CISCO VOICE OVER IP NOTES – PART 2

Gathered by John Meersma, Sunset Learning Institute Technical Instructor

GWGK Commands and Notes

Analog Gateways

- VG224 and VG248 are analog gateways connecting to FXS ports
- The VG224 can be controlled using H.323, MGCP, SIP, and SCCP
- The VG248 can only be controlled using SCCP
- CCM can interface with the IOS driven VG224, not the menu-driven VG248

MGCP

- MGCP - There are two versions, 0.1 and 1.0. All routers use 0.1, most routers support 1.0, however CCM does not. CCM 5.0 uses 0.1.
- To see what capabilities the router has regarding MGCP use: **Router(config)# mgcp package-capability ?**

There are two types of voice gateways:

- **Residential Gateways** - Interface between RJ-11 analog ports and the IP network
- **Trunking Gateways -** Interfaces between PSTN trunks such as DS0 or PRI and the VoIP network

When you use an MGCP gateway, the dial plan resides on the Call Manager

MGCP is the protocol of choice when you need any of the following features:

- Centralized dial-plan control and management
- Simplified gateway configuration
- MGCP backhaul for Q signaling (QSIG) connections, and PRI QSIG facility IE decoding

MGCP Operation

- An endpoint can be either the source or the destination for a media stream.
- Digital or analog lines or virtual endpoint link DSP resources used by a conference bridge
- Use CCM to capture/create endpoints of physical gateways/routers
- An FXS port might look AALN/S0/SU0/1@VoiceGW

ISDN Connections with Backhaul

- An MGCP gateway responds to layer 2 Q.921 signals but does not try to interpret Q.931 call control signals.
- Instead, when a call setup, gateways send Q.931 Layer 3 messages to their CCM

MGCP Fallback

- An MGCP gateway sends keep-alive messages to its primary CCM every 15 seconds.
- If CCM does not respond in 30 seconds, the gateway switches over to the next configured CCM.
- If no CCM's are available, gateway can fall back using default sessions apps
- Voice ports are controlled by a tcl (tickle) script and H.323 controls any VoIP dial peers

Basic MGCP Configuration

- Before configuring MGCP, the router must have hostname, IP address, and routing info enabled

```
Router# config t
Router(config)# mgcp
Router(config)# mgcp call-agent {ip address/hostname} (port) service-type mgcp {version
0.1 | 1.0 | rfc3435-1-0}
Router(config)# ccm-manager mgcp
```

MGCP Configuration Download

- If you would like the gateway to download much of its MGCP config from CCM, you must config that and list the IP address or DNS of the TFTP server (CCM)

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

If successful, you will see:

```
Loading VoiceGW.cnf.xml from 10.1.1.2 (via fa0/0): !
```

Next, bind MGCP to the voice ports. Use caps.

```
Router(config)# dial-peer voice 100 pots
Router(config-dial-peer)# application MGCPAPP | service MGCPAPP
Router(config-dial-peer)# service MGCPAPP (12.4)
Router(config-dial-peer)# port 1/0/0
Router(config-dial-peer)# exit
Router(config)# no mgcp (this resets the connection)
```

Configuring MGCP Fallback

- To use fallback, you must tell the router to use its default call-routing applications when it loses contact with CCM. This command varies by IOS version

```
Router(config)# application
Router(config-app)# global
Router(config-app)# service alternate Default
Router(config-app)# call application alternate default (12.3(14)T ot earlier)
Router(config-app)# exit
!
```

- With MGCP fallback, you must configure at least one dial-peer with a destination pattern so that it can route outbound calls when CCM is unavailable
- This is done with a wildcard such as 9T Use incoming called-number . wildcard if you want to enable the gateway to answer incoming calls in that port

```
Router(config)# dial-peer voice 200 pots
Router(config-dial-peer)# destination-pattern 9T
Router(config-dial-peer)# incoming called-number .
Router(config-dial-peer)# port 1/0/0
Router(config-dial-peer)# exit
```

Assigning MGCP Source IP Address

- By default, MGCP sources its messages from interface loopback 0 if present
- If not, they are sourced from the outgoing interface
- You can designate a specific interface to be used as the source IP address for either MGCP signaling, RTP media, or both
- Configure the loopback interface, then bind control and/or media to the interface, then reinitialize MGCP

```
Router(config)# interface loopback 0
Router(config-if)# ip address 5.5.5.5 255.255.255.255
Router(config-if)#exit
Router(config)# mgcp bind control | media source-interface lo0
Router(config)# end
```

Configuring CCM Redundancy

You can configure the primary CCM with:

```
Router(config)# mgcp call-agent {ip address}
```

Identify additional CCM's

```
Router(config)# ccm-manager redundant-host {ip address/hostname 1 | ip address/hostname 2
Router(config)# ccm-manager 10.1.1.2 10.2.1.2
```

- If the primary CCM returns, the gateway switches back. It does this when an established call has ended by default.

The switchback behavior can be modified

```
Router(config)# ccm-manager redundancy switchback {graceful | immediate | never |
schedul-time | uptime-delay
```

Configuring DTMF Relay

- By default, the gateway sends the DTMF (dialed digits) within the voice RTP stream
- When voice is uncompressed, this is fine
- When G.729 is used, digits can be compressed and distorted

To enable a specific type of DTMF relay:

```
Router(config)# mgcp dtmf-relay voip codec {all | low-bit-rate} mode {cisco | nse | nte-
ca | nte-gw | out-of-band}
Router(config)# exit
```

Show Commands

```
Router# show mgcp
Router# show ccm-manager
Router# show mgcp endpoint
Router# show voice port
Router# show mgcp connection {look for M (mode) to equal M=3 if the connection is able to
send/receive traffic)
```

H.323

H.323 Gateways –

- Translate between the analog ports, PSTN, and the IP network
- H.323 gateways can register with Gatekeepers
- H.323 gateways have the intelligence to place and receive calls

H.323 Gatekeepers –

- Provide a centralized point to resolve E.164 phone numbers to IP addresses and to do call admission control
- Provide call routing, control, security, and bandwidth management

H.323 Terminal –

- Like MGCP, H.323 uses the concept of endpoints
- IP phones and video conferencing stations, in addition to gateways and CCM, can be H.323 endpoints

Multipoint Control Units –

- Allows multiple participants in a conference.
- MCU is composed of MC (multipoint controller) and an MP (multipoint processor)
- The MC handles the H.245 capabilities negotiation and controls conference resources
- The MP does the actual mixing and splitting of the audio and video streams and translation between different codec or bandwidth

Dial Plan Considerations –

- Used to control the treatment of incoming and outgoing calls
- There must be at least one dial peer with a destination pattern to route outgoing calls
- There are default inbound VoIP and POTS dial-peers

The default VoIP dial peer:

- Uses G729r8
- Voice activity detection (VAD) is enabled
- Dual tone multifrequency (DTMF) relay is disabled
- Preference is 0
- Voice media has DSCP of EF, signaling is AF31
- Huntstop is disabled
- Both Req-qos and Acc-qos are best-effort
- No tcl applications are applied
- Fax relay is disabled
- Playout-delay is 40ms

The default POTS dial peer:

- Direct inward dialing is disabled
- Preference is 0
- Digit strip is enabled
- Register the E.164 phone number with a gatekeeper
- Huntstop is disabled
- No IVR applications are applied

Implementing H.323 Gateways

- Before enabling, configure the router with a hostname, IP address, and routing information

Common dial peer settings:

- Codec
- DTMF Relay method
- Dial peer preference
- VAD
- QoS DSCP values
- Call progress indicators
- Fax relay information
- Direct-inward-dial

Voice Class Configuration –

- Voice classes can be configured and applied to dial peers or voice ports

The voiceclass h323 10 commands creates a voice class that lets you configure:

- call - fast or slow H.323 start
- ccm-compatible - for CCM connections, allows CCM -specific behavior
- encoding - configures H.323 ASN.1 encoding
- H225 - includes timeout values for connect/setup/tcp
- H245 - configures H245 settings
- telephony-services - CME H323 connections

Example of Voice Class Configuration

```
Router# voice class codec 1
Router(config-class)# codec preference 1 g729r8
Router(config-class)# codec preference 2 g729br8
Router(config-class)# codec preference 3 g711ulaw
Router(config-class)# exit
!
Router(config)# dial-peer voice 100 voip
Router(config-dial-peer)# incoming called-number .
Router(config-dial-peer)# no vad
!
Router(config-dial-peer)# dial-peer voice 10 voip
Router(config-dial-peer)# destination-pattern 1...
Router(config-dial-peer)# session target ipv4:10.1.1.2
Router(config-dial-peer)# no vad
Router(config-dial-peer)# voice-class codec 1
Router(config-dial-peer)# end
```

Voice Service VoIP Configuration –

- Covers some of the commands in the voice class config, however these commands apply to the gateway as a whole
- If there are conflicts between global Voice Service and dial-peer/voice-port voice class commands, local dial-peer wins

Four config sub-modes exists

- VoFR
- POTS
- VoIP
- VoATM

One use of Voice Service is call redirection

- When the WAN is full (no available bw) CCM will not redirect the call to use another router's POTS connection
- Use Voice Service to do so
- Create another dial-peer with a higher preference (less preferred) for PSTN numbers

On 12.3(7)T and earlier, to enable this you must use:

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

- The "allow connections" allows a router or CME to route between VoIP dial-peers
- This might be used when hair-pinning or redirecting calls

Other options include:

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

H.225 Keepalives

To prevent active calls from being terminated when CCM becomes unreachable, turn off H.225 keepalives between the gateway and CCM

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# no h225 timeout keepalive
```

You can stop or restart the H.323 service in this submode

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# call service stop
Router(conf-serv-h323)# no call service stop
```

Finally you can control Fast Start globally (use a Voice Class to configure it for specific dial-peers)

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# call slow start
```

Redundancy

- In a cluster with multiple CCM's the gateway needs to be set up to use them
- Do this by creating VoIP dial peers pointing to each CCM
- Use a preference value to determine the order each CCM is used

```
Router(config)# dial-peer voice 11 voip
Router(config-dial-peer)# session target ipv4:10.2.1.2
Router(config-dial-peer)# preference 2
```

- You might need to adjust the timers when using multiple CCM, especially if using PRI
- The CCM timeout is 15 secs, whereas the PRI timeout is 10 secs. So the PRI will timeout before the next CCM is tried

To remedy this, change the H.225 TCP session establishment timer

```
Router(config)# voice class h323 10
Router(configs-class)# h225 timeout tcp establish 3
```

Apply this Voice Class to the dial peers pointing to redundant CCM's

```
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# session target ipv4:10.1.1.2
Router(config-dial-peer)# voice-class h323 10
Router(config-dial-peer)# end
```

DTMF Relay

- By default, the gateway sends the DTMF (dialed digits) within the voice RTP stream.
- When voice is uncompressed, this is fine
- When G.729 is used, digits can be compressed and distorted

There are four different ways of sending DTMF tones

- Cisco Proprietary Method
- RTP-NTE
- H.245 Alphanumeric
- H.245 Signal

You configure DTMF Relay under the dial-peer on H.323 gateways

- If no method is configured, the tones are sent in-band with the voice stream
- To configure a specific type:
- Use NTE when connecting sccp phones (CCM) to SIP gateway (router)

```
Router(config)# dial-peer voice 12 voip
Router(config-dial-peer)# dtmf-relay h245-alphanumeric | h245-signal | rtp-nte | cisco-
rtp
Router(config-dial-peer)# end
```

Show Commands

```
Router# show dialplan number (phone number)
Router# show h323 gateway
Router# clear h323 gateway
Router# csim start (phone number) <-- makes the phone number ring
```

Using Trunk Groups for Outgoing Calls

Hunt Groups are used to group multiple voice ports into a single logical target for an outgoing dial-peer

```
Router# config t
Router(config)# trunk group Emergency
Router(config-trunk-group)# description Ports to Reserve for Emergency Calls
Router(config-trunk-group)# hunt-scheme round-robin
!
Router(config-trunk-group)# trunk group Standard
Router(config-trunk-group)# hunt-scheme least-used
Router(config-trunk-group)# exit
```

Controller config to select channels

```
Router(config)# controller t1 0/2/0
Router(config-controller)# framing ef
Router(config-controller)# linecode b8zs
Router(config-controller)# ds0-group 1 timeslots 1-24 type e&m wink-start
Router(config-controller)# trunk-group Emergency timeslots 1-2
```

```
Router(config-controller)# trunk-group Standard timeslots 3-24
Router(config-controller)# end
```

Set additional voice ports into standard trunk group

```
Router# config t
Router(config)# voice-port 1/0/0
Router(config-voiceport)#trunk-group Standard
!
Router(config-voiceport)#voice-port 1/0/1
Router(config-voiceport)#trunk-group Emergency
Router(config-voiceport)#exit
```

Apply trunks to dial-peers

```
Router(config)# dial-peer voice 911 pots
Router(config-dial-peer)# destination-pattern 911
Router(config-dial-peer)# trunkgroup Emergency 1
Router(config-dial-peer)# trunkgroup Standard 2
!
Router(config)# dial-peer 11 pots
Router(config-dial-peer)# destination-pattern 91[2-9]..[2-9].....
Router(config-dial-peer)# trunkgroup Standard
Router(config-dial-peer)# end
```

Dial-Peer Hunting

- Longest Match
- Preference
- Random Selection

Matching Dial-Peers

- Longest Match is always attempted first.
- Multiple dial-peers can have the same destination-pattern assigned.
- Use the preference keyword to assign preference to which dial-peer is selected.

Modify the order logic:

```
Router# config t
Router(config)# dial-peer hunt ?
  <0-7>  Dial-peer hunting choices, listed in hunting order within each choice:
  0 - Longest match in phone number, explicit preference, random selection
  1 - Longest match in phone number, explicit preference, least recent use
  2 - Explicit preference, longest match in phone number, random selection
  3 - Explicit preference, longest match in phone number, least recent use
  4 - Least recent use, longest match in phone number, explicit preference
  5 - Least recent use, explicit preference, longest match in phone number
  6 - Random selection
  7 - Least recent use
```

Pots vs VoIP Dial Peer

- Pots dial-peer only sends the wildcard digits, whereas VoIP sends all of the digits.
- To modify the digits sent by a pots dial-peer for call placed to 555.... and force entire number to be sent:

```
Router# config t
Router(config)# dial-peer voice 555 pots
Router(config-dial-peer)# forward-digits all
Router(config-dial-peer)# prefix 555
Router(config-dial-peer)# exit
```

Dial Peer Operational Status

- For a dial-peer to be included either inbound or outbound matching, it must be operationally active (up/up) meaning it must have one of these met:

Destination pattern - configured and a target configured
Incoming called number - configured
Answer-address - configured

Some ISDN BRI circuits are only active when a call is placed, to prevent call failure in this situation:

```
Router# config t
Router(config)# no dial-peer outbound status-check pots
Router(config)# end
```

Redundant Gateways with CallManager

- If a circuit is down on the first router/gateway CCM sends a call to, the router/gateway will return an "Unallocated Number" message to CCM which causes CCM to stop trying to route the call.

To prevent this on the router/gateway:

```
Router# config t
Router(config)# no dial-peer outbound status-check pots
Router(config)# end
```

- This will cause the router/gateway to send a Temporary Failure message to CCM and CMM will continue attempting to route the call via another redundant gateway
- To prevent this on CCM: set the "Stop Routing On Unallocated Number Flag" service parameter to "False"

Digit Manipulation

Wildcards are used in digit strings to allow a single digit string to match multiple numbers

Wildcard	Function	Examples	Matc hed
.	Matches any single digit	any digit	is matched
[ ]	Range of digits. Contiguous digits are separated by a hyphen. Comma separates individual numbers	[2-4] [2,4] [2-4,7]	matches 2,3, or 4 matches 2 or 4 matches 2,3,4, or 7
+	Previous digit or pattern occurred one or more times	4085+	matches 4085 followed by any number of 5's
?	Previous digit or pattern occurred zero or more times	4085?	matches 408 or 4085
%	Previous digit or pattern occurred zero or more times	4085%	matches 408 or 408 followed by any number of 5's
( )	Used to designate a pattern	408(555)?	matches 408 or 408555

Regular Expression Characters – IOS can use characters, to create translation rules:

- **^ - match the expression at the beginning of the line**
- **$ - match the expression at the end of the line**
- **/ - delimiter that marks the beginning and ending of both the matching and replacement strings**
- **\ - escape the special meaning of the next character**
  - **indicates a range, used with the brackets**
- **[list] - match a single character in a list**
- **[^list] - do not match a single character specified in the list**
- **. - match any character**
- **- repeat the previous regular expression 0 or more times**
- **+ - repeat the previous regular expression 1 or more times**
- **? - repeat the previous regular expression 0 or 1 more time. (Use CTRL-V to enter in the IOS CLI)**
- **() - groups regular expressions**

```
Router# config t
Router(config)# voice translation-rule 1
Router(config)# rule 1 /^555\(....\)/ /444\1/
Router(config)# rule 2 /^\(555\)\(....\)/ /444\2/
Router(config)# end
```

Matching Pattern /^555\(....\)/
Replacement Pattern /444\1/

- Notice parentheses are escaped out with \ characters.
- If the \ was not used, the parenthesis would be matched as part of the string instead of being used to group the expression.
- Parentheses are used to group portions of expressions into sets so you can manipulate it.
- Since the 555 in not in a set, it is ignored, and the first set consists of the four digits following 555

Matching Inbound and Outbound dial-peers

- Incoming dial-peers wait for the entire number before trying to match an incoming dial-peer
- Outgoing dial-peers match digit by digit and respond as soon as there is a match
- POTS dial-peers strip all digits except wildcards when forwarding
- VoIP dial-peers always send the entire number
- ANI = the source phone number, or calling-number
- DNIS = the destination phone number, of called-number

Inbound Dial-Peer Matching

1. If the **called number** (DNIS) matches incoming called-number
2. If the **answer-address** (ANI) is matched
3. If the calling number (ANI) matches with the **destination-pattern**
4. If none of the above, and the inbound call is on a POTS line, the **voice-port** is searched
5. If no match is still found, the default dial-peer is used

Outbound Dial-Peer Matching

1. The called-number (DNIS) with the closest **destination-pattern** match is selected
2. If multiple equals exist, the lowest **preference** is used
3. If equal preferences exist, a random dial-peer is selected

Gateway Connected to PSTN and two internal CCM's

Default POTS dial-peer with direct-inward-dial
Provides CCM redundancy

```
Router# config t
Router(config)# dial-peer voice 1500 pots
Router(config-dial-peer)# incoming called-number .
Router(config-dial-peer)# direct-inward-dial

Router(config)# dial-peer voice 2500 voip
Router(config-dial-peer)# preference 1
Router(config-dial-peer)# destination-pattern 1…
Router(config-dial-peer)# session target ipv4:192.168.2.250
!
Router(config)# dial-peer voice 2600 voip
Router(config-dial-peer)# preference 2
Router(config-dial-peer)# destination-pattern 1…
Router(config-dial-peer)# session target ipv4:192.168.2.251
```

Digit Consumption

Various Mechanism for Digit Manipulation:

```
Digit Strip
Router(config)# dial-peer voice 911 pots
Router(config-dial-peer)# destination-pattern 911
Router(config-dial-peer)# no digit-strip
Router(config-dial-peer)# port 1/0/1

Forward-Digits
Router(config)# dial-peer voice 1000 pots
Router(config-dial-peer)# destination-pattern 1…
Router(config-dial-peer)# forward-digits 4
Router(config-dial-peer)# port 1/0/0

Prefix
Router(config)# dial-peer voice 2001 pots
Router(config-dial-peer)# destination-pattern 2…
Router(config-dial-peer)# preference 2
Router(config-dial-peer)# prefix 91616555
Router(config-dial-peer)# port 2/0:23

Number-Expansion
Router(config)# num-exp 5551... 2815551...
Router(config)# dial-peer voice 2000 pots
Router(config-dial-peer)# destination-pattern 2815551…
Router(config-dial-peer)# no digit-strip
Router(config-dial-peer)# port 2/0:23
Router(config-dial-peer)# end
```


```
Router# show num-exp
Router# show dialplan number 2815551…

Caller-ID
Router(config)# voice-port 1/0/0
Router(config-voiceport)# station-id name John Meersma
Router(config-voiceport)# station-id number 2222
```

Voice Translation Rules and Profiles

- Voice Translation rules can be used to change called number – DNIS (destination)
- Voice Translation rules can be used to change calling number – ANI (source)
- Voice Translation rules can be used to change redirected called number – RDNIS

Voice translation rules are grouped to voice translation profiles. Profiles can be linked to:

- VoIP dial-peers
- Voice ports
- Any inbound VoIP call
- Range of IP source IP addresses in VoIP calls
- Trunk group
- T1/E1 controller used for NFAS trunks
- SRST

Each of these can reference two profiles, 1 incoming, 1 outgoing calls

ORDER:
Inbound

- Global / dial-peer / trunk group / source IP / voice-port / NFAS

Outbound

- Voice-port / NFAS / trunk group / source IP / global / dial-peer

Rule:	**Match**	**Change to**
/1…/ /4085551…/	1…	4085551…
/4085551…/ /1…/	4085551…	1…

Create a rule to prepend a 9 to outgoing calls for routing through PSTN

/\(^[2-9].....\)/ /9\1/ replace \1 with 1st set of numbers in parenthesis and add 9 in front

Rule:	**Input String**	**Output String**
/^9/ //	914085550123	14085550123
/^2001/ /3001/	2001	3001
/^(23)…/ /4000/	2025 or 3051	4000
/^2…/ /801&/	2001	8012001
/^2…/ /801\0/	2001	8012001
/.*/ /91&/ type national national	3125552001 type national	913125552001 type national
/\(9\) \([^01].*\)/ /**1**1408**2**	95550134	914085550134

Ignore \1 and \2 parenthesis and place those values back into output string as is

PSTN Translation Rule/Profile

- Local calls: Prefix 9
- National Calls: Prefix 91
- International Calls: Prefix 9011

```
Router# config t
Router(config)# voice translation-rule 1
Router(cfg-translation-rule)# rule 1 /^3035554/  /4/
Router(cfg-translation-rule)# voice translation-rule 2
Router(cfg-translation-rule)# rule 1 /^.*/ /9&/ type subscriber subscriber
Router(cfg-translation-rule)# rule 2 /^.*/ /91&/ type national national
Router(cfg-translation-rule)# rule 3 /^.*/ /9011&/ type international international
Router(cfg-translation-rule)# voice translation-profile pstn-in
Router(cfg-translation-profile)# translate called 1
Router(cfg-translation-profile)# translate calling 2
```

Results

1. A PSTN user dials 13035554444 from 6164980309
2. The gateway accepts the call and modifies the DNIS and ANI. The rule /^3035554/ /4/ modifies the DNIS to 4444, and the rule /^.*/ /91&/ type national national modifies the ANI to 916164980309
3. The phone rings
4. The local user can hit redial to dial out to the 616.498. number because 91 was prepended
5. The PSTN call is routed internally as a four digit extension

Voice Translation Profile Call Blocking

```
Router# config t
Router(config)# voice translation-rule 1
Router(cfg-translation-rule)# rule 1 reject /^616498/
Router(cfg-translation-rule)# voice translation-profile block
Router(cfg-translation-profile)# translate calling 1
Router(cfg-translation-profile)# dial-peer voice 1001 pots
Router(config-dial-peer)# call-block translation-profile incoming block
Router(config-dial-peer)# call-block disconnect-cause incoming invalid_number
```

Results

1. The gateway blocks any incoming call that successfully matches inbound dial-peer 1001 and has a calling number that starts with 616498.

Verifying Voice Translation Rules

```
Router# test voice translation-rule 1 6164984123
6164984123 blocked on rule 1

Router# show voice translation-rule 1
Translation-rule tag: 10

        Rule 1:(Call block rule)
        Match pattern: ^616498
        Match type: none
        Match plan: none
```

```
Router# show voice translation-profile
Translation Profile: block
        Rule for Calling number: 1
        Rule for Called number:
        Rule for Redirect number:

Translation Profile: pstn-in
        Rule for Calling number: 2
        Rule for Called number: 1
        Rule for Redirect number:
```

Call Admission Control

CAC is used to protect the quality of voice calls by preventing call completion if not enough bandwidth or resources are available.

CAC is divided into three categories:

- Local
- Measurement Based
- Resource Based

When multiple CAC mechanisms are in place, the selection process follows these steps:

Step 1: Gateway checks for the 'max conn' config on the outbound dial peer
Step 2: Router checks for CAC based on local system resources, such as CPU usage
Step 3: If Gatekeeper is used, and configured for CAC, that is checked
Step 4: If RSVP is configured, an RSVP reservation is attempted.
Step 5: Any CAC that probes the network is now used

Note: if any step fails, nothing more is checked

Local CAC Mechanisms

- Physical DS0 Limitaions - there can only be as many outgoing calls as available DS0 timeslots
- Maximum Connections - Configure the number of calls allowed per dial-peer

```
Router(config)# dial-peer voice 9 voip
Router(config-dial-peer)# destination-pattern 9.T
Router(config-dial-peer)# max-conn 3
Router(config-dial-peer)# end
```

Local Busyout

- Used when the router is connected to a PBX and WAN interface.
- If the WAN interface goes down, the router busyout's the voice-ports connected to the PBX

```
Router(config)# voice-port 2/0:23
Router(config-voiceport)# busyout monitor serial 1/0/0
Router(config-voiceport)# busyout graceful (waits for calls to complete)
Router(config-voiceport)# end
```

Measurement-Based CAC Mechanisms

- Examines the network between originating and terminating gateways.
- Attempts to measure network latency, delay, and jitter to permit or deny calls
- Uses Service Level Agreement probes (SLA)
- These are the probes sent out through the network
- Call fallback uses the data from the probes to decide to fallback to the PSTN
- If a call is rejected, the gateway looks for a second dial-peer to use

```
Router(config)# ip sla monitor 1
Router(config-sla-monitor)# type ?
  dhcp          DHCP Operation
  dlsw          DLSW Operation
  dns           DNS Query Operation
  echo          Echo Operation
  frame-relay   Perform frame relay operation
  ftp           FTP Operation
  http          HTTP Operation
  jitter        Jitter Operation
  pathEcho      Path Discovered Echo Operation
  pathJitter    Path Discovered Jitter Operation
  tcpConnect    TCP Connect Operation
  udpEcho       UDP Echo Operation
  voip          Voice Over IP measurement


Router(config-sla-monitor)# type pathJitter dest-ipaddr 172.16.0.200 num-packets 100
interval 10
Router(config-sla-monitor)# tos 176 (equals CoS 5 and DSCP 46)
Router(config-sla-monitor)# ip sla monitor schedule 2 start-time now
Router(config-sla-monitor)# end
```

PSTN Fallback

```
Uses statistics collected by probes to decide when to reroute a call to the PSTN, another
IP path, or to deny the call.
Router(config)# call fallback cache-size 128 (default, can be 1-256)
Router(config)# call fallback cache-timeout 600 (default, can be up to 600)
Router(config)# call fallback active
Router(config)# call fallback jitter-probe dscp 46
Router(config)# call fallback jitter-probe num-packets 25 (2-50)
Router(config)# call fallback threshold delay 150 loss 2 (150ms and 2% packet loss)
Router(config)# call fallback threshold icpif 5 (default, can be 0-30 with 30 = total
packet loss)
Router(config)# end
!
Router# test call fallback probe 172.16.0.200
```

H.323 CAC

- The CAC for H.323 VoIP gateways allows you to configure thresholds for local resources, memory, and CPU resources.
- Call Threshold allows two thresholds, high and low, for each resource.
- Call treatment is triggered when the correct value of a resource exceeds the configured high

```
Router(config)# call threshold ?
 global          the global resources of this gateway
 interface       interface triggers for this gateway
 poll-interval   the poll interval for some resources
!
Router(config)# call threshold global ?
 cpu-5sec      the CPU utilization in the last 5 seconds
 cpu-avg       the average CPU utilization
 io-mem        the IO memory utilization
 proc-mem      the Processor memory utilization
```

```
 total-calls  the total number of calls (1-10,000)
 total-mem    the total memory utilization
Router(config)# call threshold global total-calls low 2 high  5 treatment busyout
Router(config)# call threshold interface serial 0/0 int-calls low 2 high 5
!
Router(config)# call treatment on
Router(config)# call treatment action ?
 hairpin  Hairpin
 playmsg  play the selected message
 reject   Disconnect the call and pass down cause code
!
Router(config)# call treatment cause-code ?
 busy         Insert cause code indicating the GW is busy (17)
 no-QoS       Insert cause code indicating the GW can't provide QOS (49)
 no-resource  Insert cause code indicating the GW has no resource (47)
```

Show Commands

```
Router# show call threshold config
Router# show call threshold stats
Router# show call threshold status
Router# show call treatment config
Router# show call treatment stats
Router# show call spike status
Router# show call resource voice stats
```

RSVP Gateway-Configured

```
Router(config)# interface serial 0/0
Router(config-if)# bandwidth 768
Router(config-if)# ip rsvp bandwidth 300 40
Router(config-if)# ip rsvp signaling dscp 31
Router(config-if)#ip rsvp resource-provider none (disable RSVP from suing WFQ so that
flows can use LLQ)
Router(config-if)#ip rsvp data-packet classification none (prevents RSVP from processing
every packet)
Router(config-if)# exit
Router(config)# dial-peer voice 1101 voip
Router(config-dial-peer)# req-qos guaranteed-delay (request)
Router(config-dial-peer)# acc-qos guaranteed-delay (acceptable - must match both ends)
```

Show Commands

```
Router# show ip rsvp interface
Router# show ip rsvp interface detail
Router# show ip rsvp installed detail
```

Class of Restriction

- COR lists restrict certain users (phones) from placing calls
- Use these only if certain phones will not be allowed to call all configured destinations
- COR lists are configured both for incoming and outgoing calls
- Outgoing COR are like partitions in CCM, only assign one COR label
- Incoming are like CSS, they must contain a label to place a call to a the pre-defined destination

Step 1: Build COR labels
Step 2: Build permission groups
Step 3: Apply COR lists to outgoing dial-peer
Step 4: Apply COR lists to incoming dial-peers

Step 1: Define call types only if some phones will be restricted from making these calls

```
Router(config)# dial-peer cor custom
Router(config-dp-cor)# name Local
Router(config-dp-cor)# name LongDistance
Router(config-dp-cor)# name Mobile
Router(config-dp-cor)# name International
Router(config-dp-cor)# exit
```

Step 2: Build permissions groups using COR lists

- All outgoing COR lists should have a single member
- Incoming COR lists should contain a member for each call type that phone should be able to place

Outgoing COR Lists

```
Router(config)#dial-peer cor list LocalCalls
Router(config-dp-corlist)# member Local
!
Router(config-dp-corlist)# dial-peer cor list LDCalls
Router(config-dp-corlist)# member LongDistance
!
Router(config-dp-corlist)# dial-peer cor list MobileCalls
Router(config-dp-corlist)# member Mobile
!
Router(config-dp-corlist)# dial-peer cor list InternationalCalls
Router(config-dp-corlist)# member International
Router(config-dp-corlist)# exit
```

- Each dial-peer list is assigned a member
- Dial-peers are restricted to calling only configured members

Incoming COR Lists

```
Router(config)# dial-peer cor list LobbyPhones
Router(config-dp-corlist)# member Local
!
Router(config-dp-corlist)# dial-peer cor list Employees
Router(config-dp-corlist)# member Local
Router(config-dp-corlist)# member Mobile
!
Router(config-dp-corlist)# dial-peer cor list Managers
```

```
Router(config-dp-corlist)# member Local
Router(config-dp-corlist)# member Mobile
Router(config-dp-corlist)# member LongDistance
!
Router(config-dp-corlist)# dial-peer cor list Executives
Router(config-dp-corlist)# member Local
Router(config-dp-corlist)# member Mobile
Router(config-dp-corlist)# member LongDistance
Router(config-dp-corlist)# member International
Router(config-dp-corlist)# exit
```

Step 3: Apply COR lists to the outgoing dial peers. Only one outgoing COR is supported per dial-peer

```
Router(config)# dial-peer voice 7 pots
Router(config-dial-peer)# description Local calls within Denver
Router(config-dial-peer)# destination-pattern [2-9].....
Router(config-dial-peer)# corlist outgoing LocalCalls
Router(config-dial-peer)# port 2/0:23
!
Router(config-dial-peer)# dial-peer voice 77 pots
Router(config-dial-peer)# description Calls to Mobile phones
Router(config-dial-peer)# destination-pattern 07[7-9].......
Router(config-dial-peer)# corlist outgoing MobileCalls
Router(config-dial-peer)# port 2/0:23
!
Router(config-dial-peer)# dial-peer voice 11 pots
Router(config-dial-peer)# description Long Distance Calls
Router(config-dial-peer)# destination-pattern 9[2-9]..[2-9].....
Router(config-dial-peer)# prefix 1
Router(config-dial-peer)# corlist outgoing LDCalls
Router(config-dial-peer)# port 2/0:23
!
Router(config-dial-peer)# dial-peer voice 100 pots
Router(config-dial-peer)# description International Calls
Router(config-dial-peer)# destination-pattern 00T
Router(config-dial-peer)# corlist outgoing InternationalCalls
Router(config-dial-peer)# port 2/0:23
Router(config-dial-peer)# exit
```

Step 4: Apply the incoming COR lists to the incoming dial-peers

- Incoming COR lists can be applied whether the gateway is servicing SRST, CME, or POTS calls
- This is an example of restricted an FXS port to Local calls only

```
Router(config-dial-peer)# dial-peer voice 4001 pots
Router(config-dial-peer)# description Denver Main Lobby Phone
Router(config-dial-peer)# destination-pattern 4001
Router(config-dial-peer)# corlist incoming LobbyPhones
Router(config-dial-peer)# port 1/0/1
Router(config-dial-peer)# exit
```

Assigning COR Lists with SRST

```
When operating in SRST mode, you are limited to 20 incoming and 20 outgoing COR lists
A default COR list, while in SRST mode, is assigned to directory numbers that don't match
COR list numbers or number ranges.
Router(config)# call-manager-fallback
Router(config-cm-fallback)# ip source address 10.1.1.100 port 2000
Router(config-cm-fallback)# max-phones 8
Router(config-cm-fallback)# max-dns 16
Router(config-cm-fallback)# cor incoming LobbyPhones default
Router(config-cm-fallback)# cor incoming Employees 1 4005 - 4009
Router(config-cm-fallback)# cor incoming Managers 2 4010
Router(config-cm-fallback)# cor incoming Executives 3 4050
Router(config-cm-fallback)# end
```

Assigning COR Lists with CallManager Express

```
Router(config)# ephone-dn 1
Router(config-ephone-dn)# description Company Admin
Router(config-ephone-dn)# number 4005
Router(config-ephone-dn)# cor incoming Employees
!
Router(config)# ephone-dn 2
Router(config-ephone-dn)# description Company Manager
Router(config-ephone-dn)# number 4010
Router(config-ephone-dn)# cor incoming Managers
!
Router(config)# ephone-dn 3
Router(config-ephone-dn)# description Company Executive
Router(config-ephone-dn)# number 4050
Router(config-ephone-dn)# cor incoming Executives
Router(config-ephone-dn)# end
```

Restricting Inbound Calls from PSTN

```
Create two new labels and assign them to a COR list with the same name
Place an outgoing COR on a local POTS dial-peer
Place an incoming COR list on the PSTN phone
Since these will not match, calls from PSTN will not be allowed to access local port
All other IP phones are not affected
All other internal phones are given membership to the local phone

Router(config)# dial-peer cor custom
Router(config-dp-cor)# name Local
Router(config-dp-cor)# name LongDistance
Router(config-dp-cor)# name Mobile
Router(config-dp-cor)# name International
Router(config-dp-cor)# name InToLocalPhone
Router(config-dp-cor)# name OutToLocalPhone
Router(config-dp-cor)# exit
```

Outgoing COR Lists – add InTo and OutTo COR members

```
Router(config)#dial-peer cor list LocalCalls
Router(config-dp-corlist)# member Local
Router(config-dp-corlist)# dial-peer cor list LDCalls
Router(config-dp-corlist)# member LongDistance
Router(config-dp-corlist)# dial-peer cor list MobileCalls
Router(config-dp-corlist)# member Mobile
Router(config-dp-corlist)# dial-peer cor list InternationalCalls
Router(config-dp-corlist)# member International
Router(config-dp-corlist)# dial-peer cor list InToLocalPhone
Router(config-dp-corlist)# member InToLocalPhone
Router(config-dp-corlist)# dial-peer cor list OutToLocalPhone
Router(config-dp-corlist)# member OutToLocalPhone
Router(config-dp-corlist)# exit
```

Incoming COR Lists – give all others access to Local Phone

```
Router(config-dp-corlist)# dial-peer cor list Employees
Router(config-dp-corlist)# member Local
Router(config-dp-corlist)# member Mobile
Router(config-dp-corlist)# member OutToLocalPhone
!
Router(config-dp-corlist)# dial-peer cor list Managers
Router(config-dp-corlist)# member Local
Router(config-dp-corlist)# member Mobile
Router(config-dp-corlist)# member LongDistance
Router(config-dp-corlist)# member OutToLocalPhone
!
Router(config-dp-corlist)# dial-peer cor list Executives
Router(config-dp-corlist)# member Local
Router(config-dp-corlist)# member Mobile
Router(config-dp-corlist)# member LongDistance
Router(config-dp-corlist)# member International
Router(config-dp-corlist)# member OutToLocalPhone
Router(config-dp-corlist)# exit
```

Assigning COR Lists to Dial-Peers – prevent LocalPhone from receiving calls from PSTN

```
Router(config-dial-peer)# dial-peer voice 1 pots
Router(config-dial-peer)# description Inbound from PSTN
Router(config-dial-peer)# incoming called-number .
Router(config-dial-peer)# destination-pattern 4001
Router(config-dial-peer)# corlist incoming InToLocalPhone
Router(config-dial-peer)# port 2/0:23
!
Router(config-dial-peer)# dial-peer voice 4001 pots
Router(config-dial-peer)# description Denver Main Lobby Phone
Router(config-dial-peer)# destination-pattern 4001
Router(config-dial-peer)# corlist incoming LobbyPhones
Router(config-dial-peer)# corlist outgoing OutToLocalPhone
Router(config-dial-peer)# port 1/0/1
Router(config-dial-peer)# exit
```

- Because the inbound COR list is not a subset of the outbound COR list, the goal of restricting PSTN calls to the LocalPhone has been met.
- All other IP phones receive the OutToLocalPhone label incoming COR lists
- Since no outgoing COR lists are assigned to IP phones, calls from PSTN to IP phones will still be completed

SRST and CME

Call Manager Fallback

- Allows IP phones to register with the gateway if there is a CCM failure
- In CCM - System/Device Pool
- If the gateway is not the SRST device, manually configure the SRST to use
- System/SRST

On the Router/Gateway

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# ip source-address 10.1.1.100
Router(config-cm-fallback)# max-ephones 6
Router(config-cm-fallback)# max-dn 12
Router(config-cm-fallback)# limit-dn 7960 2
Router(config-cm-fallback)# system message primary SRTS Mode
```

Configuring SRST Dial Plan Patterns

- IP Phones register their extensions to the Gateway/router
- If the PSTN sends the full E.164 number to the Gateway/Router, that device may not be able to match the IP phone internal extension

Example: IP registers itself as 150 to Gateway/router

- Calls to this phone from PSTN are 3035550150
- Calls from PSTN will fail because Gateway/router does not have dial-peer that matches

Solution: Configure a dialplan pattern

```
!
Router# config t
Router(config)# dialplan-pattern 1 3035550... extention-length 3
```

- This creates the virtual dial-peer needed to route the call from PSTN to IP Phone
- Also provides the E.164 number to use as ANI for outbound calls from this phone

SRST Features:

- If users expect a secondary dial-tone whereas they can dial an extension

```
!
Router(config-cm-fallback)# secondary-dialtone tone
Router(config-cm-fallback)# end
```

Transfer-Pattern

- Allows users to transfer to a device that is not an IP phone - such as a cell phone
- Specific numbers (or number range) need to be allowed for this feature to work
- Up to 32 transfer-patterns are allowed
- When configured, this allows all IP phones to use the transfered numbers
- Use COR to restrict who can/can't transfer to certain numbers

```
Router(config-cm-fallback)# transfer-pattern 16168623996
Router(config-cm-fallback)# transfer-pattern 1616.......
```

Consultative Transfers

- Blind transfers are connected to the destination prior to the ringing tone
- Consultative transfers, the person initiating the transfer is connected to the destination
- This allows the transfer initiator to make sure that the recipient is available and willing to accept the transfer
- SRST supports four transfer methods that are configurable

```
Router(config-cm-fallback)# transfer-system ?
  blind           Perform blind call transfers (without consultation) with
                  single phone line using Cisco proprietary method
  full-blind      Perform call transfers without consultation using H.450.2 or
                  SIP REFER standard methods
  full-consult    Perform H.450.2/SIP call transfers with consultation using
                  second phone line if available, fallback to full-blind if
                  second line unavailable. This is the recommended mode for most
                  systems. See also 'supplementary-service' commands under
                  'voice service voip' and dial-peer.
  local-consult   Perform call transfers with local consultation using second
                  phone line if available, fallback to blind for non-local
                  consultation/transfer target.
```

Forwarding Calls

- Call forwarding is restricted to local IP phones by default
- Allows users to forward their calls to a non-local number
- Configure specific numbers or ranges of numbers as used in transfer-patterns

```
Router(config-cm-fallback)#call-forward pattern 616.......
Router(config-cm-fallback)#call-forward busy 6168622996
Router(config-cm-fallback)#call-forward noan 6168622996 timeout  (3-60000 secs)
```

Music on Hold

- SRST gateway can play Music on Hold from a file on flash, but only for G.711 VoIP or PSTN calls
- Internal calls between IP phones will hear a tone when on hold
- MoH file can be a .wav or .au, but must be 8-bit, 8KHz

Call Preservation

- For H.323 Gateways, active calls are preserved until the H225 keepalive timer expires
- The H225 keepalive time can be disabled so that active calls through an H.323 gateway are preserved indefinitely

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(config)# voice service voip
Router(conf-voi-serv)# no h225 timeout keepalive
```

- IOS 12.4(4)XC allows calls through an H.323 gateway to be preserved when an IP phone fails over its primary CCM to its secondary CCM.
- This feature requires CCM 4.1(3)SR3

```
Router(conf-voi-serv)# call preserve
```

Secure SRST

- SRST 3.3 allows Secure SRST which supports authentication, integrity, and media encryption
- There are five steps for configuring SRST

Step 1: Configure a certificate authority (CA)

- The network must have a CA, such as a Cisco IOS certificate server or Microsoft server

Configuring a Cisco IOS Certificate Server

```
CA_Rtr# config t
CA_Rtr(config)# crypto pki server srstca
CA_Rtr(cs-server)# database level minimum
CA_Rtr(cs-server)# database url nvram
CA_Rtr(cs-server)# issurer-name CN=srstca
CA_Rtr(cs-server)# grant auto
CA_Rtr(cs-server)# no shutdown
      !issue a paraphrase to protect the private key
      !this password is not visable
      Password: colorado
      Re-enter Password: colorado
      %certificate server enabled
Router(cs-server)# end
```

NOTES:

- The “database level" command sets what type of data will be stored in the certificate database
- Default is minimal which stores the minimal info to continue issuing new certs
- Options include:
- names (which adds the serial number and name of each new cert)
- complete (which writes each cert issued - use a tftp server with this option)
- the "database url" specifies where the database entries will be stored - default is flash, but nvram is recommended

Step 2: Auto-enroll and authenticate the Secure SRST router and CA server

- SRST router must obtain a certificate from the CA server
- If using a Microsoft CA server, you need to cut and paste in the certificate or use TFTP

Autoenroll the Secure SRST Router

```
Router# config t
Router(config)# crypto pki trustpoint srst
Router(ca-trustpoint)# enrollment url http://10.1.10.1
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
!
Router(config)# crypto pki authenticate srst
! this command is not necessary if the IOS CA server is the SRST router
!
Router(config)# crypto pki enroll srst
      %start certificate enrollment..
      %create a challenge password, used to revoke a cert, will note be saved in config -
      make a note of it
      Password: denver
      re-enter Password: denver
      %include IP address is the subject name n
      %request certificate from the CA? Y
Router(config)# end
```

Step 3: Enable credentials service on the SRST router

- Enabling credentials service allows CCM to retrieve the device cert of the SRST router and place it in the IP phone config file

Enabling Credential Service

```
Router# config t
Router(config)# credentials
Router(config-credentials)# ip source address 10.1.1.100 (this is the address on the
router that is used when communicating with CCM)
Router(config-credentials)# trustpoint srst
Router(config-credentials)# end
```

Step 4: Import phone certificate files

- For the router to authenticate the IP phones, it must retrieve the cert of the phone
- The SRST router must manually import the phone certificate
- Prior to entering the SRST configuration, obtain the appropriate certificates on CCM
- Certificates on CCM are stored: C:\Program Files\Cisco\Certificates and have a .0 extention.
- Open the cert in WordPad and copy the contents between "-----BEGIN CERTIFICATE---- " and "-----END CERTIFICATE----"

```
Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-checknone
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
!
Router(config)# crypto pki authenticate 7960
       %Enter the base 64 encoded CA certificate.
       %End with a blank line or the work "quit" on a line by itself
```

```
 asjkkkkkkkkkkkfSAFFFFFFFFFFFFFFFFA
AaUISFFFFFFFFFFFFFFFFFFF-0W2EEWSFA
FRASFDUOGF9U8FEWUGEFGIUOE;IOG;EGHEWG
FEOFWFDFDOIHFD'OHFD'[['HIGDH0[GDSHGD
ETC
quit
%do you accept this certificate? y
%certificate successfully imported
Router(config)# end
```

Configuring MGCP Gateway FallBack

```
Router# config t
Router(config)# ccm-manager fallback-mgcp
Router(config)# call application alternate default
Router(config)# application
Router(config-app)# global
Router(config-app-global)# service alternate default
Router(config-app-global)# end
```

Show Commands

```
Router# show ccm-manager
Router# show ephone
Router# debug ephone
Router# debug voice dial peer
Router# debug isdn q931
Router# debug voice ccapi inout
```

DSP Resources

Configure Transcoding and Conferencing (C549) NM-HDV

- The IP address of the configured interface is used to register with CCM
- For C549 DSP's, the MAC address of the physical interface is used for the device name
- Transcoders will use device name MTPxxxxxxxxxxx
- Conference Bridges will use device name CFBxxxxxxxxxxx where xxxxxxxxxx = MAC address

Step 1 Set the interface used for Skinny

```
Router(config)# sccp local fastethernet 0/0
```

Step 2 Configure CCM address

```
Router(config)# sccp ccm 10.1.1.2 priority {1-4} default is 1
```

Step 3 Enable SCCP

- You must set up the SCCP interface before this command

```
Router(config)# sccp
```

Step 4 Configure the voice card to support transcoding and conferencing

```
Router(config)#voice-card 2
Router(config-voicecard)# dsp services dspfarm
```

Step 5 Set the number of transcoder and conferencing sessions

```
Router(config)# dspfarm transcoder maximum sessions 2
Router(config)# dspfarm confbridge maximum sessions 1
```

Step 6 Enable DSP farming

```
Router(config)# dspfarm
```

Step 7 Configure the transcoder and conference bridge resources in CCM

- After completing these steps, the gateway attempts to register with the configured CCM using a device ID of the interface MAC address proceded by:
- MTF - for transcoder resource
- CFB - for conferencing resource

```
Router# config t
Router(config)# sccp local fastethernet 0/0
Router(config)# sccp ccm 10.1.1.2 priority 1
Router(config)# sccp
Router(config)# voice-card 1
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
!
Router(config)# dspfarm transcoder maximum sessions 2
Router(config)# dspfarm confbridge maximum sessions 1
Router(config)# dspfarm
Router(config)# end
```

Show commands

```
Router# show dspfarm all
Router# show interface fa 0/0
Router# show voice dsp voice
```

Configuring Enhanced Transcoding and Conferencing (C5510)

- Used on 2811 Routers
- One of the features of ET&C is the ability to create multiple profiles
- Profiles allow more granular control of resources and enable a gateway to register resources with multiple CCM groups

Step 1: Set the interface used for SCCP

```
2811-RTR(config)# sccp local fastethernet 0/0
```

Step 2: Configure the Call Manager address

```
2811-RTR(config)# sccp ccm 10.2.2.2
```

Step3: Initialize SCCP

```
2811-RTR(config)# sccp
```

Step4: Configure the voice card to support transcoding and conferencing

```
2811-RTR(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
```

Step 5: Create a DSP farm profile for transcoding

```
2811-RTR(config)# dspfarm profile 3 transcoder
2811-RTR(config-dsp-profile)# associate application sccp
2811-RTR(config-dsp-profile)# maximum sessions 4
2811-RTR(config-dsp-profile)# no shutdown
```

Step 6 Create a DSP farm profile for conferencing

```
2811-RTR(config)# dspfarm profile /name/ conference
2811-RTR(config-dsp-profile)# associate application sccp
2811-RTR(config-dsp-profile)# maximum sessions 4
2811-RTR(config-dsp-profile)#  no shutdown
```

Step 7: Create a DSP farm profile for MTP

```
2811-RTR(config)# dspfarm profile 3 mtp
2811-RTR(config-dsp-profile)# associate application sccp
2811-RTR(config-dsp-profile)# max sessions hardware 1-8
2811-RTR(config-dsp-profile)# max sessions software 1-500
2811-RTR(config-dsp-profile)# no shutdown
```

Step 8: Associate profiles with CCM Groups

```
Step 6 Create a DSP farm profile for conferencing
2811-RTR(config)# sccp ccm group 10
2811-RTR(config-sccp-ccm)# associate ccm 1 priority 1
2811-RTR(config-sccp-ccm)# associate ccm 2 priority 2
2811-RTR(config-sccp-ccm)# associate profile 1 register XCD123456
2811-RTR(config-sccp-ccm)# associate profile 2 register CFB123456
2811-RTR(config-sccp-ccm)# associate profile 3 register MTP123456
2811-RTR(config-sccp-ccm)# bind interface fa0/0
2811-RTR(config-sccp-ccm)# end
!
2811-RTR# show dspfarm all
```

Step 9: Define the resources in Call Manager

Transcoding for CallManager Express

Step 1 Set the interface used for Skinny

```
Router(config)# sccp local fastethernet 0/0
```

Step 2 Configure CCM address

```
Router(config)# sccp ccm 10.1.1.2 {priority} default is 1, there can be up to 3 redundant
CCM's
```

Step 3 Enable SCCP

```
You must set up the SCCP interface before this command
Router(config)# sccp
```

Step 4 Configure the voice card to support transcoding and conferencing

```
Router(config-voicecard)# dsp services dspfarm
```

Step 5 Set the number of transcoder and conferencing sessions

```
Router(config)# dspfarm transcoder maximum sessions 2
Router(config)# dspfarm confbridge maximum sessions 1
```

Step 6 Enable DSP farming

```
Router(config)# dspfarm
```

Step 7 Enter telephony-service config mode

```
Router(config)# telephony-service
```

Step 8 Set the maximum number of DSP farms that can be registered to CME

```
Router(config-telephony)# sdspfarm units 1-5
```

Step 9 Specify the maximum number of transcoding sessions supported across all registered transcoders

```
Router(config-telephony)# sdspfarm transcode sessions 1-128 (total number of sessions
provided by all registered transcoders)
```

Step 10 Specify the name of the DSP farm

```
Router(config-telephony)# sdspfarm 1 MTF0006d74d49a1
```

- Device ID of the interface MAC address proceeded by:
- MTF - for transcoder resource
- CFB - for conferencing resource

```
Router# config t
Router(config)# sccp local fastethernet 0/0
Router(config)# sccp ccm 10.1.1.2 priority 1
Router(config)# sccp
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
!
Router(config)# dspfarm transcoder maximum sessions 2
Router(config)# dspfarm confbridge maximum sessions 1
Router(config)# dspfarm
!
Router(config)# telephony-service
Router(config-telephony)# sdspfarm units 3
Router(config-telephony)# sdspfarm transcode sessions 75
Router(config-telephony)# sdspfarm 1 MTF0006d74d49a1
Router(config-telephony)# end
```

Gatekeepers

Services for voice calls that Gatekeepers can provide:

- Address Resolution
- Admission Control
- Bandwidth Management
- Zone Management
- Call Authorization

Gatekeeper Signaling

IOS gatekeeper's use:

- **RAS** (Registration, Admission, and Status Protocol)
- **GUP** (gatekeeper update protocol)
- **GKTMP** (gatekeeper transaction messaging protocol)

RAS Signaling

- Gatekeepers are H.323 devices that use RAS to communicate with Cisco voice gateways
- RAS is a subset of H.225 Signaling protocol
- **Call control and setup** use **H.225** signaling
- **H.245** is a subset of H.323 used for **media control**
- **H.245 flows directly between gateways** to facilitate **setup of the media** stream

Gatekeeper Discovery Process

- Gateways send RAS messages when trying to identify the gatekeeper for its zone

An H.323 gateway can discover its zone gatekeeper in two ways:

Unicast Discovery -

- Requires the IP address of the gatekeeper to be configured on the gateway
- Gateways sends GRQ (gatekeeper request) on UDP 1718
- Multicast Discovery -
- Allows the gateway to automatically discover its gatekeeper
- Gateway sends GRQ messages to 224.0.1.41
- Gateways do not have to have the gatekeeper address statistically assigned

Zone Prefixes

- The Zone prefix is the part of a called number that identifies the destination zone (local or remote) for the call
- The Zone prefix can be based on area code and local exchanges or any characteristic of the called number prefix that makes that number unique to the call routing domain
- Multiple prefixes can exist for a single local zone
- If zone prefixes overlap, longest match rule applies

Technology Prefixes

- An optional H.323 feature that the gatekeeper uses to group gateways by type (voice, video, etc) or class, or pool of gateways

1: Assign the gateway a technology prefix

- This can be done on the gateway so that the prefix is registered with the RRQ
- This can also be done of the gatekeeper so that the tech pre is associated with the gateway IP address
- This ID's the technology (type, class, pool) the GK associates with the GW when performing call routing

2: Prepend a technology prefix to the called number sent in the ARQ to the GK

- Do this on the H.323 VoIP dial-peer config within the gateways
- The GK attempts to match the appended tech-prefix with the prefix of a registered gateway to ID the destination zone for routing

NOTE: the technology prefix is stripped from the called number when the GK matches a zone prefix, however the tech prefix is sent to the gateway along with the full dialed number.
Make sure the POTS dial-peers are updated to handle this properly

Gatekeeper Configuration

```
Denver-GK(config)# interface loopback 0
Denver-GK(config-if)# description Gatekeeper Interface
Denver-GK(config-if)# ip address 10.100.100.1 255.255.255.255
Denver-GK(config-if)# no shutdown
Denver-GK(config-if)# exit
!
Denver-GK(config)# gatekeeper
Denver-GK(config-gk)# zone local denver cisco.com 10.100.100.1
Denver-GK(config-gk)# zone local dallas cisco.com
Denver-GK(config-gk)# no shutdown
Denver-GK(config-gk)# end
```

Gateways Configuration

- Configure at least one of its interfaces as a gateway interface
- Use a reliable interface, such as a loopback

```
Denver-GW(config)# interface loopback 2
Denver-GW(config-if)# h323-gateway voip interface
```

Define the name and location of the gatekeeper for this gateway:

- The gatekeeper id must match the zone name that is defined to the gatekeeper for the zone that will control this gateway

```
Denver-GW(config-if)# h323-gateway voip id denver ipaddr 10.100.100.1
```

Optionally you can define the H.323 name of the gateway to help ID this gateway to the gatekeeper

- H.323 name is usually the hostname of gateway and the gateway domain name

```
Denver-GW(config-if)# h323-gateway voip h323-id Denver-GW
```

Gateway Config

```
Denver-GW(config)# interface loopback 2
Denver-GW(config-if)# h323-gateway voip interface
Denver-GW(config-if)# h323-gateway voip id denver ipaddr 10.100.100.1
Denver-GW(config-if)# h323-gateway voip h323-id Denver-GW
```

Gatekeeper Show Commands

```
Denver-GK# show gatekeeper endpoints
Denver-GW(config-if)# h323-gateway voip h323-id Denver-GW
```

Gatekeeper Configuration Steps:

1. Configure local and remote zones on the gatekeeper
2. Configure zone prefixes
3. Configure technology prefixes
4. Configure gateways to use H.323 gatekeepers
5. Configure dial peers

```
Router(config-gk)#?
  accounting                Enable accounting
  alias                     Configure alias entries
  arq                       Configure Admission Request (ARQ) behaviour
  bandwidth                 Configure bandwidth management
  default                   Set a command to its defaults
  endpoint                  Configure endpoint characteristics
  exit                      Exit from config-gk configuration mode
  gw-type-prefix            Set gateway technology prefix
  h323-annexg               H323 Annex G
  help                      Description of the interactive help system
  irq                       Configure Information Request (IRQ) behaviour
  load-balance              Configure gatekeeper load balancing characteristics
  lrq                       Configure Location Request (LRQ) behaviour
  no                        Negate a command or set its defaults
  rrq                       Configure Registration Request (RRQ) behaviour
  security                  Enable H.323 security option
  send-cisco-circuit-info   Send V4 circuitInfo in remoteExtensionAddress of LCF/ACF
  server                    Gatekeeper Server Configuration
  shutdown                  Shutdown Gatekeeper
  timer                     Configure various gatekeeper timers
  use-proxy                 Specify proxy usage for call scenarios
  zone                      Zone Setup
```

Gatekeeper Configuration

- SanJose and Houston are zones this GK is responsible for
- 192.168.2.100 is local GK IP address. Use it once as it is used for each subsequent listing

```
Denver-GK(config)#gatekeeper
Denver-GK(config-gk)# zone local SanJose sunset.com 192.168.2.100 (IP of GK)
Denver-GK(config-gk)# zone local Houston sunset.com
Denver-GK(config-gk)# no shutdown
```

Configuring Zone Prefixes

- Priorities range from 1-100. 50 is default. Higher is better. 0 means GW will never be used
- If multiple GW exist for zone, **blast** means send LRQ to all, **seq** means one at a time

```
Denver-GK(config)# gatekeeper
Denver-GK(config-gk)# zone local SanJose sunset.com 192.168.2.100
Denver-GK(config-gk)# zone local Houston sunset.com
Denver-GK(config-gk)# zone prefix SanJose 2... ?
  blast                 Sending simultaneous LRQ to remote zones
  gw-default-priority   Default gateway priority associated with the zone prefix
  gw-priority           Priority associated with following gateway(s) for this prefix
  seq                   Sequential LRQ sending to remote zones
  <cr>

Denver-GK(config-gk)# zone prefix SanJose 2... gw-priority 5 SanJoseRtr1
Denver-GK(config-gk)# zone prefix SanJose 2... gw-priority 10 SanJoseRtr2
Denver-GK(config-gk)# no shutdown
```

Configuring Technology Prefixes

- Tech-prefixes enable the gatekeeper to select the appropriate hop-off gateway
- Callers need to know and add the tech-prefixes that are defined
- The 99#* means callers prepend 99# to calls. * means anything after, like .T in dial-peers
- We assign tech-prefix of #99* to Houston GW w/IP address 192.168.1.1

```
Denver-GK(config)# gatekeeper
Denver-GK(config-gk)# zone local SanJose sunset.com 192.168.1.100 (GK IP address)
Denver-GK(config-gk)# zone local Houston sunset.com
Denver-GK(config-gk)# zone prefix SanJose 2…
Denver-GK(config-gk)# zone prefix Houston 3…
Denver-GK(config-gk)# gw-type-prefix 99#* gw ipaddr 192.168.1.1 1720
Denver-GK(config-gk)# gw-type-prefix 1#* default-technology
Denver-GK(config-gk)# no shutdown
```

CUBE - Cisco Unified Border Endpoint

Configuring H.323-to-H.323 Internetworking

- Enable Protocol Internetworking (Call Hair-pinning)

```
Router# config t
Router(config)# voice service voice
Router(config-voice-service)# allow-connections h323 to h323
Router(config-voice-service)# allow-connections sip to sip
Router(config-voice-service)# allow-connections h323 to sip
Router(config-voice-service)# allow-connections sip to h323
!
```

Enable H.323 to H.323 Internetworking

Configuring H.323 dial peer on CUBE between CME and CCM cluster

```
Router# config t
Router(config)# voice service voice
Router(config-voice-service)# allow-connections h323 to h323
!
Router(config)# dial-peer voice 2001
Router(config-dial-peer)# description To Cisco Unified Communications Manager
Router(config-dial-peer)# destination-pattern 2...
Router(config-dial-peer)# session-target ipv4:192.168.1.1
!
!
Router(config)# dial-peer voice 3000
Router(config-dial-peer)# description To Cisco Unified Communications Manager Express
Router(config-dial-peer)# destination-pattern 3...
Router(config-dial-peer)# session-target ipv4:192.168.2.254
!
!
```

Configuring H.323-to-SIP Internetworking

- Enable H.323 to SIP Internetworking
- Configuring H.323 and SIP dial peers on CUBE between CME and SIP Carrier

```
Router# config t
Router(config)# voice service voice
Router(config-voice-service)# allow-connections h323 to sip
                        OR
Router(config-voice-service)# allow-connections sip to h323

Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# description To Cisco Unified Communications Manager
Router(config-dial-peer)# destination-pattern 2...
Router(config-dial-peer)# session-target ipv4:192.168.1.1
Router(config-dial-peer)# dtmf-relay h245-alphanumeric
!

Router(config)# dial-peer voice 9011 voip
Router(config-dial-peer)# description To International SIP Carrier
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# destination-pattern 9011T
Router(config-dial-peer)# session target ipv4:192.168.10.254
Router(config-dial-peer)# dtmf-relay rtp-nte digit-drop h245-alphanumeric
!
```

Media Flow and Transparent Codec

- CUBE can act as a proxy for H.323 and SIP (proxy signaling)
- Media flow-through (default): All media streams are routing through the CUBE
    - Solves IP interworking issues
    - Hides IP original addresses
    - Tighter Security

Configures media flow-around or flow-through on a dial-peer

- This can also be configured globally or in a voice class

```
Router(config)# dial-peer voice 9011
Router(config-dial-peer)# media flow-around | flow-through
```

Transparent Codec

- Enables CUBE to pass codec capabilities between endpoints
- If configured, uses the codec specified by the endpoints
- This command enables endpoint-to-endpoint codec negotiation without CUBE

```
Router(config)# dial-peer voice 9011
Router(config-dial-peer)# codec transparent
```

Dial-peer config w/ Media Flow-Around and Transparency

```
!
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# description To Cisco Unified Communications Manager
Router(config-dial-peer)# destination-pattern 2...
Router(config-dial-peer)# session-target ipv4:192.168.1.1
Router(config-dial-peer)# codec transparent
Router(config-dial-peer)# media flow-around
!
```

```
Router(config)# dial-peer voice 3000
Router(config-dial-peer)# description To Cisco Unified Communications Express
Router(config-dial-peer)# destination-pattern 3...
Router(config-dial-peer)# session target ipv4:192.168.10.254
Router(config-dial-peer)# codec transparent
Router(config-dial-peer)# media flow-around
```

CUBEs and Via-Zone Gatekeeper

- Gatekeeper is configured with two local zones: SJC and CHI
- Calls between Chicago and SanJose should be routed by the GK.
- Instead of routing directly between the two zones, the GK should route the calls through the VIA-ZONE, which includes the CUBE
- CUBE and GK can reside on the same router

```
Router(config)# interface lo0
Router(config-if)# ip address 192.168.66.14 255.255.255.0
!
Router(config)# gatekeeper
Denver-GK(config-gk)# zone local SJC sunset.com 192.168.66.14 invia VIA outvia VIA
Denver-GK(config-gk)# zone local CHI sunset.com invia VIA outvia VIA
Denver-GK(config-gk)# zone local VIA sunset.com
Denver-GK(config-gk)# zone prefix SJC 1*
Denver-GK(config-gk)# zone prefix CHI 3*
Denver-GK(config-gk)# gw-type-prefix 1#* default-technology
Denver-GK(config-gk)# no shutdown
```

After GK configuration is done, the CUBE configuration is performed on the same router

```
!
Denver-GK(config)# voice service voip
Denver-GK(config-voice-service)# allow-connections h323 to h323 (enables h323
interworking)
!
Denver-GK(config)# interface loopback 1
Denver-GK(config-if)# ip address 192.168.66.15 255.255.255.0
Denver-GK(config-if)# h323-gateway voip interface
Denver-GK(config-if)# h323-gateway voip id VIA ipaddr 192.168.66.14 1719 (ID this GW uses
to register w/ the GK that has this IP address)
Denver-GK(config-if)# h323-gateway voip h323-id IPIPGW
Denver-GK(config-if)# h323-gateway voip tech-prefix 1#
!
Denver-GK(config)# dial-peer voice 10 voip
Denver-GK(config-dial-peer)# destination-pattern 1...
Denver-GK(config-dial-peer)# session target ras
!
Denver-GK(config)# gateway
```

Verifying CUBES and Via-Zone Gatekeepers

```
GKIPIPGW# show gatekeeper endpoints
GKIPIPGW# show gatekeeper calls
```

MEDIA TERMINATION POINT - CUBE

- MTP Co-resident with the Cisco Unified Border Element
- If software MTP is required by the Cisco Unified Communications Manager configuration, this can be configured on the same router used for the Cisco Unified Border Element.

Configuration of the Cisco Unified Border Element for an MTP:

```
sccp local FastEthernet0/1
sccp ccm 15.5.34.1 identifier 1 version 4.1
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
associate profile 1 register MTP
!
dspfarm profile 1 mtp
codec g711ulaw
maximum sessions software 100
associate application SCCP
!
```

TRANSCODING - CUBE

- The Cisco Unified Border Element can do transcoding between G.711µ-law/a-law and various flavors of G.729
- Transcoding can be invoked for any call whether it originates from Cisco Unified Communications Manager towards the PSTN, or from the PSTN towards Cisco Unified Communications Manager
- The main criterion is if the two call legs on the Cisco Unified Border Element have different codecs - G.711 and G.729
- The configuration of transcoding on the Cisco Unified Border Element requires DSPs to be available on the platform

Configuration of the Cisco Unified Border Element for transcoding:

```
voice-card 2
dspfarm
dsp services dspfarm
sccp local FastEthernet 0/0
sccp ccm 200.1.1.100 identifier 1
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
associate profile 1 register MTP123456782012
keepalive retries 5
switchover method immediate
switchback method immediate
switchback interval 15
!
dspfarm profile 1 transcode
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec gsmfr
```

```
codec g729r8
maximum sessions 5
associate application SCCP
telephony-service
load 7960-7940 P00303020214
max-ephones 48
max-dn 48
ip source-address 200.1.1.100 port 2000
!
sdspfarm units 1
sdspfarm transcode sessions 50
sdspfarm tag 1 MTP123456782012
create cnf-files version-stamp 7960 Jul 29 2002 13:50:03
```

TCL - CUBE

Using Tcl IVR on the Cisco Unified Border Element

The Cisco Unified Border Element supports Tcl scripts, and you can configure them under the VoIP dial-peers. There is no need for a DSP in order to use the Tcl functionality. There are a number of Tcl applications already built into Cisco IOS Software that can be used for Cisco Unified Border Element deployments. The Cisco IOS authentication, authorization, and accounting (AAA) functionality can also be used in conjunction with Tcl scripting and the Cisco Unified Border Element to provide authentication and authorization of calls.

```
aaa new-model
!
aaa authentication login h323 group radius
aaa authorization exec h323 local group radius
aaa accounting exec h323 start-stop group radius
!
application
service debitcard tftp://15.5.27.11/app_debitcard.2.0.2.8.tcl
paramspace english index 1
paramspace english language en
paramspace english location tftp://15.5.27.11/prompts/en/
param pid-len 4
paramspace english prefix en
param uid-len 6
!
gw-accounting aaa
!
radius-server host 15.5.27.11 auth-port 1645 acct-port 1646
radius-server timeout 10
radius-server key lab
radius-server vsa send accounting
radius-server vsa send authentication
!
```

LOGGING

```
logging console informational
logging buffer 200000 debug
service sequence-number
service timestamp debug date msec•show—This is relevant output:
```

SHOW COMMANDS

```
show version
show run
show voip rtp connection (once the call is up)
show call active voice brief (once the call is up)
```

H.323 to H.323 Debug

```
debug h225 asn1
debug h225 q931
debug h225 events
debug h245 asn1
debug h245 events
debug h225 q931
debug cch323 all
debug voip ipipgw
debug voip ccapi inout
```

H.323 to SIP Debug

```
debug h225 asn1
debug h225 q931
debug h225 events
debug h245 asn1
debug h245 events
debug cch323 all
debug voip ipipgw
debug voip ccapi inout
debug ccsip allSIP to SIP Scenarios

debug ccsip all
debug voip ccapi inout

debug dspfarm all
debug sccp messages
debug voip rtp session named-events
```