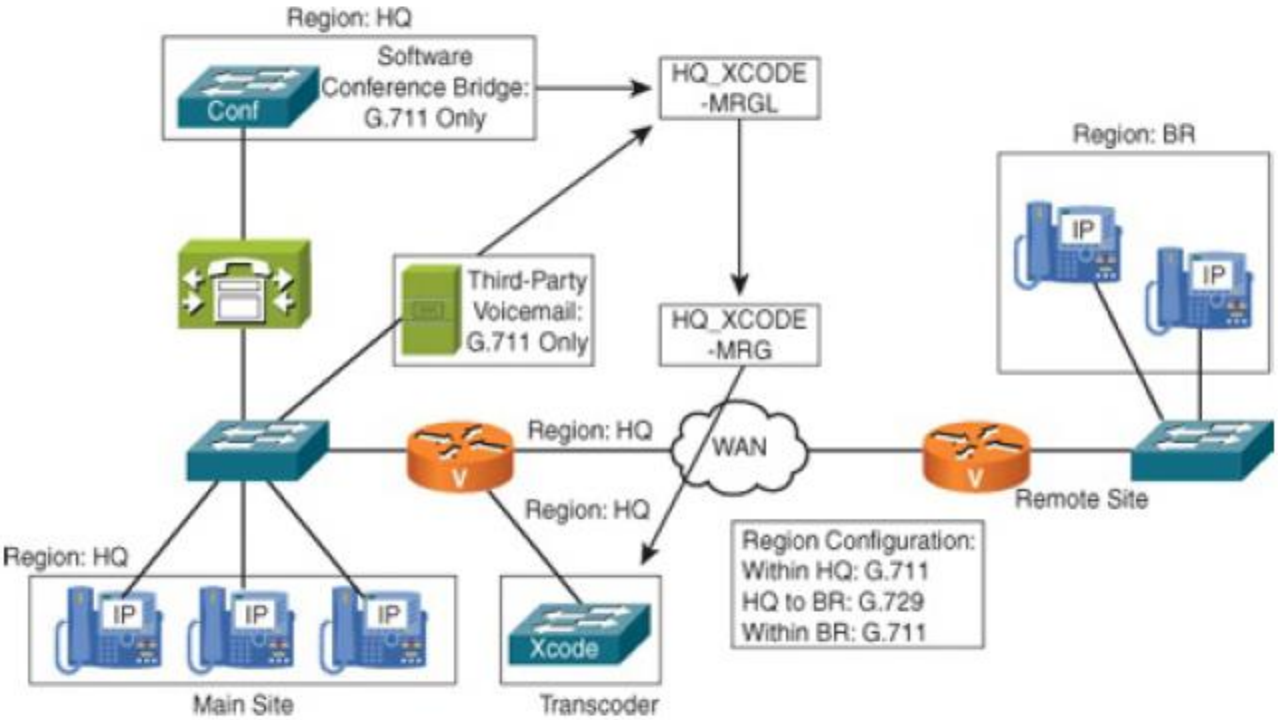
Name: BR_MRGL

1. BR_HW_MRG

→ Save

Transcoder Implementation

Transoder should be implemented at centralsite.



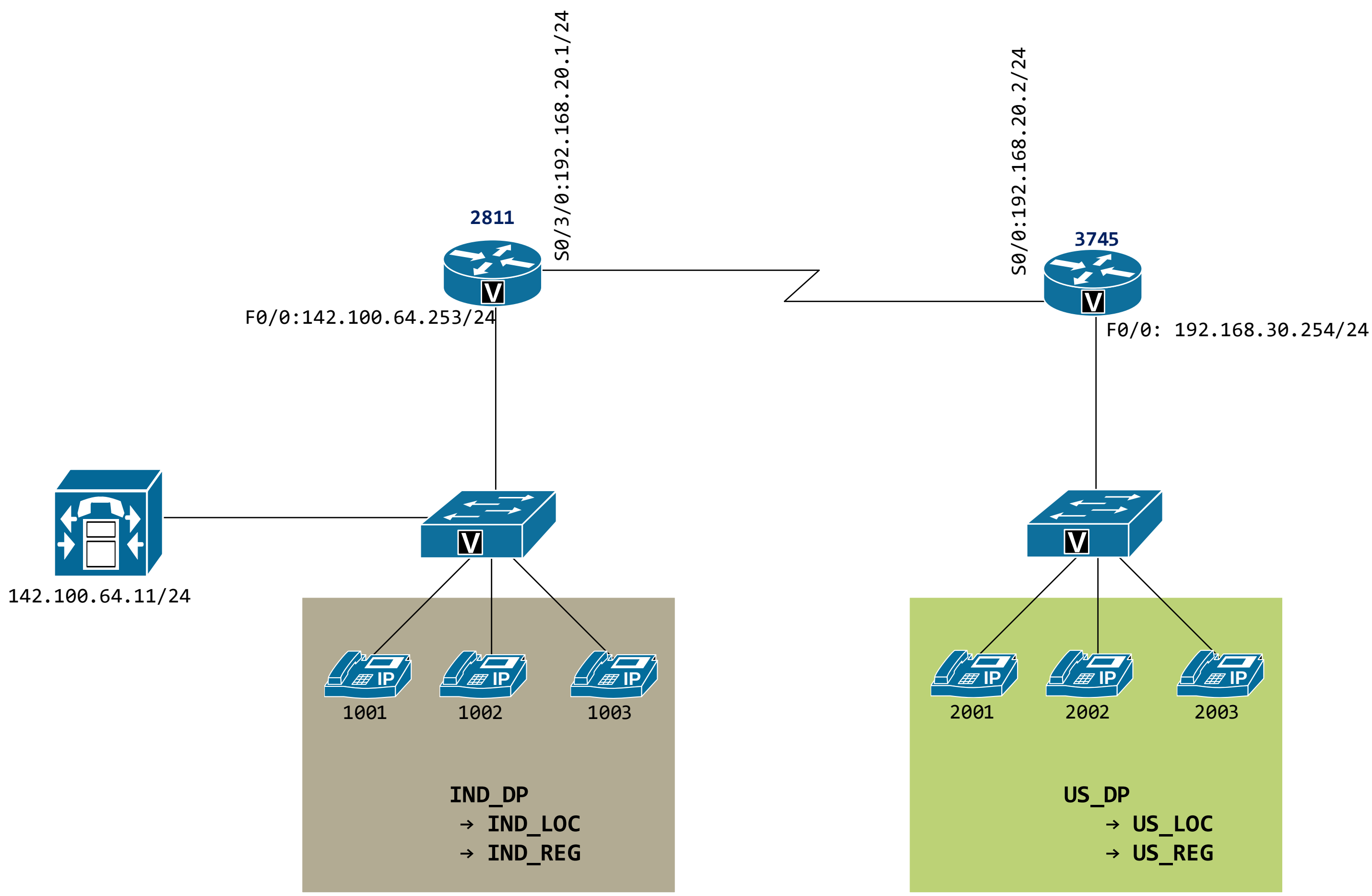
Implementing Call Admission Control (CAC)

- When IP WAN connects multiple sites in UC network QoS has to be implemented to priorities voice packet over data packets. However to avoid over subscription caused by too many voice calls can be limited using a mechanism called CAC
- is needed to limit the number of calls allowed at the same time between certain locations.
- CAC ensures that the voice calls do not oversubscribe the WAN bandwidth.
- If CAC is not configured CUCM assumes that all links everywhere have infinite bandwidth, which can result over subscription of WAN links at the expense of audio quality. If over subscription occurs, any packet of any voice stream can be affected not just a single call, it results Packet delays, Packet droops of all voice calls
- The default CAC settings in CUCM is disabled. In centralized call processing deployment Standard locations and Recourse Reservation Protocol (RSVP) enabled locations can be used to provide CAC.
- If a call is blocked by any of these methods, AAR (Automatic Alternate Routing) can be used to reroute the call over PSTN instead of denying the call. AAR designed to work within the cluster only.

Standard Locations (No topology awareness CUCM7)

- Each device in CUCM can be assigned to a Location, assignment can be direct of via device pool.
- CUCM calculates the actual audio codec bandwidth plus IP overhead, means G.711 = 80Kbps, G.729 = 24Kbps, iLBC = 24Kbps.
- In real time the bandwidth will be higher than these values based on the routing technology used. But CUCM CAC is hardcoded with these values.
- Works well with Hub-and-Spoke topology

Configuration



- Configure Centralized deployment
- Configure Region and set codecs

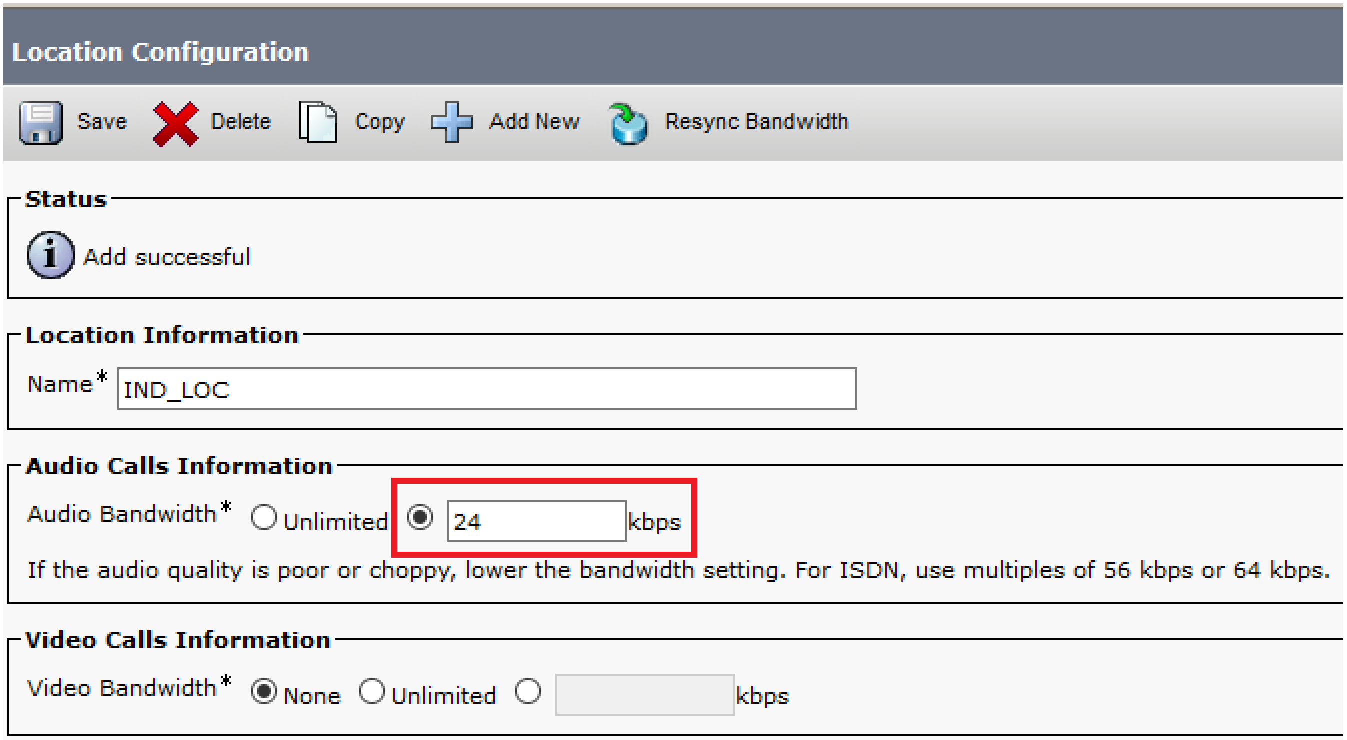
Step 1: Add Locations

System → Location → Add New

Name* : IND_LOC

Audio Bandwidth* : 24Kbps (Only allows 1 call)

→ Save



→ Add New

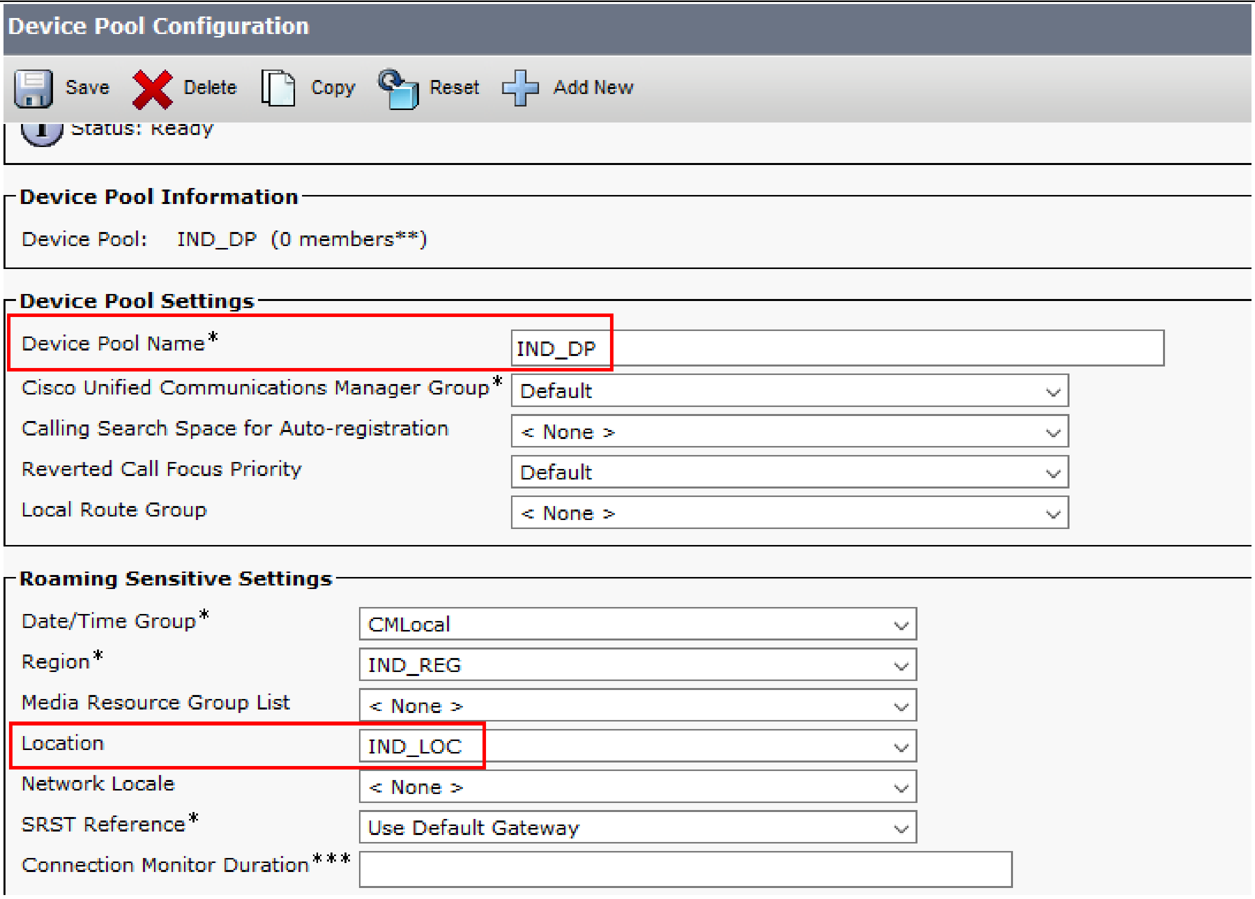
Name* : US_LOC

Audio Bandwidth* : 48Kbps (Only allows 2 call)

→ Save

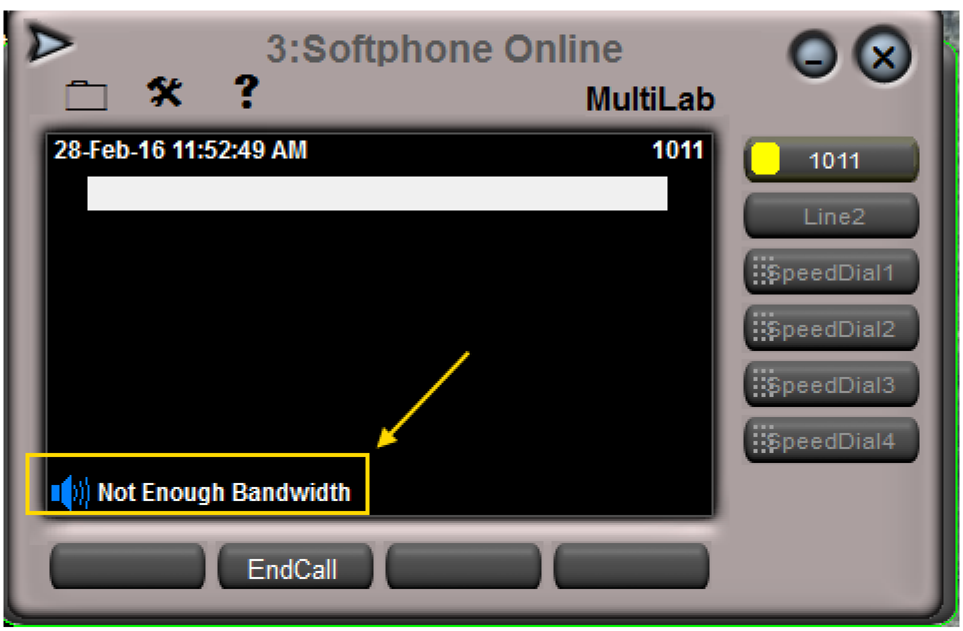
Step 2: Configure Device Pool

Associate above created locations to specific device pool



[Note: You can assign to individual phone also in device page]

Workaround: Try to make two simultaneous calls to us, 1st call will be OK, for the next call you can see the message "**Not Enough Bandwidth**"



Whenever call going to US_LOC, call manager subtract the codec bandwidth from available bandwidth of both location.

i.e. Available BW (24) – Codec BW (24) = 0, then 0Kbps remaining

Enhanced Locations (CUCM9+)

- We can assign weight (0-100) to each path (like Matric)
- Activate Cisco Location Bandwidth Manager (LBM) from Service ability page.
- LBM Group for Single Cluster
- LBM Hub Group for Multiple clusters
- CUCM9 and later version have updated their location configuration, It allows topology awareness CAC

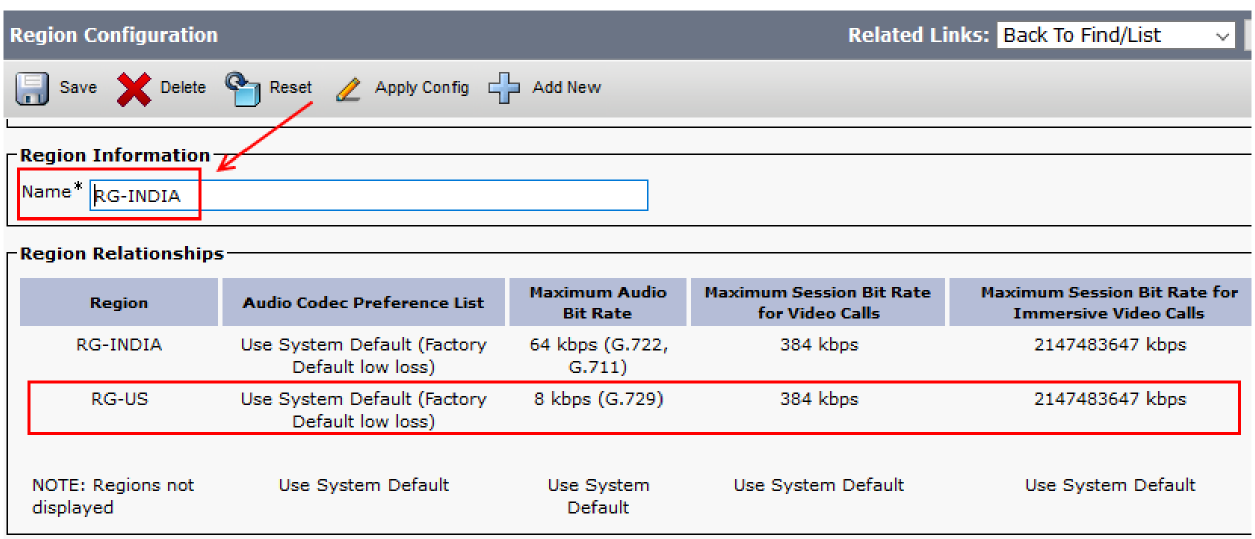
Configurations

Step 1: Activate Cisco Location Bandwidth Manager (LBM)

Cisco Unified Service Ability → Tools → Service Activation → Cisco Location Bandwidth Manager

Step 2: Add Region

System → Region Information → Region



Step 3: Add Locations

In this step do not consider anything, just Add locations that you required

System → Location Info → Location → Add New

Name* : INDIA_LOCATION

→ Add New

Name* : US_LOCATION

Step 4: Set Location to Location Bandwidth Relation

Go to **INDIA_LOCATION,** Under Links, click **Add** button → Select another location

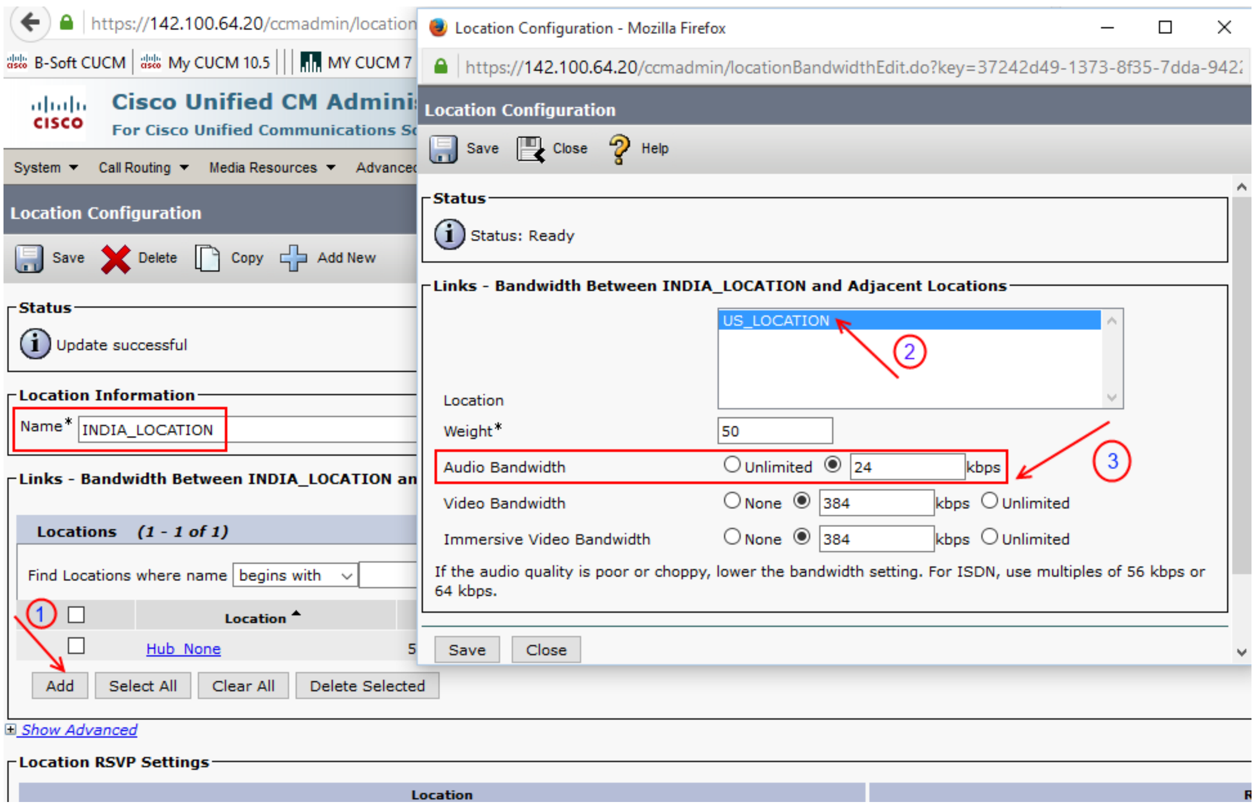
Weight* : 50

(If multiple paths are available, set different values like metric, lower value highly preferred)

Audio Bandwidth : 24Kbps

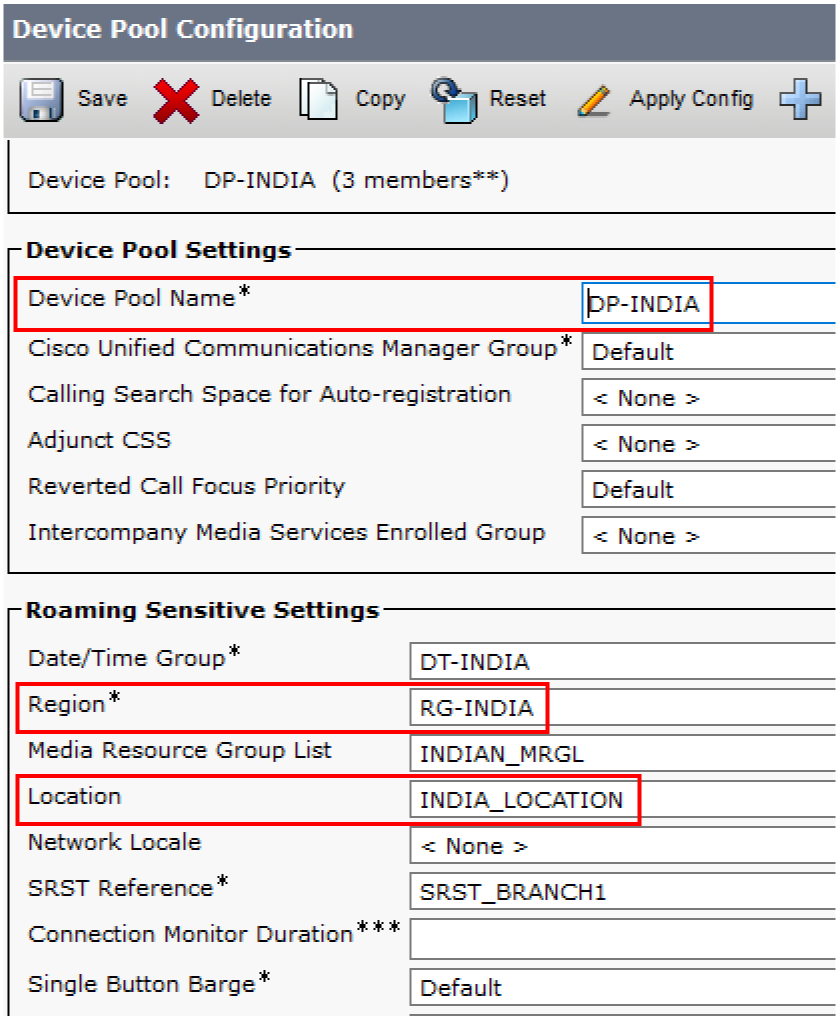
Video Bandwidth : For Vide End points

Immersive Video Bandwidth : For TelePresence



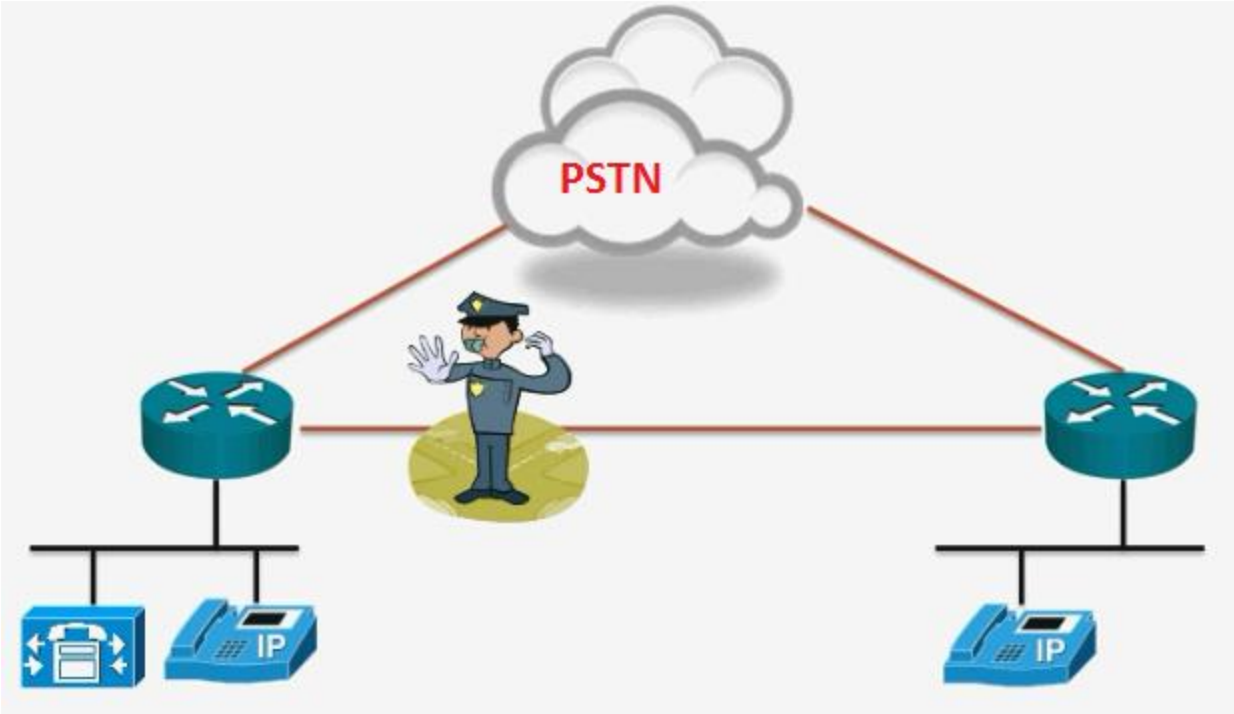
Configure every location relations

Step 5: Configure Device Pool



Associate Locations in each device pool, Reset device pool

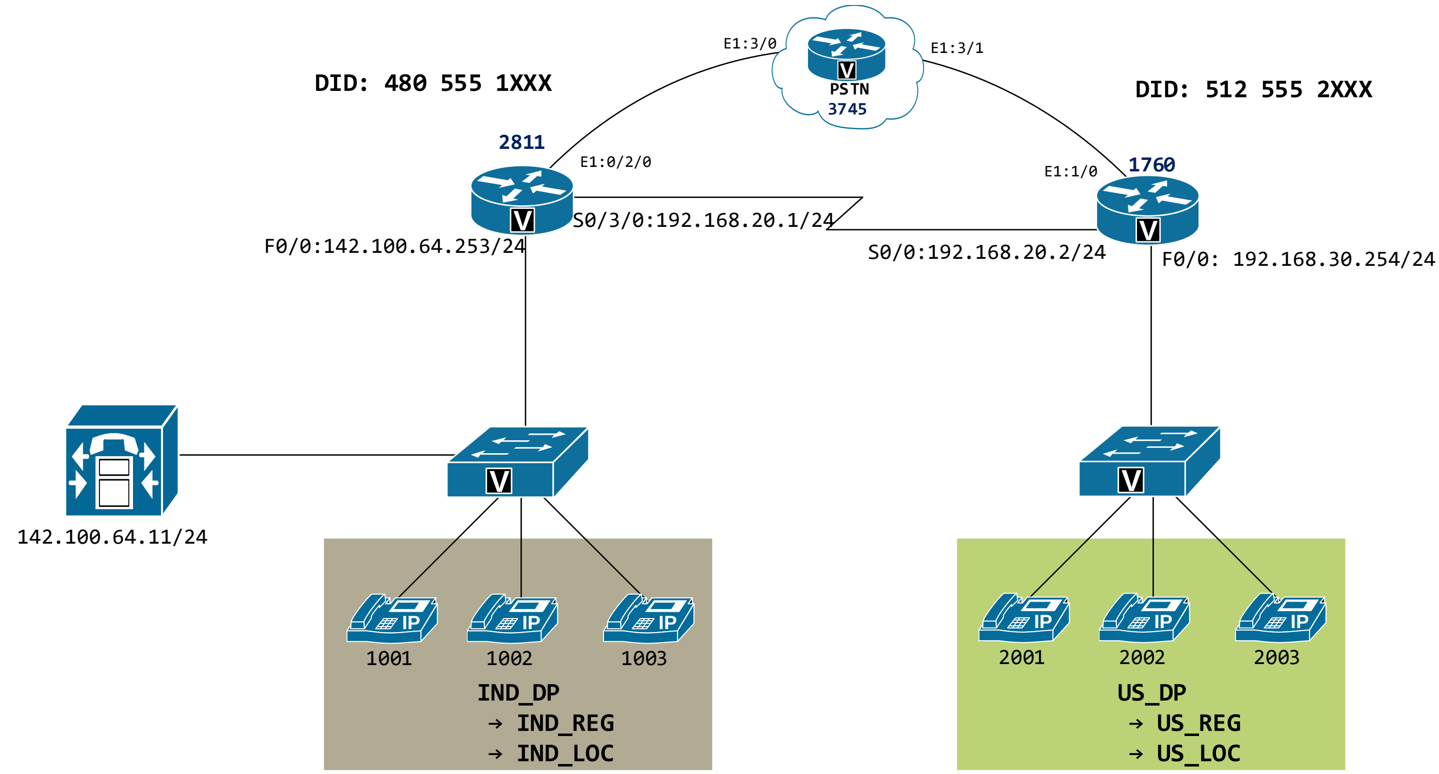
Automated Alternate Routing (AAR)



- Alternate routing of any call that has been blocked by CAC or RSVP. It is not a failover mechanism (only CAC denied call bounces to PSTN)
- Routes call in internal directory numbers only. Without AAR user gets a reorder tone and IP Phone displays “Not Enough Bandwidth”
- In AAR, the caller doesn’t need to hang up and redial the called partie’s DID number, instead CUCM automatically route the call via PSTN
- AAR Pulls called parties AAR Destination mask, add the internal extension and PSTN access code as AAR Prefix.
- AAR Prefix can be obtained from AAR Group

Rerouting Number = AAR Prefix + AAR Destination Mask + DN

Configurations



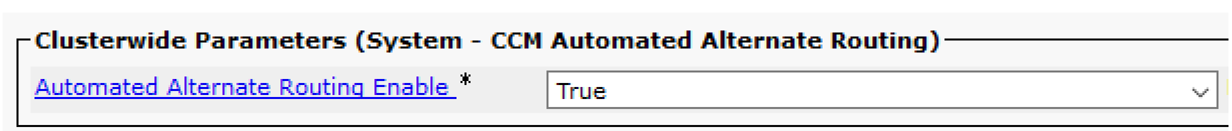
Step 1: Configure Location Based CAC

Step 2: Configure LRG Based Call Routing with 9 as PSTN Access Code (9.!)

Step 3: Service Parameter Configuration

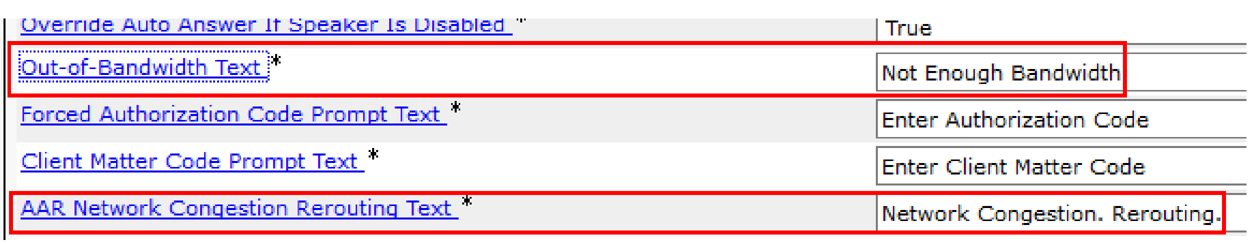
System → Service Parameter → Server: <Select Server> → Service: Call Manager Active

Automated Alternate Routing Enabled: True



Out-of-Bandwidth Text : Not Enough Bandwidth

AAR Network Congestion Rerouting Text : Network Congestion Rerouting



Step 4: Create AAR Group

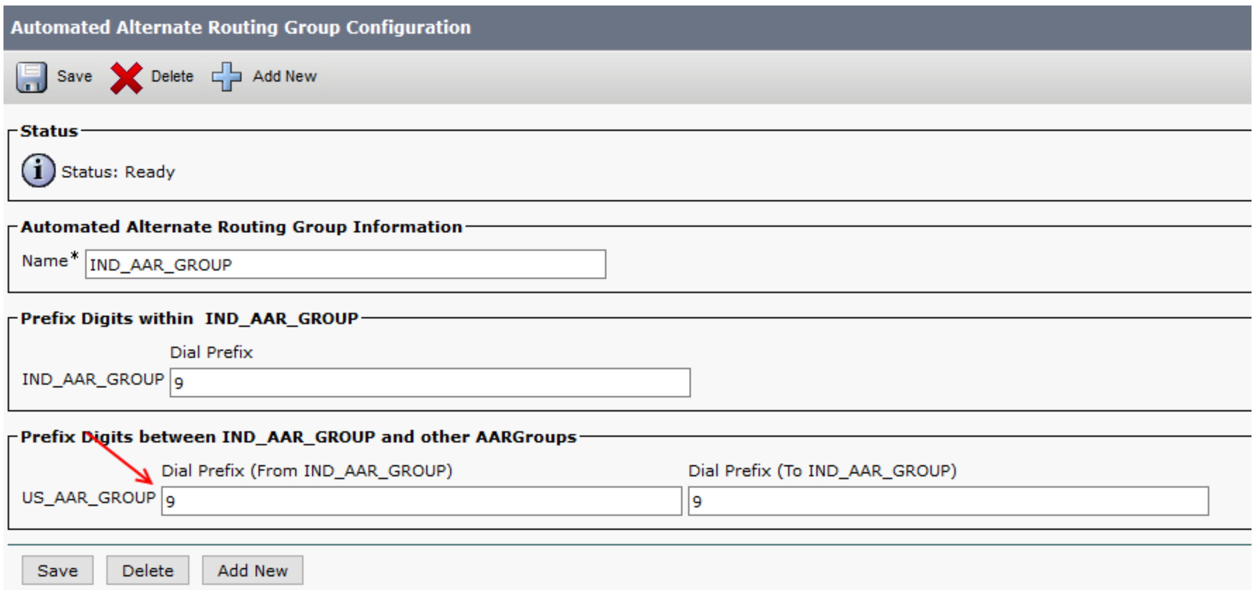
Call Routing → AAR Group → Add New

Name* : IND_AAR_GROUP

→ Add New

Name* : US_AAR_GROUP

Now configure Dial Prefix relation between these groups



Step 5: Configure AAR Destination Mask

Line page → 1001

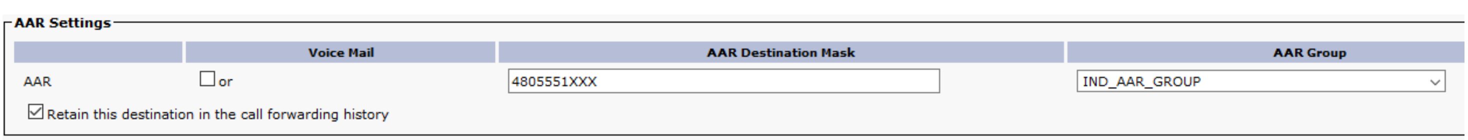
AAR Settings

AAR Destination Mask : 48055510XX

AAR Group : IDNA_AAR_GRP

Similarly 1002 → 48055510XX

2001 → 51255520XX, etc.



[Note: If normal CSS not allowing you to make external calls, we can configure AAR Calling Search Space with elevated calling privileges under Phone page]