Kofax Communication Server

VoIP / FoIP Environment Guide

Version: 10.3.0

Date: 2019-12-13

KOFAX

Table of Contents

Preface....6
Related Documentation....7
Chapter 1: Overview....8
Fax over IP Integration....8
Supplementary Services - Redirecting Number (Call Diversion)....10
Chapter 2: Integration with Gateways....11
Cisco Gateways....11
FoIP Integration....11
Redirecting Number (Call Diversion) Using H.323....17
SIP VoIP IPV6 Integration....17
Hints for Cisco Gateways....17
Dialogic Media Gateway DMG4000 Series....17
Hints for Dialogic Media Gateway....18
Patton Gateway....18
Configuring the Gateway....18
Configuring FoIPv3....20
Hints for Patton Gateway....20
Chapter 3: Integration with Software PABX....22
Cisco CallManager....22
KCS FoIP T.38 and Voice Integration Overview....22
Functional Blocks on the CCM/CUCM Side....23
CUCM 6.x and 7.1 Remarks....24
Integration Without Encryption....24
Integration with Encryption....47
Hints....60
Cisco Gatekeeper....61
Integration of a Cisco Gatekeeper....61
Configuration of the Cisco Gateway....61
Configuration of the Cisco Gatekeeper....62
Configuration of FoIP....62
Configuration of Multiple Zones....63
GNUGk 2.0.8....63
VoIP Integration via H.323....63
Huawei SoftX3000-Softswitch....66

Fax Integration via SIP Trunk..... 66
Mitel 3300 ICP Voice.....67
Fax Integration via SIP Trunk..... 67
Siemens HiPath 4000 V4.0.....69
Example Integration via H.323..... 69
Example Integration via SIP.....72
Siemens HiPath 4000 V6.0.....74
Siemens OpenScape Voice V3.1 R2..... 75
Configuration as Subscriber..... 75
Configuration as Endpoint..... 77
Siemens OpenScape Voice V4.....83
Siemens OpenScape Voice V6.....84
Siemens OpenScape Voice V7.....84
Siemens OpenScape Voice V8.....84
Avaya Aura Communication Manager 5.2.1..... 84
Avaya Aura CM General Configuration.....87
H.323 Integration..... 100
SIP Integration..... 104
Useful Troubleshooting/Tracing Options.....111
Avaya Aura Communication Manager 6.01..... 114
Avaya Aura Communication Manager 6.2..... 114
Avaya Aura Communication Manager 6.3..... 115
Avaya Aura Communication Manager 7.0..... 115
Avaya Aura Communication Manager 7.0.1..... 116
Microsoft Lync Server 2013..... 116
Integration as SIP Trunk Without Encryption..... 116
Enable Encryption of SIP Messages.....125
Enable Media Encryption (SRTP)..... 139
Troubleshooting and Hints.....141
Chapter 4: Integration with SIP Providers.....146
Swisscom SIP Trunk..... 146
FoIP Configuration.....146
Chapter 5: Recommended Tools and Hints..... 149
Tools.....149
MyPhone (H.323 Telephone Software)..... 149
OpenPhone (H.323 Telephone Software)..... 152
SIP SoftPhone..... 155
Wireshark..... 158

Audacity....161
Hints....161
Check for Open H.323 Listeners on the Local Interfaces....162
Check the LAN Connections....162
Set Caller ID for Outgoing Calls....163
SIP Protocol Basics and Examples....163
Concurrent Operation with KCS H.323 Integration for Voice on the Same Machine....166
Check the ISDN Line Synchronization Up to the CISCO Gateway (BERT)....166
Bad Fax Quality Due to RTP-NTE....168
Outgoing Secure SIP Call Fails with Error Code 12700....168

Preface

This guide describes integration of Kofax Communication Server with Fax over IP and Voice over IP.

Related Documentation

This document refers to the following documentation:

- Voice Platform Technical Manual
- Fax over IP Technical Manual

For information about Cisco products, see the Cisco documentation.

- Cisco Fax Relay Trouble Shooting Guide: http://www.cisco.com/en/US/customer/tech/tk652/tk777/technologies_tech_note09186a0080114565.shtml (free http://www.cisco.com registration required)
- Cisco IOS Documentation (use the search function at http://www.cisco.com to look up IOS configuration parameters or topics)
- Cisco Feature Navigator (http://www.cisco.com/go/fn)

Chapter 1

Overview

This chapter provides an overview of Fax over IP integration and supplementary services.

Fax over IP Integration

Third Party IP System	Protocol(s)	Min. FoIPv3 version	Outbound Modes				Inbound Modes				Notes
			10	20	40	60	10	20	40	60	
Alcatel PABX	SIP	3.02.03	#	#	#						5)
Cisco Gatekeeper	H.323+RAS (Term.)	3.02.03									5)
	H.323+RAS (GW)	3.03.01									5)
Cisco Gateway	H.323, SIP	3.02.03	#	#	#		#	#	#		5)
Cisco CM 4.x + Cisco GW	H.323	3.02.03	#				#				5)
Cisco UCM 6.x + Cisco GW	H.323, SIP	3.02.03	#				#				5)
Dialogic DMG300x or DMG 400x	SIP	3.11.06	#	#	#		#	#	#		3), 5)
Huawei SoftX3000-Softswitch	SIP	3.10.00	#	#			#	#			5)
Mitel 3300 Voice	SIP	3.09.04	#				#				5)
Patton GW R4.2	H.323, SIP	3.02.03	#	#	#						5)
Patton GW R5.2	H.323	3.02.03	#	#	#						5)
	SIP	3.03.02									#14637, 5)
Siemens HiPath 4000 V4	H.323, SIP	3.02.03	#	#	#		#	#	#		1), 5)
Siemens HiPath 4000 V6	H.323, SIP	3.13.03	#	#	#		#	#	#		5)
Siemens OpenScape Voice V3.1 with Siemens RG87xx	SIP+Reg	3.02.03	#	#	#		#	#	#		2), 5)
Siemens OpenScape Voice V3.1 with Mediatrix 4404	SIP+Reg	3.02.03	#	#	#		#	#	#		5)

Third Party IP System	Protocol(s)	Min. FoIPv3 version	Outbound Modes				Inbound Modes				Notes
			10	20	40	60	10	20	40	60	
Siemens OpenScape Voice V4 with Mediatrix 4402 with Mediatrix 4124 with Mediatrix 1104 with AP1120 with RG8702	SIP+Reg	3.10.07	#	#	#		#	#	#		5)
Siemens OpenScape Voice V6 with Mediatrix 4104 with Mediatrix 4404 with RG8702 with OSV Branch 50i	SIP+Reg	3.13.03	#	#	#		#	#	#		5)
Siemens OpenScape Voice V7 with Mediatrix 4124 with Mediatrix 4404 with RG8702 with OSV Branch 50i	SIP+Reg	3.18.03	#	#	#	#	#	#	#	#	
Siemens OpenScape Voice V8 with Mediatrix 4124 with Mediatrix 4404 with RG8702 with OSV Branch 50i	SIP+Reg	3.24.08	#	#	#	#	#	#	#	#	
Swisscom SIP trunk	SIP	3.23.00		#		#		#		#	
Avaya Aura CM 5.2.1 with SES for SIP	SIP+H.323	3.12.07	#	#	#		#	#	#		4), 5)
Avaya Aura CM 6.0.1 With Session Manager for SIP	SIP+H.323	3.12.07	#	#	#		#	#	#		4), 5)
Avaya Aura CM 6.2 With Session Manager for SIP	SIP+H.323	3.16.20	#	#	#	#	#	#	#	#	4)
Avaya Aura CM 6.3 With Session Manager for SIP	SIP+H.323	3.22.05	#	#	#	#	#	#	#	#	
Avaya Aura CM 7.0 With Session Manager for SIP	SIP+H.323	3.24.22	#	#	#	#	#	#	#	#	
Avaya Aura CM 7.0.1 With Session Manager for SIP	SIP+H.323	3.26.11	#	#	#	#	#	#	#	#	

Inbound/(Outbound Modes:

10 = Switch to T.38 w/o G.711 pass-through support

20 = Try T.38 with a fallback to G.711 pass-through

40 = Use G.711 pass-through unless T.38 is requested by remote side (default)

60 = Use G.711 pass-through and prevent switch to T.38

Symbol usage:

Supported and most recommended option

Supported

Not supported

Notes:

1) Minimum software release on Siemens HiPath 4000 V4, HG3550 is HG35xx LW pzksti40.o4.019-15. T.38 does not work reliable with older releases. See Hint 14385 or Siemens problem number NA03559307.

2) Minimum software release on Siemens RG8702 Gateway is V1.3. T.38 did not work with older releases.

3) Inbound calls with V.34 may fail due to SPR70456.

4.) MWI does not work.

5.) The columns with the supported inbound/outbound mode does not consider G.711 pass-through mode. This means that operation may be supported even if the column is marked as “not supported”.

Supplementary Services - Redirecting Number (Call Diversion)

Redirecting numbers can be delivered in various ways. We have tested four implementations for H.323 protocol and one SIP implementation:

	VoIP	GW 2600 12.3(11)	GW 2600 12.3(7)	GW 2821	CCM6	HiPath 4000
H.450.3	+	-	+	-	-	-
Q.931	+	-	-	-	+	-
Cisco CM prop.	+	-	-	-	+	-
Cisco GW prop.	-	+	-	+	-	-
Tunneled Signaling Message	+	-	-	-	-	+
SIP diversion header	+	?	?	?	+	+

The first two implementations are standardized. Cisco CallManager and Cisco gateways have a proprietary implementation.

The Q.931 standard can deliver only a single number. The H.450.3 standard delivers two numbers: the first one (original called number) and the last one (diverting number).

On Cisco gateways, the support of various implementations may depend on the IOS version.

Chapter 2

Integration with Gateways

This chapter provides information about integration with gateways.

Cisco Gateways

This section provides information about integration with Cisco gateway.

FoIP Integration

This section describes a setup example of Kofax FoIP solution with a Cisco Router as VoIP/FoIP gateway.

The installation is done in two steps.

1. Configuring the gateway. A VoIP application can be used to test if the gateway is working correctly.
2. Installing FoIP instead of the VoIP application.

Prerequisites

- A voice and fax over IP gateway which supports H.323 or SIP and T.38.

  If you use a Cisco router as gateway, you need a proper IOS software version installed on the router. The third party products we use for testing can be found in the *Tools* section. Any problems arising with different products or versions are not supported by Kofax.

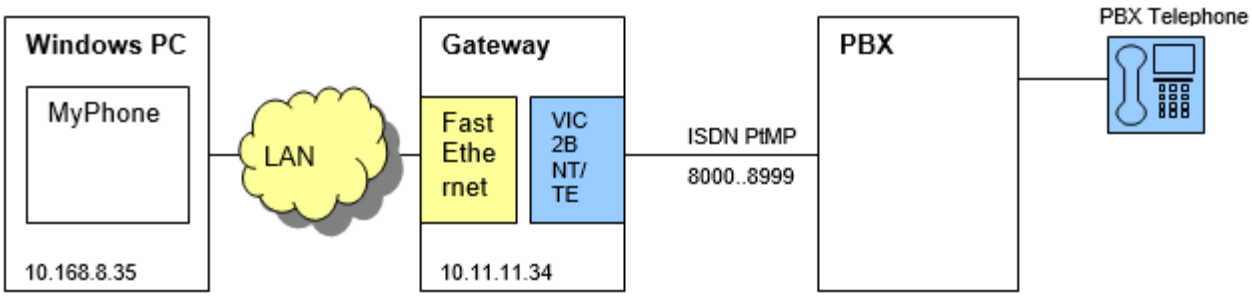
  In this guide we assume that the LAN interface and the ISDN interfaces are properly configured. Refer to the Cisco documentation for details.

  Tip
  If you use a Cisco gateway and you want to know if it is compatible to TC/FoIP you can use the Cisco Feature Navigator (http://www.cisco.com/go/fn). It is required to register an account at Cisco website before you can use it. The Feature Navigator lets you select a particular feature and shows you a complete list all Cisco products, which support this feature. Select the feature “T.38 Fax Relay for VoIP H.323”. If your Cisco hardware appears in the list, your gateway is compatible to TC/FoIP.

- Windows computer with a static IP address (preferably the TCOSS server; with soundcard)

Configuring the Gateway

This section describes how to set up the gateway. An overview of this step is shown below:



1. Boot the gateway and plug in the ISDN line to the ISDN BRI S/T 0-Port VIC 2B NT/TE. The OK-LED must be activated. Make sure that the gateway has a LAN connection (10 or 100 Mbps) on the FastEthernet 0/0 interface.
2. Initially, a Cisco gateway is configured over the serial port. Connect the "CONSOLE" port of the gateway to a machine where a terminal application is running. Baud rate: 9600; Data 8 bit; Parity: none; stop: 1 bit; Flow control: none.
   Hint: If the gateway already has an IP configuration it can also be accessed via telnet or SSH. If you do that, you have to enter “terminal monitor” to see traces in the telnet session.
   If the gateway is booted and you press enter in the terminal, the standard prompt appears which ends with ">". Type "enable" and type the enable password. Then type "configure terminal" to enter the configuration mode. The configuration prompt appears which ends with "(config)#".

   ```
   Cisco2620>
   Cisco2620>enable
   Password:
   Cisco2620#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   Cisco2620(config)#
   ```

   By typing "show run" in the enable mode you can display the configuration which is currently running. It contains all configured interfaces, services, dial-peers and more. If you type "?" you get a list of commands available in the current context. Typing "exit" gets you back to the previous mode. In the configuration mode you have to precede the “show” command with “do” (“do show run”). Auto completion and “?” are not available in this mode.

   The next two steps are only necessary if your gateway has no ISDN interface configured and no voice service defined yet. If you configure on a gateway where this is already set up correctly, you can continue with step 7.
3. Configure the gateway’s LAN interface for H.323. This step is not necessary when you use SIP. Type "interface FastEthernet 0/0" in the configuration mode. You will see the following prompt.

   ```
   Cisco2620(config)#interface FastEthernet 0/0
   Cisco2620(config-if)#
   ```

   Let’s assume that the IP address of the gateway is 10.11.11.34. Type "h323-gateway voip interface" and "h323-gateway voip bind srcaddr 10.11.11.34". Then type "exit" to return to the configuration mode. If you type "show" something like this must appear in the configuration.

   ```
   interface FastEthernet0/0
    ip address 10.11.11.34 255.0.0.0
    no ip mroute-cache
    speed auto
    half-duplex
    h323-gateway voip interface
    h323-gateway voip bind srcaddr 10.11.11.34
   ```

4. Configure a VoIP/FoIP service on the gateway. As a prerequisite for the dial-peer created in the next step, a service is needed on the gateway. Type "voice service voip" in the configuration mode. The following prompt appears. You are now in the configuration menu for this service.

```
Cisco2620(config)#voice service voip
Cisco2620(conf-voi-serv)#
```

Configure the fax protocol by typing "fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none". If you use H.323, type "h323". With the command "exit" you can return to the configuration mode. Check the service with show.

```
voice service voip
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none
 h323
```

5. Configure a dial-peer on the gateway. A dial peer is used to assign an MSN to an IP address. If you want to associate the Windows machine (10.168.8.35) with the MSNs 8000 – 8999 (this means that the gateway makes a connection to 10.168.8.35 if a call to one of the MSNs 8000 - 8999 comes in from ISDN) you have to do the following. Type "dial-peer voice 8000 voip" to create a new dial-peer with the ID 8000

You are now in the configuration mode for this dial-peer. After configuring type "exit" to return to configuration mode. If you type "show" the dial-peer must appear in the configuration like this.

```
dial-peer voice 8000 voip
 destination-pattern 8...
 session target ipv4:10.168.8.35
 dtmf-relay h245-alphanumeric
 codec g711alaw
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none
 no vad
```

Note The number specified at the destination-pattern (8…) in our example is used to match the dial-peer on an inbound call to this number but also on an outbound call due to the calling party number which the TCOSS server sets. “8…” like in this example matches exactly to inbound calls to number 8000 - 8999 and outbound calls from calling party numbers 8000 - 8999. In this example we use wildcards ‘.’ for exactly one arbitrary digit. You can also specify ‘T’ (interdigit timeout) for any number of arbitrary digits. For details please search for “Configuring Dial Plans, Dial Peers, and Digit Manipulation” on http://www.cisco.com/ and then look for “Destination Pattern” in this document.

If you use SIP you need to specify the protocol with “session protocol sipv2”and select “dtmf-relay sip-notify”.

```
 dial-peer voice 8000 voip
 destination-pattern 8...
 session target ipv4:10.168.8.35
 session protocol sipv2
 dtmf-relay sip-notify
 codec g711alaw
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none
 no vad
```

6. Save the configuration to the router by typing "write" in the enabled mode. This saves the changes to the startup configuration, i.e., that they are not lost at the next restart of the gateway.

```
Cisco2620#write
Building configuration...
[OK]
Cisco2620
```

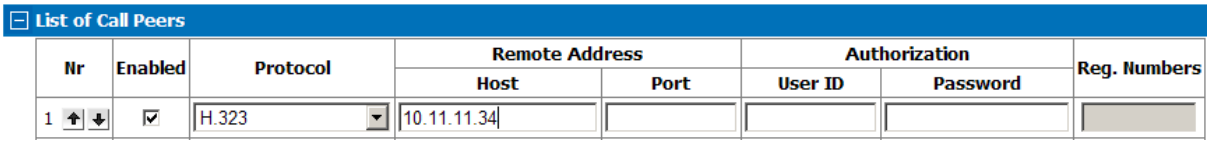
Now that the gateway is configured, it is recommended to test the configuration with MyPhone. See *MyPhone (H.323 Telephone Software)*.

Configuring FoIPv3

Open the KCS FoIP configuration tool and configure a call peer:

1. Select the signaling protocol you use: H.323 or SIP.
2. In the field Remote Address/Host, type the gateway IP address or host name.
3. In the field Set Remote Address\Port, type the port number if you use a port other than the well-known ports (H.323: 1720, SIP: 5060).
4. Other fields are optional.

An example configuration is shown below:



Troubleshooting Hints

This section provides troubleshooting information.

Check ISDN Line

This works only with PtMP BRI lines, because common ISDN telephones do not support PtP lines directly.

Connect an ISDN telephone to the BRI interface. It must have power and a dial tone must be heard. Try to make a call to any other phone. Try to call the phone from another phone. The phone must be configured to accept the MSN that you dial.

Check ISDN Interface on the Gateway

If you unplug the ISDN line from the interface the gateway should display something like this on the terminal.

```
16:12:227633266687: %ISDN-6-LAYER2DOWN: Layer 2 for Interface BRI1/0, TEI 68 changed to
 down
16:12:52: %ISDN-6-LAYER2DOWN: Layer 2 for Interface BR1/0, TEI 68 changed to down
16:12:52: %LINK-3-UPDOWN: Interface BRI1/0, changed state to down
```

This should appear, if you plug in the line. The OK-LED should be activated.

```
16:12:59: %ISDN-6-LAYER2UP: Layer 2 for Interface BR1/0, TEI 69 changed to up
16:12:59: %LINK-3-UPDOWN: Interface BRI1/0, changed state to up
```

If this is not the case, there might be something wrong with the ISDN interface on the gateway or the configuration of the interface.

When you call the interface from a telephone (i.e. dial 8000), the B1- or B2-LED should be activated on the VIC.

Disable Faststart on the Gateway

If you have mysterious problems with call establishment try to add the red config line to the gateways global voice service (see above how this is done).

```
voice service voip
 ...
 h323
  call start slow
```

Check Fax Relay and Signaling Activity on Gateway

You can enable debug traces on the gateway and then attempt to send a fax.

To enable T.38 trace, activate the enabled mode and enter "debug fax t30 all". With "debug fax ?" and "debug fax t30 ?" you get a list of possible levels. Sending a single page fax from the IP to the ISDN side created the following trace.

```
Cisco2620#debug fax relay t30 all
Debugging fax relay t30
Cisco2620#
5d04h: %ISDN-6-CONNECT: Interface BRI1/0:1 is now connected to unknown
5d04h: 1/0/0 (24965)  447214020 fr-entered (10ms)
5d04h: 1/0/0 (24965)  447214700 fr-msg-det CSI
5d04h: 1/0/0 (24965)  447215390 fr-msg-det DIS
5d04h: 1/0/0 (24965)  447216710 fr-msg-tx  TSI
5d04h: 1/0/0 (24965)  447217570 fr-msg-tx  DCS
5d04h: 1/0/0 (24965)  447222490 fr-msg-det CFR
5d04h: 1/0/0 (24965)  447281510 fr-msg-tx  EOP
5d04h: 1/0/0 (24965)  447283060 fr-msg-det MCF
5d04h: 1/0/0 (24965)  447284280 fr-msg-tx  DCN
5d04h: %ISDN-6-DISCONNECT: Interface BRI1/0:1  disconnected from N/A N/A, call lasted
 77 seconds
5d04h: %ISDN-6-DISCONNECT: Interface BRI1/0:1  disconnected from unknown , call lasted
 77 seconds
5d04h: 1/0/0 (24965)  447286290 fr-end  cause unknown 0x1
```

By entering "debug ?" you will get a list of all debug levels. The levels for h225 and h245 could also give relevant information for troubleshooting.

You can disable a debug level by entering the same command that enabled it with at preceding "no". Example "no debug fax relay t30 all".

Note If you access the gateway via telnet, you have to enter “terminal monitor” to see the debug output on the telnet session.

Check If Correct Parameters (Codec, Etc.) Are Used for Calls

Make a call (outgoing or incoming) and type “show call active voice compact” while the call is active to find out if the parameters (codec, protocol, vad, etc.) from the associated dial peer are used.

This is the output for one active outgoing call (from FoIPv3 to an ISDN telephone). The call shows two lines, which represent the two calls legs. The first line is the call leg to FoIPv3, the second line is the call leg to the ISDN device with the number 0172.

```
Cisco2620#show call active voice compact
G<id>  A/O FAX T<sec> Codec       type  Peer Address       IP R<ip>:<udp>
Total call-legs: 2
```

```
G202   ANS     T1     g711alaw    VOIP  P8000     10.168.8.35:8002
G202   ORG     T2     g711alaw    TELE  P0172
```

Check Errors on the ISDN Interfaces of the Gateway

If received faxes sent over the gateway have missing pixel lines or the fax transmissions are even interrupted (mostly XL on sender side) or if interruptions and other distortions can be heard when making a call to FoIPv3 over the gateway with a telephone, then the ISDN line or the ISDN interface on the gateway might have a problem. These problems can be caused by defective hardware or clock synchronization problems (ISDN configuration of the interface).

By typing “show controller bri” for basic rate interfaces or “show controller E1” for primary rate lines, ISDN dependent line or interface problems on the gateway can be detected. Examine the error counters and the clockmode settings shown.

Check Active Calls for Packet Loss, Jitter and Network Delay on the Gateway

If you have irregular interruptions in sent or received faxes you should take a look at the LAN quality. The Cisco gateways offer a simple method to check the jitter and network delay for received RTP data on active calls.

To do this connect to the gateway with telnet, enter the enabled mode and activate the debugging by typing “terminal monitor”. Send a multi-page test fax and then type “show voice call summary”. You will see a table with all open calls on the gateway. In the first column you can see the used interface, port and B-channel.

```
Cisco2620#show voice call summary
PORT           CODEC    VAD VTSP STATE            VPM STATE
============== ======== === ==================== ======================
1/0/0.1        -        -  -
1/0/0.2        14400    n  S_FAX                 S_TSP_CONNECT
1/0/1.1        -        -  -
1/0/1.2        -        -  -
```

Pick your test call from the list and display the call’s DSP statistics by typing for example “show voice call 1/0/0.2”.

```
Cisco2620#show voice call 1/0/0.2
1/0/0 2
      vtsp level 0 state = S_FAX
callid 0x0372 B02 state S_TSP_CONNECT clld 8400 cllg 4318635348
Cisco2620#      ***DSP FAX RELAY STATISTICS***
Max Jit Depth: 23, Max Nwk RxQ Depth 1, Jitter Overflow Pkt Drops: 0
Nwk RxQ Overflow: 0, Tx Pkts: 432, Tx Pkts Drops(Nwk Busy): 0
Rx Pkts: 11, Rx Pkts Loss: 0, Rx Invalid Pkts: 0, Rx Pkts Out Of Seq: 0
Recent Hi-Speed Modulation: 4TX Pages: 0
Max SendInQ Depth 2, Max RecvOutQ Depth 0
Max Hi-Speed Buf Usage 5SendInQ Overflow 0,RecvOutQ Overflow 0
Cisco2620#
```

Repeat this command about every 5 seconds while the call is active and keep watching the value Jitter Overflow Pkt Drops. It is normal that this value increases a little at the beginning of a call. If it increases steadily until the end of the call, you probably have a serious problem on the LAN side.

Redirecting Number (Call Diversion) Using H.323

Cisco gateways 2620 and 2821 were used to test Call Diversion with H.450.3. The Cisco gateway 2821 with IOS version 12.4(10) delivers the redirecting number in an H.221 non-standard identifier (different to the non-standard identifier the Cisco CallManager uses). Also the Cisco gateway 2620 with IOS version 12.3(11) uses a non-standard identifier to transmit the redirecting number. With IOS version 12.3(7) the gateway uses H.450.3 to deliver the redirecting number. With H.450.3 it is possible to transmit two numbers when using multiple forwarding. The first redirecting number, to be termed original called number, and the last redirecting number, to be termed diverting number.

SIP VoIP IPV6 Integration

Cisco gateways with IOS version 12.4(22) or later, support SIP VoIP signaling using IPV6 protocol.

Given the gateway has at least one LAN interface IPV6 enabled and connected to the IPV6 network, SIP protocol can be enabled for both IPV4 and IPV6 in this way:

```
!
sip-ua
protocol mode dual-stack
!
```

Then configure dial-peer(s) as usual, either using symbolic names or direct IPV6 addresses.

In the case IPV6 addresses are used, they must be enclosed in the “[]” brackets:

```
dial-peer voice 8000 voip
destination-pattern 8...
session protocol sipv2
session target ipv6:[fd96:eb5f:7508:5760:202:b3ff:feb8:fb29]
dtmf-relay rtp-nte
codec g711alaw
fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none
no vad
```

Hints for Cisco Gateways

With Cisco gateway 28xx and IOS 12.4T(22) the T.38 FoIP does not work via IPV6 protocol.

The problem is that the UDP packets generated for T.38 stream by the gateway do not have the UDP checksum set (UDP checksum is always set to zero), which is mandatory with IPV6 protocol.
As a consequence, receiving FoIPV3 running on Windows 2008 server doesn’t receive any T.38 packets from the gateway as these packets are obviously being silently ignored by Windows IPV6 protocol stack due to missing UDP checksum.

Dialogic Media Gateway DMG4000 Series

Dialogic produces VoIP/FoIP media gateways which use a Windows Server 2008 operating system and a Dialogic Diva PCI fax board for ISDN connectivity. The SIP integration is done via DIVA SipControl. The gateway can be managed like any other Windows computer; it includes nice features like remote desktop

connection and Wireshark network protocol analyzer. The main benefit of these gateways is that they support V.34 fax via T.38.

Hints for Dialogic Media Gateway

Integration Hints

- Activation of T.38 did not worked correctly if the T.38 was activated by the Gateway. The problem was that Gateway signaled T.38 but continued with G.711 packets. Therefore only mode 10 (=default) is support both for fax inbound and fax outbound.
- Inbound calls with V.34 may fail due to SPR70456 (which is fixed since 3.12.02)

Additional Hints Specific for DMG300x

Dialogic also delivered Media Gateway DMG300x. It is the predecessor of DMG400x, also supports V.34 via T.38 but is now out of sales. All hints for DMG400x also apply to DMG300x, but here are some additional hints specific for DMG300x:

- The DMG3008BRI (Diva System 8.5.6 / SIPcontrol 2.0.2) requires a patch for prober support of outgoing fax calls with V.34/T.38 mode. This patch was provided as part of the Dialogic support case C81394.
- The DivaSIPcontrol service of DMG3008BRI (Diva System 8.5.6 / SIPcontrol 2.0.2) may crash with an application error in sipcontrol.exe 2.04.49 at address 0x00033d05 after an internal call via Elmeg ISDN BAPX to a none connected ISDN line. In such a case the outgoing call is terminated with error code IF (I:NOANS;40;12487;9-103) and the DivaSIPcontrol service will be restarted. If the problem happens at least 3 times within one day, the service remains stopped!!! This problem also happens with sending with Brooktrout SR-140 to the Dialogic Gateway. It has never been recognized with DMG4008BRI.

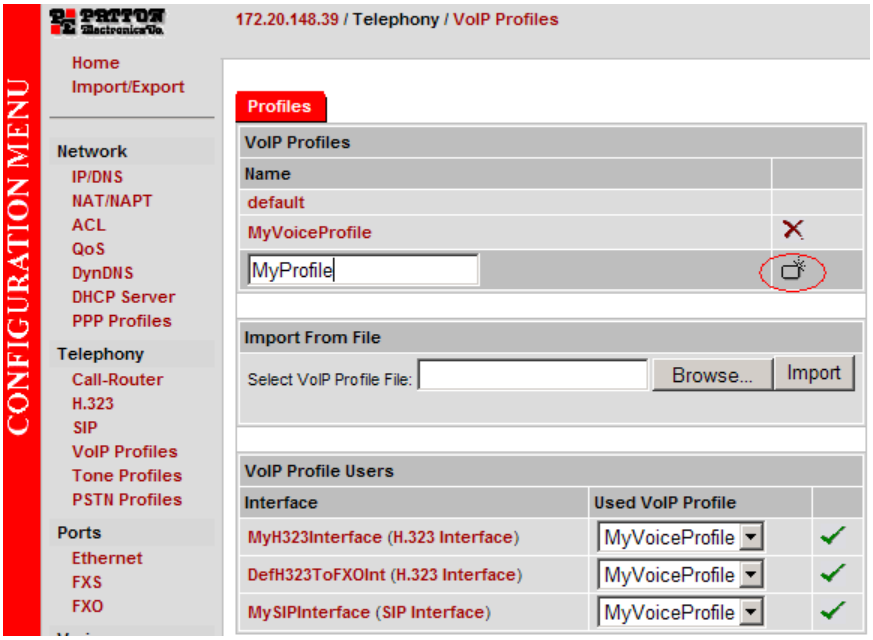
Patton Gateway

This section provides information about integration with Patton gateway.

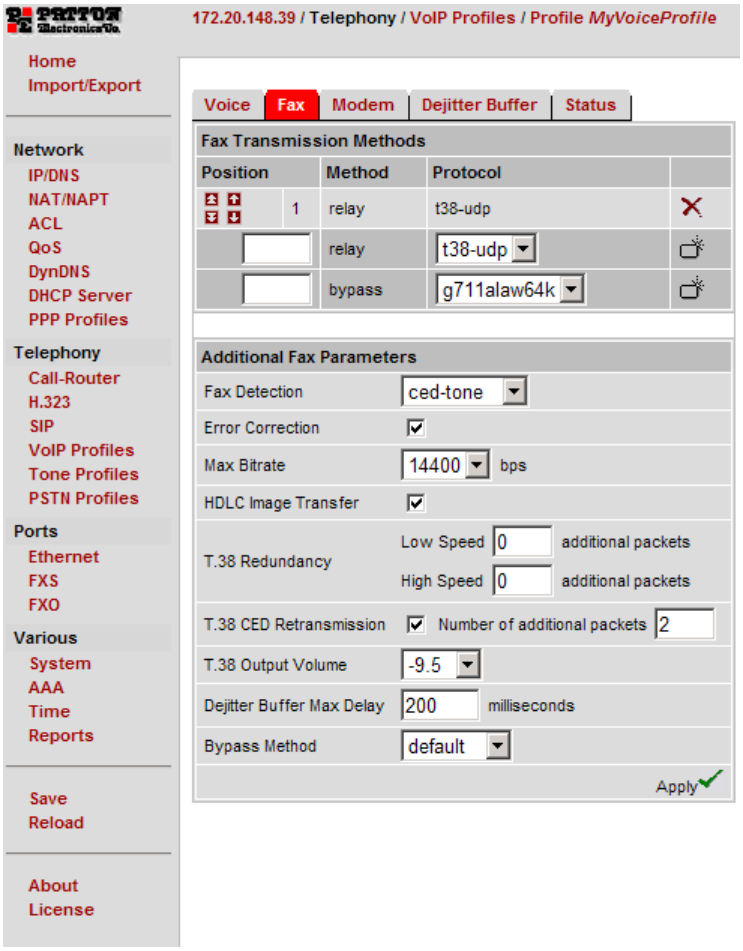
Configuring the Gateway

1. Start the Patton gateway configuration utility.

2. To enable fax transmission with T.38, configure a Voice Profile. In the **Telephony** menu select **VoIP Profiles**. Type the name of the profile and click the add icon.

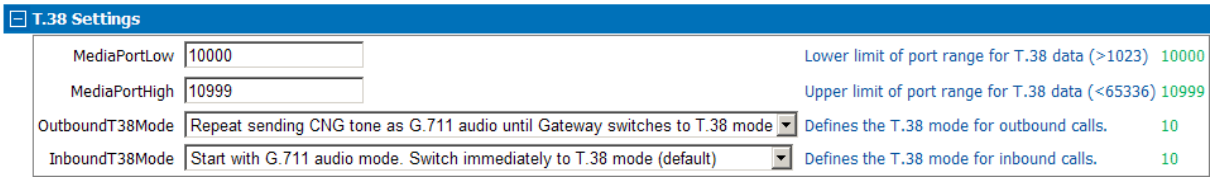


3. Go to the **Fax** tab and add “t38-udp” to the Fax Transmission Methods as shown in the following figure.



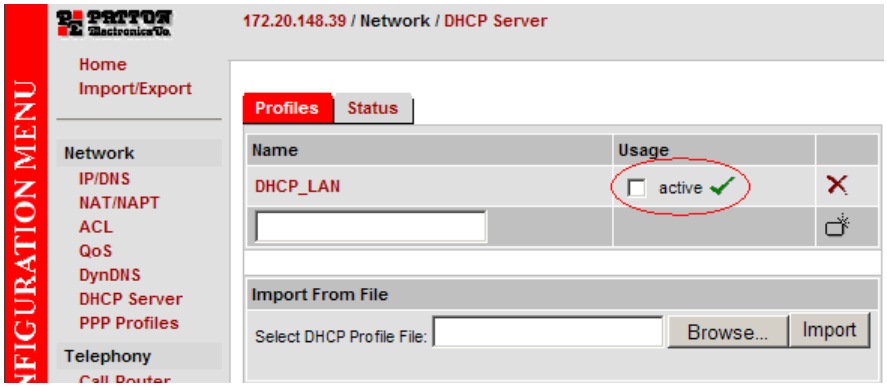
Configuring FoIPv3

Since some Patton gateways send a corrupted CNG signal it can be necessary to set the **Outbound T.38 Mode** to **Repeat sending CNG tone as G.711 audio until Gateway switches toT.38 mode**.



Hints for Patton Gateway

It happened that after a firmware update the DHCP server was activated. If you do not use the DHCP server make sure that after an update the server is disabled. Click DHCP Server in the main menu. Make sure that “active” is not selected.


NFIGURATION MENU
PATTON Electronics Co.
172.20.148.39 / Network / DHCP Server
Home
Import/Export
Network
IP/DNS
NAT/NAPT
ACL
QoS
DynDNS
DHCP Server
PPP Profiles
Telephony
Profiles
Status
Name
Usage
DHCP_LAN
active
Import From File
Select DHCP Profile File:
Browse...
Import

Chapter 3

Integration with Software PABX

This section provides information about integration with software PABX.

Cisco CallManager

This chapter describes integration with CISCO Call Manager 4 (CCM) and later. Note that since release 6.0 the CCM is being referred to as *Cisco Unified Communication Manager* (CUCM).

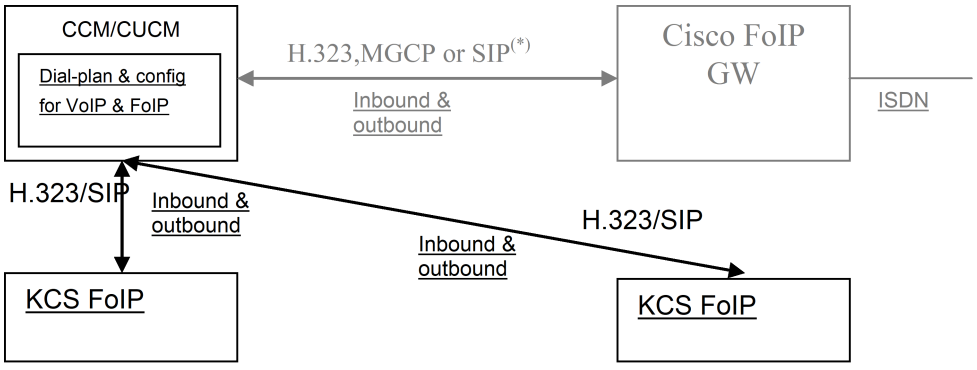
In this guide we use:

- Both names as synonyms regardless of the CCM/CUCM release
- For the common CCM/CUCM features which have been available since CCM 4 the installation description is based on screenshots taken on the CCM 4, only new features available on later versions (CUCM 6 or 7) are described based on their respective screenshots.

Kofax Communication Server integrates with the CCM/CUCM by the means of H.323 or SIP signaling protocol.

KCS FoIP T.38 and Voice Integration Overview

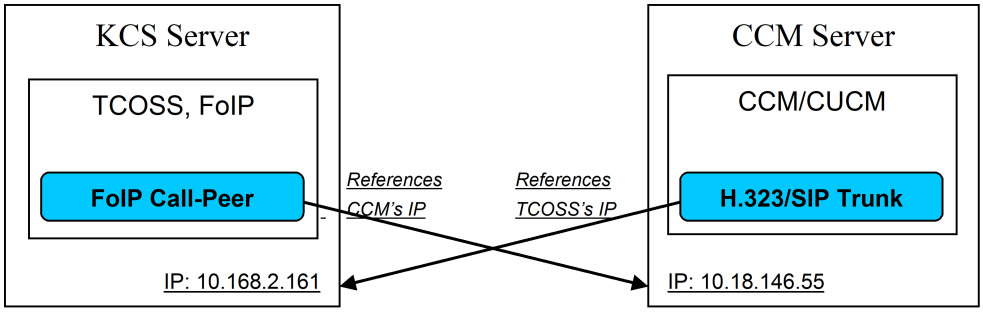
Since version 4.2(3), the CCM has supported the T.38 Fax over IP protocol (also in case of calls over gateways which are connected to the CCM via the Media Gateway Control Protocol – MGCP). This enables KCS FoIP to integrate with the CCM instead of talking directly to particular gateway(s).



(*) See *Prerequisites* for details

The dial-plan and configuration for the KCS FoIP is maintained on the CCM. The CCM is the central routing point for all VoIP and FoIP calls. Calls from or to the Cisco FoIP gateways are established via the CCM.

Consider the following CCM environment example:



Prerequisites

- CCM version 4.2(3), CUCM version 6.1(2) or 7.1 (available from http://www.cisco.com).

  Note T.38 fax relay over MGCP gateways is only supported by CCM 4.2(3). Not even CCM 5.0 (which was released earlier) supports it. MGCP support was not tested with CCM 6.0.

- T.38 fax relay must be enabled on all used gateways (see *Configuring the Gateway* for information on how to enable T.38 fax relay on a Cisco FoIP H.323 gateway, and learn how to enable it on MGCP CA-controlled gateways from the *Cisco IOS Documentation*).
- KCS 9.0 or higher
- KCS "FAX over IP Channel (T.38)" license

Gateway Integration Protocols

In theory, the KCS FoIP integration protocol is independent of the one used to interconnect the CISCO Gateway with the CCM. But in the real life there are some limitations which are described in the following table:

Recommended Cisco Gateway Integration Type (H.323, MGCP, or SIP) for particular CCM version/KCS FoIP integration combination are stated in the following table.

CCM/CUCM version	KCS FoIP Integration Type		
	H.323	SIP	
< 4.2(3)	H.323	N/A	
4.2(3)	H.323, MGCP	N/A	
6.1(2)	H.323,MGCP, SIP	SIP,MGCP(1), H.323	See Hints on possible MGCP gateway issues.
7.1	H.323,MGCP	SIP,MGCP(1), H.323	

Functional Blocks on the CCM/CUCM Side

Given below is an overview of the required functional blocks on the CCM/CUCM side.

- Either H.323 inter-cluster trunk(s) in the case of H.323 integration (CCM 4 or later) or SIP trunk(s) in the case of SIP integration (CCM 6 or later)
- Route pattern(s)

- Route group and route/hunt list in the case of integrating several instances of the KCS FoIP component (fault-tolerant installations)
- Message waiting on/off control numbers (in the case of MWI functionality)
- VoiceMail profiles (in the case of voice integration)

CUCM 6.x and 7.1 Remarks

Since release 6.0, CUCM supports T.38 along with SIP protocol.

The configuration interface of CUCM 6.0 is similar to the interface of CCM 4 but some menu items have changed. For example:

- Button to add new trunks etc. is now called “Add New” and is on the left.
- The button “Insert” is named “Save”.
- The menu item “Route Plan” is named “Call Routing”.
- The menu item “Route/Hunt List” is separated in two items.
- The menu item “Voice Mail” is in the menu bar.

Integration Without Encryption

This section describes about integration without encryption.

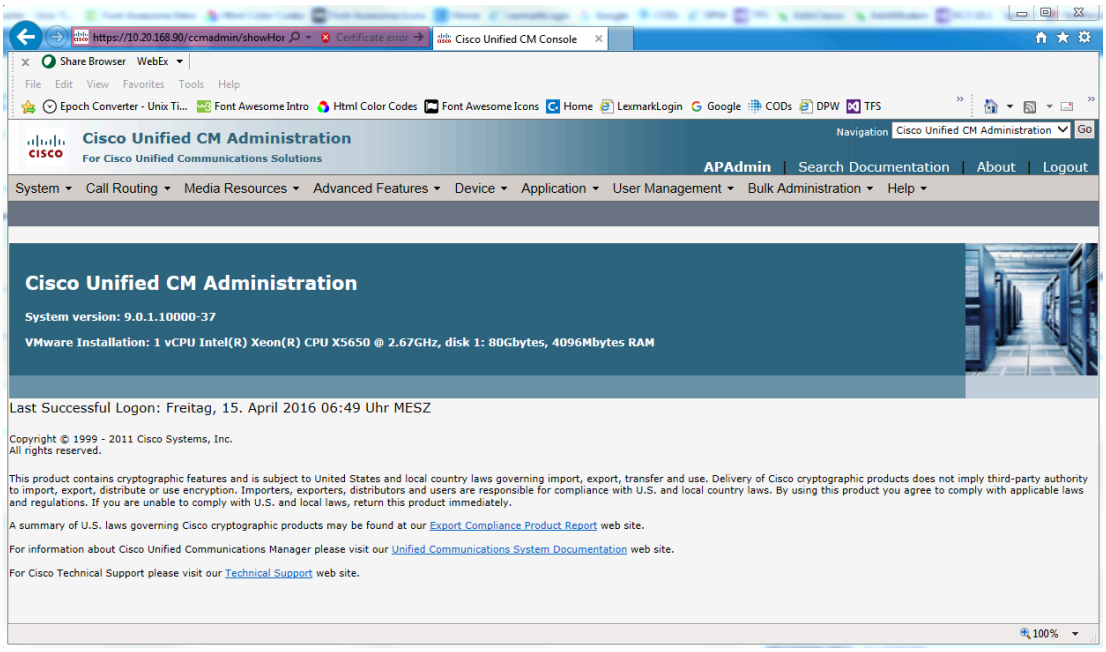
CCM/CUCM Configuration

Simply put, the CCM/CUCM configuration comprises following steps:

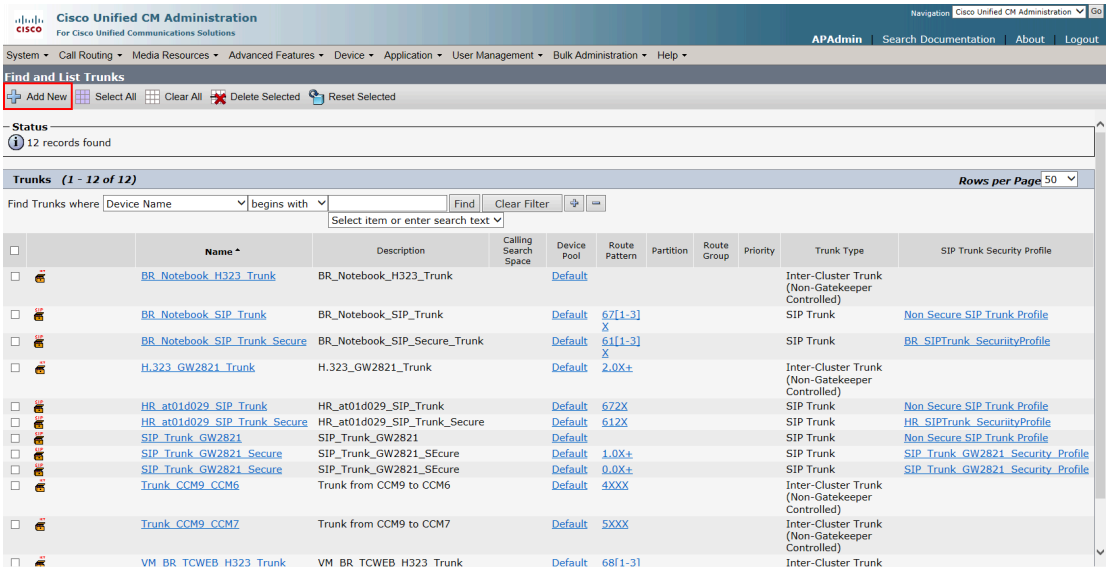
1. Configure appropriate trunk type (mandatory).
   - H.323 Inter-Cluster Trunk Without Gatekeeper
   - H.323 Inter-Cluster Trunk With Gatekeeper
   - SIP Trunk (CUCM 6.0 or Later)
2. In case of fault-tolerant installation configure Route group and Route/Hunt List (optional).
3. Configure Route Pattern.
4. Configure Message waiting control numbers (optional).
5. Configure VoiceMail profiles (optional).

H.323 Inter-Cluster Trunk Without Gatekeeper

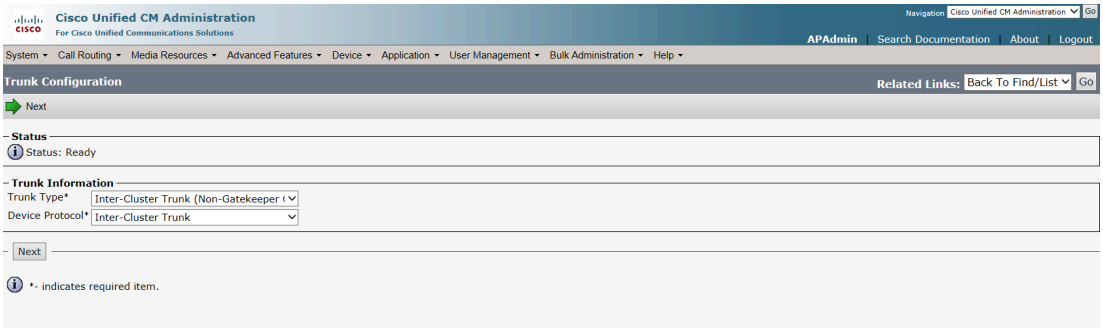
1. Open a web browser (such as Internet Explorer) and type the following URL: http://<CALLMANAGER>/ccmadmin. Note: Replace <CALLMANAGER> with the computer name of CCM.



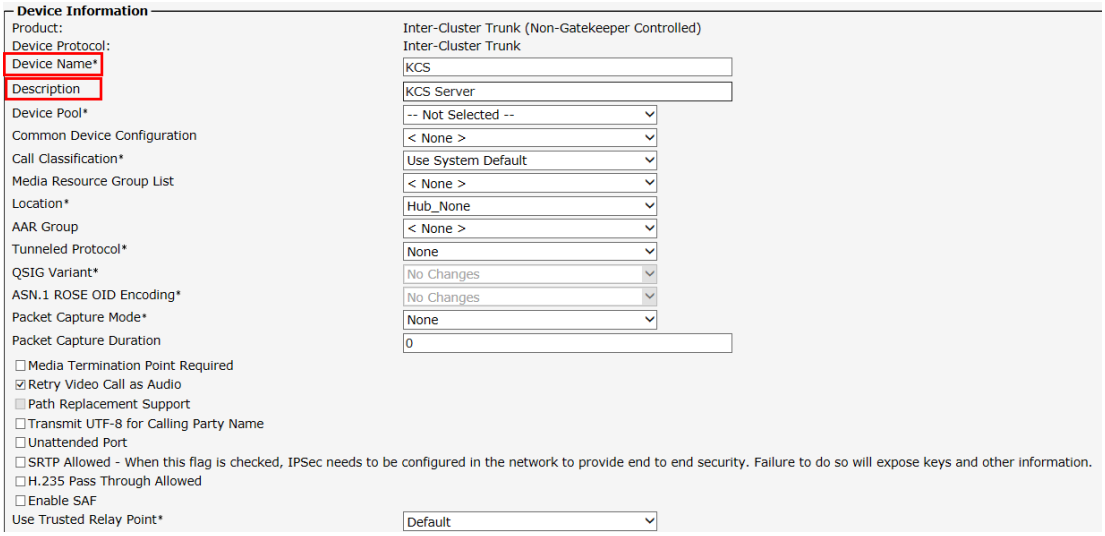
2. From the Device menu, select “Trunk”. Click “Add New”.



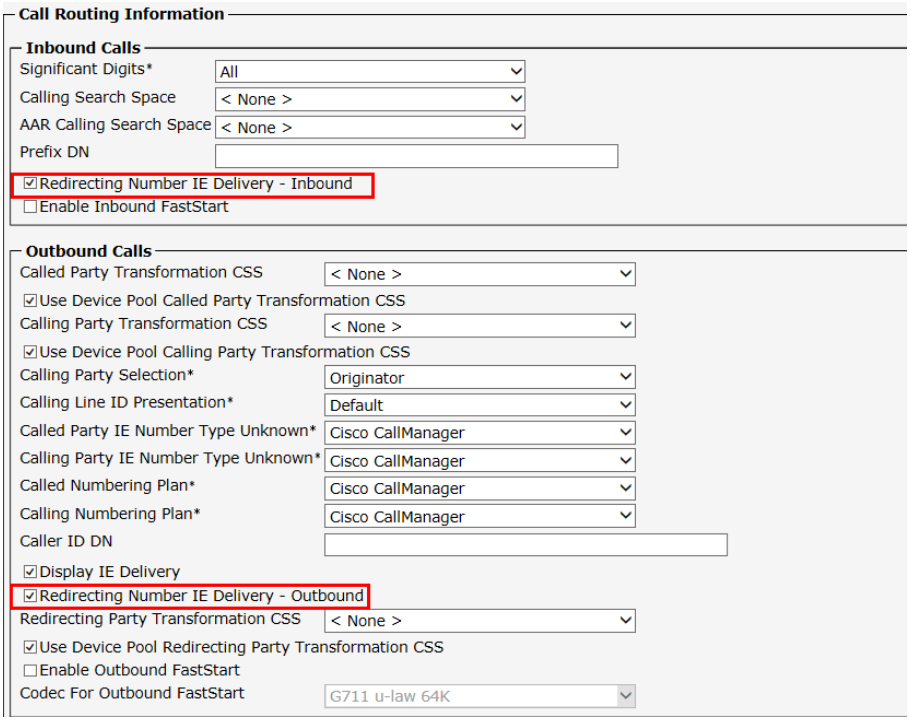
3. As the trunk type, select “Inter-Cluster Trunk (Non-Gatekeeper Controlled)”. As the device protocol, select “Inter-Cluster Trunk”.



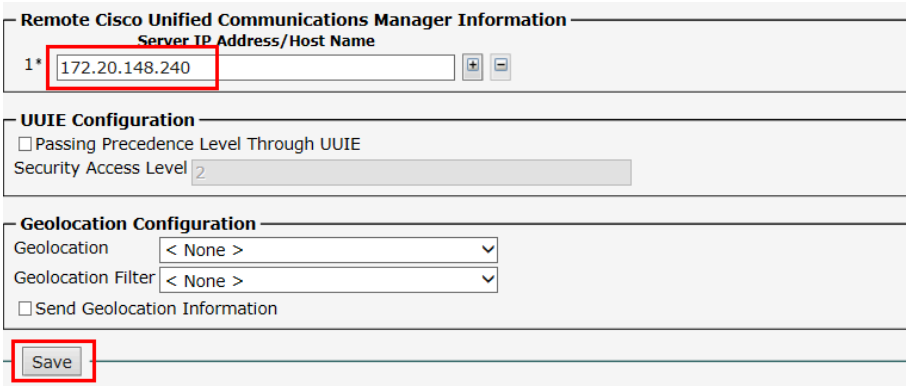
4. Click “Next” and fill the required fields like “Device Name” and “Device Pool”.



5. Enable “Redirecting Number IE Delivery – Inbound” and “Redirecting Number IE Delivery – Outbound”.



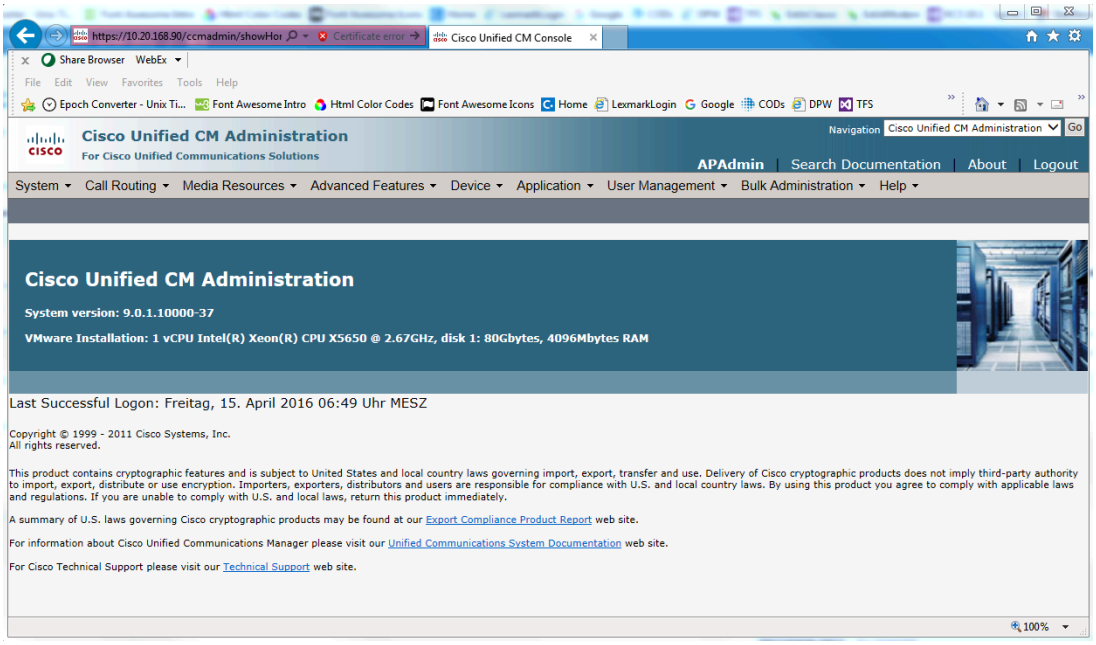
6. In the field “Server IP Address/Host Name”, type the IP address of the FoIP component and click “Save” to save this configuration of the trunk.



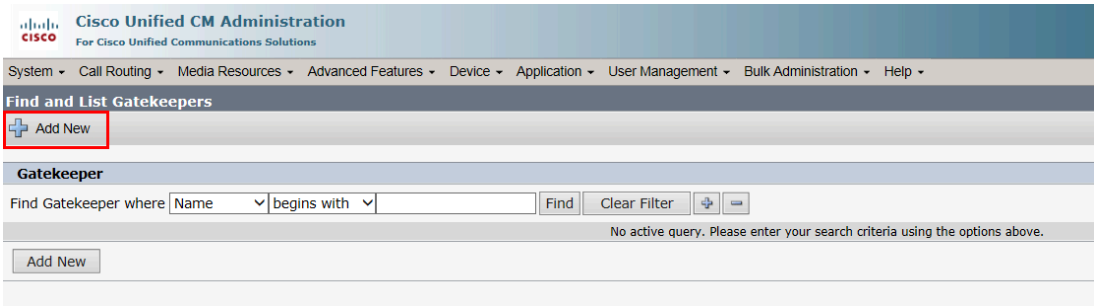
Also, if a second KCS FoIP component is installed (fault-tolerant scenario), do not add the second field “Server IP Address/Host Name” of the trunk, but create another inter-cluster trunk for it (repeat steps 1-6 and choose another name for it, for example “KCS2”).

H.323 Inter-Cluster Trunk With Gatekeeper

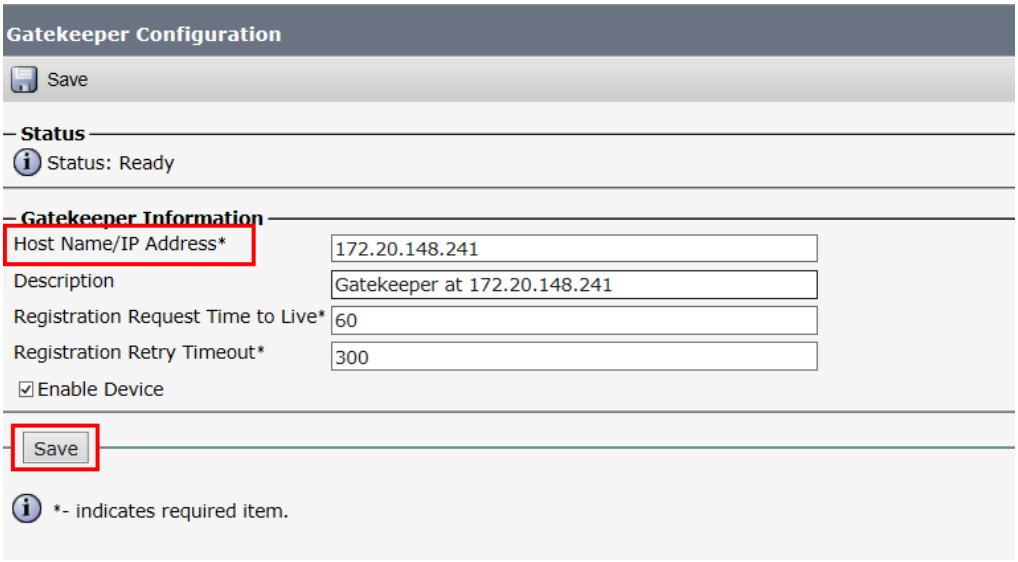
1. Open a web browser (such as Internet Explorer) and type the following URL: http://<CALLMANAGER>/ccmadmin. Note: Replace <CALLMANAGER> with the computer name of Cisco CallManager.



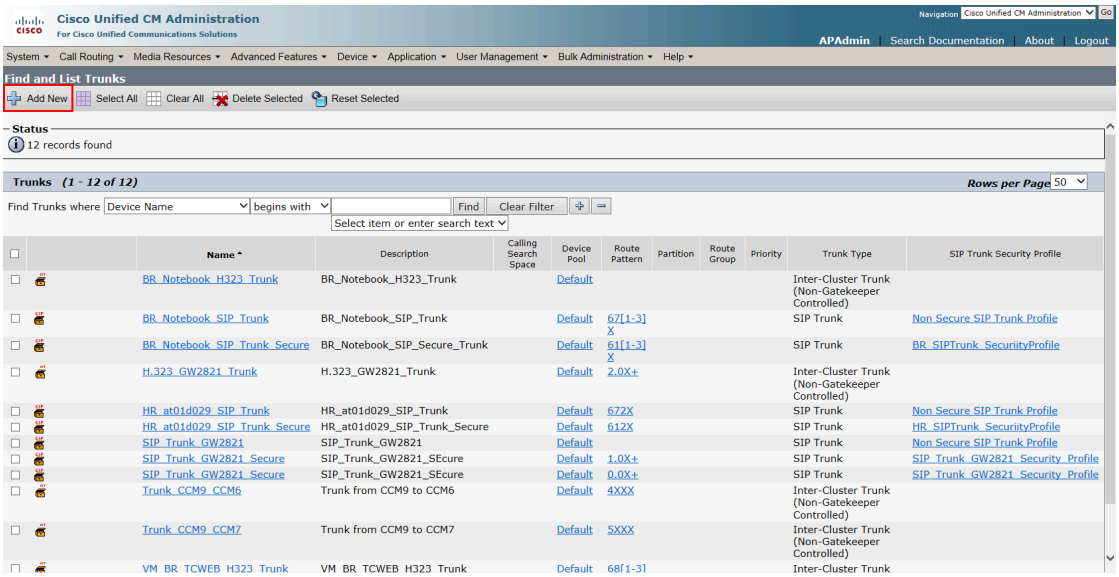
2. From the Device menu, select Gatekeeper. Click “Add New”.



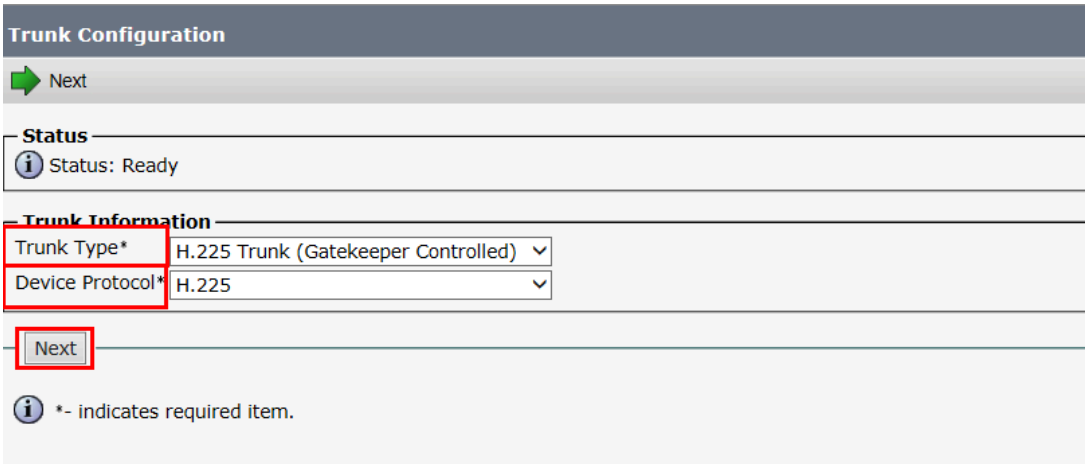
3. Type the IP address in the field “Host Name/IP Address” and click “Save”.



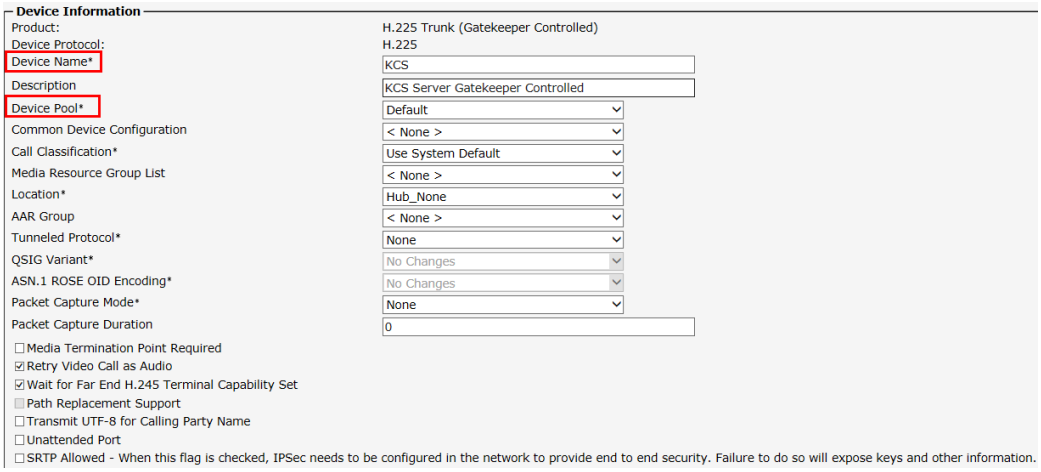
4. From the Device menu, select Trunk. Click “Add New”.

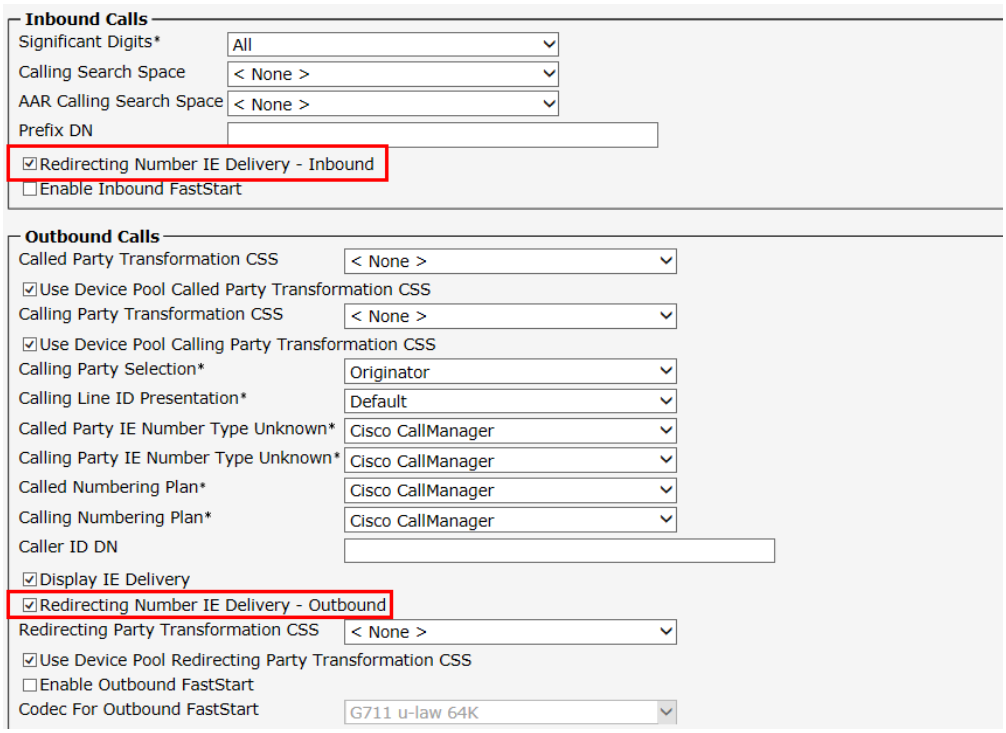


5. Select “H.225 Trunk (Gatekeeper Controlled)” in “Trunk Type” and “H.225” in “Device Protocol” and click “Next”.



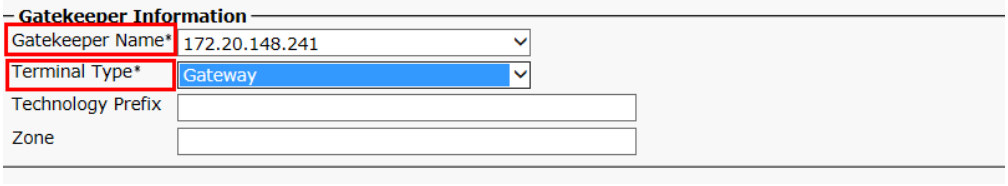
6. Click “Next” and specify all required information.





7. In the field “Gatekeeper Name”, pick one of the configured gatekeeper entries. Set the “Terminal Type” to “Gateway”. In the (optional) field “Technology Prefix”, enter the prefix of the numbers that

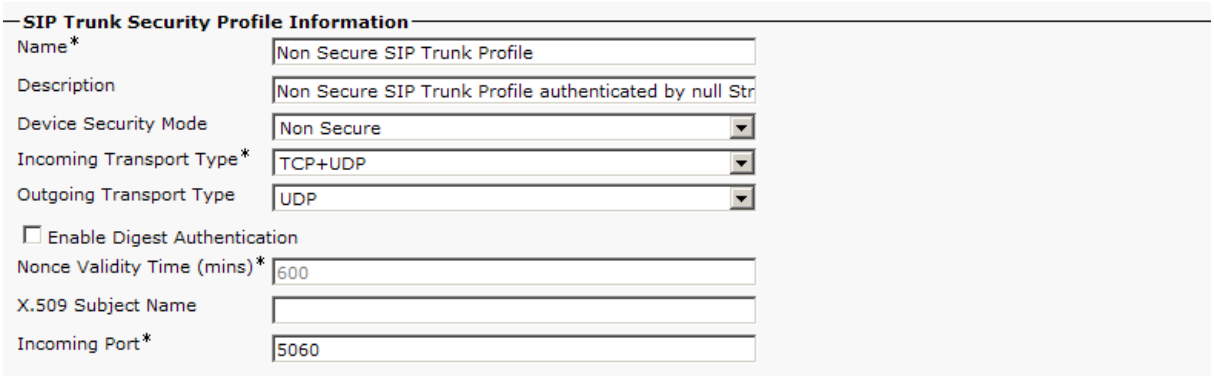
the gatekeeper should route towards CCM through this trunk (such as type “91” to route all numbers starting with “91” to this trunk).



Note The parameter “Technology Prefix” matches the “Reg. Numbers setting” in the Call-Peers configuration of the KCS FoIP component.

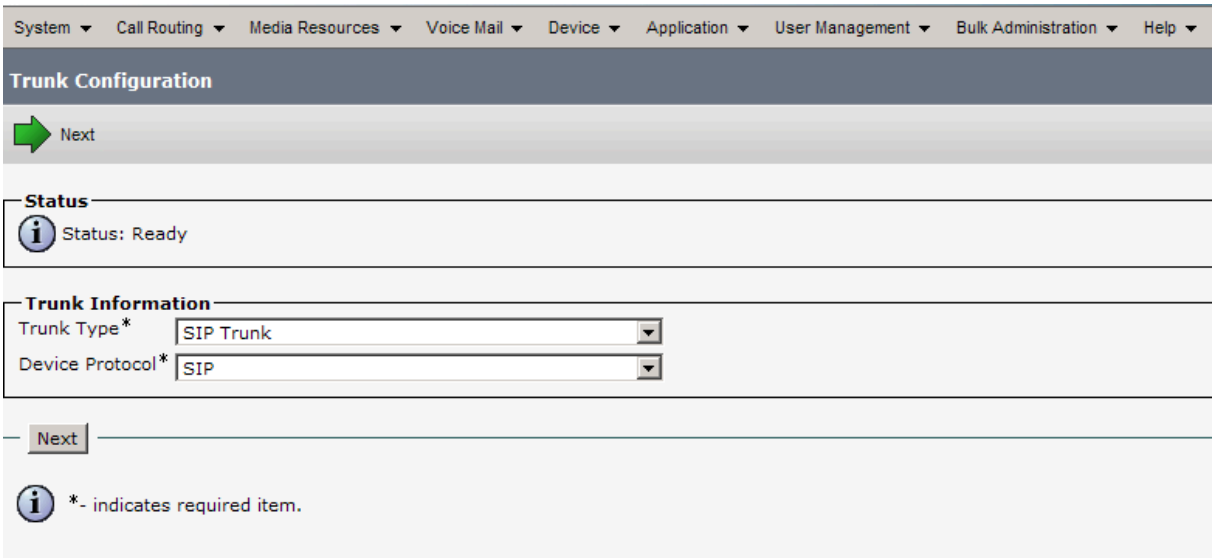
SIP Trunk (CUCM 6.0 or Later)

1. The first step is to create a SIP Trunk Secure Profile. Go to System | Security Profile | SIP Trunk Security Profile.

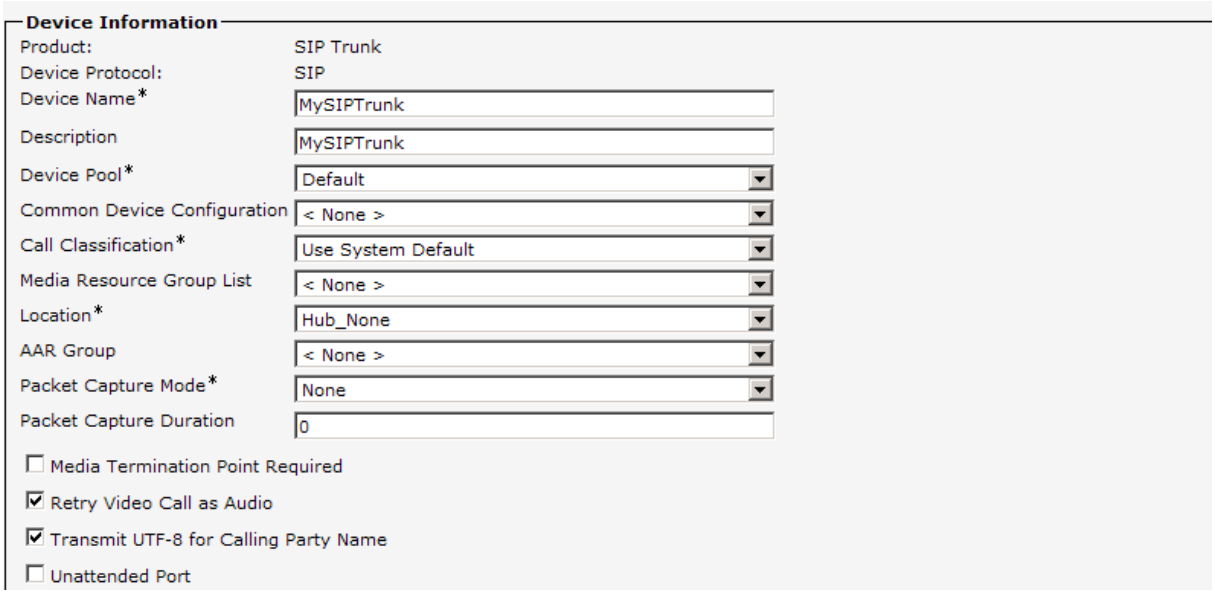


2. Enter a name and a description and set **Outgoing Transport Type** to “UDP”. Save the profile.

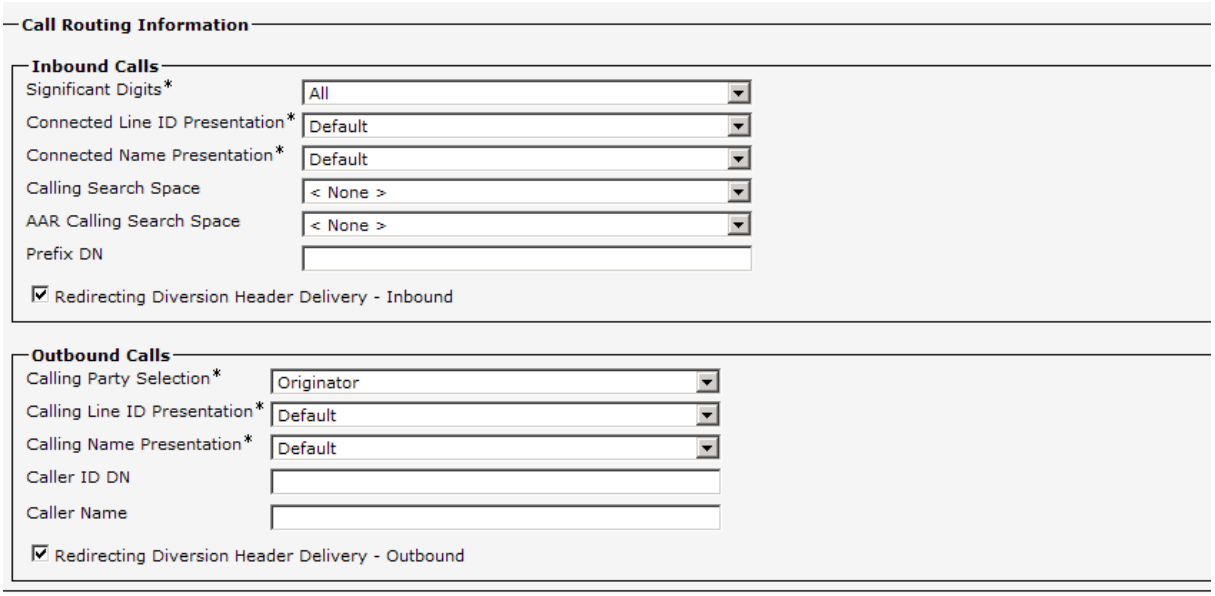
3. The next step is to configure a SIP trunk. Go to **Device** > **Trunk** and click **Add New**:



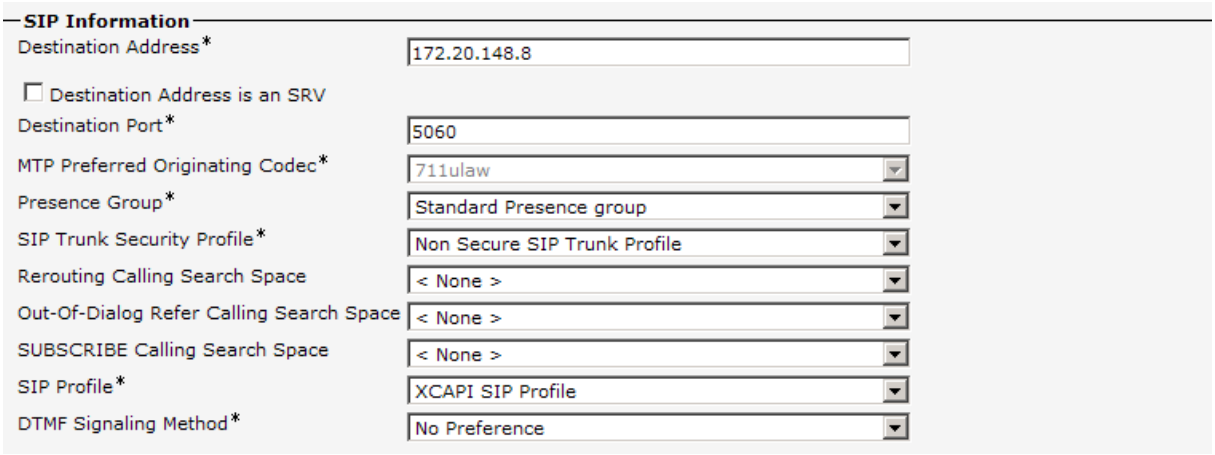
4. Select “SIP Trunk” as Trunk Type and click **Next**.



5. Type a name and a description of the trunk and set Device Pool to Default. Transmit UTF-8 for calling Party Name is enabled to support 8-bit Unicode Transformation Format.



6. Select **Redirecting Diversion Header Delivery** for inbound and outbound.



7. Type the IP address of the KCS FoIP as Destination Address and select the SIP Trunk Security Profile you created. Save and reset the trunk. A Routing Pattern for the SIP Trunk can now be created.

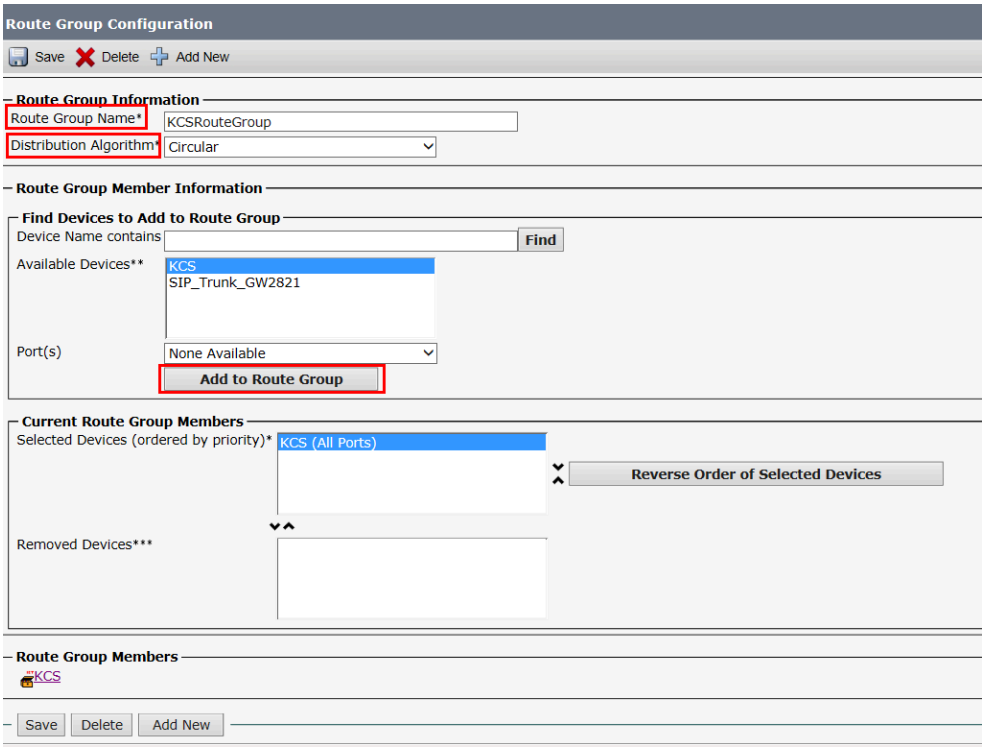
Route Group and Route/Hunt List (Optional)

Route group and Route/Hunt List are only necessary in the case of fault-tolerant installations (more than one KCS FoIP).

1. From the Call Routing menu, select Route/Hunt | Route Group (for fault-tolerant configuration only, if more than one voice server is connected to the CCM). Click “Add New".

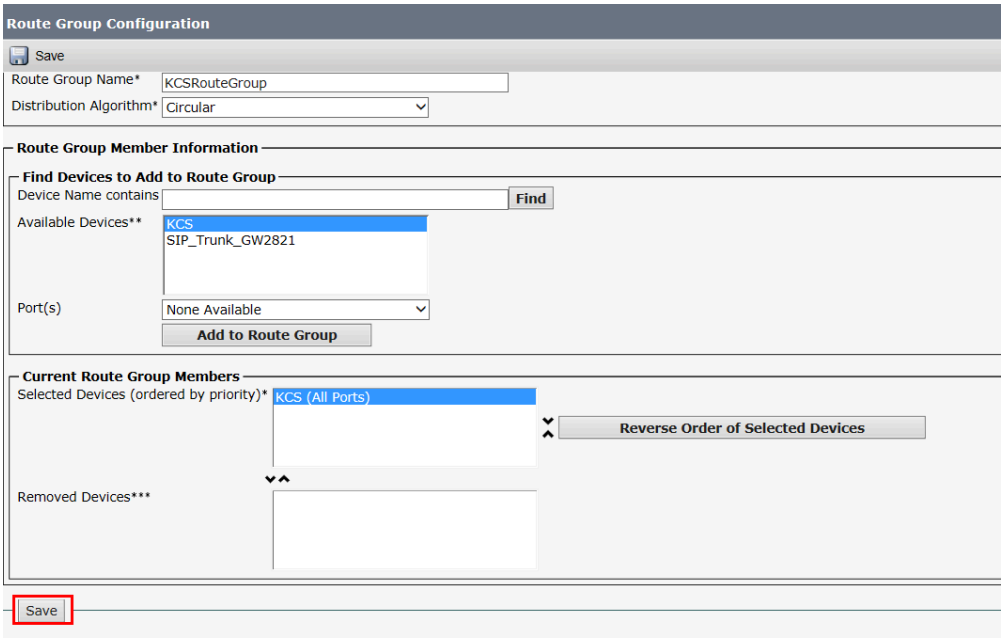
2. Enter the Route Group Name. Select the trunk(s) created in steps 1-6 as Available Devices and click “Add to Route Group”. In the “Distribution Algorithm” select “Circular” if you want CallManager to perform load-balancing among available voice servers (preferred setting). If you (for any reason) needed CallManager to route all calls to the first (primary) voice server and use the second one only as the fall-back, choose “Top Down” algorithm.

Click “Add to Route Group” to add the selected device to the group:

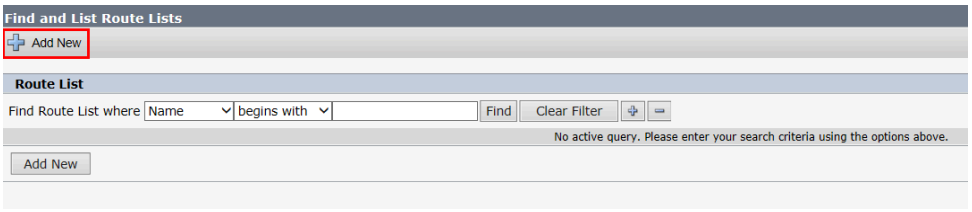


Note Only the trunks which are not yet assigned to any other route group or routing pattern/hunt pilot will appear as Available Devices.
If you want to assign any existing trunk (such as “KCS1”) to a new route group which was already entered into the routing pattern/hunt pilot before (see *Route Pattern*) you have to delete the corresponding route pattern from routing pattern/hunt pilot table.

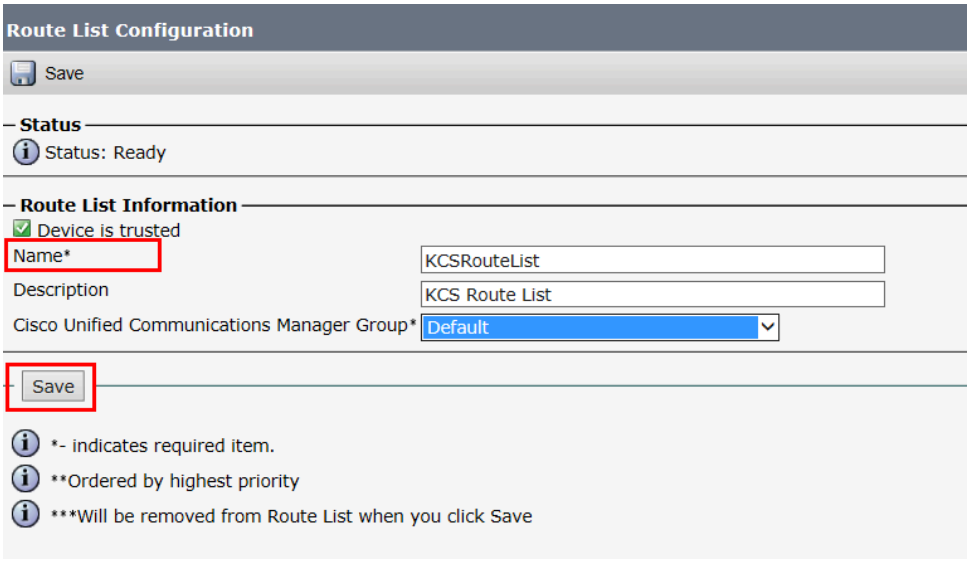
3. After you have added all desired trunks into the group, click Save (you will see all chosen trunks under “Selected devices”):



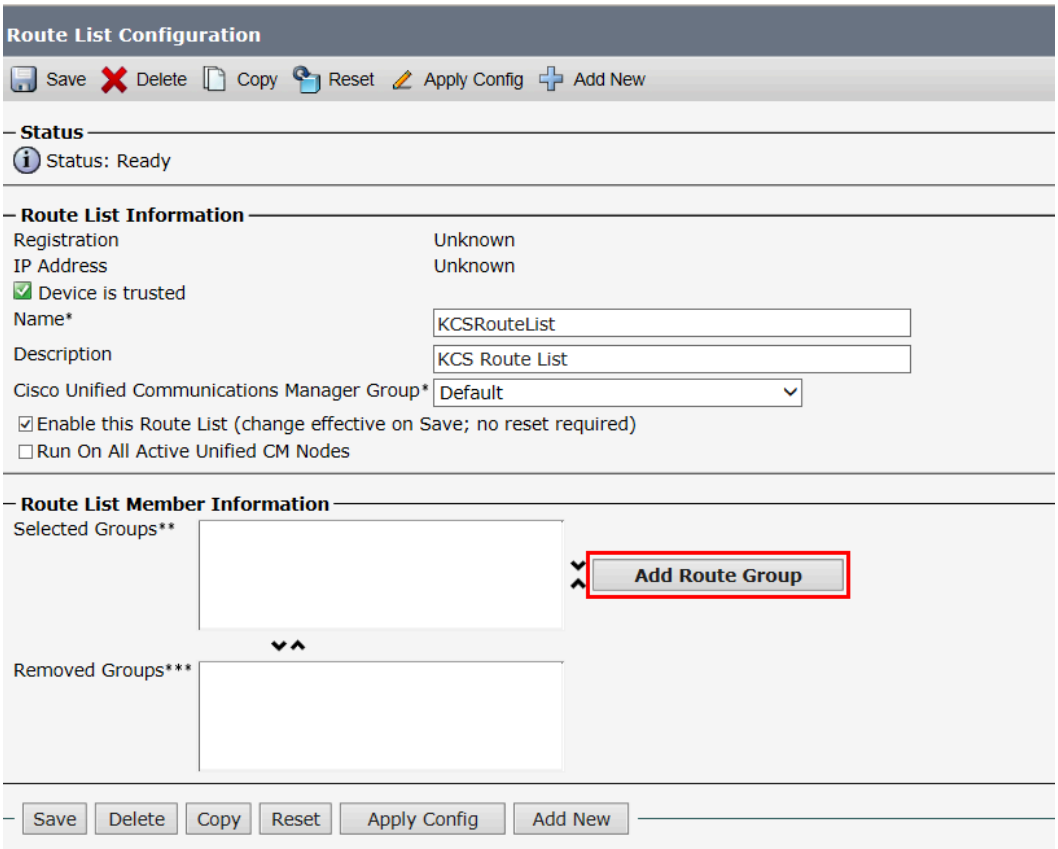
4. From the CallRouting menu, select Route/Hunt | Route List. Click Add New.



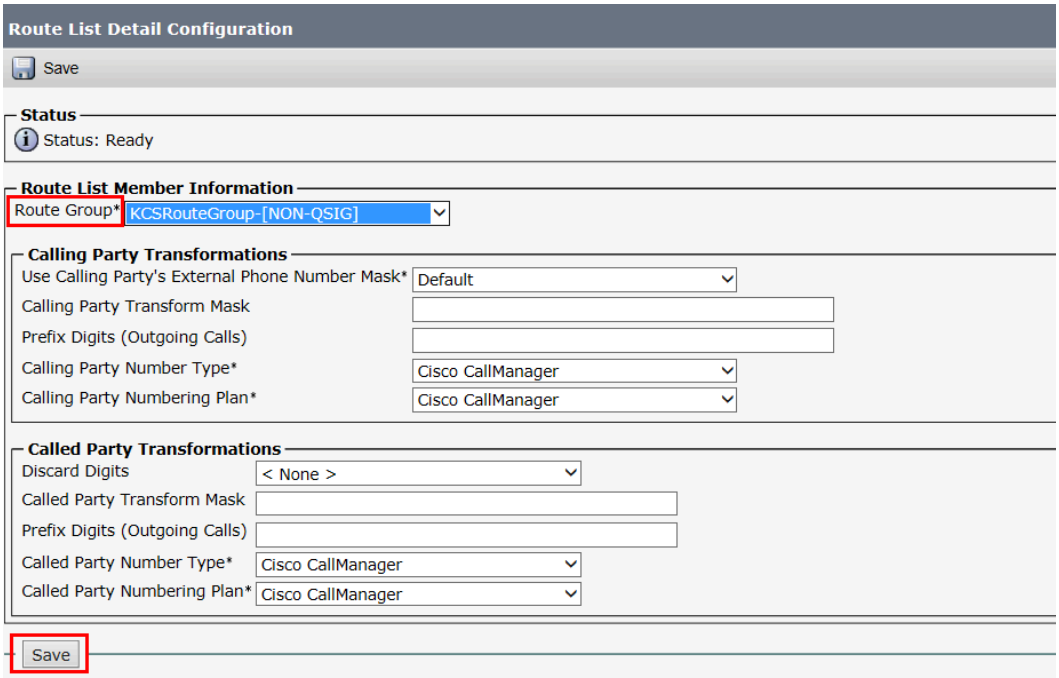
5. Enter the name of the Route List into the required filed “Route/Hunt List Name” and click Save:



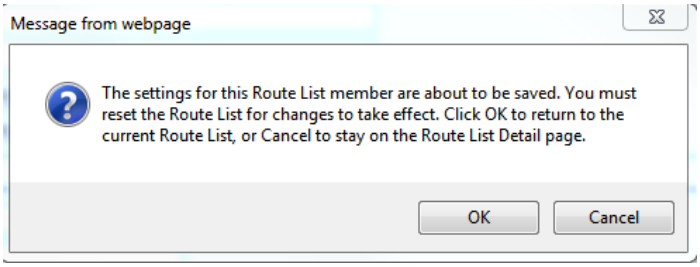
6. Click Add Route Group:



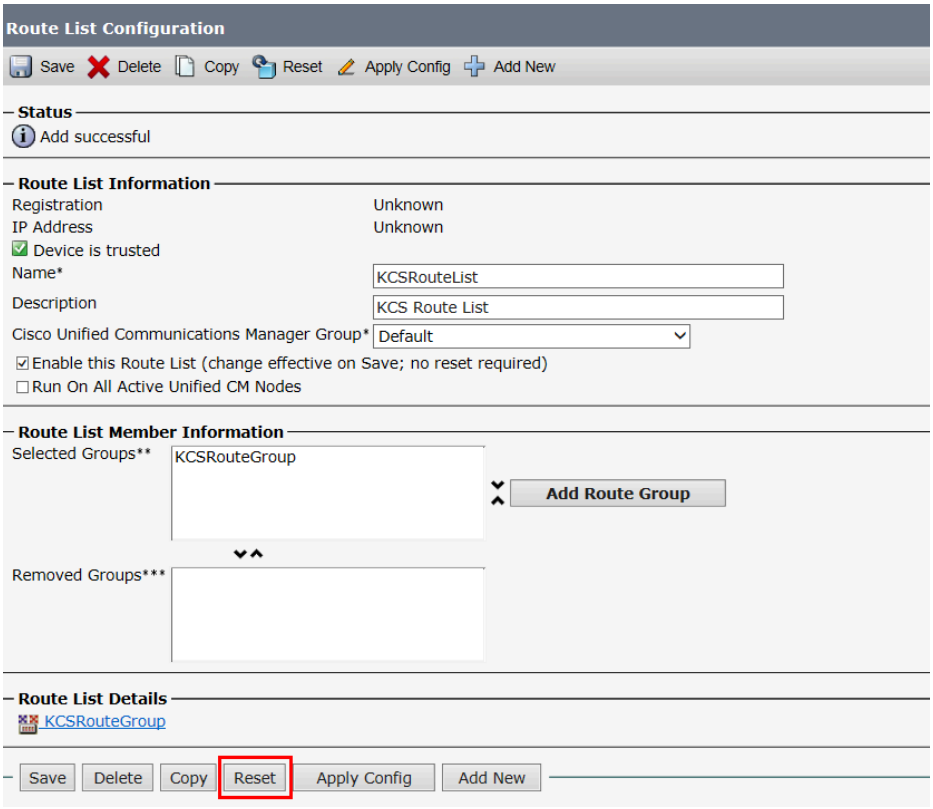
7. Select the corresponding Route Group and click “Save”:



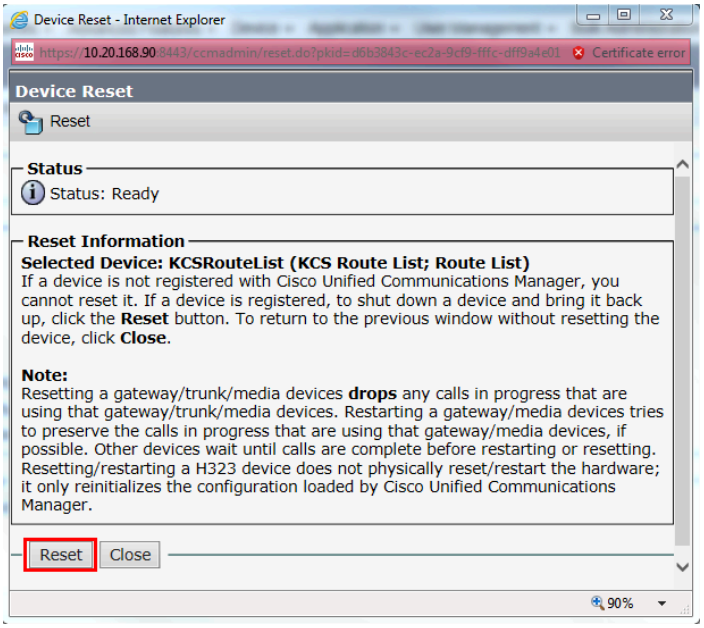
8. You will be informed that the route group has been inserted into the Route/Hunt List. Click OK.



9. Click Reset in order to reset the Route/Hunt List:

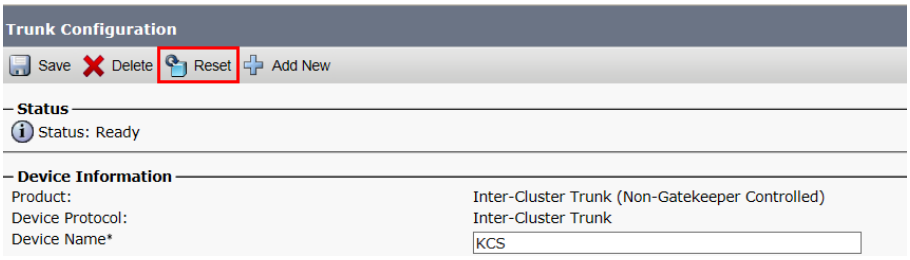


10. Click “Reset” in the Device Reset screen:



11. It is also recommended to reset all trunks that have been entered into the Route/Hunt list.

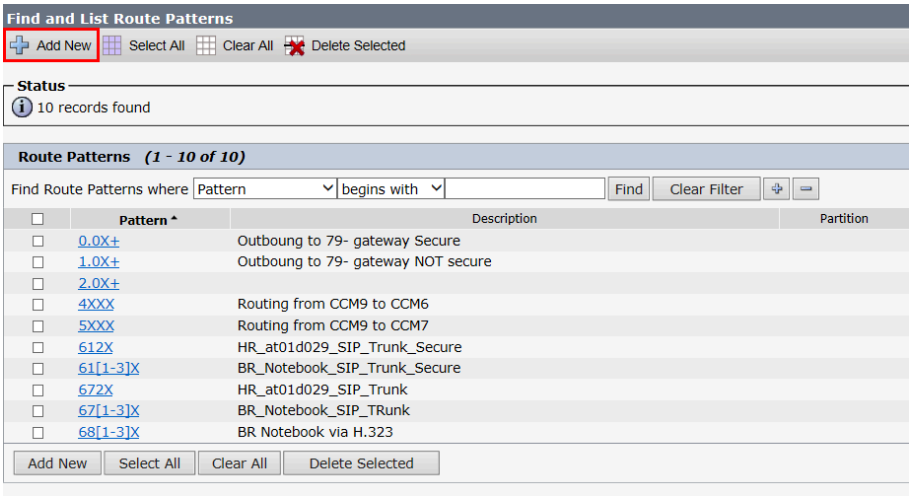
From the Device menu, select Trunk. Click Find to display all configured trunks. Open the desired trunk's configuration by clicking it, then click Reset Trunk:



12. Continue with Route Pattern.

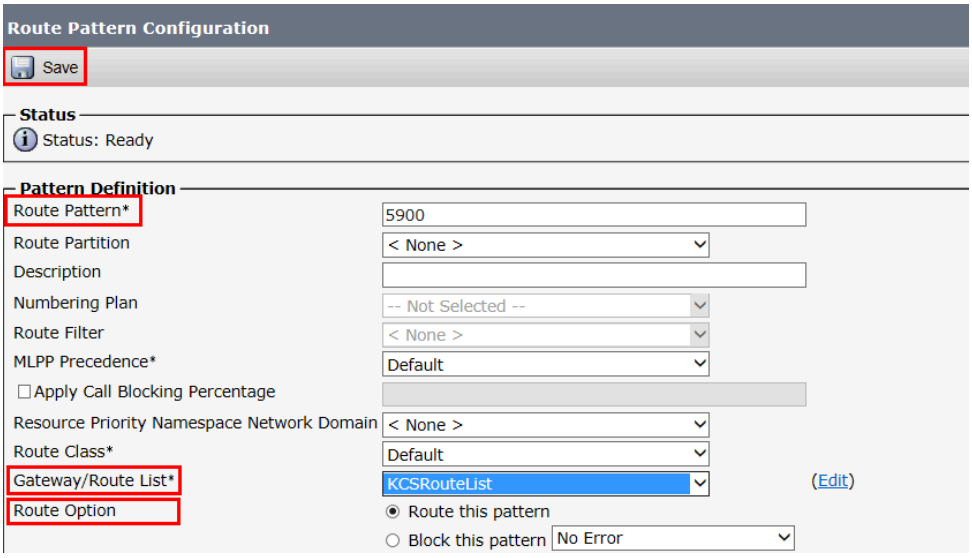
Route Pattern

1. From the Call Routing menu, select Route/Hunt | Route Pattern and click "Add New".



2. Type the required number (to be routed to KCS Trunk or Route List) in the field "Route Pattern" (for example, in our case "5900"), the Route Option must be set to "Route this pattern".

In the field “Gateway or Route List” select the inter-cluster trunk (for a single KCS server) or the route list (for multiple KCS servers). Click “Save”.



Messages Wait Integration (Optional)

CCM 4.0 or later supports a simple proprietary MWI signaling method which works in the following way:

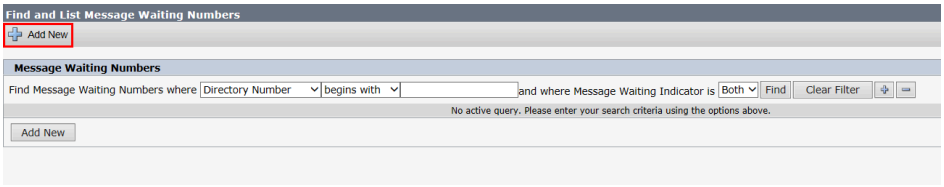
There are two MWI control numbers defined in the CCM – the first one to turn the MWI lamps on (“MWIOn” number) and the second to turn the MWI lamps off (“MWIOff” number).

In order to control the MWI lamp on particular CCM directory number (or extension such as 1234) the call originating entity (Cisco IP phone, incoming call via H.323 or SIP trunk) has to issue a call with following parameters:

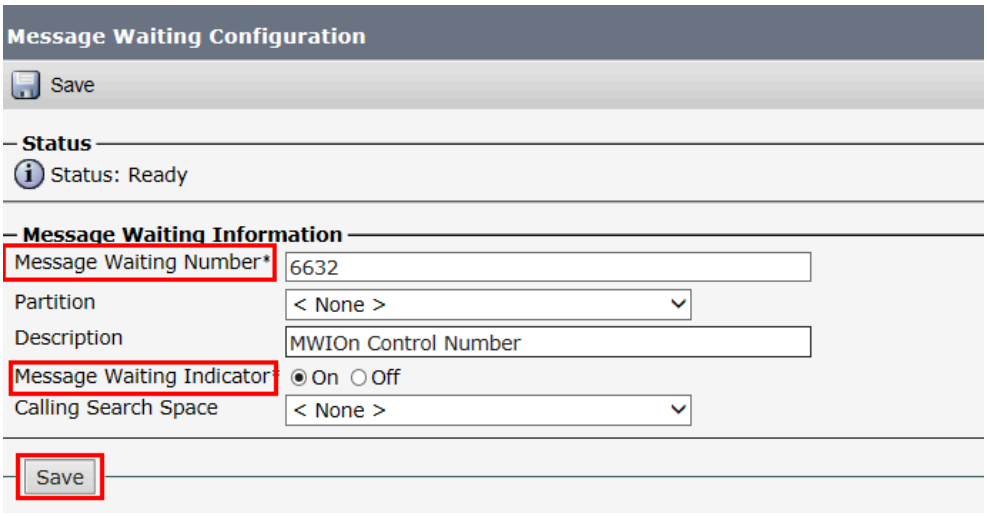
- Calling party number equals the DN number to be controlled (such as 1234)
- Called party number equals to the proper MWI control number (MWIOn or MWIOff numbers)

Open a web browser and go to CallManager administration.

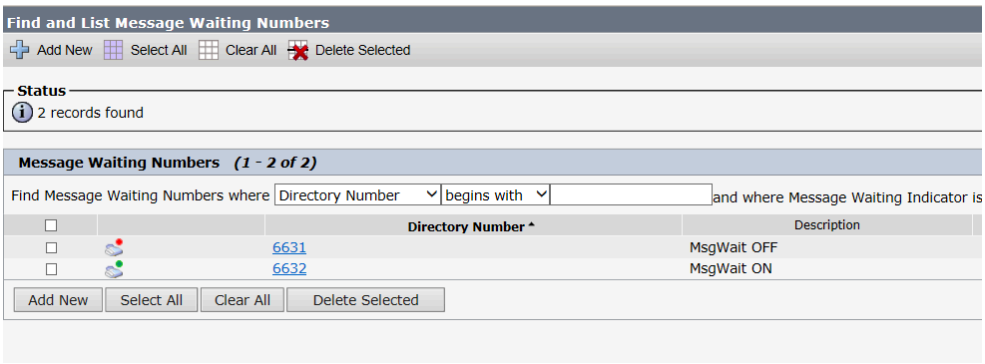
1. From the menu, select Advanced Feature | Voice Mail | Message Waiting, then click “Add New”:



2. Add a unique Message Waiting Number for Message Waiting Indicator On (such as 6632 as in our case) and click Save. Repeat the same for Message Waiting Indicator Off (the number for MWI Off must be different):



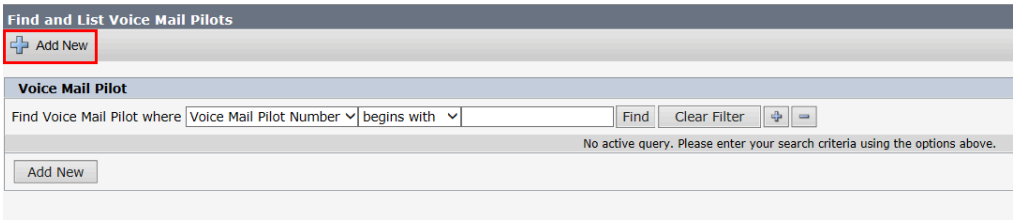
3. Click “Back to Find and List Message Waiting Numbers” to display the list of numbers:



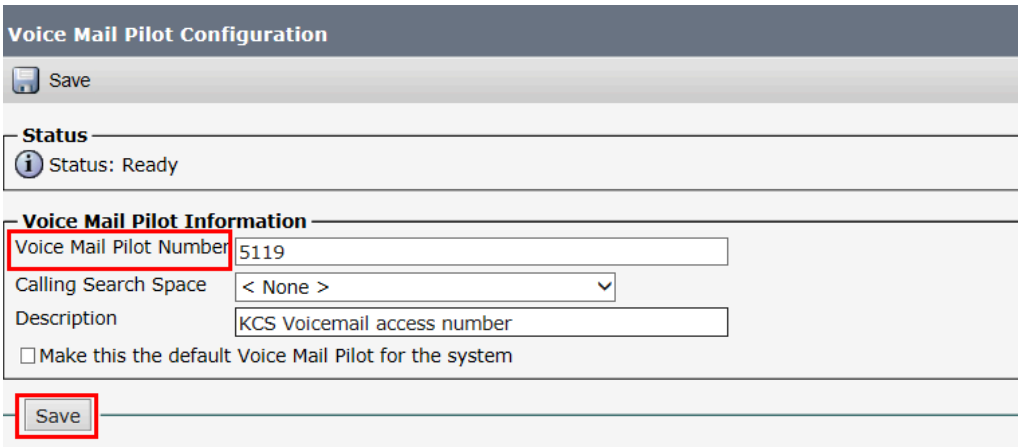
Voicemail Profile (Optional)

Voicemail profile can be optionally configured on the CCM in the case of KCS voice integration in order to simplify handling of call diversions/call forwards for DN numbers towards KCS Server.

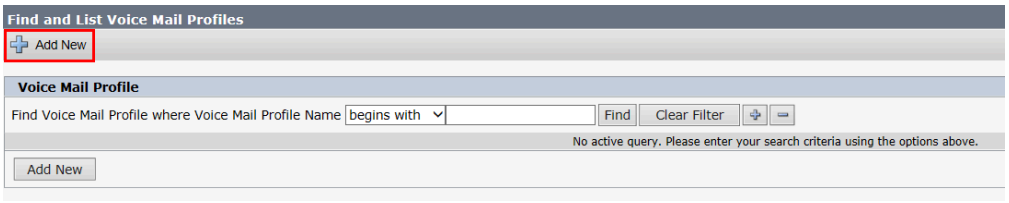
1. Open a web browser and go to CallManager administration.
2. From the menu, select Advanced Features | Voice Mail | VoiceMail Pilot, then click “Add a New Voice mail Pilot”:



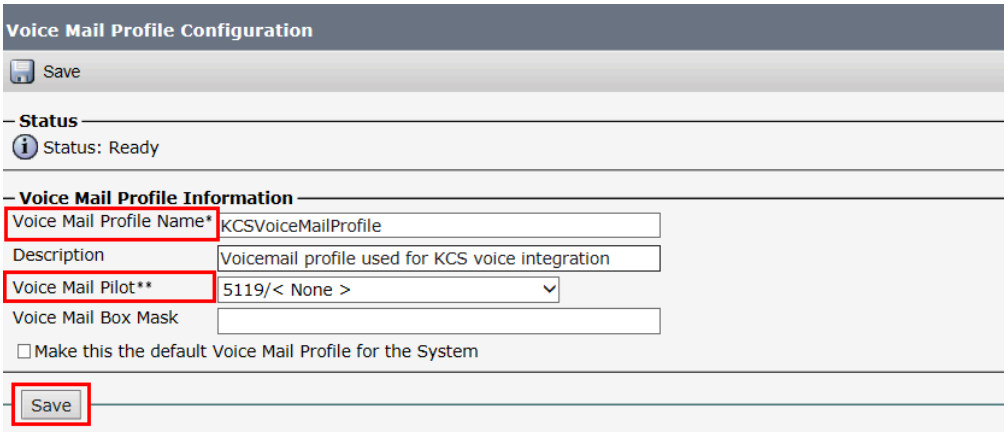
3. Enter the KCS Voice access number into the field Voice mail Pilot Number and appropriate description and click Save button (refer to the Voice Platform Technical Manual for definition of Voice Access Number).



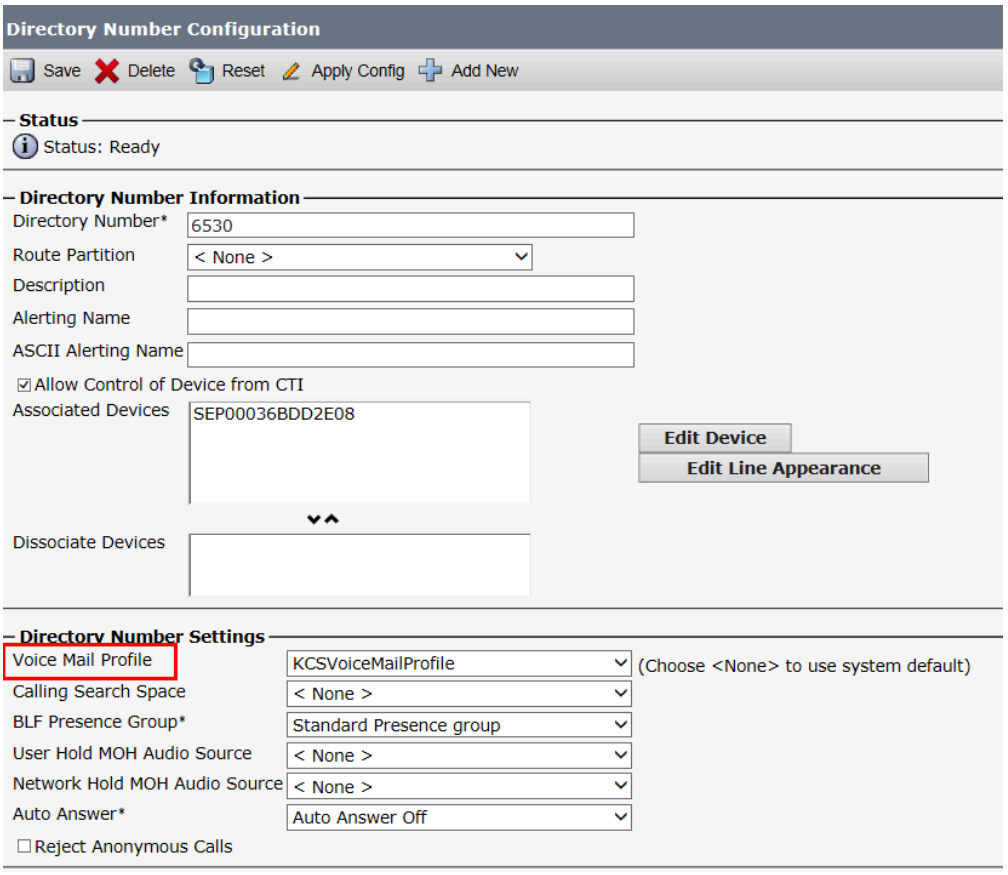
4. From the menu, select Advanced Features | Voice Mail | VoiceMail Profile, then click “Add New:

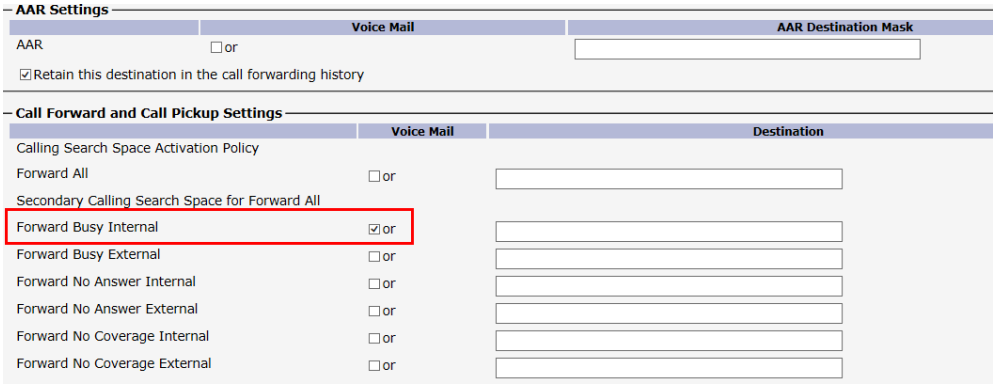


5. Enter the name of the profile, choose the Voice Mail Pilot created before and click Insert:



Having created the Voice Mail Profile, it is easy to activate the desired call diversion(s) on particular DN number to KCS Voice Server simply by choosing the created profile and selecting desired call forward variants for example:





Note The mandatory prerequisite for using CCM Voice mail profiles in this way is the Redirecting Number function activated on the H.323 or SIP trunk towards KCS FoIP.

KCS FoIP Configuration

This section describes the KCS FoIP configuration.

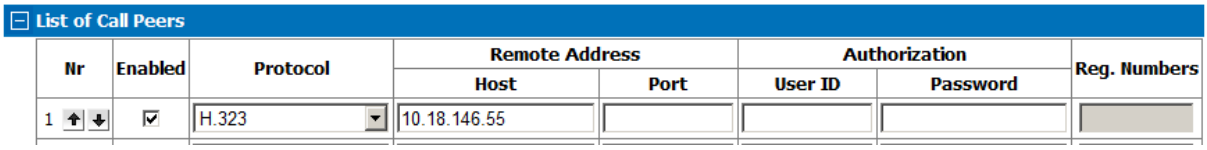
KCS FoIP Configuration for H.323 Integration

Open the KCS FoIP configuration tool and set any call peer to the following values:

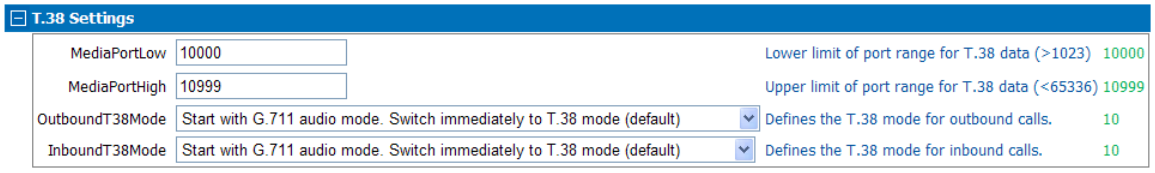
- Protocol must be set to “H.323”
- Remote Address\Host must be set to the CCM IP.
- Remote Address\Port must be set only if the port used by CCM inter-cluster trunk is different to the standard H.323 port 1720.
- The Authorization is not required
- Reg. Numbers are only required only in the case of H.323 Inter-cluster Trunk with Gatekeeper integration

Refer to the Fax over IP Technical Manual for details.

An example configuration is shown below:



Since FoIPv3 3.02.00 it is possible to define how T.38 mode is activated. These settings can be found under the T.38 settings. Unless you experience any trouble it is recommended to use the default settings as shown in the screen shot below:



Refer to the Fax over IP Technical Manual for details.

FoIPv3 Configuration for SIP Integration

Open the KCS FoIP configuration tool and set any call peer to the following values:

- Protocol must be set to “SIP”
- Remote Address\Host must be set the CCM IP.
- Remote Address\Port must be set only if the port used by CCM SIP Trunk is different to the standard SIP port 5060.
- The Authorization and Reg. Numbers are not required.

Refer to the Fax over IP Technical Manual for details.

An example configuration is shown below:

List of Call Peers

Nr	Enabled	Protocol	Remote Address		Authorization		Reg. Numbers
			Host	Port	User ID	Password	
1	☑	SIP	172.20.148.35				

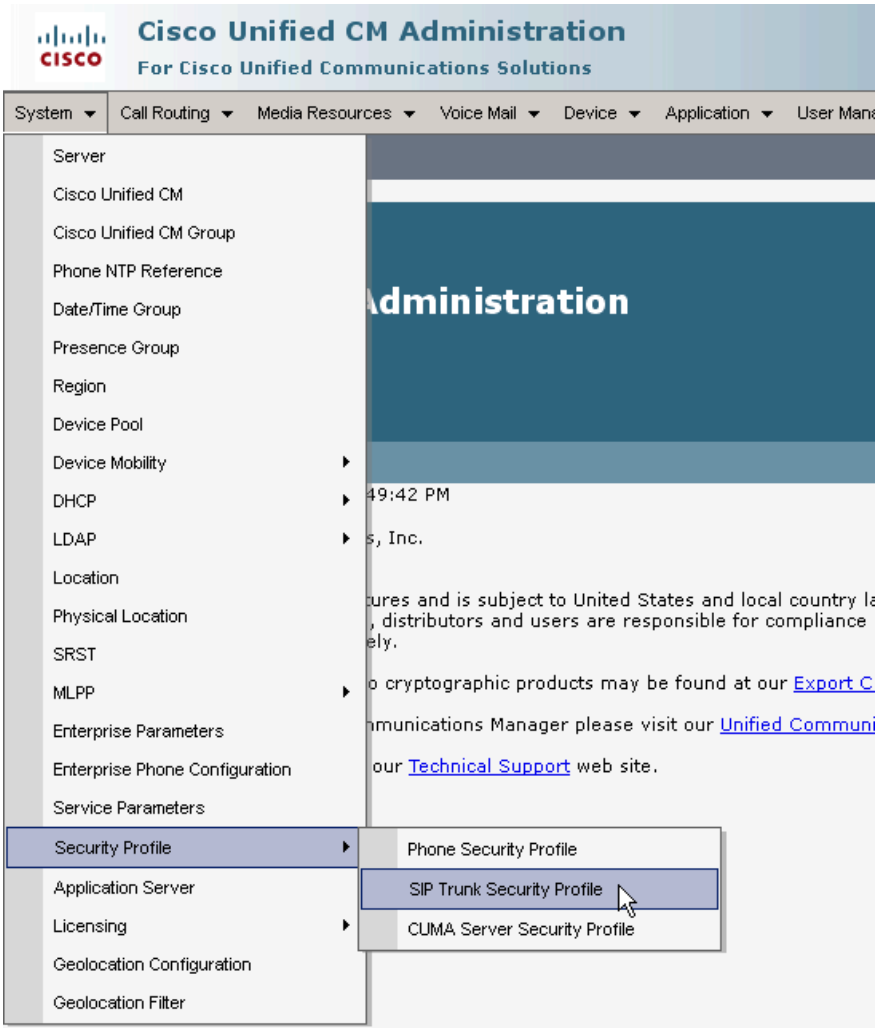
Refer to the Fax over IP Technical Manual for details.

Integration with Encryption

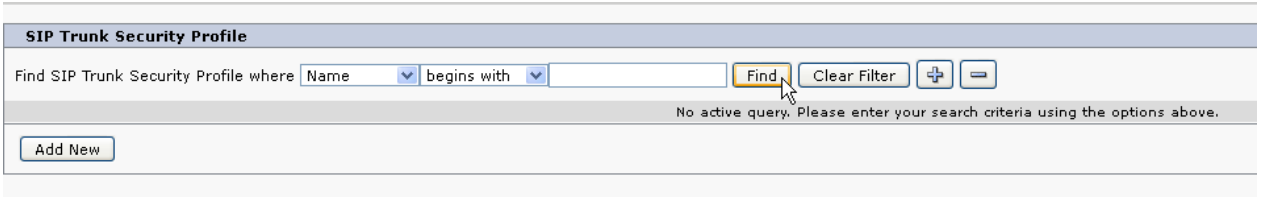
Encryption is supported via SIP only as described in this chapter. It assumes that you already have a working integration via SIP without encryption. Note that media security is not supported via T.38 fax. If you need media security with fax then G.711 pass through mode is required.

CCM/CUCM Configuration

1. Open “Cisco Unified CM Administration” and create a “SIP Trunk Security Profile”.

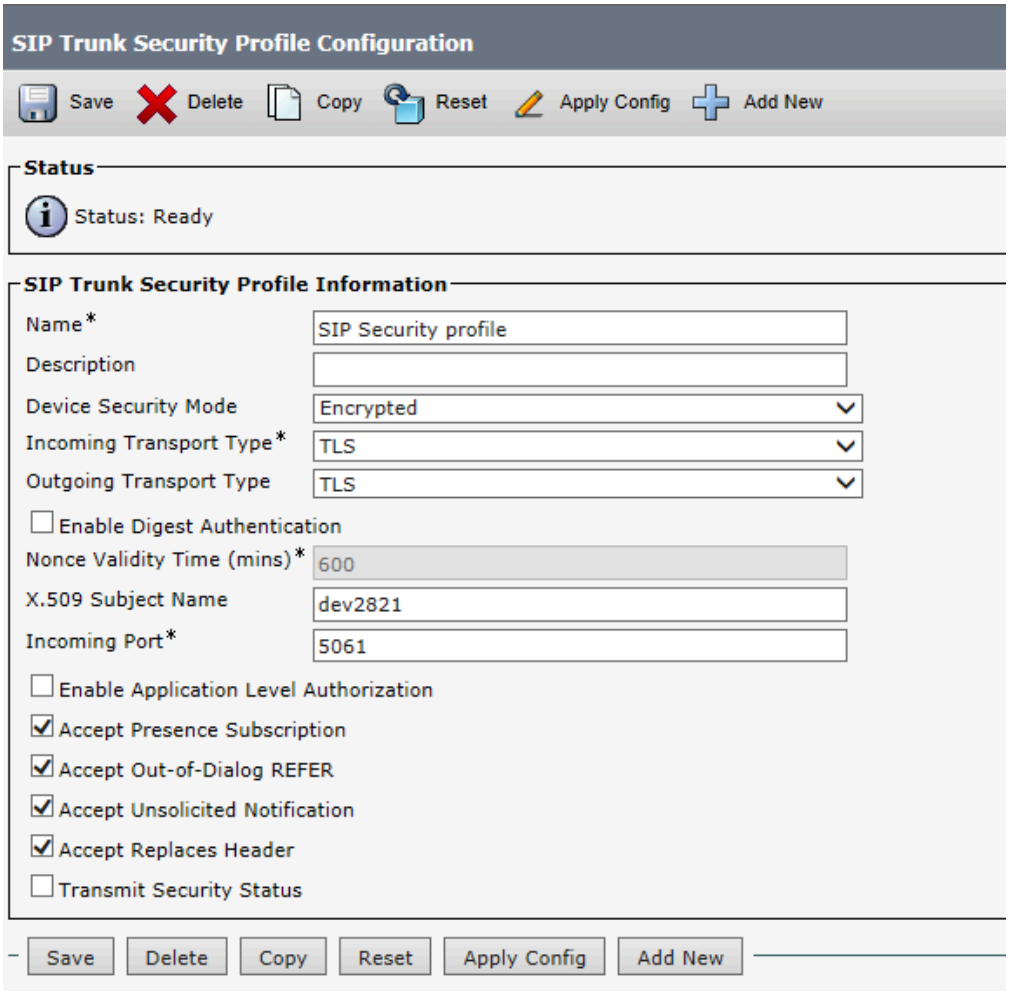


2. Click **Add New**.

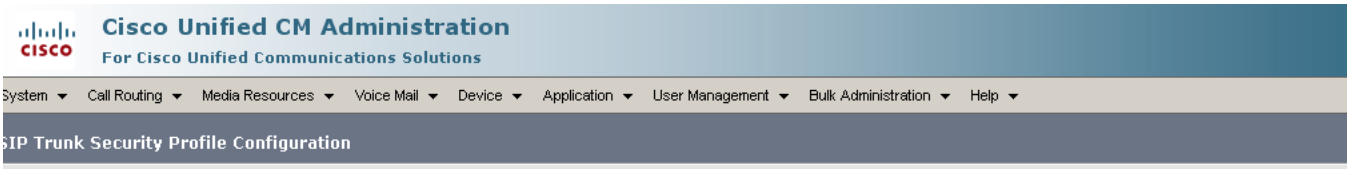


3. Enter a name and a description. Change Port from default 5060 to 5061. Enter an X.509 Subject Name (such as default FoIP: kic-electronic-documents-test-cert.kofax.com).

4. Set Device Security Mode to Encrypted. Set Incoming Transport Type and, Outgoing Transport Type to TLS.

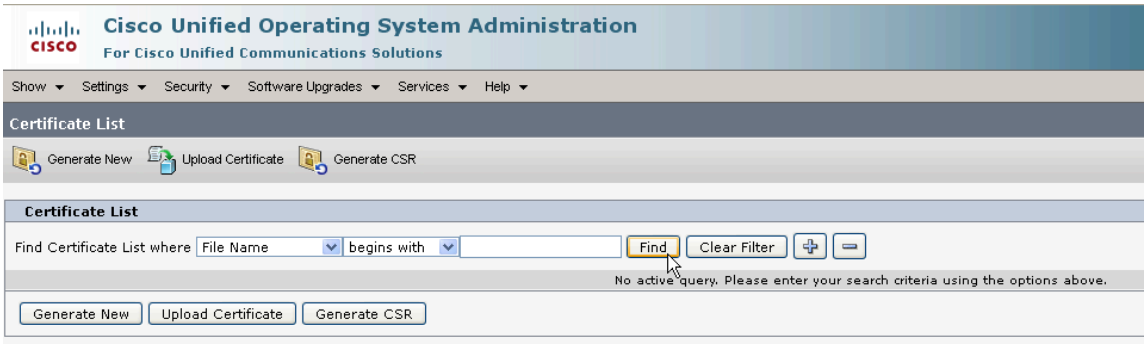


5. Switch to “Cisco Unified OS Administration” and log in (typically with a different user as used for “Cisco Unified CM Administration”).

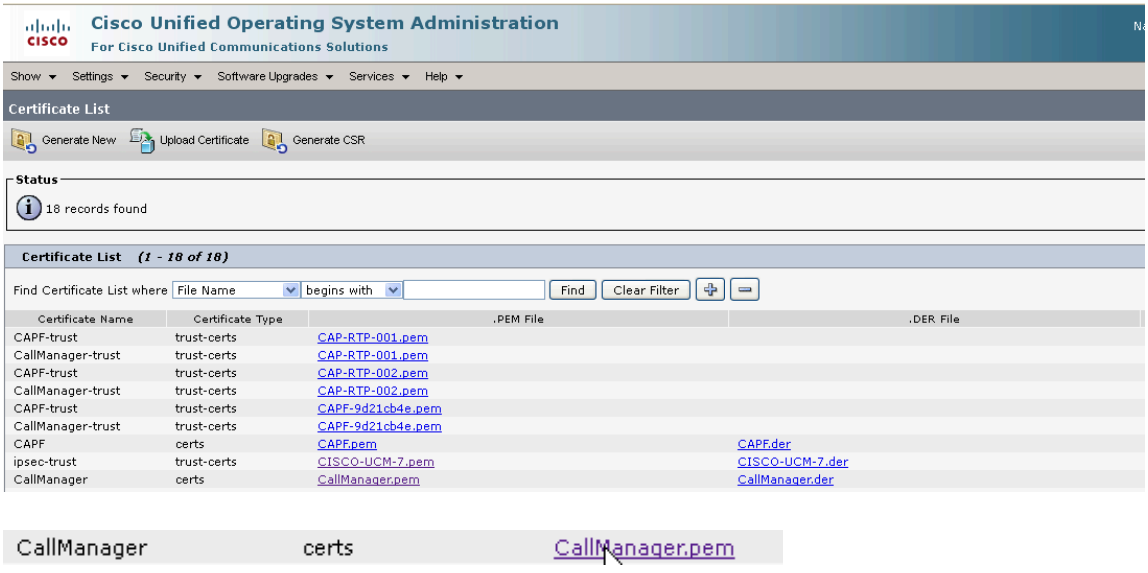


6. On the Security menu, click **Certificate Management**.

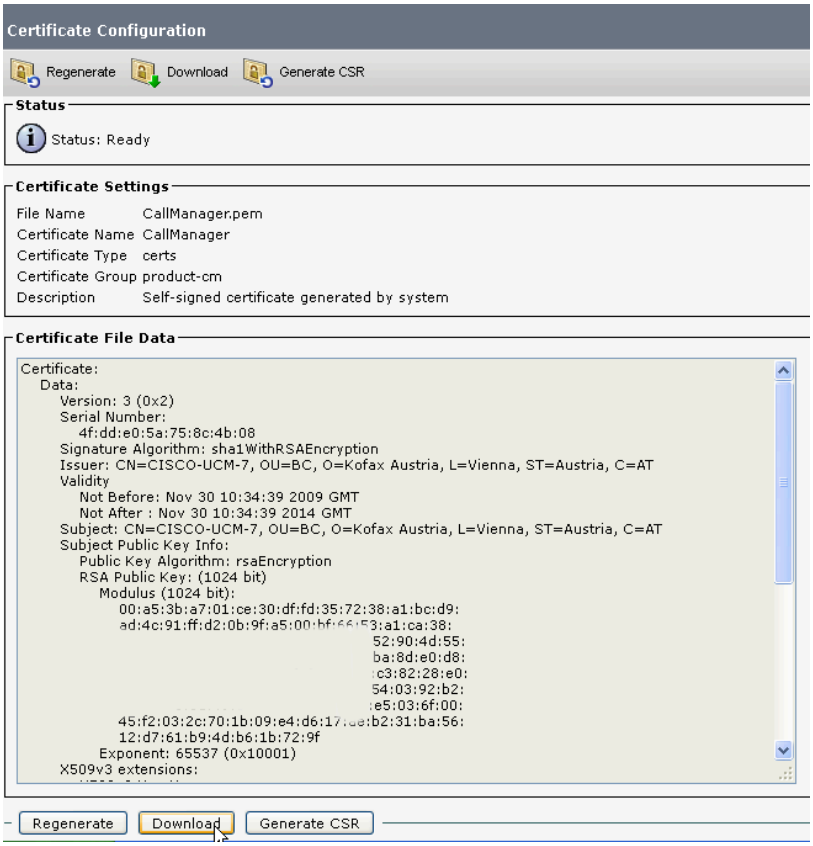
7. Click **Find**.



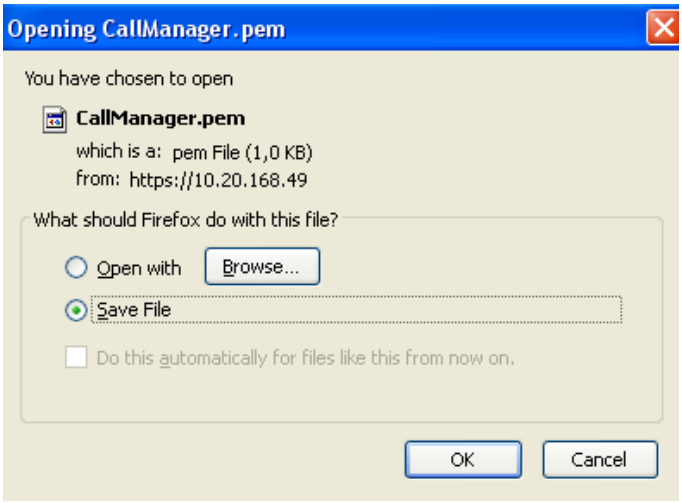
8. Select the **CallManager.PEM**.

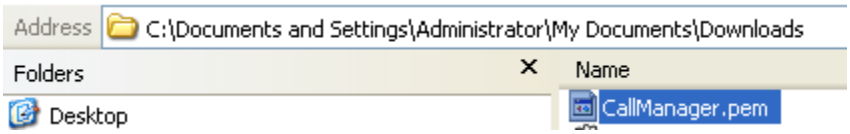


9. Click **Download**.



10. Save it as a PEM file.

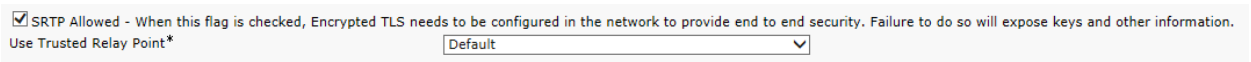




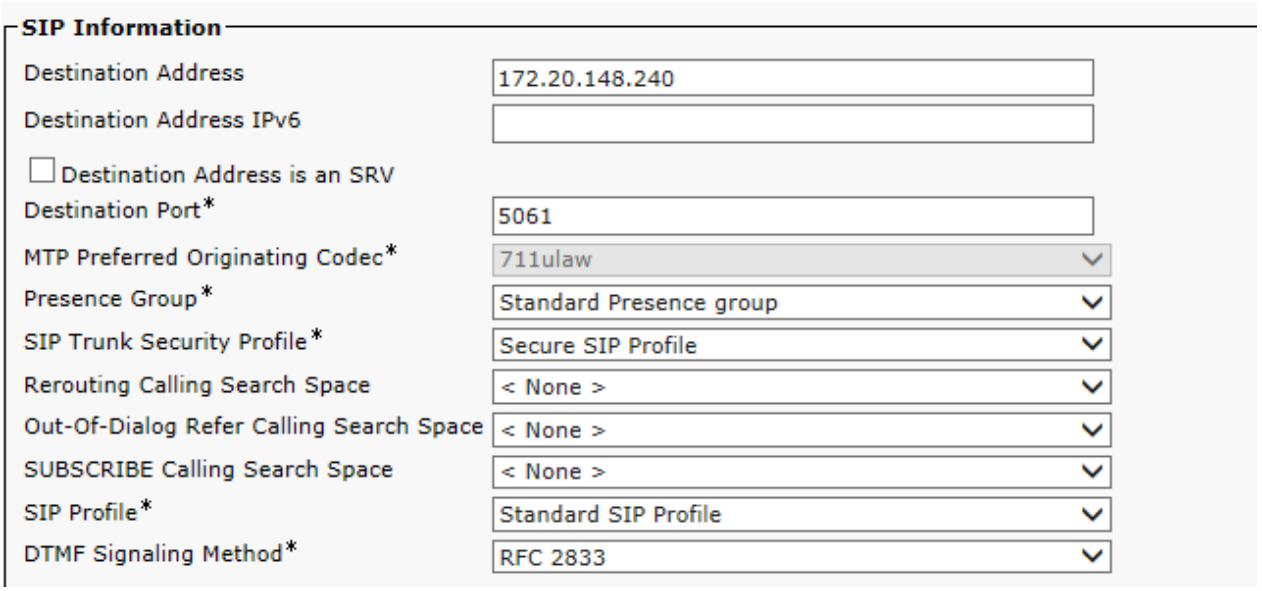
11. Open the saved PEM file with a text editor.

12. Adapt following parameters in ALL relevant SIP trunk configurations:

a. Enable SRTP mode:

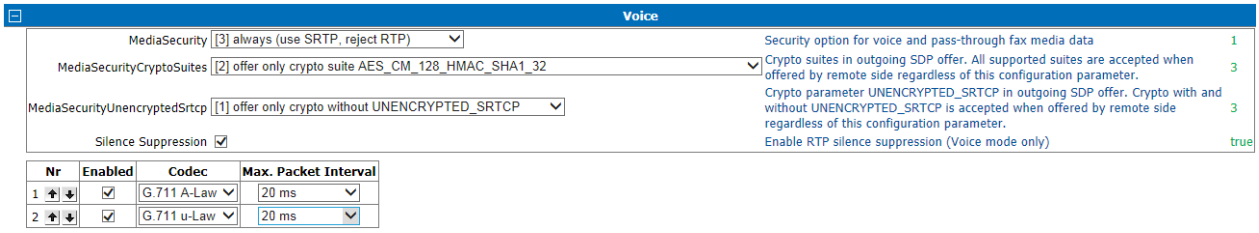


b. In SIP Trunk Security Profile field, select the newly created secure profile. Set the Destination Port to 5061.

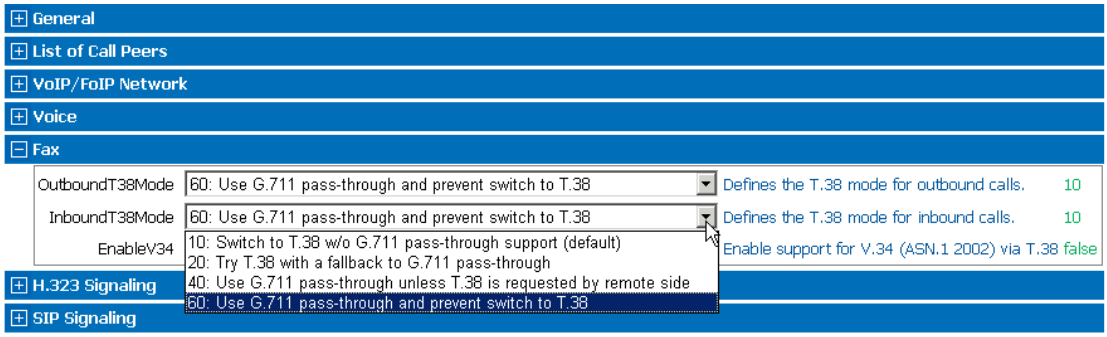


KCS FoIP Configuration

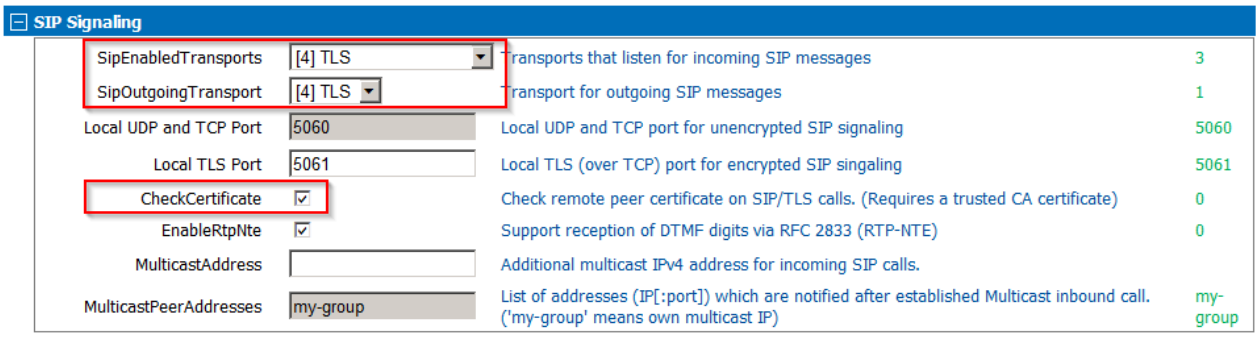
1. In the Voice tab, set “Media Security” to 2 or 3, MediaSecurityCryptoSuites to 2 and MediaSecurityUnencryptedSrtcp tp 1:



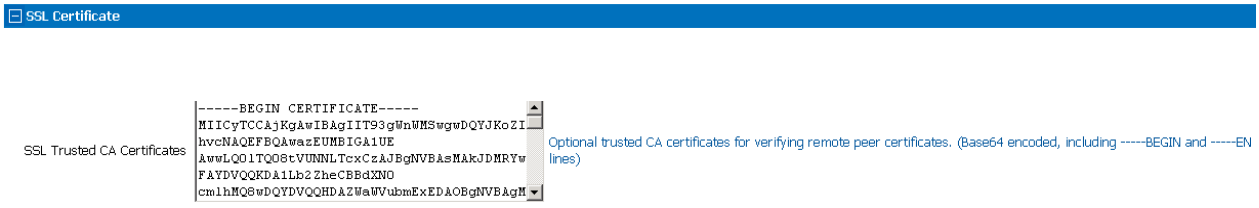
2. In the Fax tab, set the “OutboundT38Mode” and “InboundT38Mode” to 60 in order to prevent T.38.



3. In the SIP Signaling tab, set the “SipEnabledTransports”, “SipOutgoingTransport” and “Check Certificate” as shown in the example screen shot below:



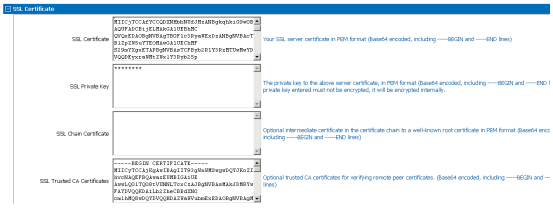
4. Go to the “SSL Certificate” tab. Copy the whole content of the saved Callmanager.PEM certificate file and paste it in the “SSL Trusted CA Certificates” field.



In case you want to use an own SSL key, copy the SSL public key content to the field “SSL Certificate” and your SSL private key to the field “SSL Private Key”. The “SSL Private Key” is encrypted when the configuration is saved. You can also use the self- signed KCS FoIP certificate which is provides as default FoIP configuration. Note that the self-signed KCS FoIP certificate does not provide reliable server authentication.

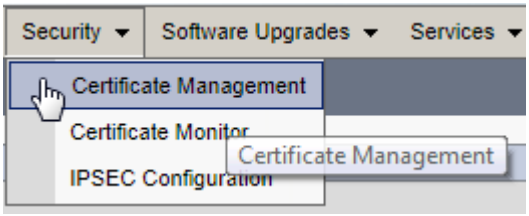
Upload the FoIP Certificate to Cisco CallManager

1. Open the KCS FoIP configuration, copy the complete content of the “SSL Certificate” field and paste it to a text file. Save it as PEM file (such as FoIP.PEM).

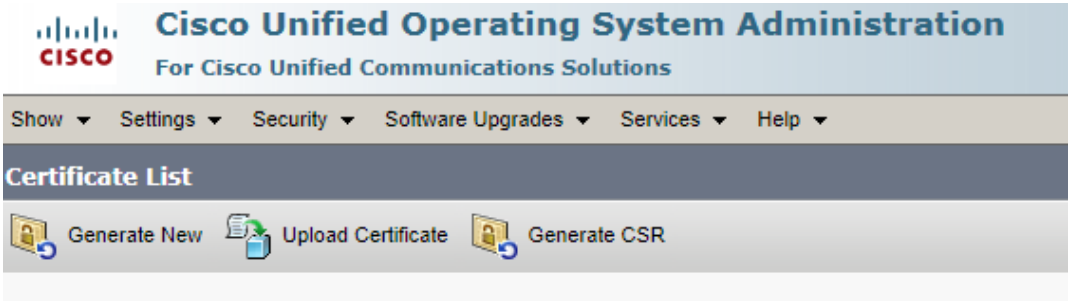


   In case you want to use your certificate, copy the SSL public key content to the “SSL Certificate” field and your SSL private key to the “SSL Private Key” field. The “SSL Private Key” is encrypted when the configuration is saved.

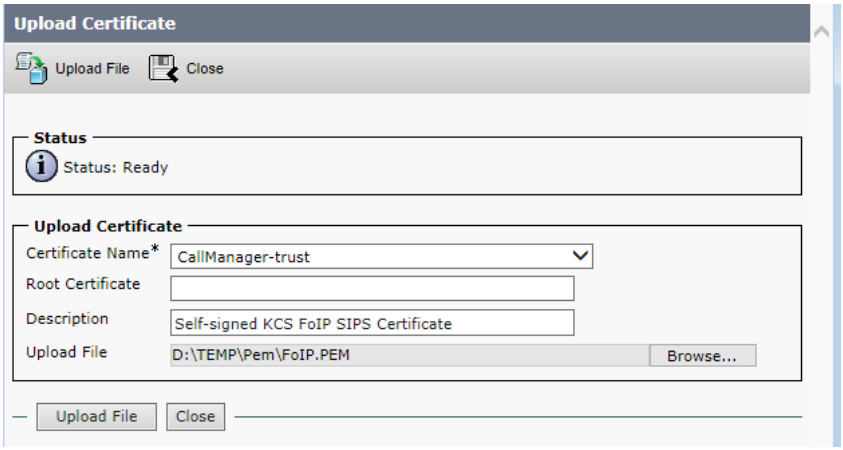
2. Open “Cisco Unified OS Administration” and log in. On the Security menu, click Certificate Management.



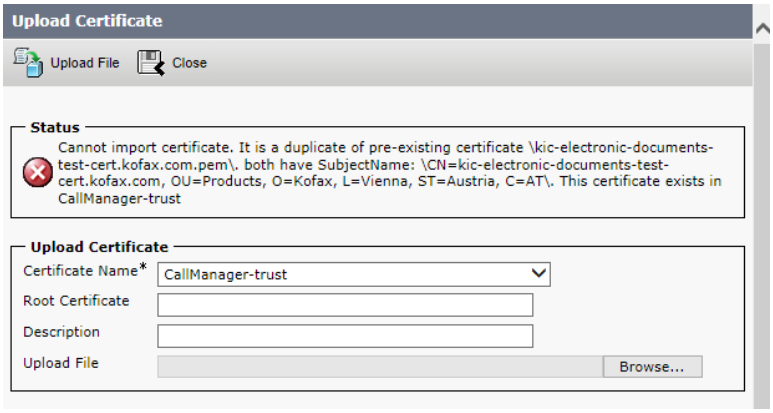
3. Click **Upload Certificate**.



4. Browse to the location, where the FoIP.PEM is stored, select “CallManager-trust” as certificate name and click Upload File.



Cisco Callmanager checks during upload for duplicate certificates.



CISCO Gateway Configuration Example

In the case of FoIP integration with encryption, also the Cisco gateway should be configured correspondingly to support SRTP and secure signaling.

This section provides an example as how to do it in the case the gateway is interconnected with CUCM through SIP Trunk.

The SIP gateway has to perform the certificate exchange with the CUCM (like the FoIP).

1. Upload the CUCM certificate to Cisco gateway

   Download the CUCM certificate from the CUCM in the same way as described for FoIP in the PEM format,
   open the terminal connection with the gateway and upload the certificate to the gateway utilizing following steps (the name “CCM-Cert” can be freely chosen):

```
crypto pki trustpoint CCM-Cert
enrollment terminal
revocation-check none
```

```
!--- Download the Cisco CallManager certificate, and paste
          !--- the contents of the certificate, pem format.
crypto ca authenticate CCM-Cert

Enter the base 64 encoded CA certificate.
         End with a blank line or the word "quit" on a line by itself

          -----BEGIN CERTIFICATE-----
          MIICIjCCAYugAwIBAgIIS4xQN3bIZUowDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1UE
          ……
          /DV5TbDUdre6Org1mn4uaMdrYzt1kQ==
           -----END CERTIFICATE-----

        Certificate has the following attributes:
          Fingerprint MD5: 1EF154E3 70E40379 1C7003B9 B29E111B
          Fingerprint SHA1: CAFA0F83 B04B2E65 71104B73 64BF6AEB ABE9EED9

        % Do you accept this certificate? [yes/no]: yes
        Trustpoint CA certificate accepted.
        % Certificate successfully imported
```

2. Generate self-signed certificate of the gateway (for example, set its CN=dev2821)

```
crypto pki trustpoint dev2821
     enrollment selfsigned
     fqdn none
     subject-name CN=dev2821
     revocation-check none
     rsakeypair dev2821
```

```
 crypto ca enroll dev2821
   % The fully-qualified domain name will not be included in the certificate
   % Include the router serial number in the subject name? [yes/no]: no
   % Include an IP address in the subject name? [no]: no
   Generate Self Signed Router Certificate? [yes/no]: yes
   Router Self Signed Certificate successfully created

   !— View the certificate in PEM format, and copy the Self-signed CA certificate
   !--- (output starting from “----BEGIN” to “CERTIFICATE----“) to a file named
 such as dev2821.pem

 crypto pki export dev2821 pem terminal
   % Self-signed CA certificate:
    -----BEGIN CERTIFICATE-----
    MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZTSVAt
    ….
    s980Np7dLJU=
    -----END CERTIFICATE-----

    % General Purpose Certificate:
    -----BEGIN CERTIFICATE-----
    MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZTSVAt
    …
    IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4m1sIMzDAHfsl7dJlB2IOw9Sk
    s980Np7dLJU=
    -----END CERTIFICATE-----
```

3. Import the dev2821.pem certificate to the CUCM in the same way as the FoIP certificate gets imported
4. Configure the SIP stack to use the self-signed certificate of the router in order to establish a SIP TLS connection from/to CUCM (the ip address is that of the CUCM)

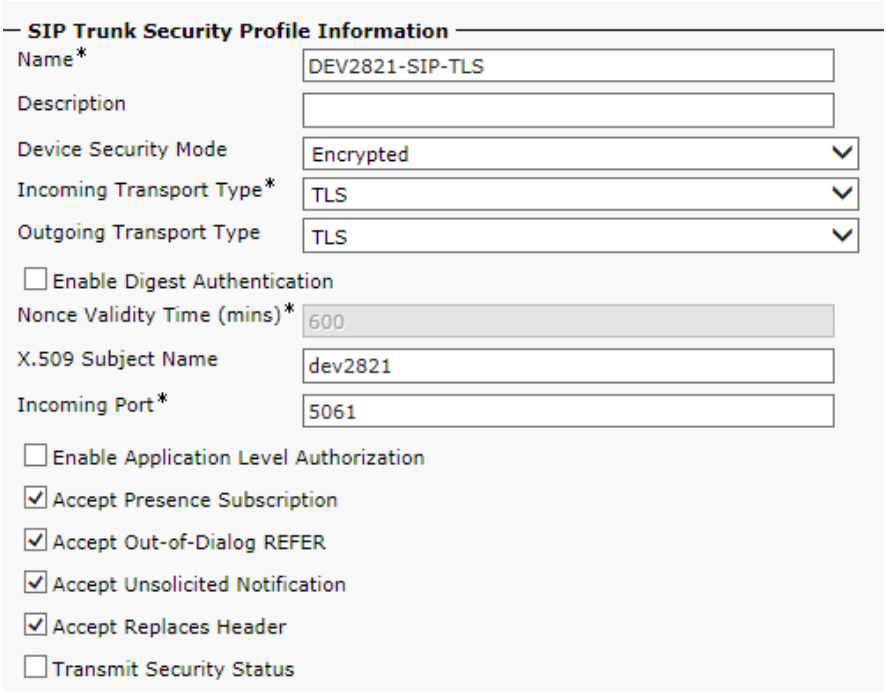
Note that the CN name (“dev2821” in the example) must be the same as the X.509 subject name configured in the corresponding CUCM’s “SIP Trunk Security Provider” of the SIP trunk connected to the gateway:

```
sip-ua
    crypto signaling remote-addr
         10.20.168.90 255.255.255.255
         trustpoint dev2821 strict-cipher
```

5. Enable SIP TLS and SRTP support at dial-peer level:
dial-peer voice 6000 voip

```
description 6000-6999 - CUCM 9.0
destination-pattern 6...
session protocol sipv2
session target ipv4:10.20.168.90
session transport tcp tls
srtp
dtmf-relay rtp-nte
codec g711ulaw
no fax-relay sg3-to-g3
no vad
```

6. Apply SIP Security provider on the SIP trunk configured for the gateway with these settings:



7. Enable SIP Trunk for the gateway for SRTP

Assigning Outbound CUCM Calls with Particular Inbound VoIP Dial-Peer

Each call on a Cisco gateway has to match particular inbound and outbound dial-peer.

While matching of the outbound dial-peers automatically occurs based on the dialed called party and the destination-pattern attribute of the dial-peer, matching of the incoming calls (such as from FoIP through CUCM) can occur by the means of several methods utilizing calling or called party number of a call.

The most straightforward and logical way to match an incoming FoIP call with an incoming dial-peer would be to match its calling party number with the destination-pattern attribute of the dial-peer: but the problem is that by default, FoIP calls doesn't set any calling party number in the outgoing calls.

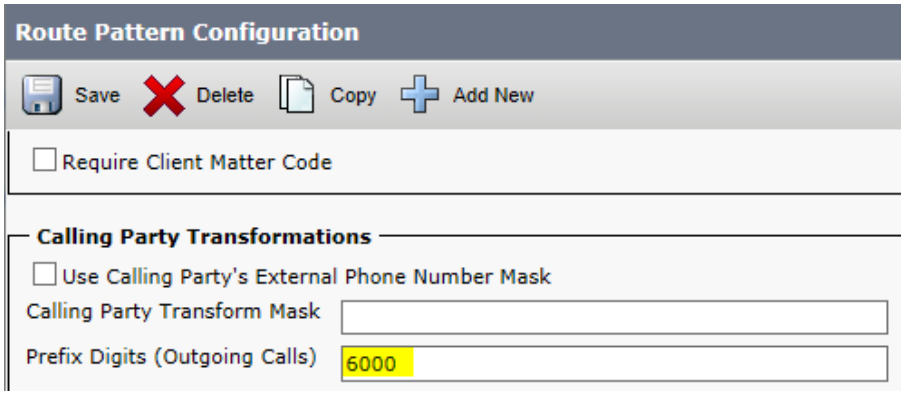
FoIP calls without calling party number can't be matched with any concrete dial-peer (except for a possibility to match the inbound dial-peer based on the called party number, which doesn't seem to make a real sense), and therefore the call uses the global parameters configured in the voip service. In this way, the Cisco gateway can be globally setup either for secure SIP with SRTP, or without security, for all possibly connected FoIP instances and CUCM servers.

The simple workaround is to insert a prefix for the calling party number in the CUCM SIP trunk for the gateway
to match particular incoming dial-peer (per destination-pattern attribute) and then remove it through number translation profile on the gateway in the inbound dial-peer just matched for the call.

Example:

Assume dial-peer for the CUCM with number range 6XXX.

Define the calling party prefix 6000 in the route pattern configuration for calls routed to the gateway's SIP trunk:



Define translation profile (named such as CUCM90) to remove the prefix 6000 from the number:

```
voice translation-rule 6000
rule 1 /^6000/ //
voice translation-profile CUCM90
translate calling 6000
```

Apply this translation profile to the incoming numbers in the related dial-peer:

```
dial-peer voice 6000 voip
description 6000-6999 - CUCM 9.0
translation-profile incoming CUCM90
destination-pattern 6...
no voice-class sip srtp negotiate
session protocol sipv2
session target ipv4:10.20.168.90
session transport tcp tls
dtmf-relay rtp-nte
srtp
codec g711ulaw
no fax-relay sg3-to-g3
no vad
```

In this way, all incoming FoIP calls without or even with some particular calling party number are assigned with the inbound dial_peer 6000 where the prefix 6000 is removed from the calling party number (prior to routing the call further).

Hints

This section provides additional information about integration with Cisco CallManager.

T.38 Mode Does Not Work with MGCP Gateways

It has been recognized that in the case of SIP integration, CUCM rejects the activation of T.38 mode (with SIP error code 488) in the following case:

1. An MCGP gateway is used
2. The feature “mgcp package-capability fm-package” is not enabled in the MGCP gateway
3. FoIPv3 has enabled reception with RTP named telephone events (RTP-NTE) according to RFC 2833. RTP-NTE is always enabled in FoIPv3 3.06.00. Since FoIPv3 3.08.09 it can be enabled/disabled in the SIP part of the configuration as shown in the screen shot below:

Note RTP-NTE is required for voice operation with SIP on order to received DTMF digits. It not required for Fax. The problem is that if RTP-NTE is enabled, is has also been added to the SDP session of the INVITE message and this may prevent the activation of T.38 mode using CCM and an MGCP gateway.

Solution:

Either enable “mgcp package-capability fm-package” in the MGCP gateway or disable reception of DTMF digits via RFC 2833 (RTP-NTE) in FoIPv3.

More details can be found in the CISCO Support Community article: *MGCP Gateway Design with CVP* (link: https://supportforums.cisco.com/docs/DOC-1172) and in the SPR00053967

Redirecting Number (Call Diversion)

In the case of the voice integration, it is always recommended to activate the inbound function “Redirecting Number IE Delivery” on each H.323 trunk towards KCS and “Redirecting Diversion Header Delivery” on each SIP trunk.

Example:

The redirecting number is delivered in the H.323 setup message (4636 in this example). The CCM 6 inserts this number in the Q.931 part of this message.

```
    .000 .... = Number type: Unknown (0x00)
    1... .... = Extension indicator: last octet
    Called party number digits: 4511
  Redirecting number: '4636'
    Information element: Redirecting number
    Length: 7
    .... 0000 = Numbering plan: Unknown (0x00)
    .000 .... = Number type: Unknown (0x00)
    0... .... = Extension indicator: information continues through the next octet
    .... ..00 = Screening indicator: User-provided, not screened (0x00)
    .00. .... = Presentation indicator: Presentation allowed (0x00)
    0... .... = Extension indicator: information continues through the next octet
    Reason for redirection: Call forwarding unconditional or systematic call redirection
    Redirecting party number digits: 4636
  User-user
    Information element: User-user
    Length: 199
```

In addition, it also delivers the redirecting number encapsulated in an H.221 non-standard identifier in the H.225 section.

```
          0... .... maintainConnection: False
      0... .... h245Tunneling: False
    nonStandardControl: 1 item
      Item 0
        Item
          nonStandardIdentifier: h221NonStandard (1)
            h221NonStandard
                t35CountryCode: United States (181)
                t35Extension: 0
                manufacturerCode: 18
              H.221 Manufacturer: Cisco (0xb5000012)
            data: 19 octets
            Data (19 bytes)

0020  94 08 b2 81 06 b8 da 40  dd 51 f2 56 2f a3 80 18   .......@ .Q.V/...
0030  16 d0 29 90 00 00 01 01  08 0a 0f 69 11 25 00 00   ..)..... ...i.%..
0040  00 00 03 00 00 f1 08 02  00 0d 05 04 03 80 90 a2   ........ ........
0050  6c 07 00 81 35 35 32 32  37 70 05 80 34 35 31 31   l...5522 7p..4511
0060  74 07 00 00 8f 34 36 33  36 7e 00 c7 05 20 b0 06   t....463 6~... ..
0070  00 08 91 4a 00 05 02 02  00 88 55 a4 1f 00 35 00   ...J.... ..U...5.
0080  35 00 32 00 32 00 37 00  00 00 00 00 00 00 00 00   5.2.2.7. ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 22 c0 b5   ........ .....".. 
00c0  00 00 12 0f 43 69 73 63  6f 43 61 6c 6c 4d 61 6e   ....Cisc oCallMan
00d0  61 67 65 72 00 31 00 01  01 80 78 44 00 80 3d b8   ager.1.. ..xD..=.
00e0  89 b0 ab 41 9d 0d 00 29  01 ac 14 94 23 00 d5 0d   ...A...) ....#...
00f0  80 00 07 00 0a 14 a8 30  06 b8 11 00 80 3d b8 89   .......0 .....=..
0100  b0 ab 41 9d 0d 00 29 01  ac 14 94 23 01 00 01 00   ..A...). ...#....
0110  01 00 01 00 10 a0 01 00  1a 01 40 b5 00 00 12 13   ........ ..@.....
0120  90 09 74 07 00 00 8f 34  36 33 36 14 40 00 04 00   ..t....4 636.@...
0130  01 03 00                                          ...
```

In case of multiple forwarding only the first number (original called number) is delivered.

Cisco Gatekeeper

This section describes how to use a Cisco gatekeeper with a Cisco gateway and FoIP.

Integration of a Cisco Gatekeeper

This chapter describes how to use a Cisco gatekeeper with a Cisco gateway and FoIP. In this example the gateway and the gatekeeper are running on the same physical device.

Configuration of the Cisco Gateway

The following configuration steps must be taken to use a Cisco gatekeeper with a Cisco gateway:

```
h323-gateway voip interface
h323-gateway voip id gk-zone ipaddr 172.20.148.35 1718
h323-gateway voip h323-id gw_35
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 172.20.148.35
```

These lines must be added to the interface configuration, such as interface GigabitEthernet0/0. In the second line gk-zone is the name of gatekeeper zone and 172.20.148.35 is the IP address of the gatekeeper. Line 3 defines the H.323-ID of the gateway. Line 4 defines the technology prefix which the gateway should register. The last line binds the interface with address 172.20.148.35 to the gatekeeper.

For incoming calls you need to define a dial peer with a number range:

```
dial-peer voice 98000 voip
 destination-pattern 98..
 session target ras
 codec g711alaw
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback Cisco
 no vad
```

As session target select ras.

In the configuration mode you need to type:

```
gateway
```

Configuration of the Cisco Gatekeeper

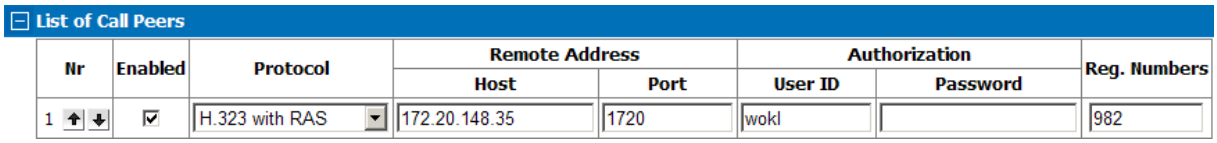
To enter the gatekeeper configuration type *gatekeeper* in the configuration mode. Then define a gatekeeper zone and a default technology prefix. Type “no shutdown” to activate the gatekeeper.

```
gatekeeper
 zone local gk-zone kofax.com 172.20.148.35
 gw-type-prefix 1#* default-technology
 no shutdown
```

In this example gk-zone is the name of the gatekeeper zone, Kofax.com is the domain and 172.20.148.35 is the IP address of the interface of the gatekeeper.

Configuration of FoIP

Open the configuration web page. Configure a call peer for the gatekeeper:



Select “H.323 with RAS” as protocol. Enter User ID and Password if required. Under Reg. Number specify the number with should be registered when FoIP is a terminal or the prefix if FoIP is a gateway.

Under H.323 Settings you can configure if FoIP registers as terminal or gateway. If FoIP works as gateway you can give the name of the gatekeeper zone.

Configuration of Multiple Zones

On a gatekeeper you can configure multiple zones:

```
gatekeeper
 zone local gk-zone kofax.com 172.20.148.35
 zone local myzone kofax.com
 gw-type-prefix 1#* default-technology
 gw-type-prefix 982* hopoff myzone
 gw-type-prefix 981* hopoff gk-zone
 gw-type-prefix 0* hopoff gk-zone
 no shutdown
```

So that the gatekeeper relays a call to a different zone you need to configure the prefixes of the numbers that should be forwarded.

GNUGk 2.0.8

Kofax Communication Server Voice over IP can be integrated with GNUGK 2.0.8 using the H.323 protocol.

VoIP Integration via H.323

This integration corresponds with the most general use case. It uses open-source H.323 components that are available for free and is dedicated mainly for test and educational purposes.

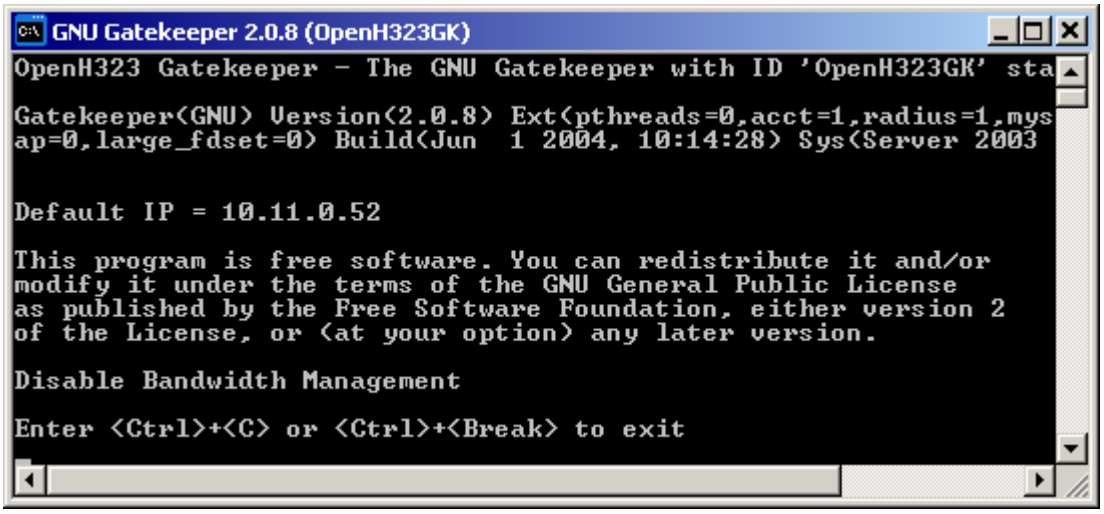
Configure the GNUGk Gatekeeper

1. Download the Windows executables (available as Windows ZIP file) and manual (PDF file) from http://www.gnugk.org/h323download.html (for version 2.0.8 or later).
2. Unzip all files into a directory of your choice (such as GNUGk).
3. Create the configuration file “gatekeeper.ini” in the subdirectory `GNUGk\bin`. Another subdirectory `GNUGk\etc` contains a couple of sample config files. You can start with the simplest one named “gnugk.ini”. Copy it into `GNUGk\bin` and rename to “gatekeeper.ini”.

   This config file contains following lines:

```
##
## A very simple configuration file.
## Everyone is allowed to connect to the status port.
##
[Gatekeeper::Main]
Fourtytwo=42
TimeToLive=300
Name=MyGnuGk
[GkStatus::Auth]
rule=allow
```

4. Start gnugk.exe in the `GNUGk\bin` directory. The following screen appears:



Now the gatekeeper is running.

Configure the KCS Voice Server

1. Setup the KCS voice server for H.323 integration in the auto-discovery gatekeeper mode using registration type gateway.

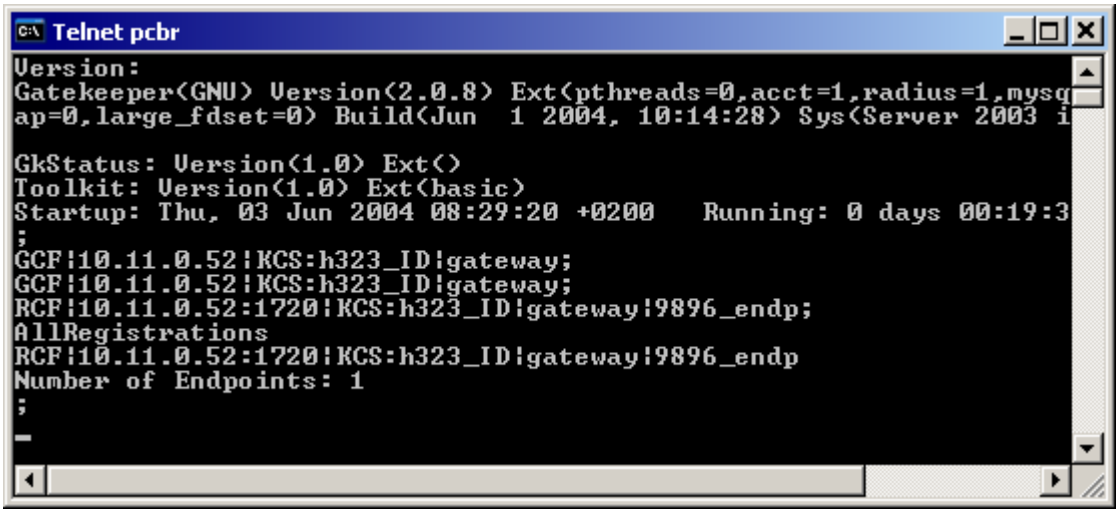
   Choose any endpoint name, such as “KCS”, and prefix you would like to use to route calls towards KCS server, such as “9” (that is, all numbers starting with “9” are routed to KCS server).

   It is possible to install the voice server on the same computer along with the GNUGk gatekeeper although it is not recommended (see *Check for Open H.323 Listeners on the Local Interfaces*).

   Note If you have several gatekeepers running in your network, it would be better not to use the auto-discovery method, but locate the GNUGk per IP address.

2. Open the Telnet session to the server where GNUGk is running using port 7000 (open the command line box, and type telnet *server_name* 7000).
3. Start KCS voice server and wait until TCECP starts.

4. Type ‘r’ and <Enter> in the telnet session. The following screen that informs you that the endpoint with H323_ID=KCS has been registered as gateway, appears.



Now KCS voice server has already been registered on the gatekeeper and it is prepared to receive (and originate) H.323 calls.

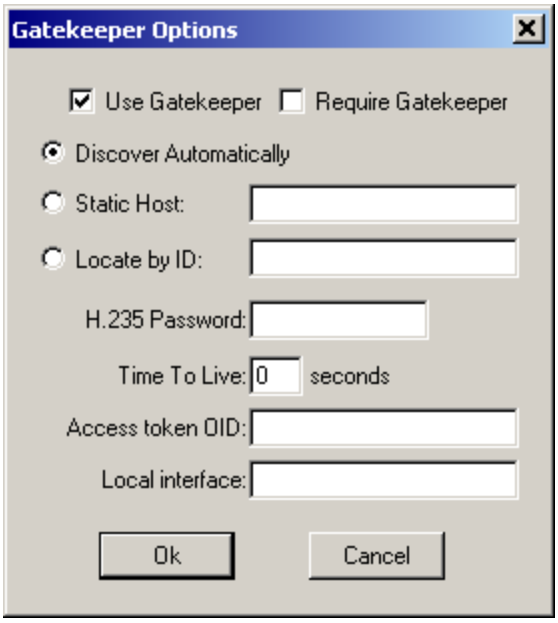
Configure the OpenPhone Application

What we need at this point is an H.323 compatible terminal to be able to register on the GNUGk and make an incoming call.

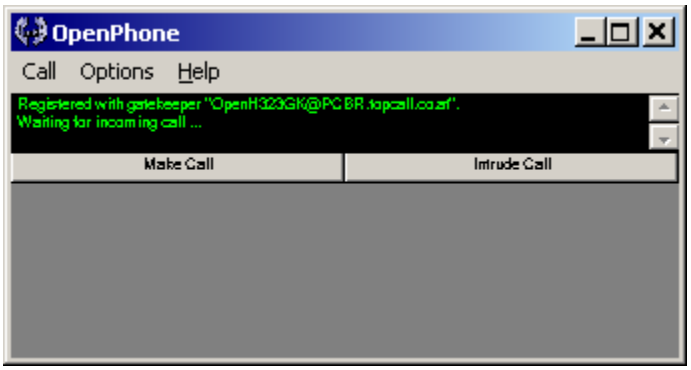
Although we can use one of the H.323 telephones available in the market (like Tiptel Innovaphone IP200), it is also possible to use the open-source software telephone application called “OpenPhone”:

1. Download and install the software is described in OpenPhone (H.323 Telephone Software).

2. In the gatekeeper options check “Use Gatekeeper” and “Discover Automatically”:



3. Restart OpenPhone. The following screen that informs you on the successful gatekeeper registration, appears.

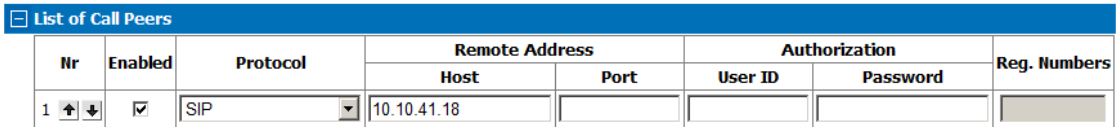


Now if you dial any number starting with digit 9, the call will be routed towards KCS server.

Huawei SoftX3000-Softswitch

Fax Integration via SIP Trunk

We can integrate via SIP trunk like a SIP Gateway. A call-peer with type SIP and the IP of the Huawei Softswitch is required. See example below:



Notes:

- The Softwitch does not support T.30 error correction mode. There all fax call uses the fall-back to none-ECM.
- The Softwitch may fails if a single T.38 packet contains more than 64 data Bytes. This issue has been considered since FoIP 3.10.00. With FoIPv3 3.09.03 - 3.09.10 the configuration value T38\NoneEcmTxInterval must be set to 36ms. Versions before 3.09.03 are not recommended.
- The Softswitch does not correctly handle a collision of Change-to-T38-mode Re-Invite transaction. Such a problem may happen during loop tests from KCS FoIP to KCS FoIP if both the outgoing and the incoming side are using the T.38 activation mode 10 (start with G.711audio mode. Switch immediately to T.38 mode). Do avoid this problems, it is recommended to change the T.38 mode for outgoing calls to 20 (Send one CED tone as G.711 audio and then switch to T.38 mode)

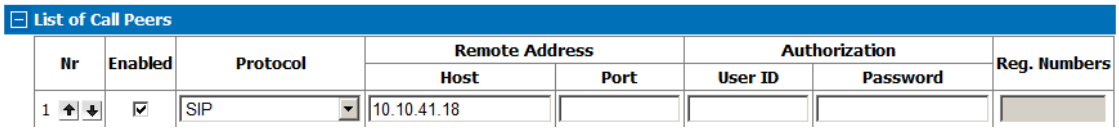
Mitel 3300 ICP Voice

Fax Integration via SIP Trunk

The integration with Mitel 3300 ICP voice requires FoIP 3.09.04 or higher (correction of SPR56467). It is important to disable the session timer for the used SIP trunk because Mitel uses SIP UPDATE method which is optional and currently not supported by FoIP. The most important configuration parameters are shown below:

FoIP Configuration:

Use Protocol “SIP” and configure the IP (and optional port) used by Mitel. An example is shown below:



Mitel Configuration:

A sample configuration of the SIP trunk for KCS FoIP is shown below. It is important to set the session timer to “0”.

Parameter	Value
SIP Peer Profile Label	Kofax
Network Element	2a72f460-1dd2-11b2-bb36-08000f1e9808
Registration User Name	
Address Type	IP Address: 10.10.10.10
Outbound Proxy Server	
Default CPN	
Restriction	FALSE
Trunk Service	10

Parameter	Value
Interconnect Restriction	1
Maximum Simultaneous Calls	2
Session Timer	0
Zone	2
SMDR Tag	0
NAT Keep alive	FALSE
Enable Mitel Proprietary SDP	No
Use P-Asserted Identity Header	No
Use Restricted Character Set For Authentication	No
Disable Reliable Provisional Responses	Yes
Use Alternate Destination Domain	No
FQDN or IP Address	
Ignore Incoming Loose Routing Indication	No
Suppress Use of SDP Inactive Media Streams	No
Enable Special Re-invite Collision Handling	No
Enable sending '+' for E.164 numbers	No
Force sending SDP in initial Invite message	Yes
Use To Address in From Header on Outgoing Calls	No
Force Answer - send SDP in initial Invite	No
Prevent the Use of IP Address 0.0.0.0 in SDP Messages	Yes
Use P-Preferred Identity Header	No
Route Call Using To Header	No
Private SIP Trunk	Yes
Public Calling Party Number Pass-through	No
Use Diverting Party Number as Calling Party Number	No
Build Contact Using Request URI Address	No
Renegotiate SDP To Enforce Symmetric Codec	No
Repeat SDP Answer If Duplicate Offer Is Received	No
Allow Peer To Use Multiple Active M-Lines	No
User Name	
Password	
Confirm Password	
Authentication Option for Incoming Calls	No Authentication

Siemens HiPath 4000 V4.0

KCS FoIP can be integrated with Siemens HiPath 4000 using either H.323 or SIP protocol. See *Fax over IP Integration* for the exact versions required.

The most important configuration setting on HiPath is setting the protocol to native SIP or native H.323. On FoIP side, HiPath has to be connected like a standard gateway; choose the protocol and type the IP address. See the examples below.

Example Integration via H.323

This section provides an example of integration using H.3.2.3.

HiPath 4000 – Native H.323 10 B Channels

```
ADD-BUEND:314,"NATIVE H323 KOFAX ",120,0,*,2,ON,0,0,NEUTRAL;

ADD-BFDAT:33,HG3550,BCHL60&BCHL120;
CHANGE-BFDAT:CONT,33,HG3550,1,1,;
CHANGE-BFDAT:OK,33,YES;

ADD-BCSU:IPGW,1,1,14,"Q2316-X10 ",1,"0",33,,,,10,,,0;

ADD-CGWB:1,14,NORMAL,10.10.40.114,255.255.255.0,,,,,,,,,,,;
CHANGE-CGWB:CGW,1,14,GLOBIF,,,213,NO,0,10.10.40.1,,"100MBFD",0,0,30,0,4060,0.0.0.0;
CHANGE-CGWB:CGW,1,14,SERVIF,"TRM",;
CHANGE-CGWB:CGW,1,14,ASC,29100,29339,"48","184",YES,YES,YES,YES,PRIO1,G711A,NO,"30";
CHANGE-CGWB:CGW,1,14,ASC,,,,,,,,,PRIO2,G711U,NO,"30";
CHANGE-CGWB:CGW,1,14,ASC,,,,,,,,,PRIO3,NONE,NO,"30";
CHANGE-CGWB:CGW,1,14,ASC,,,,,,,,,PRIO4,NONE,NO,"20";
CHANGE-CGWB:CGW,1,14,ASC,,,,,,,,,PRIO5,NONE,NO,"20";
CHANGE-CGWB:CGW,1,14,ASC,,,,,,,,,PRIO6,NONE,NO,"20";
CHANGE-CGWB:CGW,1,14,ASC,,,,,,,,,PRIO7,NONE,NO,"20";
CHANGE-CGWB:CGW,1,14,DSP,"60";
CHANGE-
CGWB:CGW,1,14,GKDATA,,1719,"PRIMARYRASMANAGERID",,,1719,"SECONDARYRASMANAGERID",,120;
CHANGE-CGWB:CGW,1,14,MGNTDATA,,8000,,443;
CHANGE-CGWB:CGW,1,14,DMCDATA,0;
CHANGE-CGWB:CGW,1,14,WBMDATA,"HP4K-DEVEL",,ENGR;
CHANGE-CGWB:CGW,1,14,WBMDATA,"HP4K-SU",,SU;
CHANGE-CGWB:CGW,1,14,WBMDATA,"HP4K-ADMIN",,ADMIN;
CHANGE-CGWB:CGW,1,14,WBMDATA,"HP4K-READER",,READONLY;
CHANGE-CGWB:CGW,1,14,GWDATA,"PRIMARYRASMANAGERID",;
CHANGE-CGWB:CGW,1,14,H235DATA,NO,NO,"siemensGateway2003",,100,242-191-30-119-188-
83-173-161-43-0-70-36-218-74-169-221-78-102-174-170;
CHANGE-CGWB:CGW,1,14,LEGKDATA,314,888314,NO;
CHANGE-CGWB:CGW,1,14,SIPTRERH,NO,,,;
CHANGE-CGWB:CGW,1,14,SIPTRSSA,NO,0.0.0.0,5060,5061,120,0.0.0.0,5060,5061;
CHANGE-CGWB:CGW,1,14,DLSDATA,,10444,NO;
CHANGE-CGWB:CGW,1,14,JB,40,120,20,4,60,200,2;

ADD-GKREG:314,INTGW&HG3550V2&H323,,,0,0,1,,;
ADD-GKREG:114,EXTGW&HG3550V2&H323,10.10.40.115,888114,0,0,1,"NATIVE H323",TRADITIO;

ADD-COT:114,PRI&RCL&XFER&ANS&KNOR&CEOC&CEBC&CBBN&CBFN&FWDN&FNAN&BSHT&BLOC&LWNC&ATR
S&ROPT&NLCR&TSCS&ICZL&TRSC&DFNN&CFTR&CTAL&NLRD&AOCC&CDRD&MCIW&BCNE&AMFC&NTON,,;
```

```
ADD-COP:114,SDL&BR64&TIM1&IDP4,,,,;

CHANGE-COSSU:COS,100,TA&TNOTCR&TTT,,,,,,;
CHANGE-COSSU:COS,100,,NOCO&NOTIE,,,,,;
CHANGE-COSSU:COS,100,,,TA&TNOTCR&BASIC&MULTRA,,,,,;

ADD-TDCSU:NEW,1-01-014-0,114,114,0,0,100,1,1,"TRUNKING    ",0,"ECMAV2",8,,NONE,,,,G
DTR,N,TIE,NONE,N,0,,,,,,,31,MANY,,0,1,1,EMPTY,20,1,N,,,,,,16,8,1,10,,EC&G711&G729
AOPT,,314,DSC,Y,TRADITIO,HG3550IP,1&&10,Y,1,2,0,0,0,0,0,N,;
```

Note The Class Of Trunk (line ADD-COT) must not include the feature CFVA (CALL FORWARDING VALIDATION PROCEDURE POSSIBLE; German: PRZL = ERREICHBARKEITSPRUEFUNG DES UMLEITUNGSZIELES MOEGLICH). If CFVA is enabled then each activation / deactivation triggers a destination number validation check (special control call) which is not supported by KCS FoIP. As a consequence, this unsupported function may cause the following problems:

1. The call-forwarding activation may fail
2. The HiPath 4000 v4 may block any calls the used H.323 trunk for about 1 minute

Number Assignment

The chapter provides some configuration hints how to assign a range of internal telephone numbers for native H.323.

1. If you have an access code with a fixed number of digits you can use an LCR digit pattern as shown below:

```
H500:  AMO LDPLN STARTED
   +-------------------------------------------------------------+
   | CD                          --->                            |
   +-------+-------------------------------------+-------------+
   | LDPNO | LDP                                 | DIPLNUM     |
   +-------+-------------------------------------+-------------+
   …
   |   34  | 73-XXXX                             |    0        |
```

   - This configuration expects 4 digits (represented by X's) after 73 which means that the number range is between 730000 and 739999. "34" is an internal LCR dialing plan number used the native H.323 trunk. The actual used number is installation specific.

2. Sample using closed numbering where numbers from 1120 to 1169 are routed to FoIPv3

```
ADD-RICHT:CD,114,114,,,0,ALL,"N H323
 ",,,314,,,,114,,,,,,1-1-114,YES,,1-1-114,NEUTRAL,NO,NO,;
ADD-LODR:7,,,,NPI,UNKNOWN,UNKNOWN;
ADD-LODR:7,,,,ECHO,1;
ADD-LODR:7,,,,END;
ADD-LODR:7,,,"7-CLOSED NUMBERING",;
ADD-LDAT:114,ALL,1,,314,7,1,,1,EMPTY,NONE,,4,,,,,,,,114-0,,,,;
ADD-WABE:1120&&1169,,,STN,N,,,,,114;
```

   - ADD-WABE defines the destination for the extensions
   - ADD-RICHT makes the relation of this destination to the trunk that has to be used.

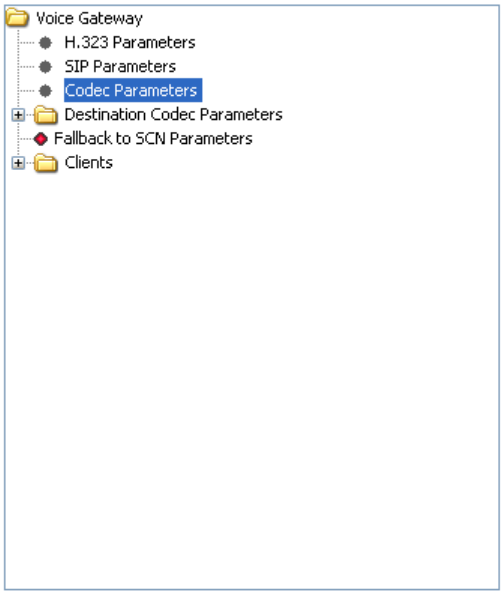
3. Sample using open numbering where numbers starting with 8 are routed to FoIPv3

```
ADD-WABE:8,,,TIE,N;
ADD-RICHT:LRTENEW,8,ALL,"N H323
 ",314,1-1-114,YES,,FIX,,,PP300,NO,,,,NO,NO,,1-1-114,NEUTRAL,NO,NO,NO,NO,NO,NO,NO;
ADD-LODR:8,,,,NPI,UNKNOWN,UNKNOWN;
ADD-LODR:8,,,,ECHO,1;
```

```
ADD-LODR:8,,,,ECHO,2;
ADD-LODR:8,,,,END;
ADD-LODR:8,,,"8-OPEN NUMBERING",;
ADD-LDAT:8,ALL,1,,314,8,1,,1,EMPTY,NONE,,4,,,,,,,,114-0,,,,;
ADD-LDPLN:LCRPATT,0,"8"-"Z",,8,,,1;
```

- The 8 in ADD-WABE is the access code or prefix
- The “8”-“Z” in ADD-LDPLN is the dialing rule with time out. Here parameter BLOC must be set in the used COT (Class of trunk) is important.

HiPath 4000 – Codec Parameters



Codec Parameters

Codec	Priority	Voice Activity Detection	Frame Size
G.711 A-law	Priority 1	Off	30 msec
G.711 µ-law	Priority 2	Off	30 msec
G.723	not used	Off	30 msec
G.729	not used	Off	20 msec
G.729A	not used	Off	20 msec
G.729B	not used	On	20 msec
G.729AB	not used	On	20 msec

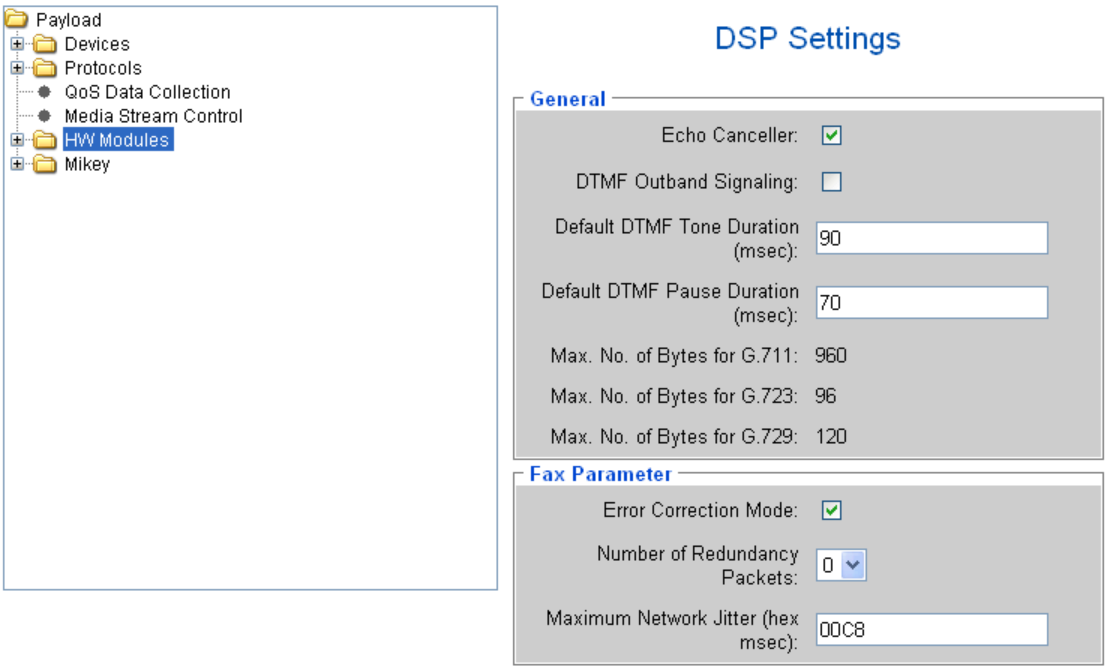
T.38 Fax

T.38 Fax:	On
Use FillBitRemoval:	On
Max. UDP Datagram Size for T.38 Fax (bytes):	1472
Error Correction Used for T.38 Fax (UDP) :	t38UDPRedundancy

Misc.

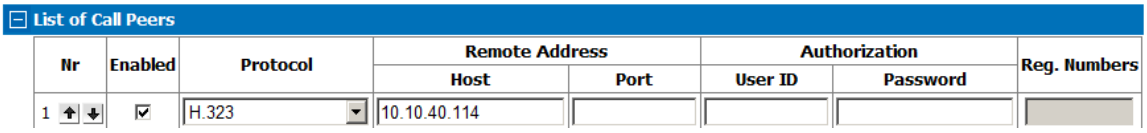
ClearChannel:	On	Frame Size:	20 msec
Transmission of Fax/Modem Tones according to RFC2833:	On		
Transmission of DTMF Tones according to RFC2833:	On		
Redundant Transmission of RFC2833 Tones according to RFC2198:	On		

HiPath 4000 – DSP Settings



KCS FoIP Configuration

The connection to HiPath 4000 has to be configured like a standard H.323 Gateway. No user authorization or number registration is required. A typical screen shot is shown below:



Example Integration via SIP

This section provides an example of integration using SIP.

HiPath 4000 – Native SIP (30 Channels)

```
ADD-BUEND:313,"NATIVE SIP TRUNK ",120 ,0 ,* ,2 ,ON ,0 ,0 ,NEUTRAL;
  ADD-BFDAT:3,HG3550,BCHL60&BCHL120;
  CHANGE-BFDAT:CONT,3,HG3550,2,3,;
  CHANGE-BFDAT:OK,3,YES;
  ADD-BCSU:IPGW,1,1,13,"Q2316-X ",1,"0",3,,,,60,,,0;
  ADD-CGWB:1,13,NORMAL,10.10.40.18,255.255.255.0,,,,,,,,,,,;
  CHANGE-CGWB:CGW,1,13,GLOBIF,,,213,NO,0,10.10.40.1,,"100MBFD",30,0,0,0,4060,0.0.0.0;
  CHANGE-CGWB:CGW,1,13,SERVIF,"TRM",;
  CHANGE-CGWB:CGW,1,13,ASC,29100,29219,"184","104",YES,YES,YES,YES,PRIO1,G711A,NO,"30";
  CHANGE-CGWB:CGW,1,13,ASC,,,,,,,,,PRIO2,G711U,NO,"30";
  CHANGE-CGWB:CGW,1,13,ASC,,,,,,,,,PRIO3,NONE,NO,"30";
  CHANGE-CGWB:CGW,1,13,ASC,,,,,,,,,PRIO4,NONE,NO,"20";
```

```
  CHANGE-CGWB:CGW,1,13,ASC,,,,,,,,PRIO5,NONE,NO,"20";
  CHANGE-CGWB:CGW,1,13,ASC,,,,,,,,PRIO6,NONE,NO,"20";
  CHANGE-CGWB:CGW,1,13,ASC,,,,,,,,PRIO7,NONE,NO,"20";
  CHANGE-CGWB:CGW,1,13,DSP,"60";
  CHANGE-
CGWB:CGW,1,13,GKDATA,,1719,"PRIMARYRASMANAGERID",,,1719,"SECONDARYRASMANAGERID",,120;
  CHANGE-CGWB:CGW,1,13,DMCDATA,0;
  CHANGE-CGWB:CGW,1,13,WBMDATA,"HP4K-DEVEL",,ENGR;
  CHANGE-CGWB:CGW,1,13,WBMDATA,"HP4K-SU",,SU;
  CHANGE-CGWB:CGW,1,13,WBMDATA,"HP4K-ADMIN",,ADMIN;
  CHANGE-CGWB:CGW,1,13,WBMDATA,"HP4K-READER",,READONLY;
  CHANGE-CGWB:CGW,1,13,GWDATA,"PRIMARYRASMANAGERID",;
  CHANGE-CGWB:CGW,1,13,H235DATA,NO,NO,"siemensGateway2003",,100,242-191-30-119-188-
  83-173-161-43-0-70-36-218-74-169-221-78-102-174-170;
  CHANGE-CGWB:CGW,1,13,LEGKDATA,10,888010,NO;
  CHANGE-CGWB:CGW,1,13,SIPTRERH,NO,,,;
  CHANGE-CGWB:CGW,1,13,SIPTRSSA,NO,0.0.0.0,5060,5061,120,0.0.0.0,5060,5061;
  CHANGE-CGWB:CGW,1,13,DLSDATA,,10444,NO;
  CHANGE-CGWB:CGW,1,13,JB,40,120,20,4,60,200,2;
  ADD-GKREG:10,INTGW&REGGW&HG3550V2&SIP,,,0,0,1,,;
  ADD-GKREG:114,EXTGW&HG3550V2&SIP,10.10.40.152,888158,0,0,1,,TRADITIO;
  ADD-COT:113,PRI&RCL&ANS&CEBC&FWDN&BSHT&BLOC&ATRS&TSCS&TRSC&CTLS&HGTR&NTON,,;
  ADD-COP:113,,TA,TA,,;
  CHANGE-COSSU:COS,100,TA&TNOTCR&TTT,,,,,,,;
  CHANGE-COSSU:COS,100,,NOCO&NOTIE,,,,,,;
  CHANGE-COSSU:COS,100,,,TA&TNOTCR&BASIC&MULTRA,,,,,;
  ADD-TDCSU:NEW,1-01-013-0,113,113,0,0,100,7,7,"N SIP
  ",113,"ECMAV2",8,,NONE,
  ,,,GDTR,N,TIE,NONE,N,0,,,,,,,10,MANY,1-1-113,0,10,1,EMPTY,113,10,N,,,,,16,8,1,10
  ,,EC&G711&G729AOPT,,313,DSC,Y,TRADITIO,HG3550IP,1&&30,N,1,2,0,0,0,0,0,N,;
```

For codec and DSP configuration, see *Number Assignment* and *HiPath 4000 – DSP Settings*.

Number Assignment

The chapter shows two example configurations how to assign an internal telephone number

1. Sample using closed numbering where number from 1120 to 1169 are routed to FoIPv3

```
ADD-RICHT:CD,113,113,,,0,ALL,"N SIP
 ",,,314,,,,113,,,,,,1-1-113,YES,,1-1-113,NEUTRAL,NO,NO,;
ADD-LODR:7,,,,NPI,UNKNOWN,UNKNOWN;
ADD-LODR:7,,,,ECHO,1;
ADD-LODR:7,,,,END;
ADD-LODR:7,,,"7-CLOSED NUMBERING",;
ADD-LDAT:114,ALL,1,,314,7,1,,1,EMPTY,NONE,,4,,,,,,,,114-0,,,,;
ADD-WABE:1120&&1169,,,STN,N,,,,,113;
```

   - ADD-WABE defines the destination for the extensions
   - ADD-RICHT makes the relation of this destination to the trunk that has to be used.

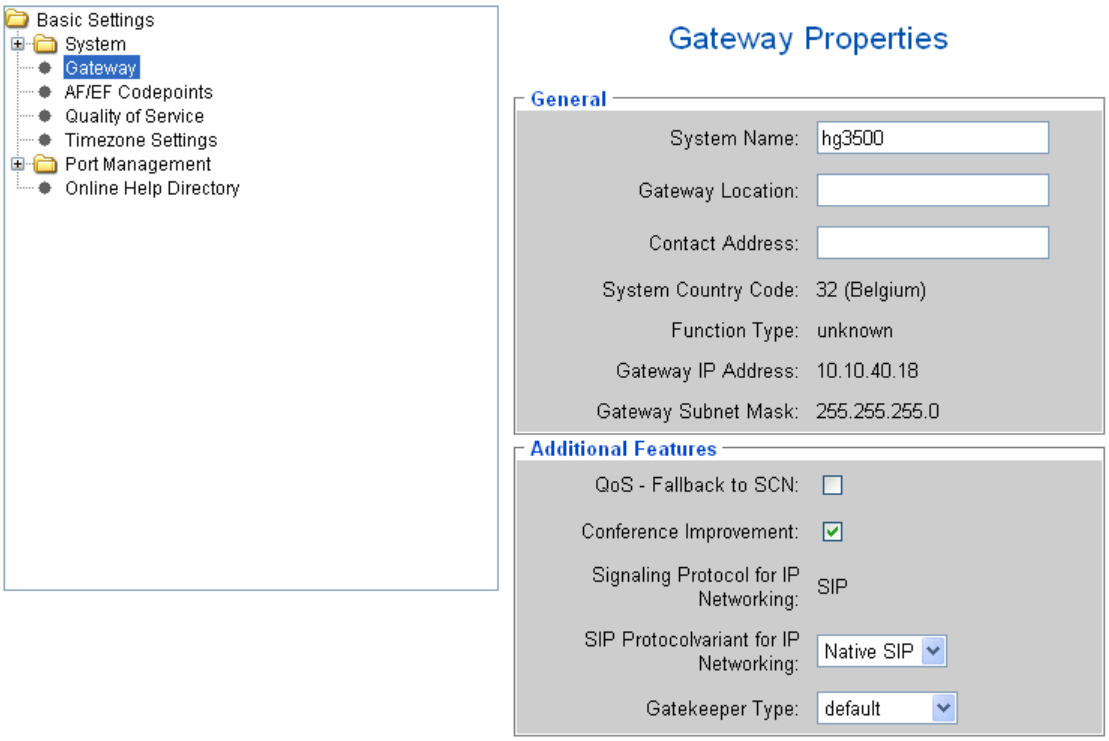
2. Sample using open numbering where number starting with 8 are routed to FoIPv3

```
ADD-WABE:8,,,TIE,N;
ADD-RICHT:LRTENEW,8,ALL,"N SIP
 ",314,1-1-113,YES,,FIX,,,PP300,NO,,,,NO,NO,,1-1-113,NEUTRAL,NO,NO,NO,NO,NO,NO,NO;
ADD-LODR:8,,,,NPI,UNKNOWN,UNKNOWN;
ADD-LODR:8,,,,ECHO,1;
ADD-LODR:8,,,,ECHO,2;
ADD-LODR:8,,,,END;
ADD-LODR:8,,,"8-OPEN NUMBERING",;
ADD-LDAT:8,ALL,1,,314,8,1,,1,EMPTY,NONE,,4,,,,,,,,113-0,,,,;
```

```
ADD-LDPLN:LCRPATT,0,"8"-"Z",,8,,,1;
```

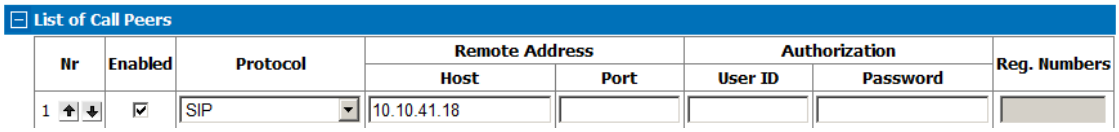
- The 8 in ADD-WABE is the access code or prefix
- The “8”-“Z” in ADD-LDPLN is the dialling rule with time out. Here the COT parameter BLOC is important.

HiPath 4000 – Gateway Properties



KCS FoIP Configuration

The connection to HiPath 4000 has to be configured like a standard SIP Gateway. No user authorization or number registration is required. A typical screen shot is shown below:



Siemens HiPath 4000 V6.0

KCS FoIP can be integrated with Siemens HiPath 4000 V6.0 using either H.323 or SIP protocol, both interconnection types were certified in the Siemens certification lab. See *Fax over IP Integration* for the exact versions required.

The detailed test report of the certification including the configuration description for both KCS FoIP and Siemens Hipath4000 V6.0 as well is available for Siemens technicians in the Siemens intranet.

Siemens OpenScape Voice V3.1 R2

KCS FoIP can be integrated with Siemens OpenScape Voice V3.1 R2 (formerly known as HiPath 8000) using SIP protocol. See Fax over IP Integration for the exact versions required.

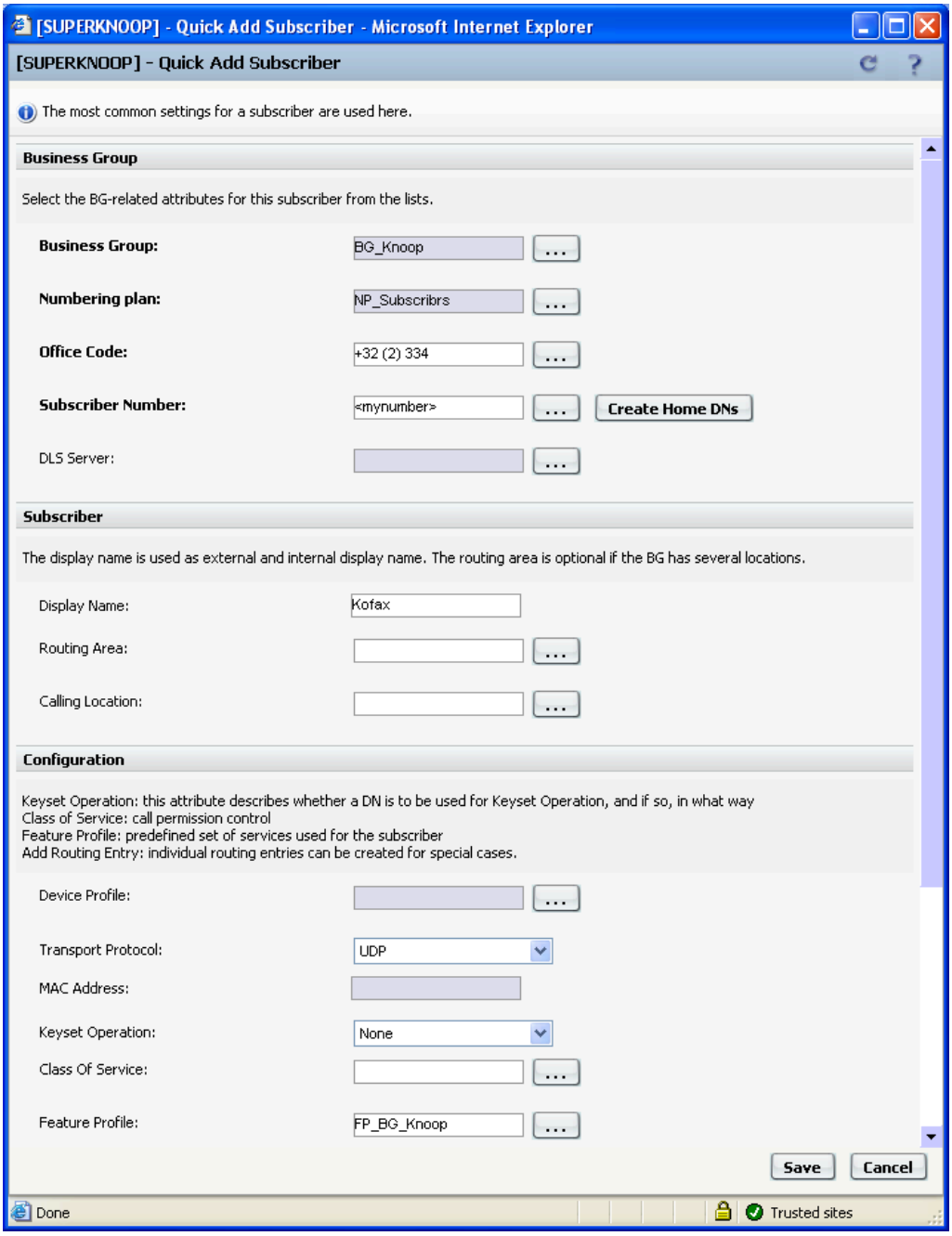
OpenScape Voice can integrate with FoIP in two ways, as a subscriber (BGL) or as an endpoint profile (EPP). Configuration as a subscriber is simpler. Configuration as an endpoint is recommended.

On FoIP side, OpenScape Voice has to be connected like a standard gateway; choose the “SIP with registration” protocol, type the IP address and type a number in the Reg. Numbers field. See the examples below.

Configuration as Subscriber

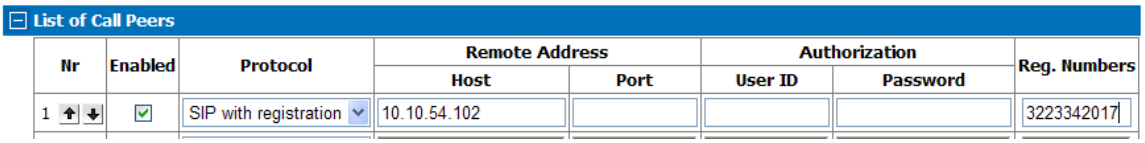
1. In OpenScape Voice, create a subscriber as you would do for a SIP phone. Kofax FoIP is able to register dynamically on the subscriber number you just created.

2. In the feature profile, enable all appropriate features such as Call Transfer; Music on Hold, and Name Delivery options.



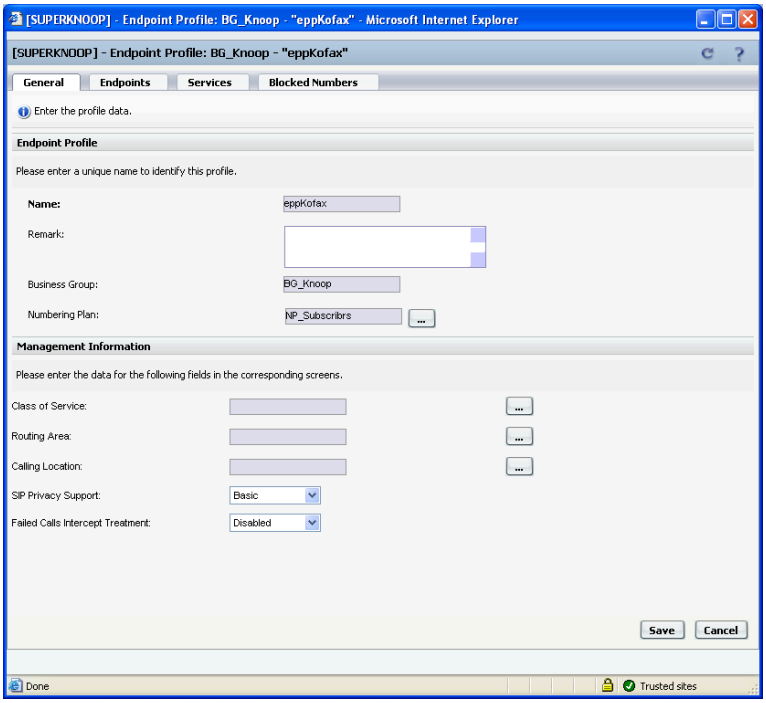
3. In the KCS FoIP configuration tool, configure a call-peer to the following values:
   a. Set the Protocol to “SIP with registration”
   b. Set the Remote Address\Host to HiPath 8000 IP. (Default port is 5060)
   c. Set the Reg. Numbers to the subscriber number assigned for KCS FoIP.

An example configuration is shown below:

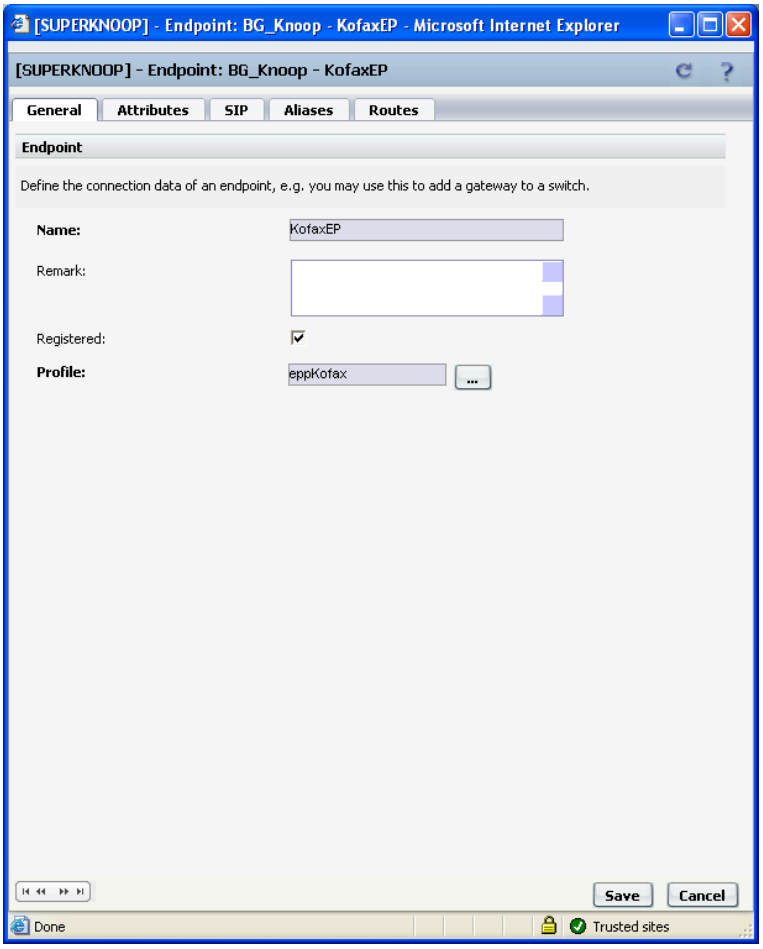


Configuration as Endpoint

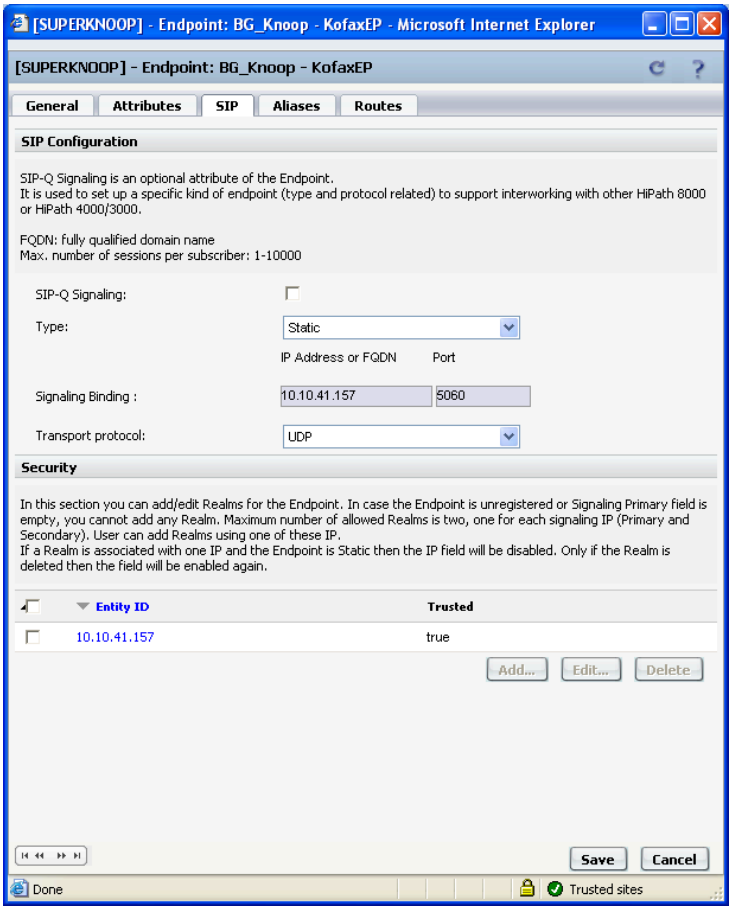
1. In the OpenScape Voice:
   First create an endpoint profile (EPP). Select the Call Transfer feature as well as Name delivery, etc.



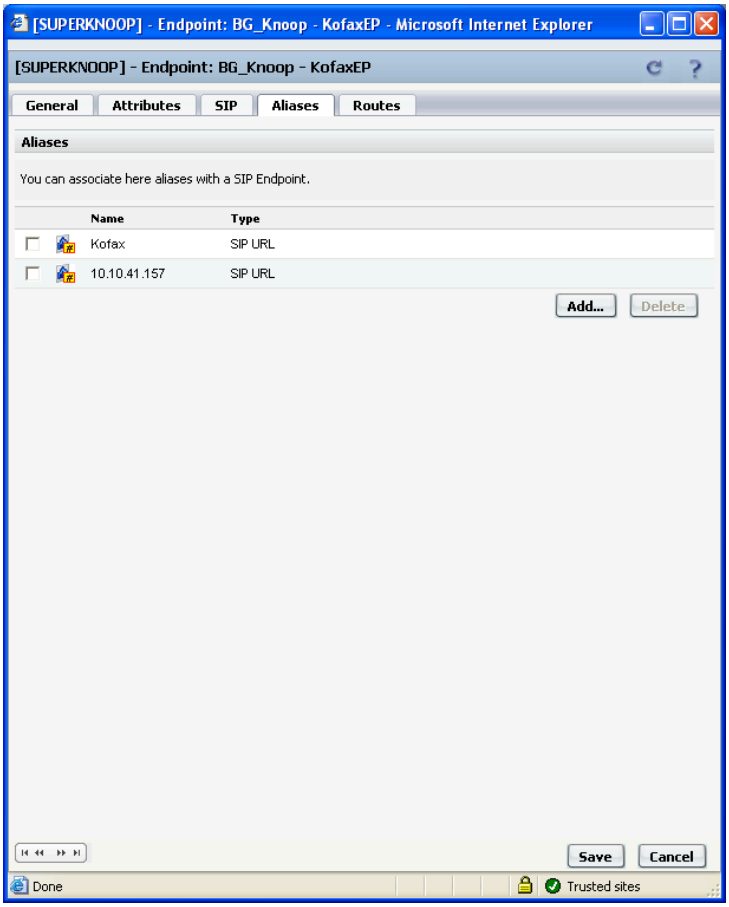
2. Create an Endpoint and assign the EPP to it. In the tab Attributes nothing needs to be selected.



3. Go to the SIP tab and choose your registration type. Kofax supports both dynamic and static registration.

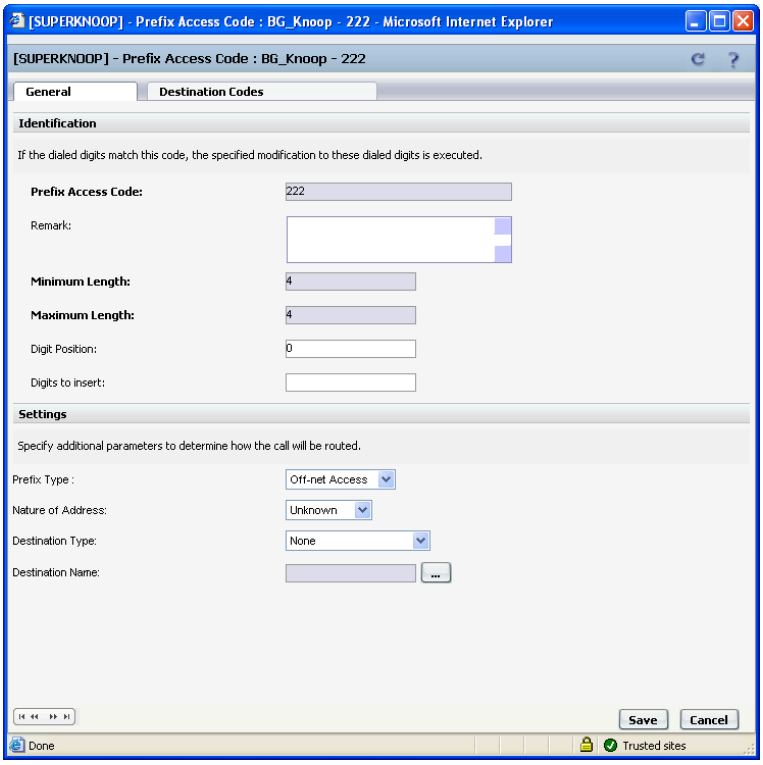


4. It is also important to add one or more aliases, from which at least one is the IP address or DNS record the endpoint is operating under.

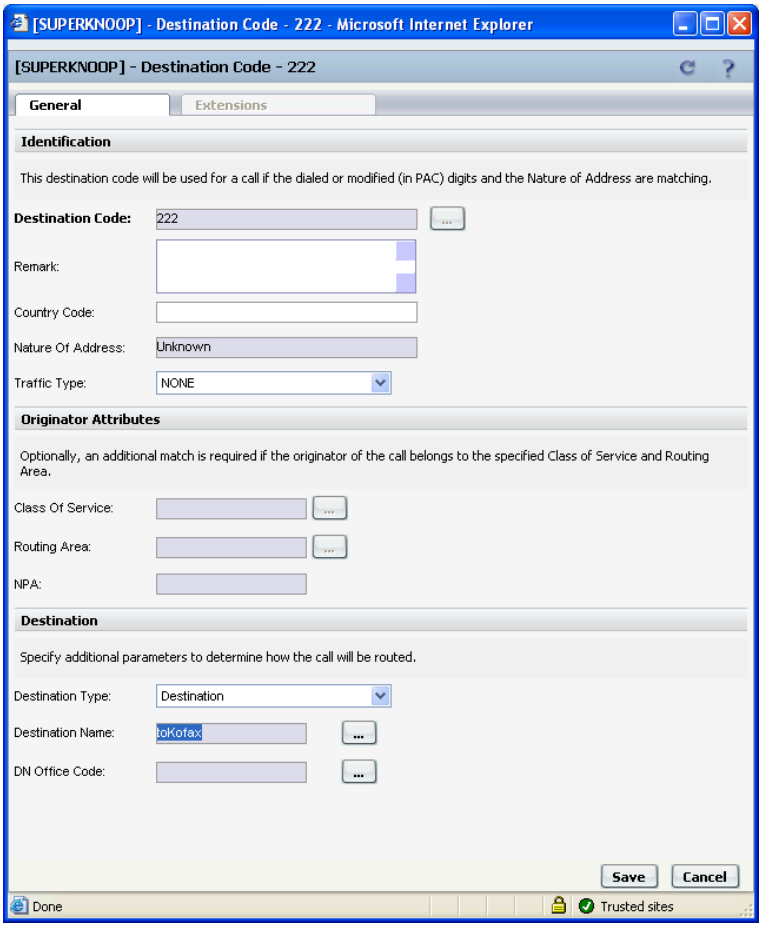


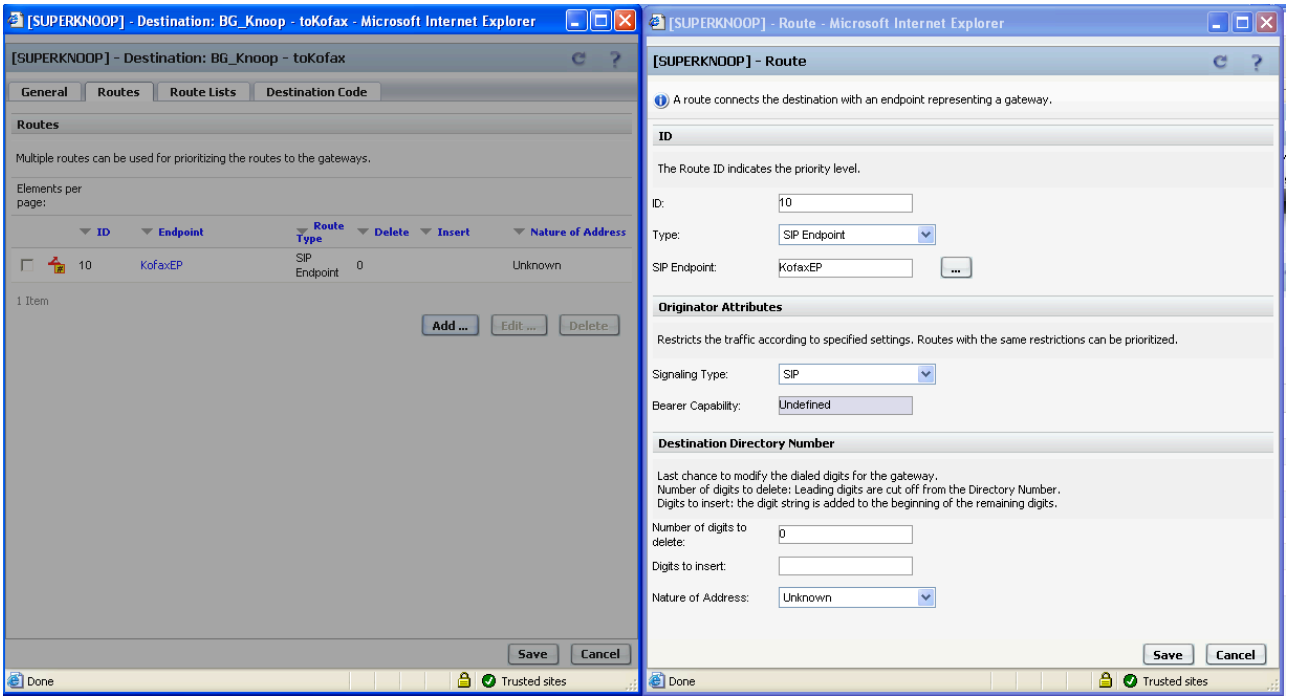
The endpoint has now been set up. The next step is creating an empty destination (under Destinations and Routes). Simply call it “toKofax” and click Save. We will fill in the details later on. Now we can start creating a prefix access code.

5. Create a prefix access code to route all numbers starting with “222” to the KCS FoIP.



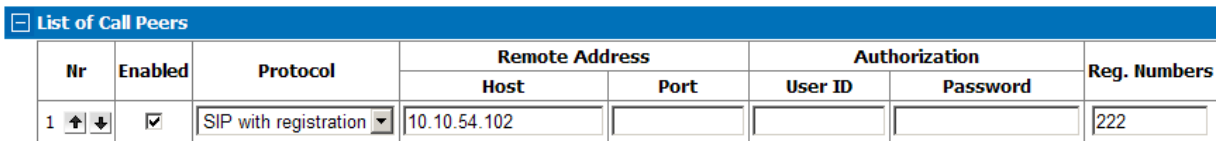
6. Create a Destination Code “222” which points to the Kofax destination we created earlier.





7. Open the destination and add a new route that points to the correct endpoint. Click **Save** to remember the configuration.
8. In the KCS FoIP configuration tool, configure a call-peer to the following values:
   a. Set Protocol to “SIP with registration”
   b. Set Remote Address\Host to HiPath 8000 IP. (Default port is 5060)
   c. Set Reg. Numbers to any non-empty number.

An example configuration is shown below:



Inbound Failover

If you want to support inbound failover (inbound calls may be handled by multiple instances of FoIP), you have to bundle multiple IP-trunks. Please contact your Siemens specialist for more details.

Siemens OpenScape Voice V4

KCS FoIP can be integrated with Siemens OSV V4.0 using either H.323 or SIP protocol, both interconnection types were certified in the Siemens certification lab. See *Fax over IP Integration* for the exact versions required.

The detailed test report of the certification including the configuration description for both KCS FoIP and Siemens OSV V4.0 as well is available for Siemens technicians in the Siemens intranet.

Siemens OpenScape Voice V6

KCS FoIP can be integrated with Siemens OSV V6.0 using SIP protocol, both interconnection types were certified in the Siemens certification lab. See *Fax over IP Integration* for the exact versions required.

The detailed test report of the certification including the configuration description for both KCS FoIP and Siemens OSV V6.0 as well is available for Siemens technicians in the Siemens intranet.

Siemens OpenScape Voice V7

KCS FoIP can be integrated with Siemens OSV V7.0 using SIP or SIP/TLS/SRTP protocol, all three interconnection types were certified in the Siemens certification lab. See *Fax over IP Integration* for the exact versions required.

The detailed test report of the certification including the configuration description for both KCS FoIP and Siemens OSV V7.0 as well is available for Siemens technicians in the Siemens intranet.

Siemens OpenScape Voice V8

KCS FoIP can be integrated with Siemens OSV V8.0 using SIP or SIP/TLS/SRTP protocols, all three interconnection types were certified in the Siemens certification lab. See *Fax over IP Integration* for the exact versions required.

The detailed test report of the certification including the configuration description for both KCS FoIP and Siemens OSV V8.0 as well is available for Siemens technicians in the Siemens intranet.

The summary of all Siemens certifications can be found here:

http://partnerdialog.unify.com/portal/tecpartner/node/5&char=K&partnerid=270#

Avaya Aura Communication Manager 5.2.1

KCS FoIP 3.12.07 or later can be integrated with Avaya Aura Communication Manager (CM) using either SIP or H.323 protocol. See Fax over IP Integration for the exact versions required.

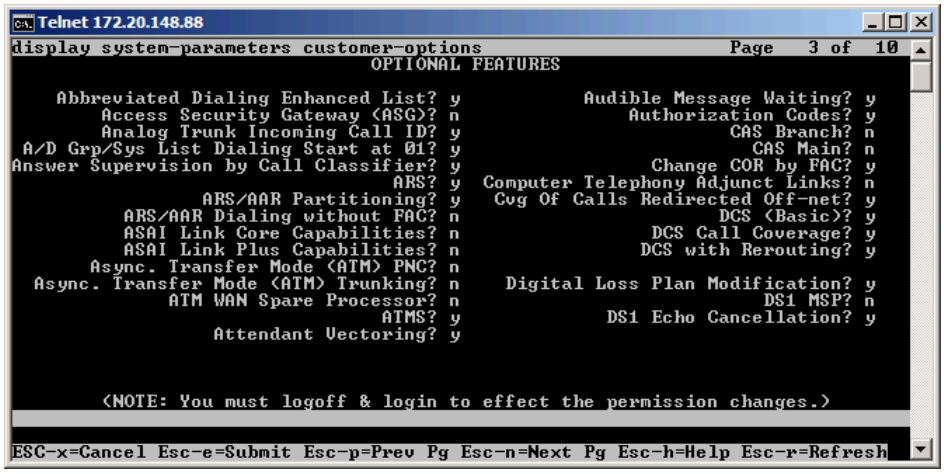
When using the H.323 integration, KCS FoIP communicates directly with Avaya CM via H.323 trunks. On the other hand, in the case of the SIP integration another component referred to as SIP Enablement Services (SES) is necessary on the Avaya side. Then KCS FoIP talks via SIP with the SES, and SES communicates via dedicated SIP trunk (using TCP/tls transport only) with the Avaya CM.

This chapter describes an example of a simple Avaya CM/SES installation with the following dialplan/routing, including one ISDN BRI trunk towards another test PBX (Siemens Hicom300), one H.323 and SIP trunk towards KCS FoIP solution:

- There are a few telephones (stations) in the range 58xxx (such as 58410, 58411, 58412)
- Numbers starting with leading 0 are dialed to the ISDN BRI line (trunk group 1)
- Numbers starting with 7xxx are routed to the trunk group 13 (H.323 trunk)
- Numbers starting with 8xxx are routed to the trunk group 29 (SIP trunk)
- The routing is performed by the Automatic Route Selection (ARS) system which is triggered by the feature access code (FAC) 9

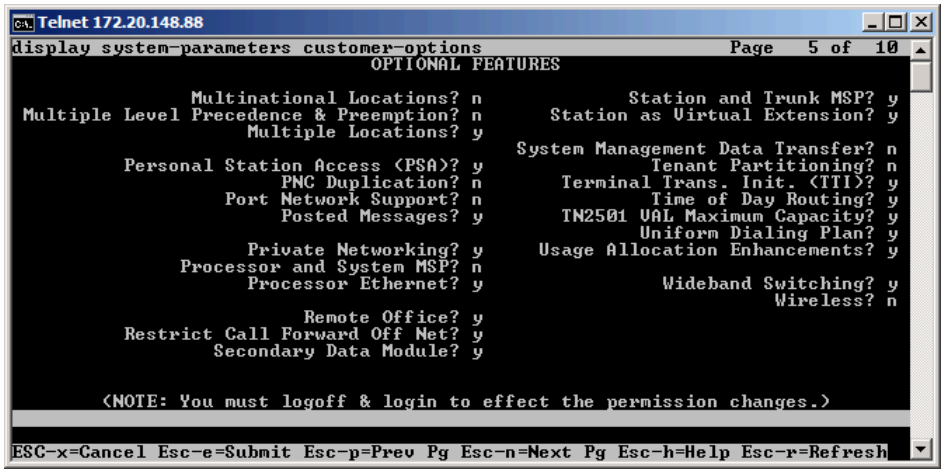
With the Avaya CM systems, it is a common practice to perform routing by the means of ARS or AAR features, and the usage for one of them is usually triggered by dialing the configured FAC code, typically 9.

Note that ARS/AAR dialing without the FAC option is available in the “system-parameters customer-options”, page 3, but by default it is switched off and it can only be enabled by Avaya:



AAR is often used for internal dialing, typically used for routing calls between private "TIE Trunks", while ARS is used for routing calls to the PSTN. Most businesses use the “9” as the FAC to access the ARS dial plan.

Uniform dialing plan



This is why you can assign one "Dialed Access Code (DAC)" for AAR and one for ARS. Most use 9 for ARS.

This FAC code can be then inserted automatically in the trunk groups, but with our example we assume to always explicitly dial the 9 in order to route the call to any of the configured trunks, and without 9 to dial any of the local extensions. For example:

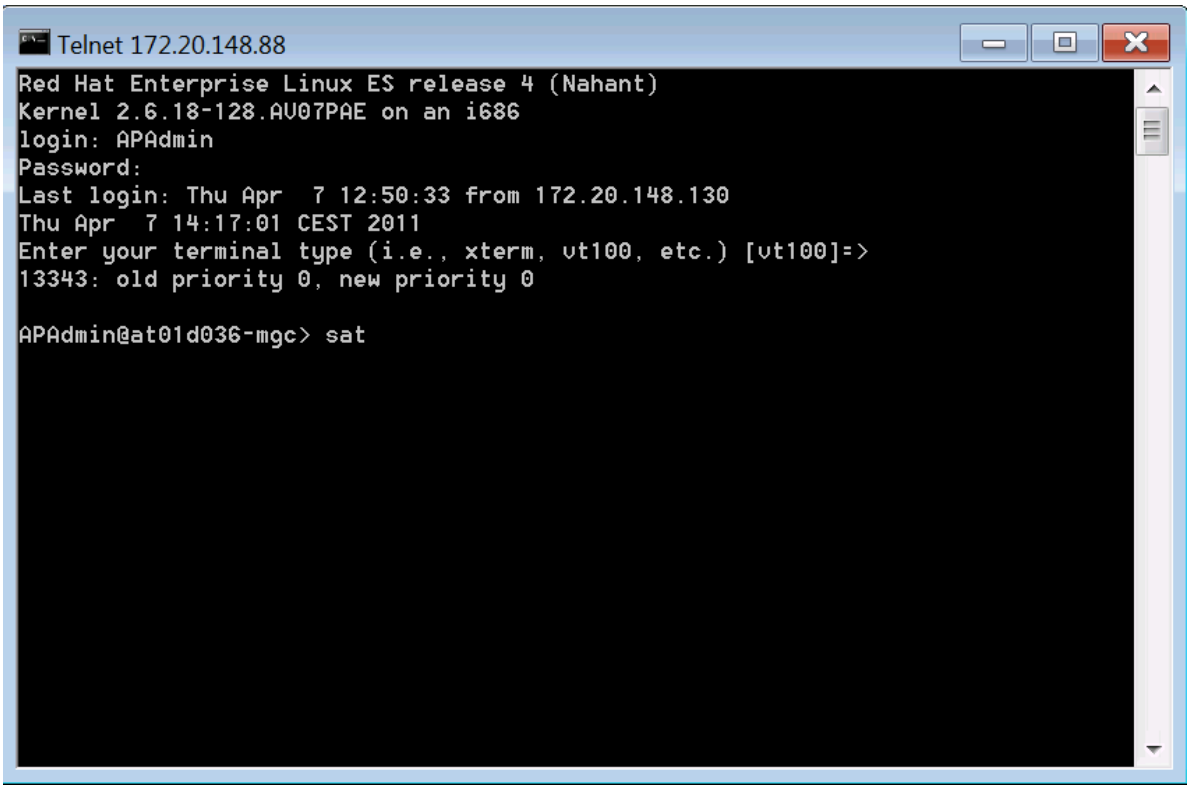
- dial 901234567 to go out to the trunk 1 => ISDN BRI line
- dial 989123 to go out to the trunk 29 => SIP trunk towards KCS FoIP

Avaya Aura CM General Configuration

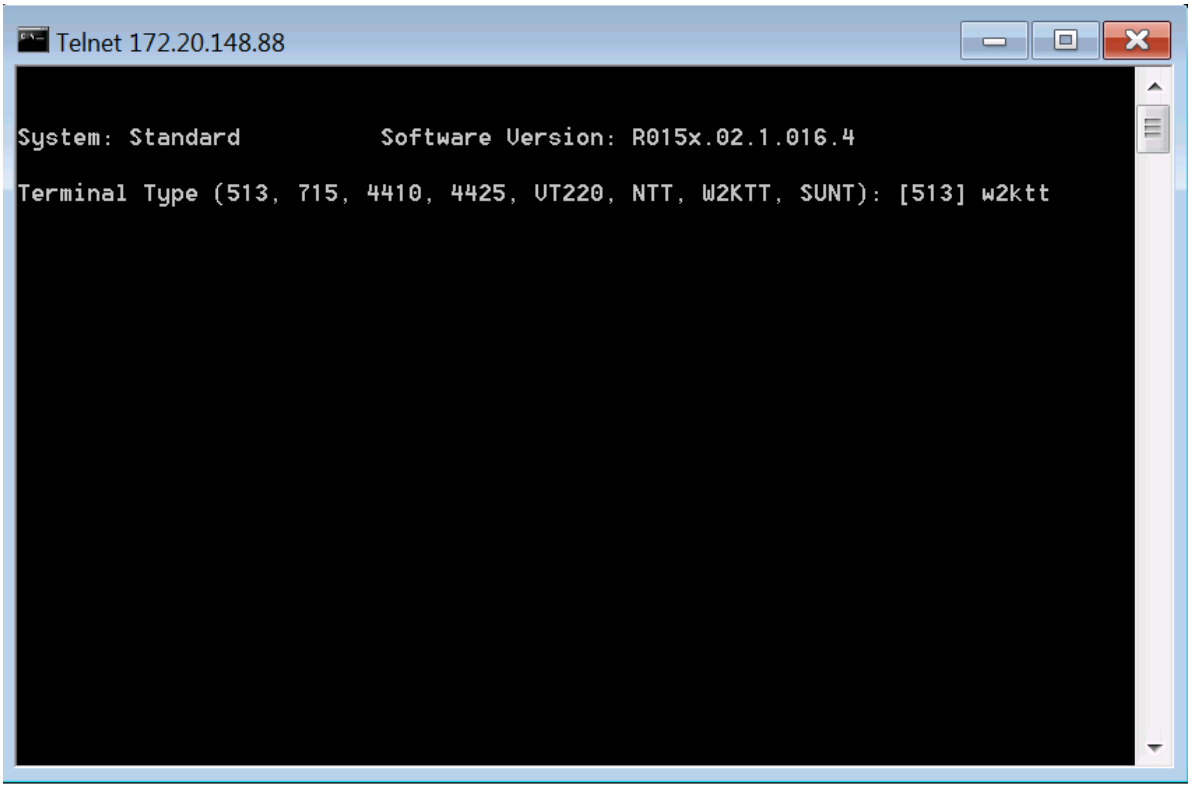
Avaya CM is being configured using so called System Access Terminal (SAT) which can be used with the telnet client connected to the CM server.

1. Start the telnet session with the CM server, authenticate with the system user and start the sat command:

```
telnet 172.20.148.88 <Enter>
```



2. Choose w2ktt terminal type.



There are four general commands that can be used for the following purposes:

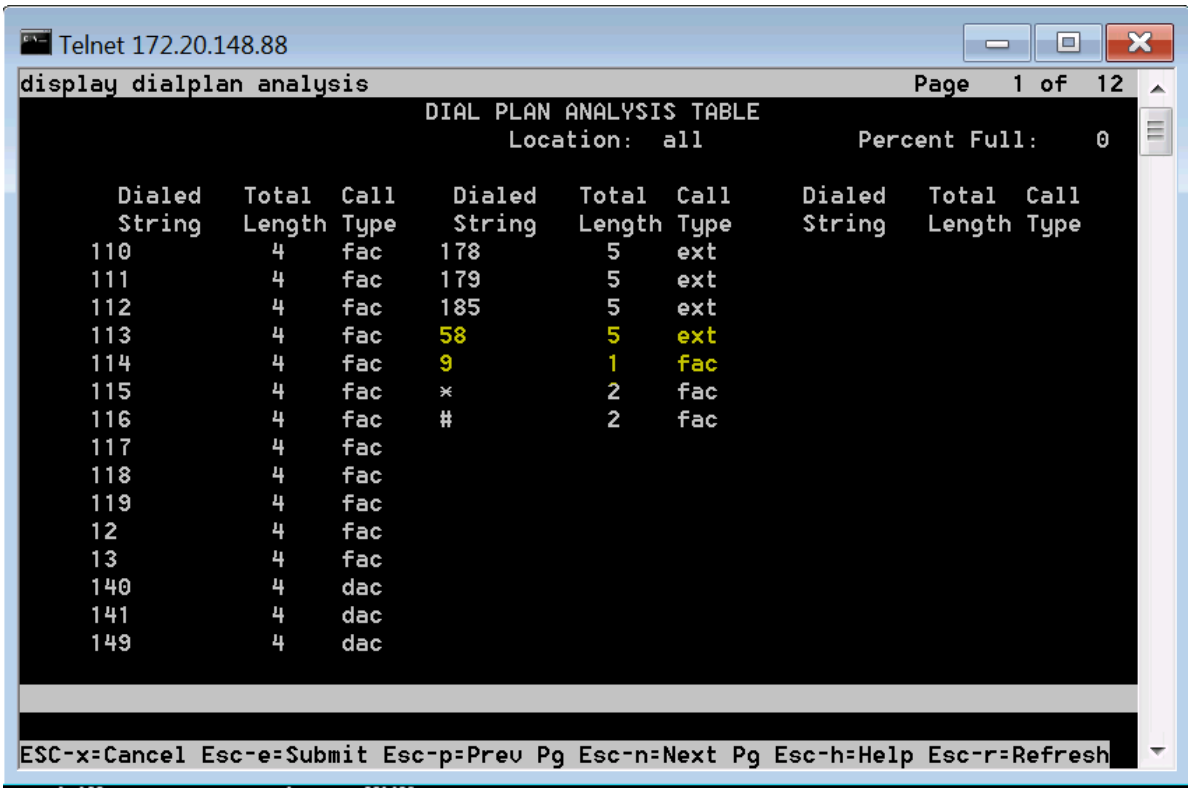
- **Add**: To add new objects such as trunk group, signaling group and more.
- **Change**: To change parameters of an existing object.
- **Display**: To show parameters of an existing object.
- **List**: To show a list of objects of the same class, such as trunks.

Usually, the configuration of particular object consists of several pages. In order to scroll through them press **ESC-n** for the next page and **ESC-p** for the previous page.

In order to cancel a command, press **ESC-x**. To execute (in the case of making changes), press **ESC-e**.

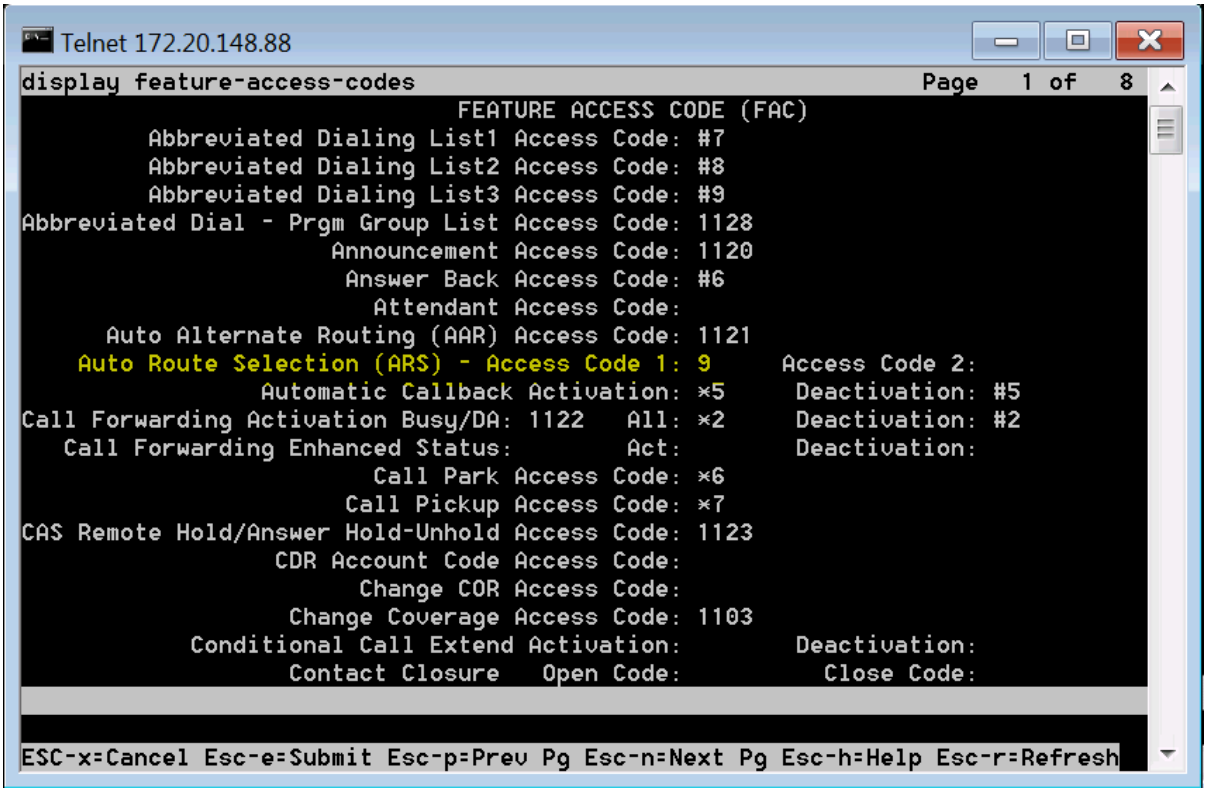
3. Execute command "`display dialplan analysis`".

Note In this example digit "9" is being used as Feature Access Code (FAC) and number range "58XXX" are extensions (telephones).

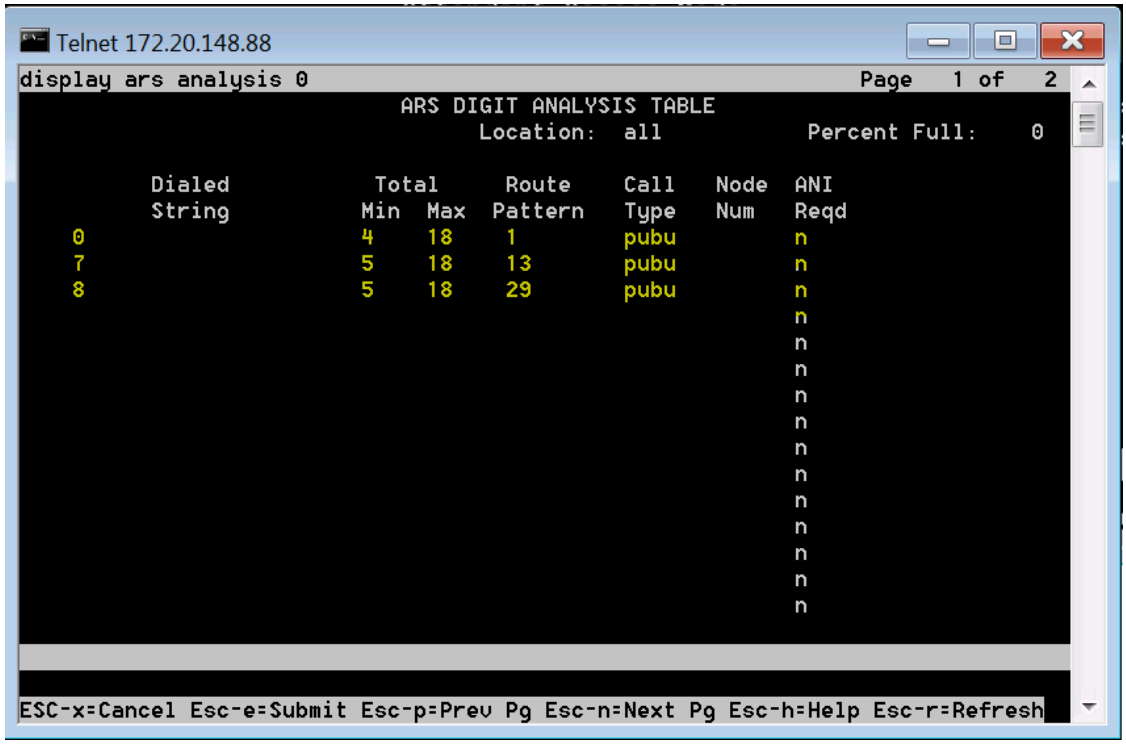


4. Execute command "`display feature-access-codes`".

Note The digit "9" triggers the Automatic Route Selection (ARS) feature which in the fact performs to call routing in the CM (alternatively, also the similar feature Automatic Alternate Routing (AAR) could be used).



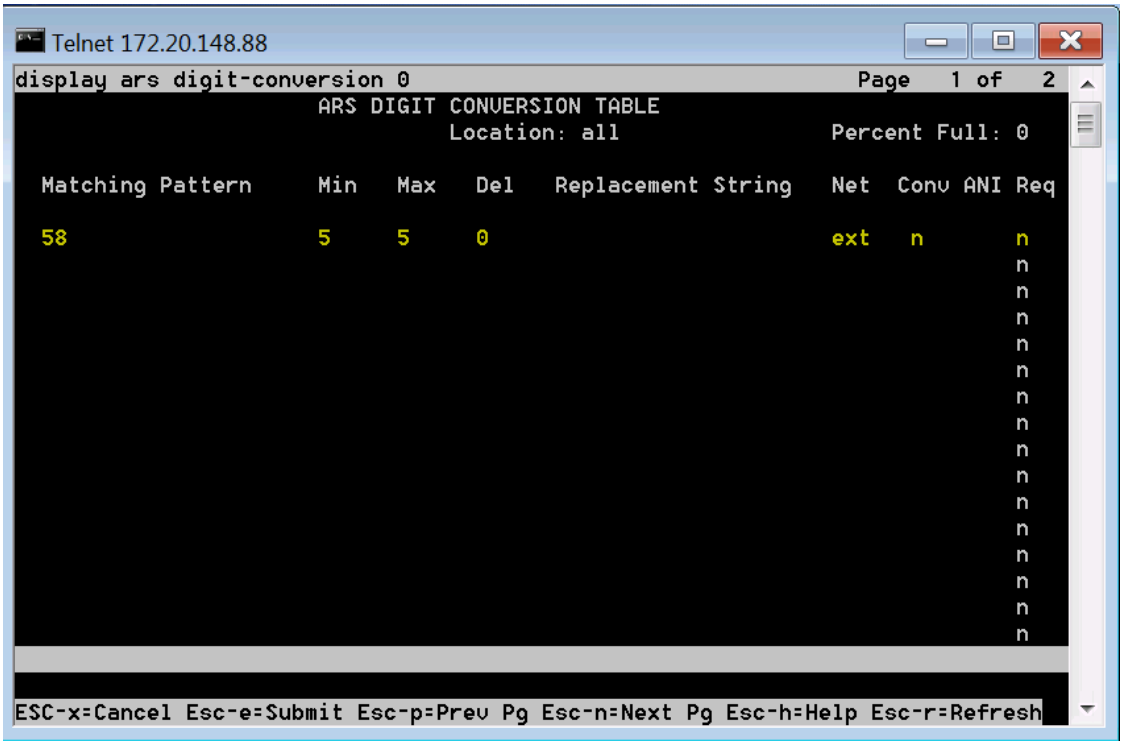
5. Execute command “`display ars analysis`”.



This means the following:

- All dialed numbers starting with 0, min. length 4 and max. length18, are routed further through route pattern 1.
- All dialed numbers starting with 7, min/max. length 5/18 are routed further through route pattern 13.
- All dialed numbers starting with 8, min/max. length 5/18 are routed further through route pattern 29.

6. Execute command "`display ars digit-conversion 0`".

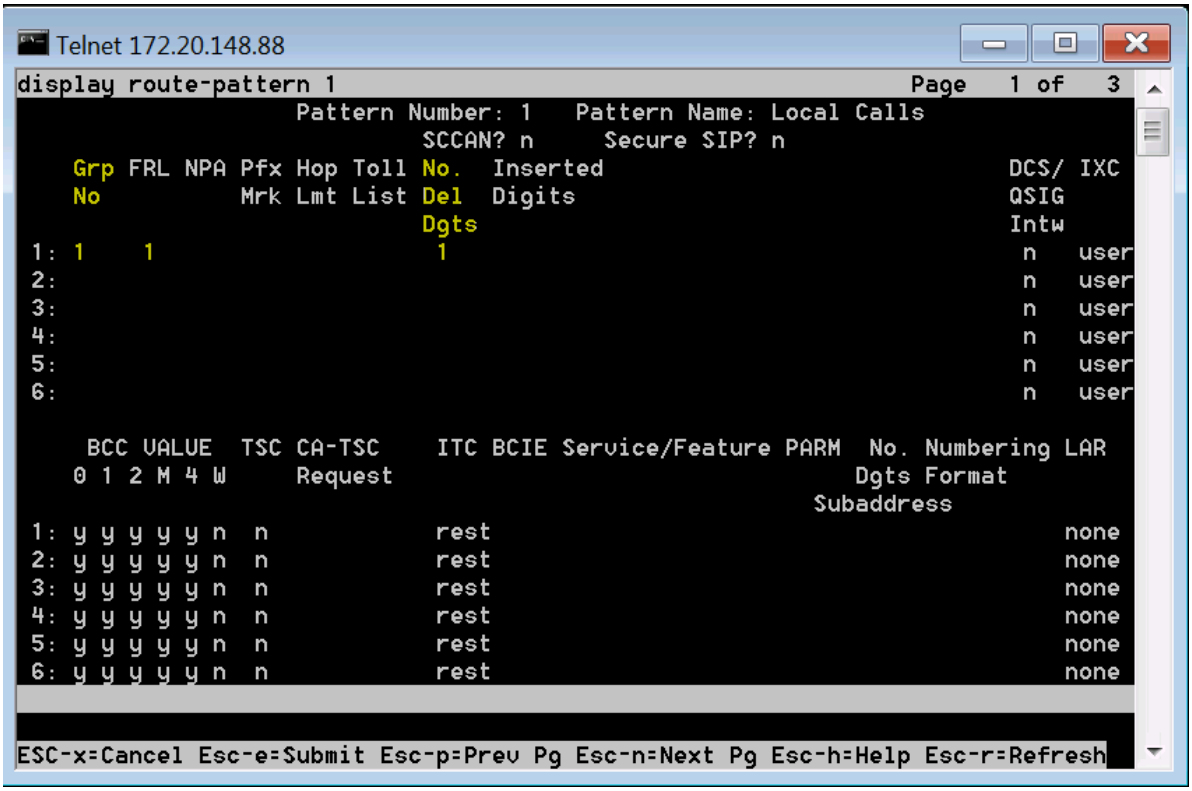


This screen gives a possibility to perform some digit conversions after the dialed number has triggered the ARS:

In this example, if we dial 958411, the number 58xxx is recognized as extension/station number, and the 9 is automatically dropped from the number.

Note The Avaya phones often automatically insert the FAC codes to the dialed number and the users do not need to dial them explicitly. In that case, this entry would handle the local extension range 58xxx correspondingly.

7. Execute command "`display route-pattern 1`".

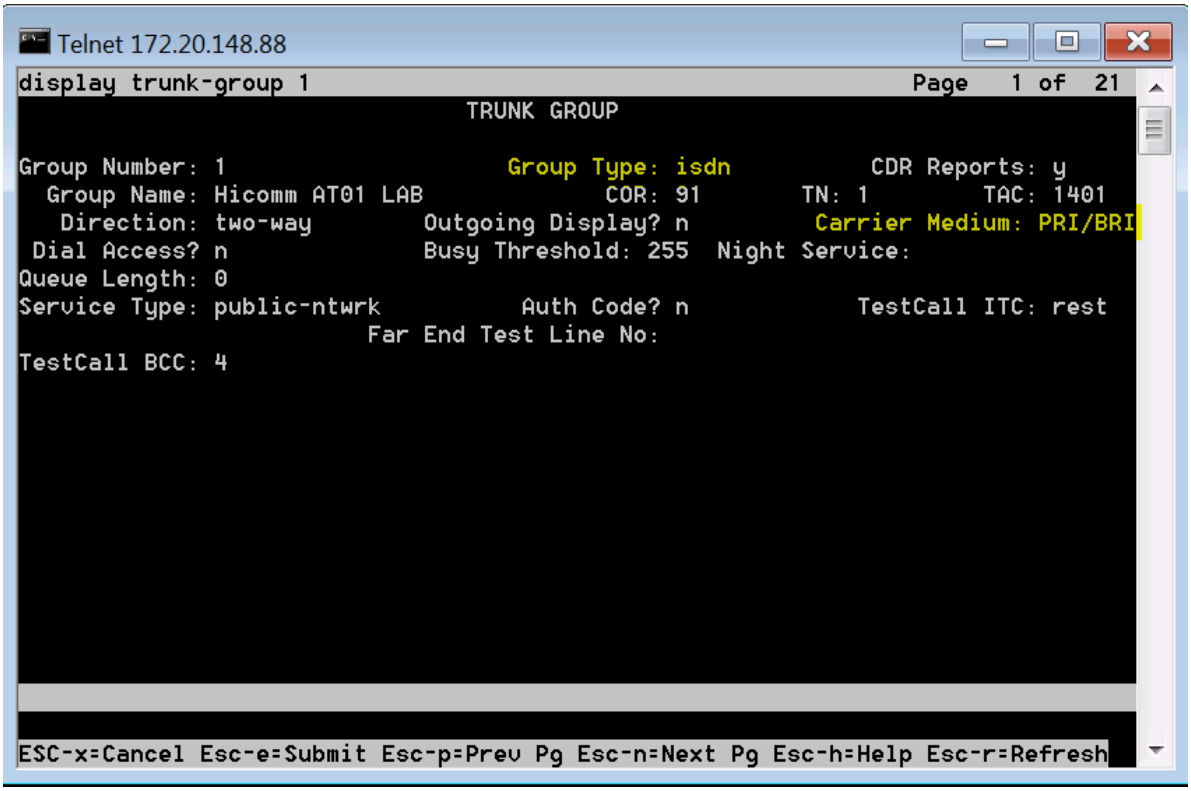


See that the route pattern points to the trunk group number 1 (Grp No) and prior to dialing the number further into the trunk group 1, (the first) digit is removed at first.

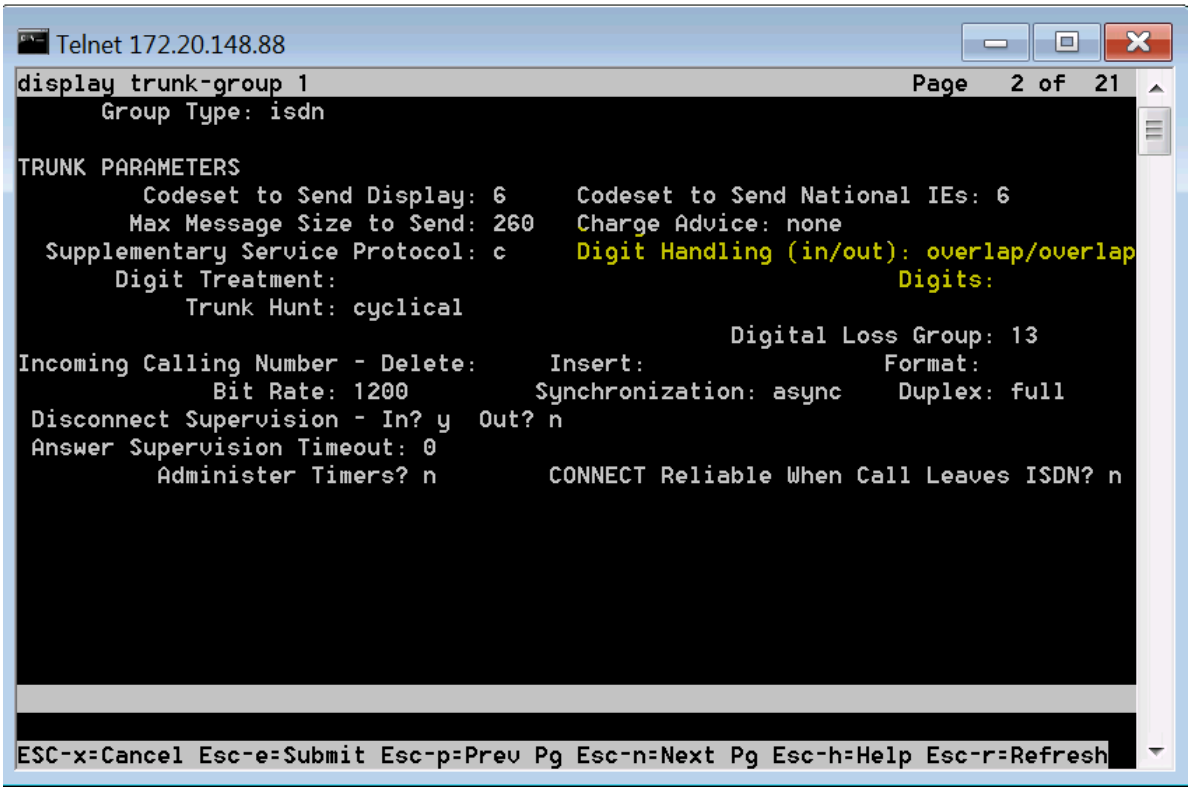
Note Check route patterns 13 and 29, respectively in the same way (the only difference with our configuration is that those route patterns do not remove any digits from the number as it is not necessary for SIP or H.323 trunks).

8. Execute command "`display trunk-group 1`" and inspect pages 1, 2 and 5.

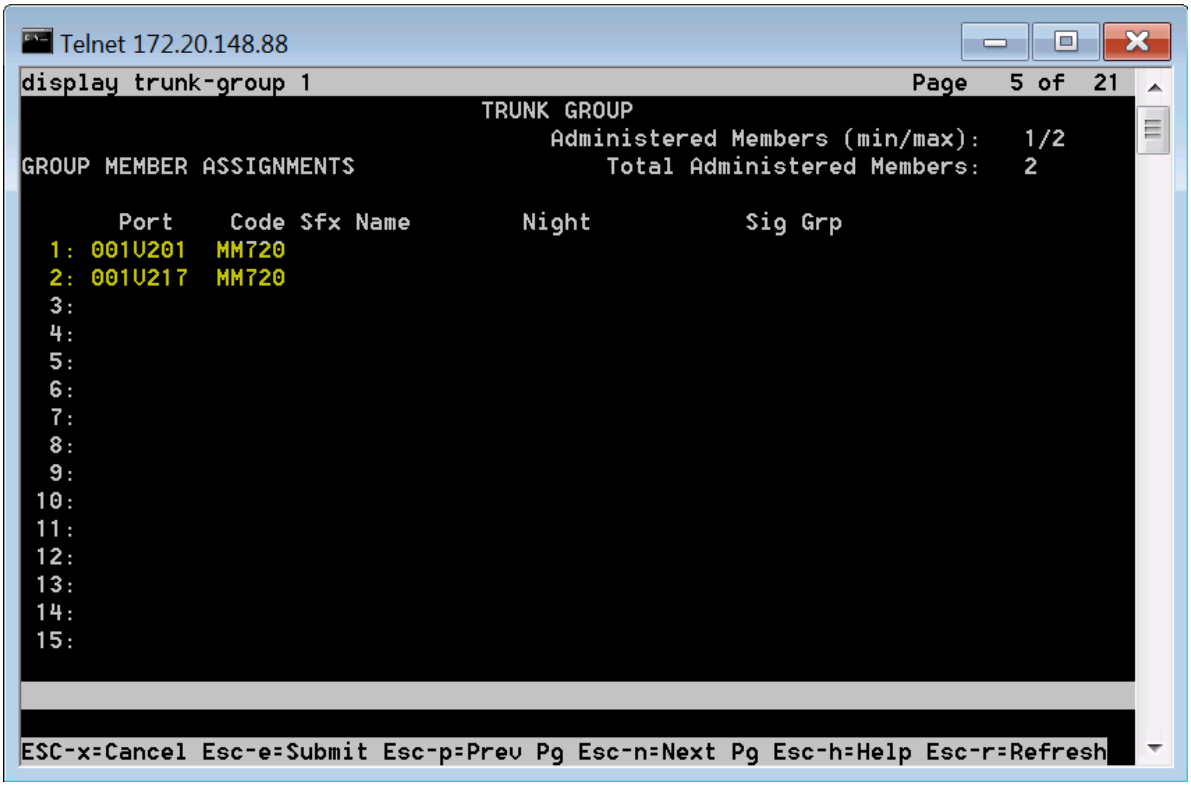
Note The trunk type ISDN doesn't need any signaling group to be assigned to.



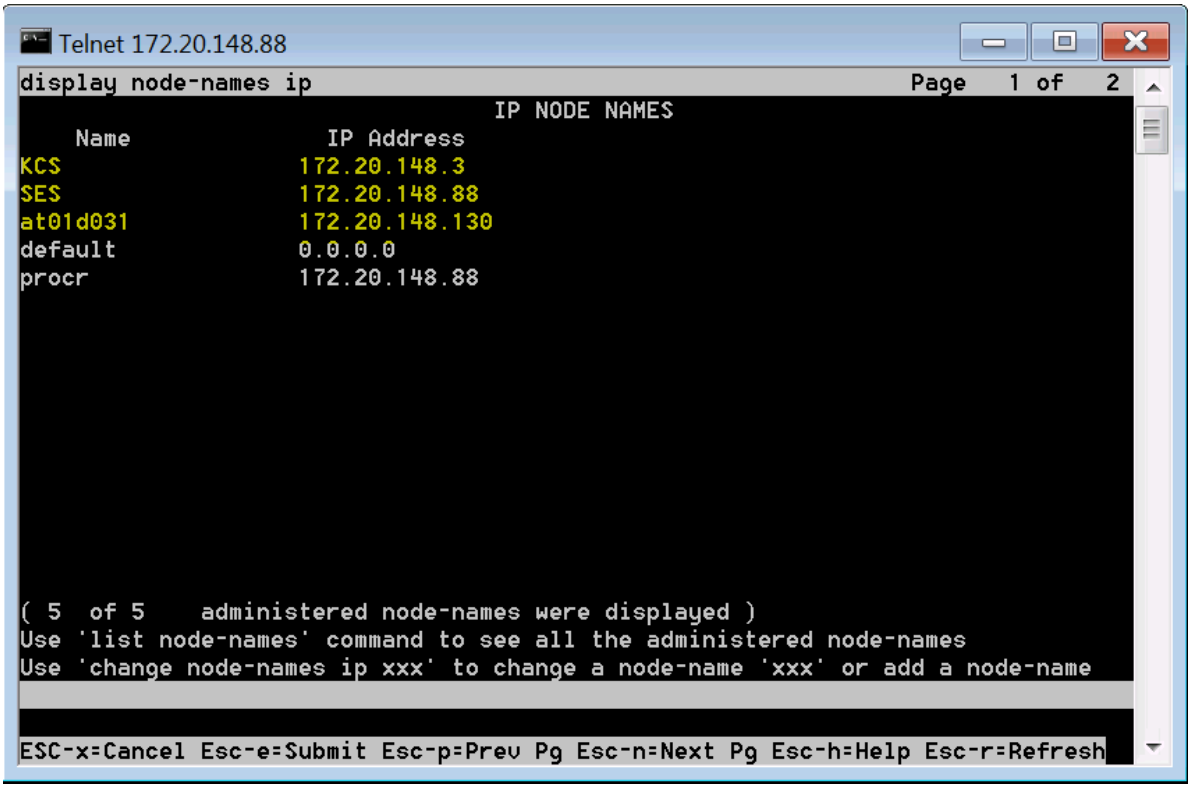
9. Select digit handling overlap/overlap (in countries like Austria and Germany) to be able to use overlap sending and receiving over the trunk. Select enbloc/enbloc in countries that use a strict numbering plan not allowing any overlap dialing procedures.



10. Assign some hardware ports to the trunk group.

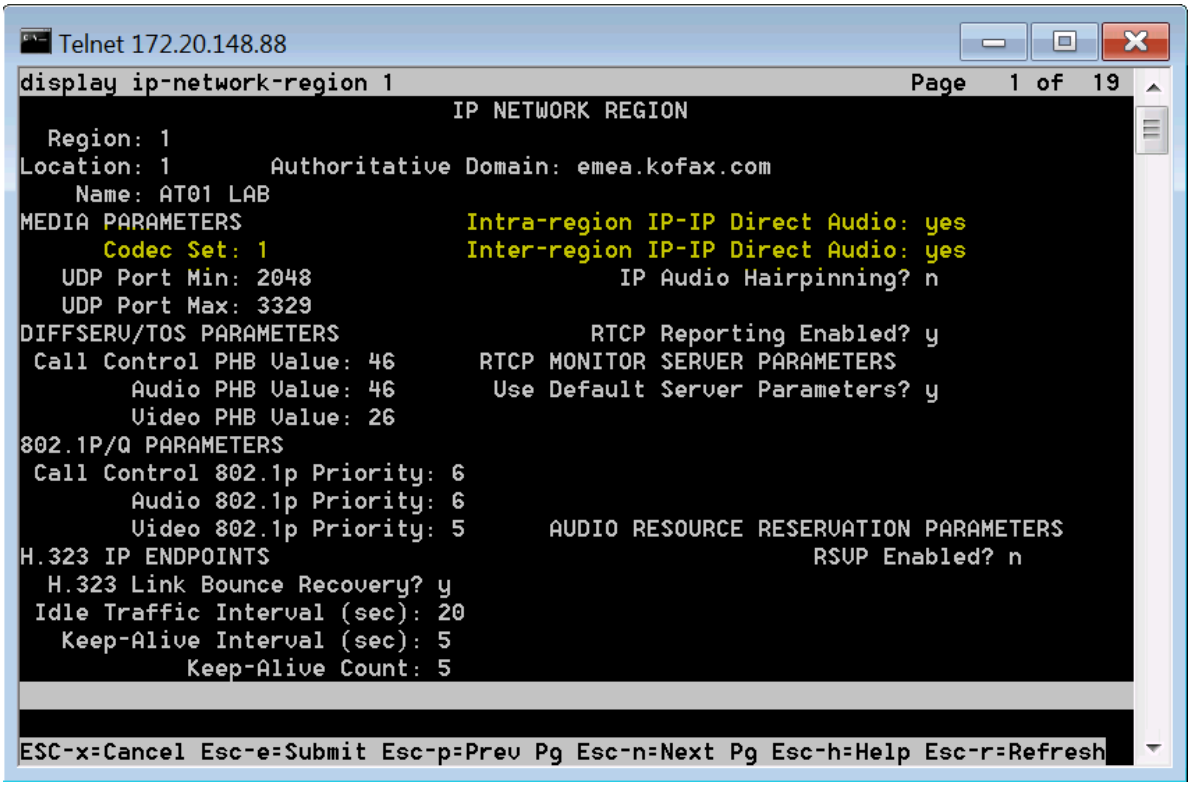


11. Execute the “`display node-names ip`” in order to see assigned symbolic host names for the KCS FoIP instances.



Note The node “procr” has been created by the Avaya CM automatically for the own processor node.

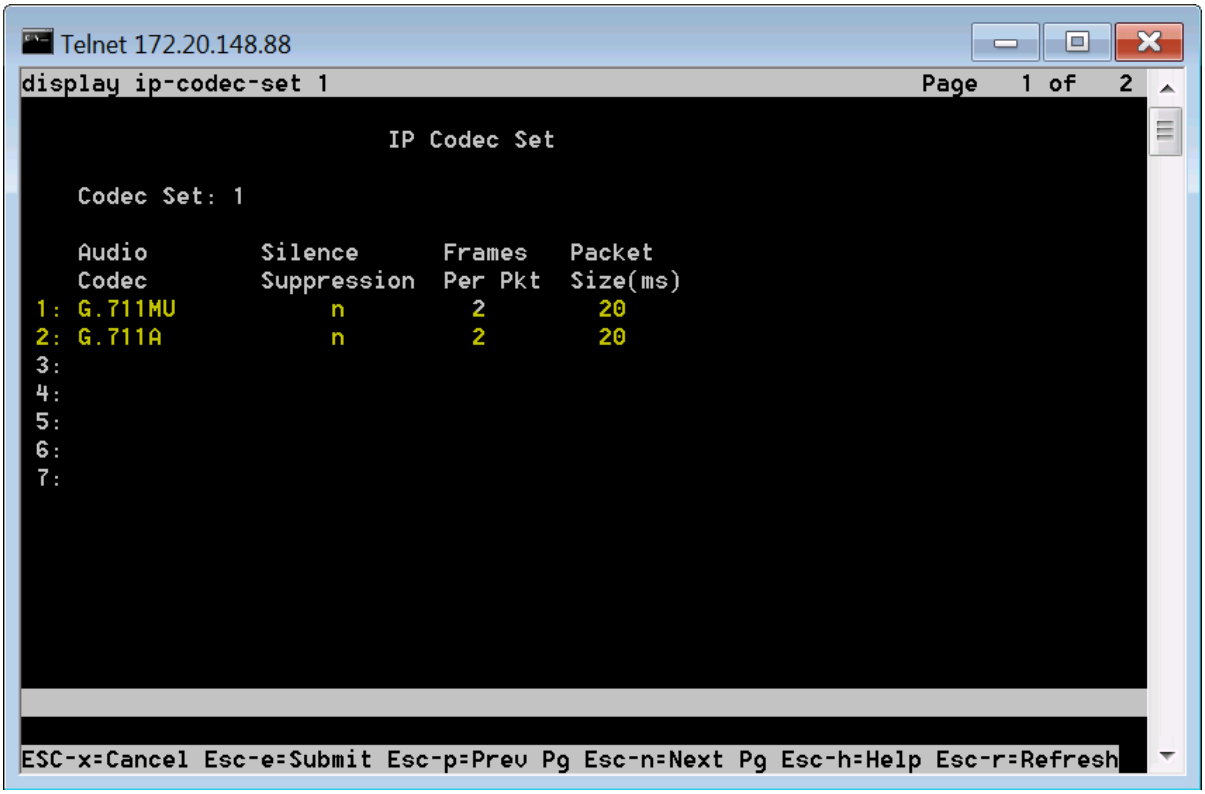
12. Execute command "`display ip-network-region 1`".



This network region is using codec set 1 (which will be shown in the next screen).

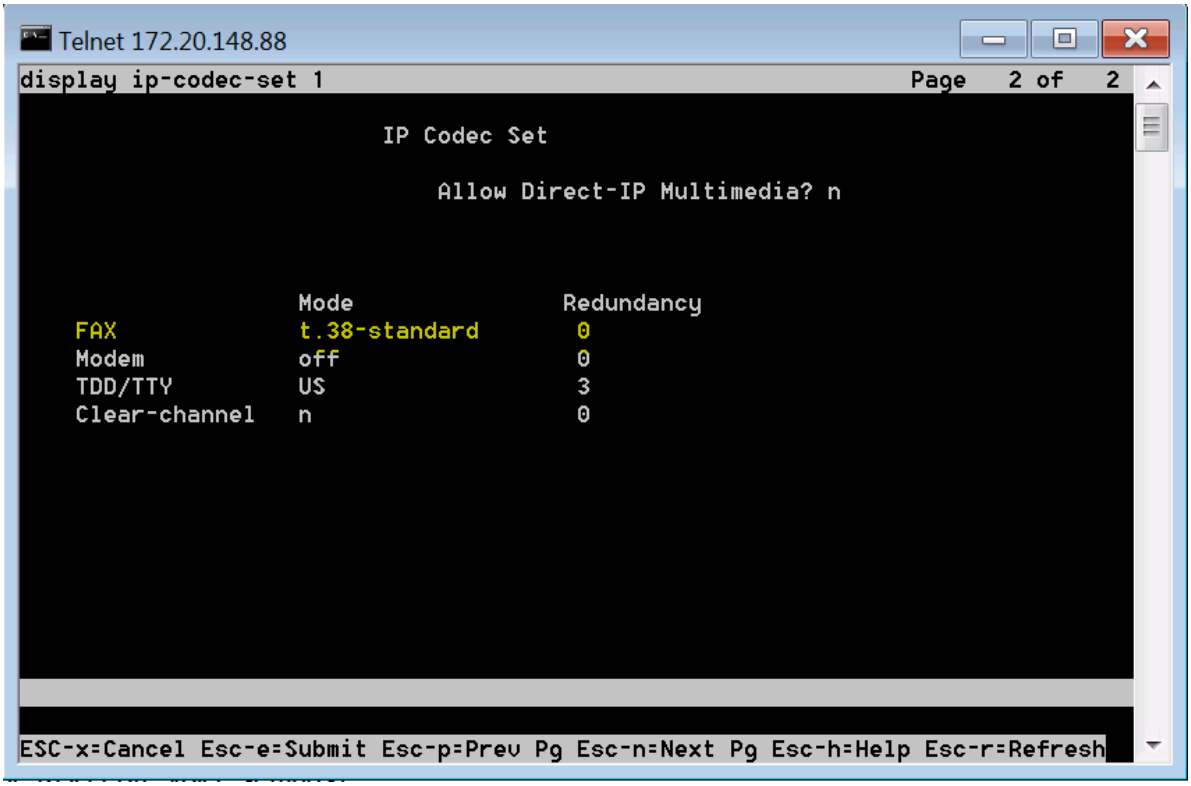
Note This example is using only one network region, but in a more complex Avaya system several network regions may be defined, using different codec sets, but this is outside of scope of this guide)

13. Execute command "`display ip-codec-set 1`".



Note On the first page, either both or at least one of the G.711 codec must be configured (at least the one which is also configured in the KCS FoIP voice settings). The silence suppression must be disabled when using G.711 pass-through FoIP.

14. Proceed to the next page (ESC-n), and see that the T.38 standard is configured.



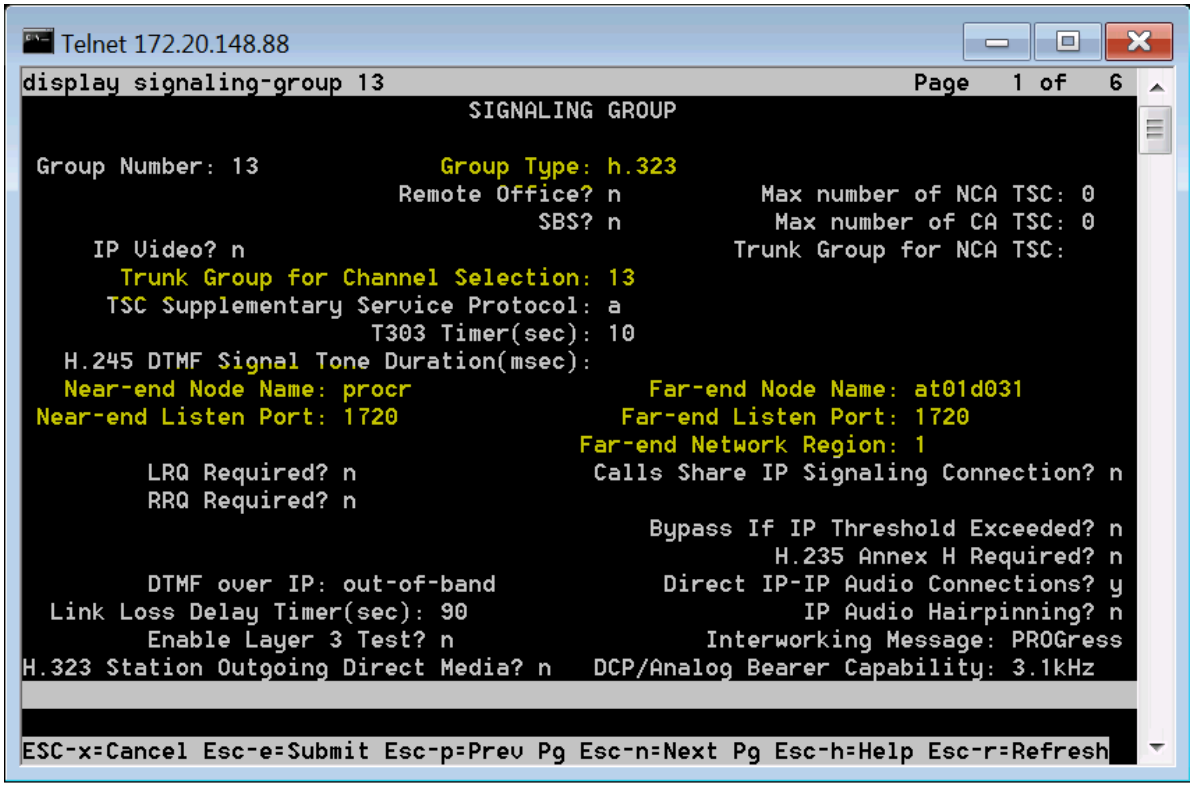
Note

- Set the Fax mode to “Pass-through” instead of “T.38 standard” if you want to use G.711 pass-through FoIP.
- The network region and codec settings performed above are relevant for both H.323 and SIP trunks configured in next chapters.

H.323 Integration

As for the H.323 integration, at first the signaling group (number 13 in our example) must be created and it must be assigned to the H.323 trunk (number 13 in our example).

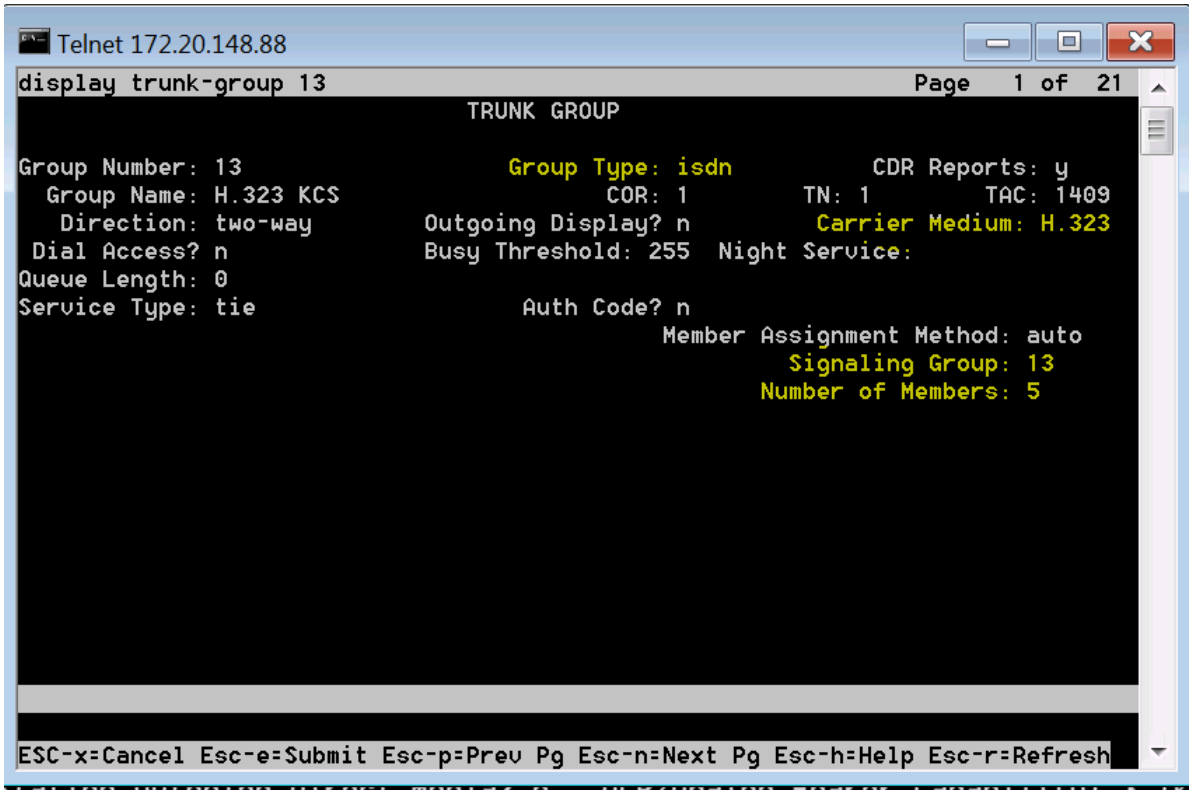
Execute the command “display signaling-group 13”:



As the far-end node name, enter the host name of the KCS FoIP host (at01d031 in our example).

As the near-node name, you should choose the node name of the local Avaya CM node (which is typically “procr” for a small system).

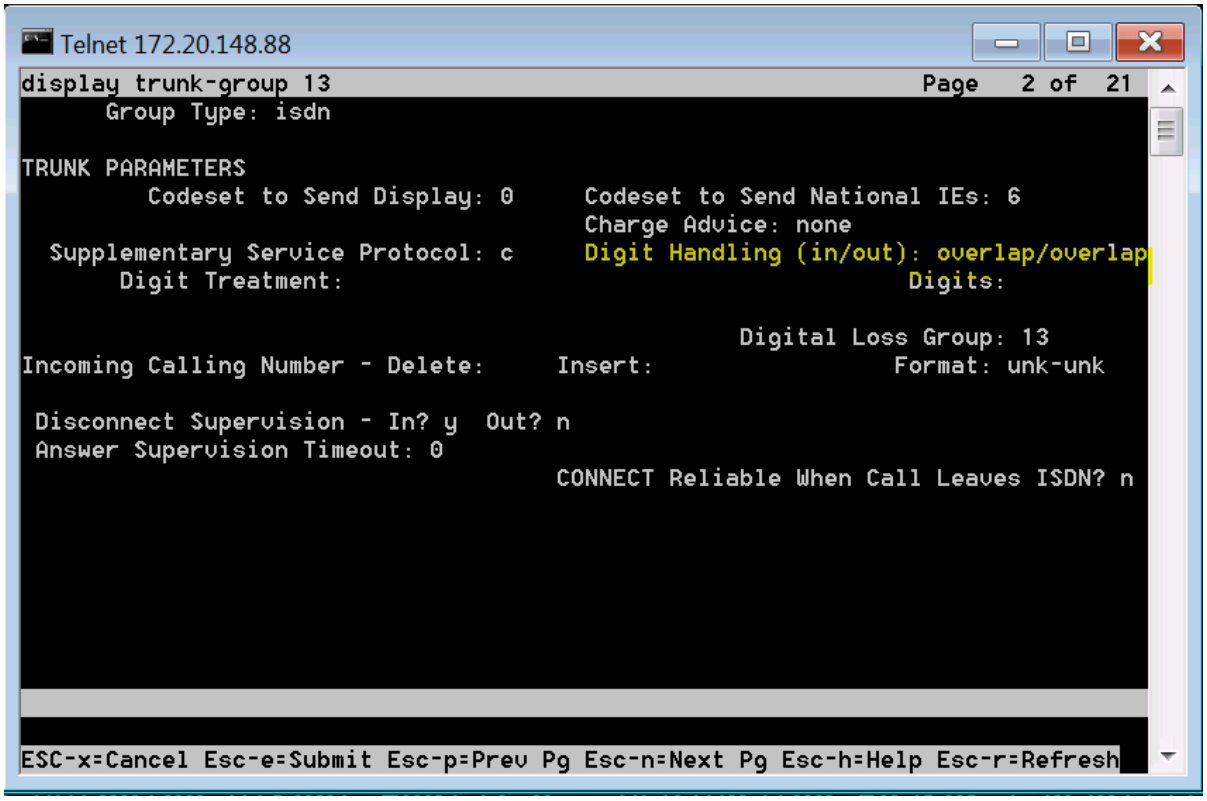
Execute command “display trunk-group 13” and check pages 1 and 2:



Note The trunk group is surprisingly isdn, but the carrier medium is set to H.323.

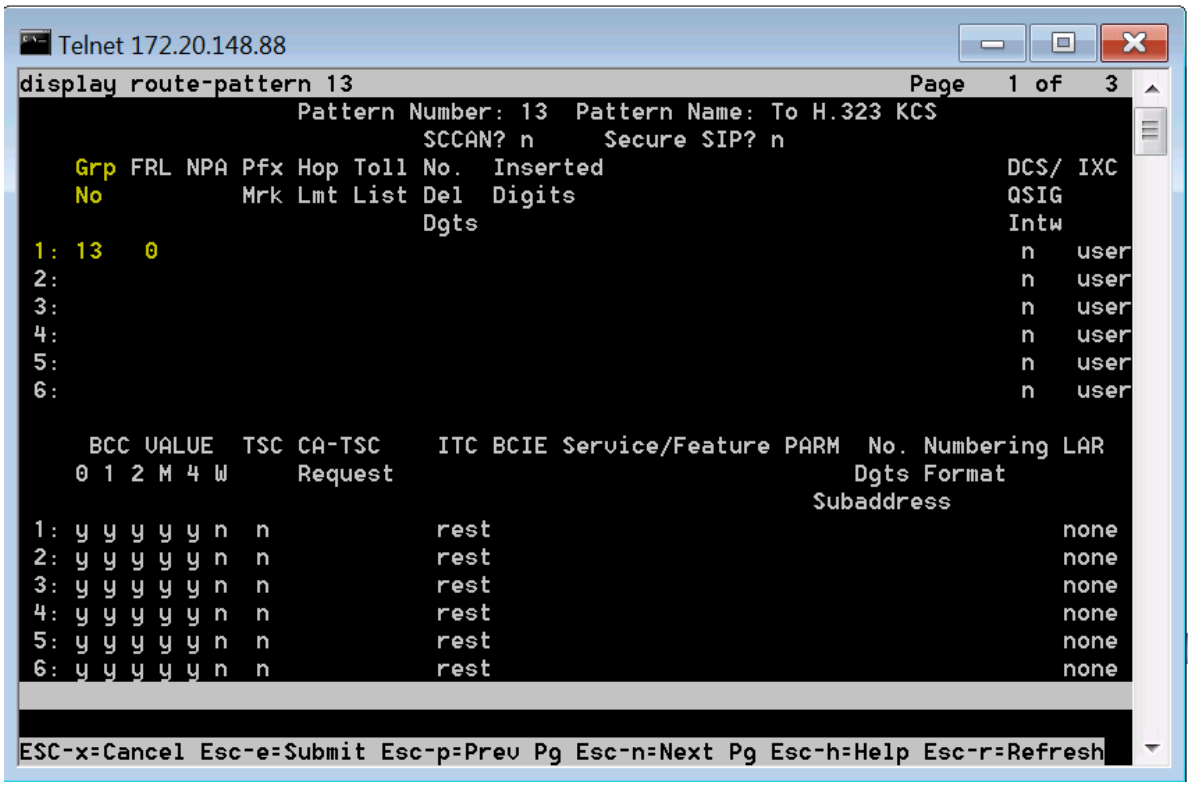
The signaling group must be set to the one created before (which has also the number 13 for simplicity), and also number of members should be great than 0 (number of members denotes the maximum parallel calls through this trunk).

Press ESC-n to see the next page:



Note The digit handling (overlap/overlap) set in this configuration page.

Execute the command “display route-pattern 13” to see the route pattern pointing to this trunk group (13):



Note This route-pattern is assigned with desired number range to be routed to this trunk in the ARS (see above).

SIP Integration

Unlike to the H.323 integration where the H.323 trunk in the CM points directly to the KCS FoIP server, for SIP an additional system component is needed – SIP Enablement Services (SES) – where the KCS FoIP is connected. And on the CM side, a SIP trunk along with assigned SIP signaling group must be created for the communication between CM and the SES.

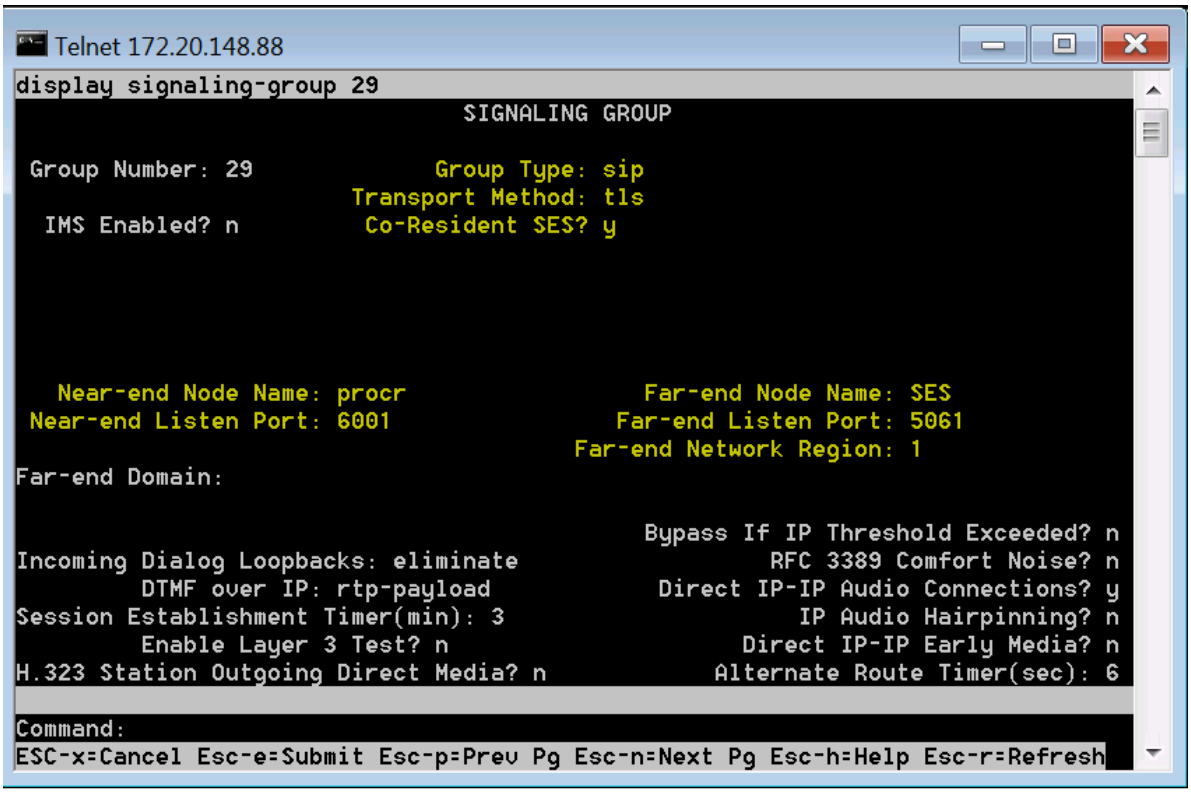
The SIP configuration consists of two parts:

1. CM
2. SES

Note The following screen shots show a co-resident configuration where CM and SES run on the same processor (S8300 in this case).

CM Configuration

1. Execute command "`display signaling-group 29`".



Note Both near and far end node names in the fact point to the same IP address (see node-names configuration) as this is a co-resident system running CM and SES on the same S8300 processor).

2. Set the **Group Type**/**Transport Method** to SIP/tls.

Note tls is the only transport supported for the SIP trunk interconnecting SES with the CM.

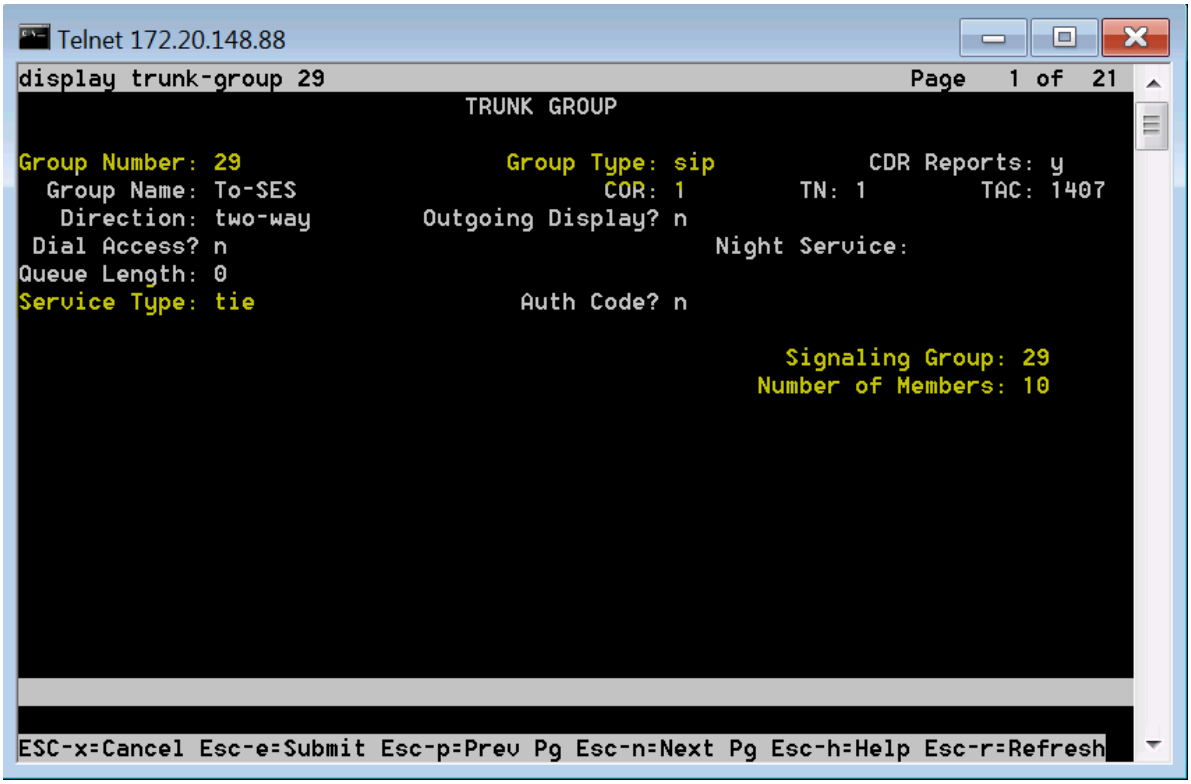
3. The **Near-end Listen Port** is by default set to the value 6001 and it is the port where CM listens for the SIP calls arriving from the SES.

Note This port will also be configured in SES.

4. The **Fear-end Listen Port** is by default set to the value 5061 and it is the port where SES listens for the SIP calls arriving from the CM.

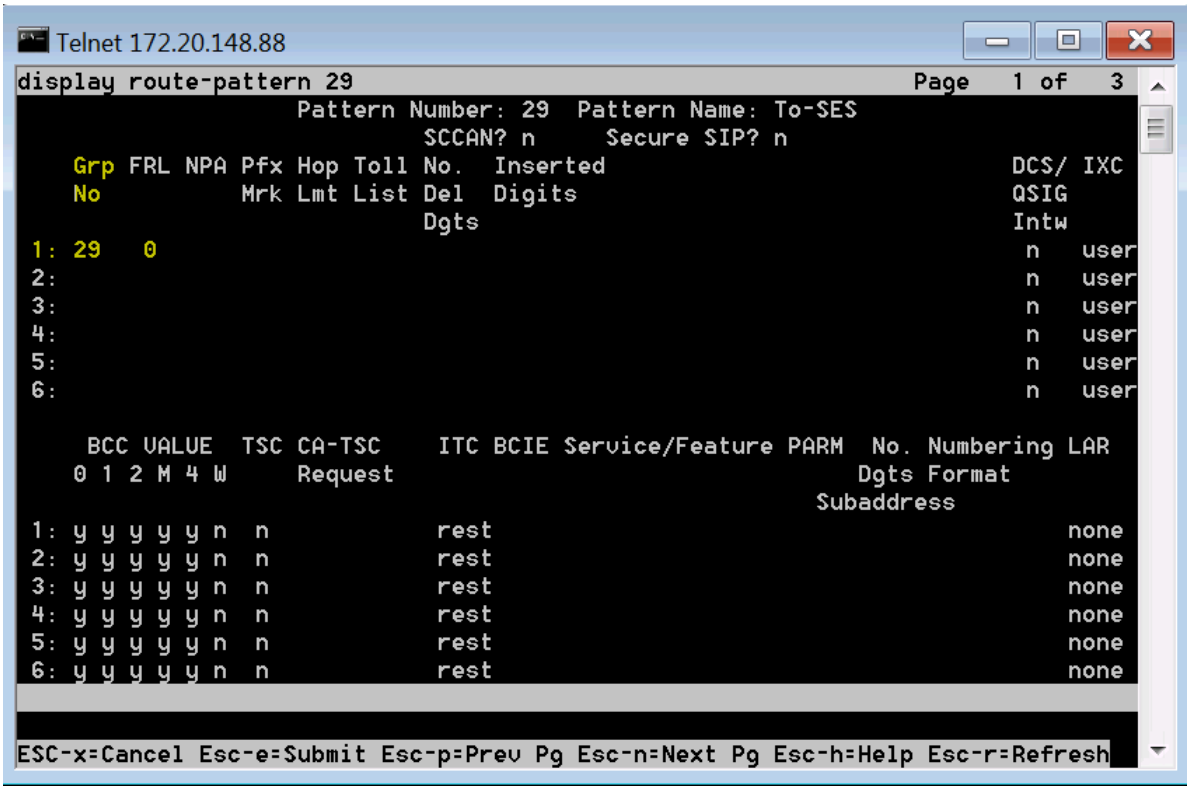
Note This port will also be configured in SES.

5. Execute command "`display trunk-group 29`".



The signaling group must be set to the one created before (which has also the number 29 for simplicity), and also number of members should be great than 0 (number of members denotes the maximum parallel calls through this trunk).

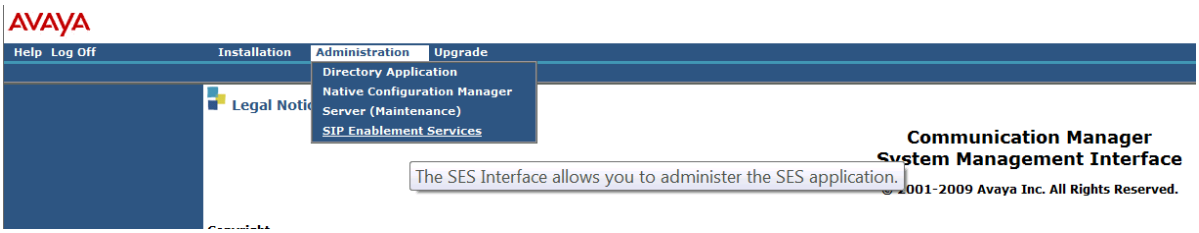
6. Execute the command "`display route-pattern 29`" to see the route pattern pointing to this trunk group (29).



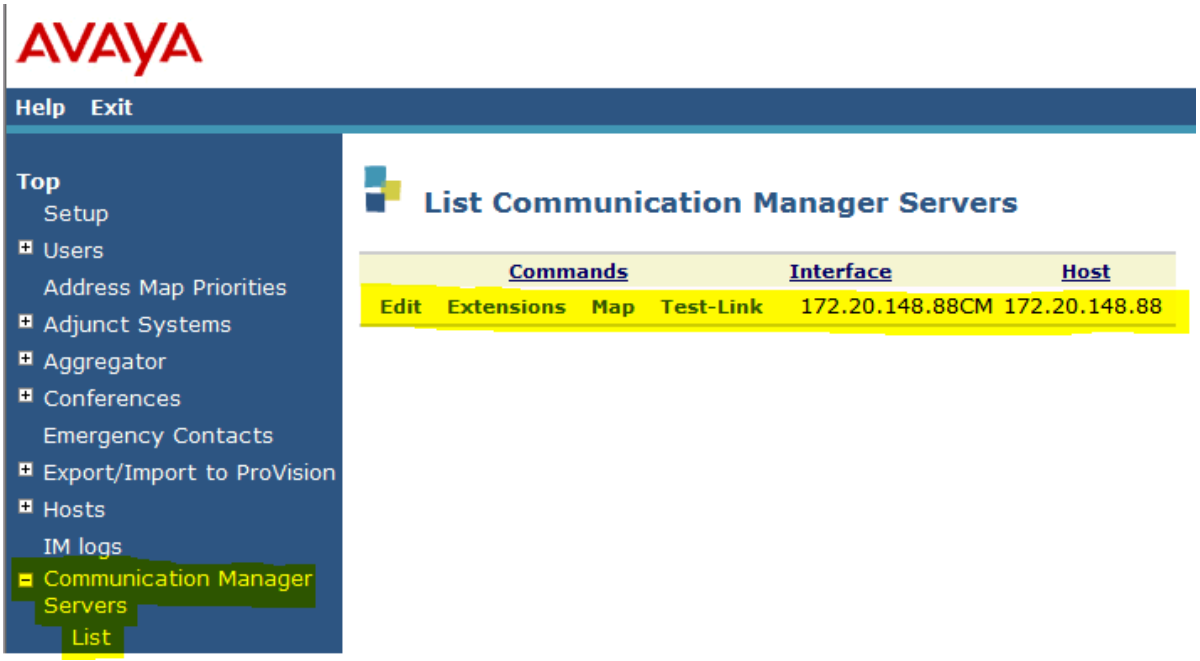
SES Configuration

Given the SES has already been enabled (basic Avaya CM/SES configuration, CM added to the SES and others), the following configuration tasks are necessary.

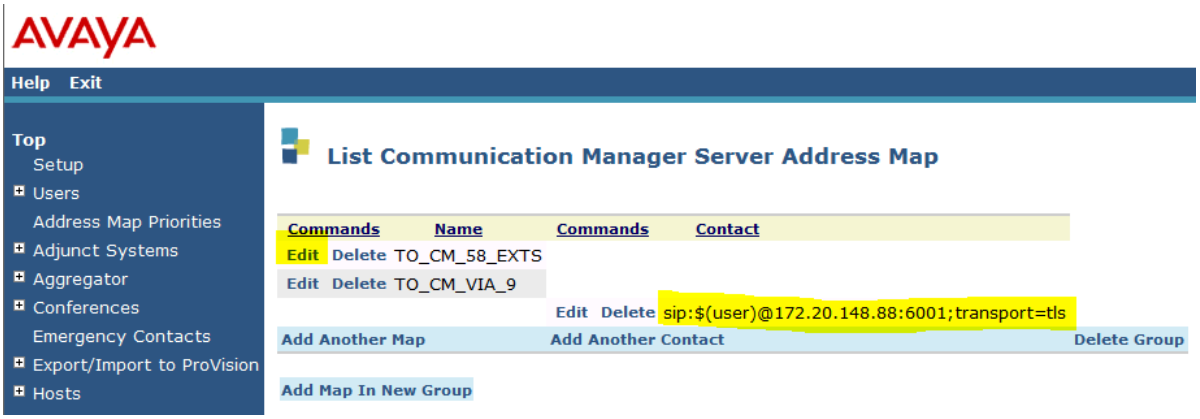
1. Login to your CM via web interface and go to **Administration->SIP Enablement Services**.



2. Go to **Communication Manager Servers->List** and you will see the list of entered CM servers.

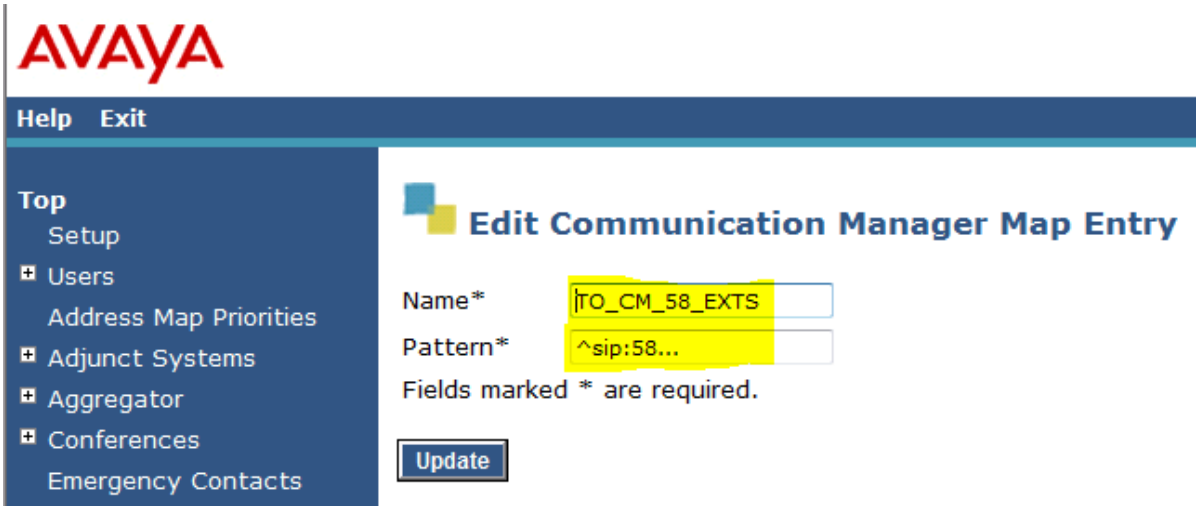


3. Click **Map**.



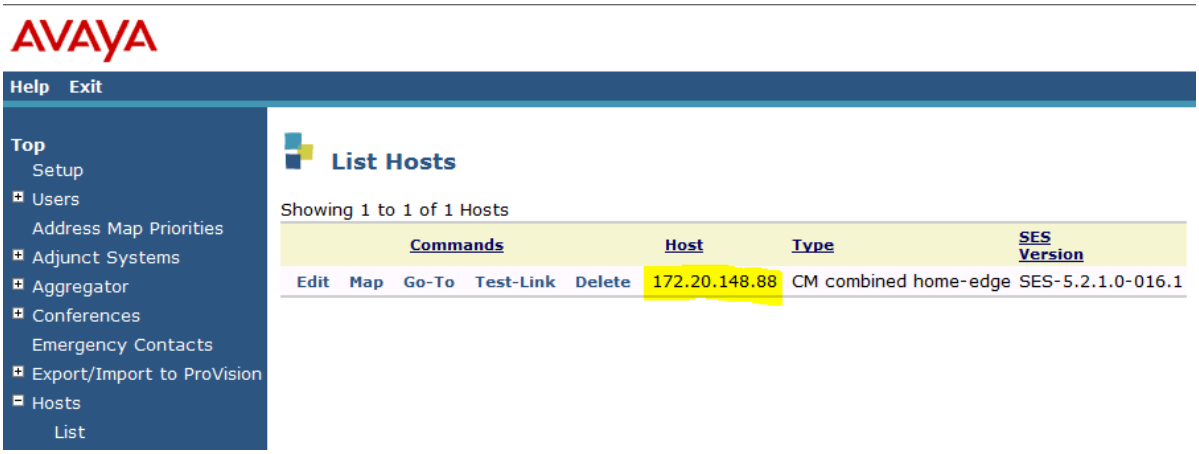
Note You will see the “Contact” (sip:$(user)172.20.148.88:6001;tls) pointing to the SIP listener port 6001 that was configured in the signaling group 29 on the CM, using the transport tls.

4. Click **Add Another Map** or edit one of the existing maps to define the route pattern to be routed to this CM.

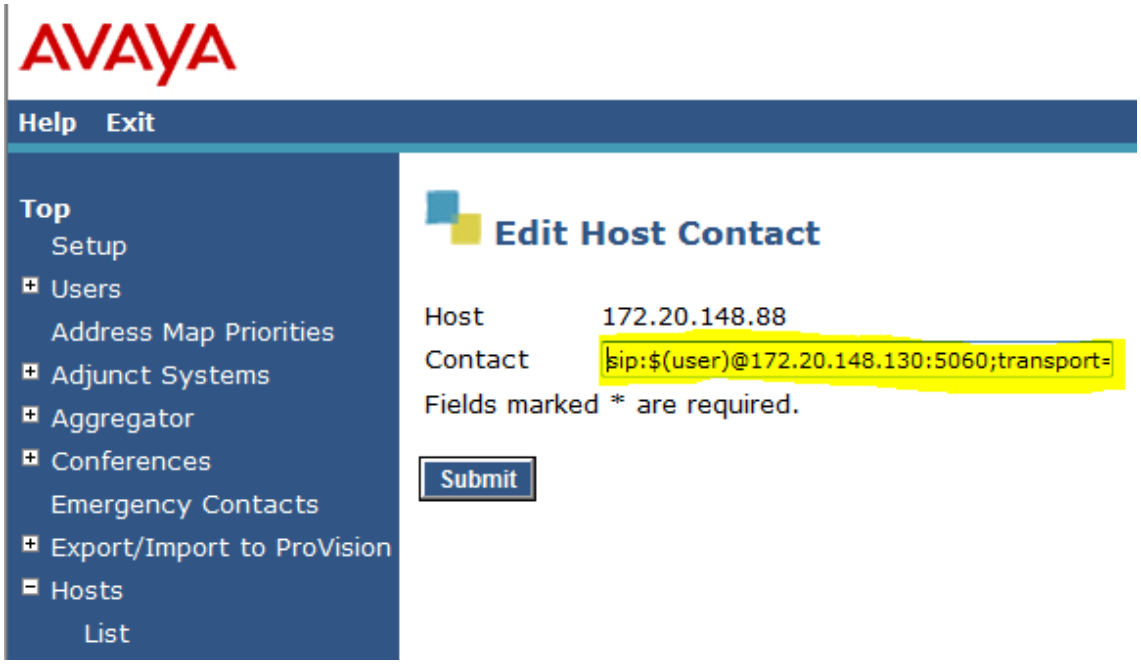


5. Choose a name of this map entry and define the number to be routed to this CM by the means of regular expression.
   In this example, the number 58xxx would be routed to this CM instance.
6. Configure the number map which would be routed to the KCS FoIP. Go to **Hosts->List**. You will again see the list or at least one CM server as Host there.

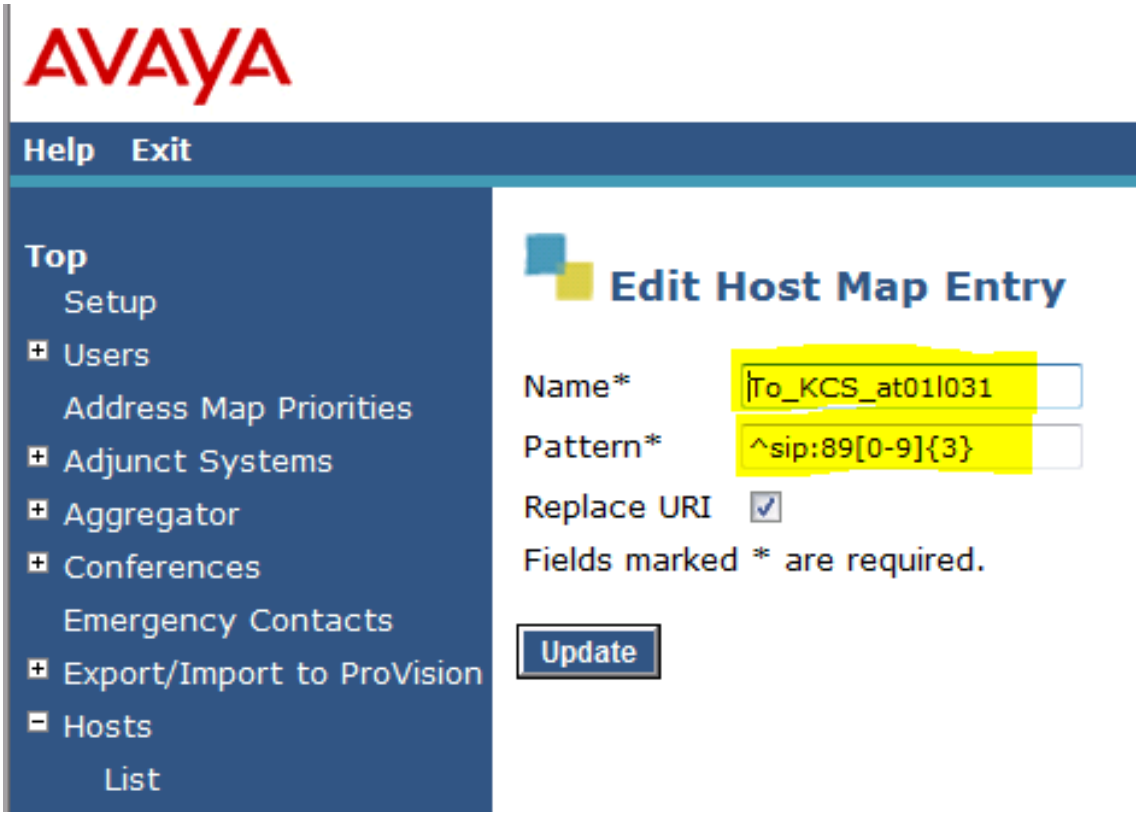
Note One would expect to define IP addresses of other SIP servers like KCS FoIP here, but it is not the case. They are entered via contact fields for each configured CM Host.



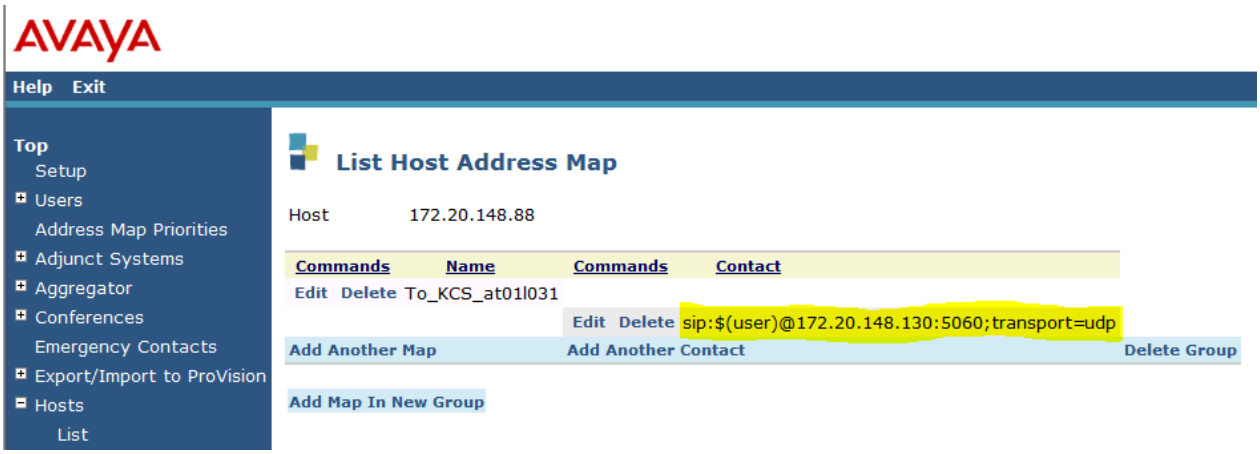
7. Click **Map** and then add the following:
   a. **Contact**: To define the IP address of the KCS FoIP server (incl. port number 5060 and transport=udp) and click Submit to enter it to the SES.



   b. **Map**: To define the number to be routed to the KCS FoIP by the means of regular expression. Click **Update** to enter it to the SES. (In this example, all numbers of the type 89xxx are routed to this KCS FoIP.

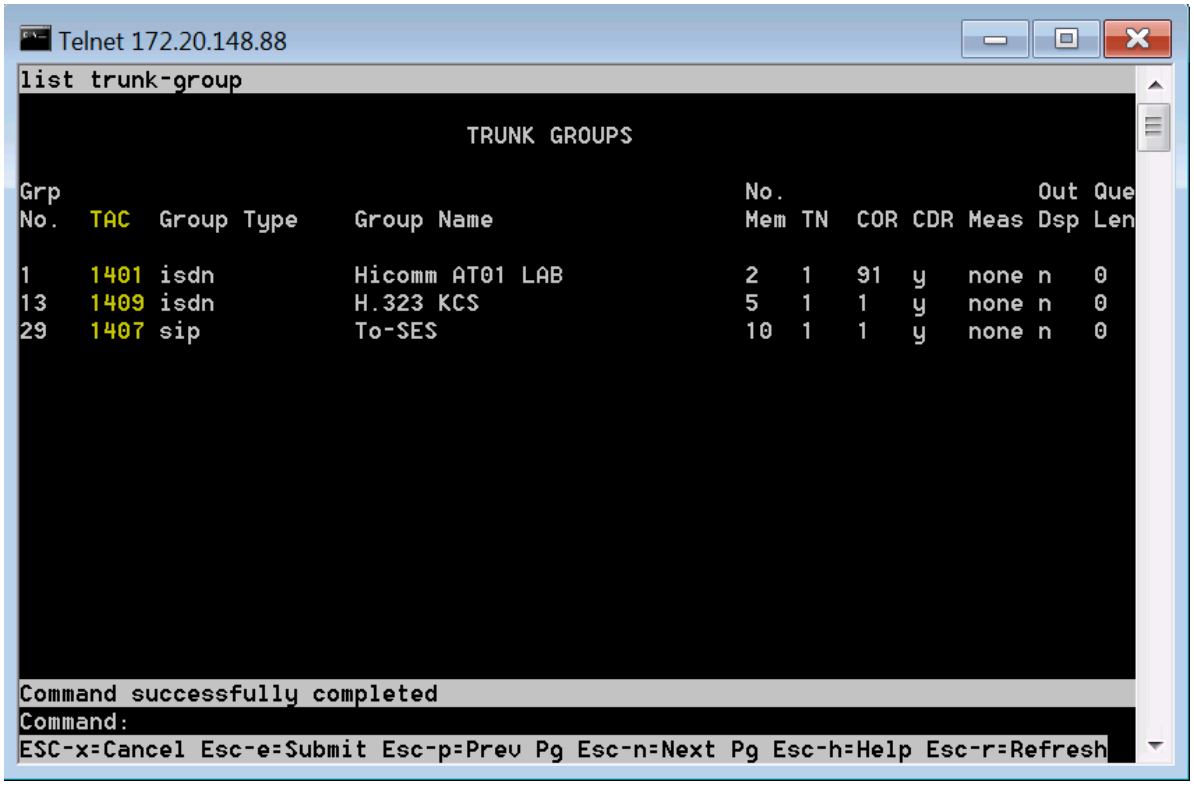


At the end, it looks like this.



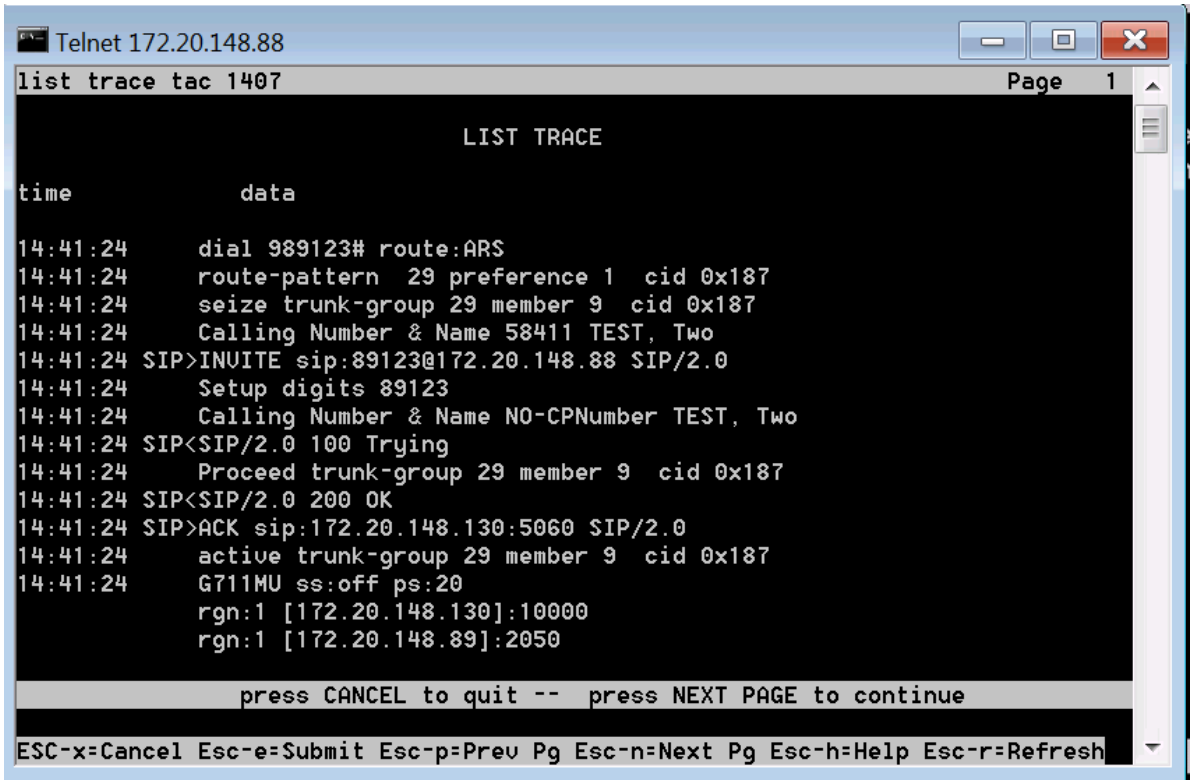
Useful Troubleshooting/Tracing Options

On the CM, useful traces may be activated on each trunk and /or station using the trunk number (the TAC) or the station's extension. In order to see the TAC numbers, execute the command "list trunk-group":



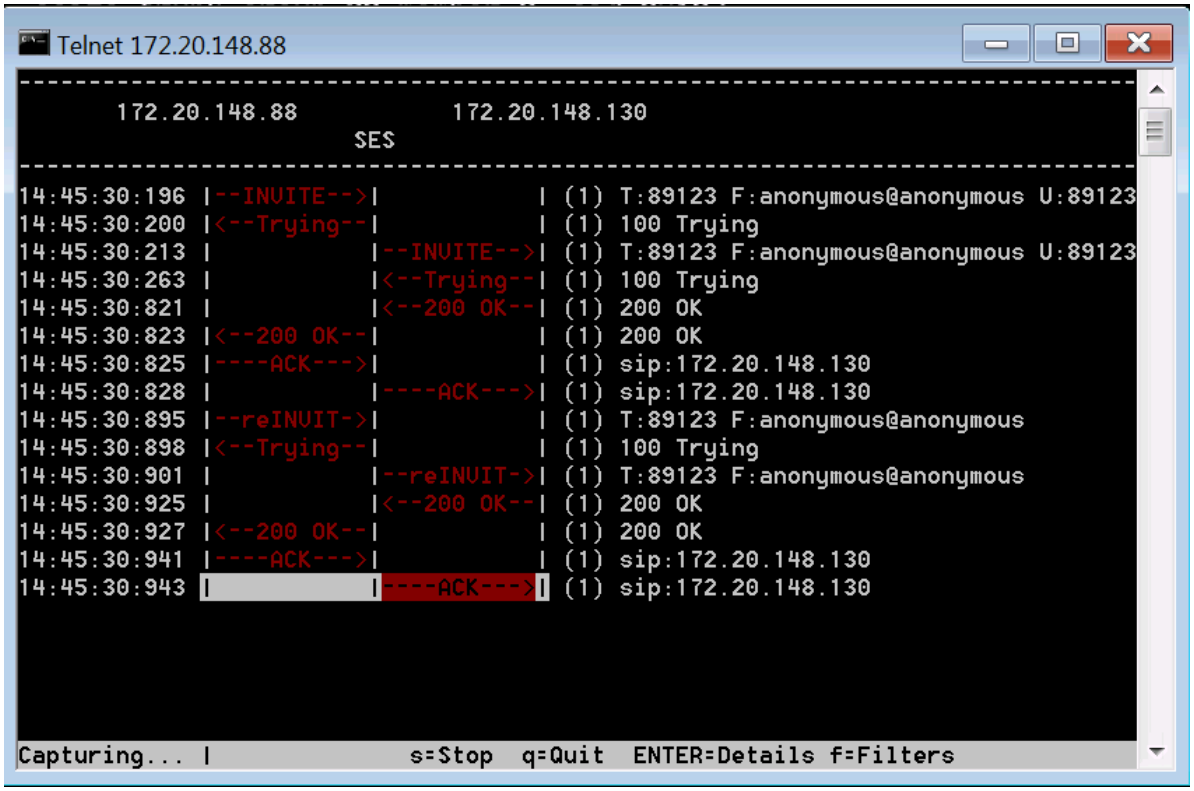
And see the TAC numbers of our trunks.

In order to trace the trunk number 29, execute the command “list trace tac 1407” and make appropriate SIP call:



As for the SIP calls, there is another useful utility called “traceSES” which can be started in the telnet session with the CM server.

Open the telnet session with your Avaya server, log on there, execute the command “traceSES” and press “s” to start the capture. Make a SIP call and observe the trace:



Avaya Aura Communication Manager 6.01

KCS FoIP 3.12.07 or later can be integrated with Avaya Aura Communication Manager (CM) 6.01 using either SIP or H.323 protocol. See Fax over IP Integration for the exact versions required.

This version of Avaya CM (6.01) has been certified in the Avaya's certification lab and there are two application notes written by Avaya which describe both types of the integrations – the H.323 and SIP, as well.

H.323:

http://downloads.avaya.com/css/P8/documents/100141486

SIP:

http://downloads.avaya.com/css/P8/documents/100140202

Avaya Aura Communication Manager 6.2

KCS FoIP 3.16.20 or later can be integrated with Avaya Aura Communication Manager (CM) 6.2 using either SIP or H.323 protocol. See Fax over IP Integration for the exact versions required.

This version of Avaya CM (6.2) has been certified in the Avaya's certification lab and there are two application notes written by Avaya which describe both types of the integrations – the H.323 and SIP, as well.

H.323:

http://www.devconnectprogram.com/fileMedia/download/8779508b-fff5-4082-948d-ba5f27a4f284

SIP:

http://www.devconnectprogram.com/fileMedia/download/c6c66c4c-66e1-4cee-bff3-70adcf8a9b7f

Avaya Aura Communication Manager 6.3

KCS FoIP 3.22.05 or later can be integrated with Avaya Aura Communication Manager (CM) 6.3 using either SIP, H.323 or SIPS/SRTP protocols. See Fax over IP Integration for the exact versions required.

This version of Avaya CM (6.3) has been certified in the Avaya's certification lab and there are three application notes written by Avaya which describe both types of the integrations – the H.323, SIP, and SIP/TLS/SRTP as well.

The highlight with Avaya Aura version 6.3 is that it finally supports T.38 with ECM, the drawback is that it works only up to the baud rate 9600.

H.323 (T.38 ECM and Pass-through)

https://downloads.avaya.com/css/P8/documents/100182742

SIP (T.38 ECM and Pass-through)

https://downloads.avaya.com/css/P8/documents/100182743

SIP/TLS/SRTP (Pass-through)

https://downloads.avaya.com/css/P8/documents/100182744

Avaya Aura Communication Manager 7.0

KCS FoIP 3.22.24 or later can be integrated with Avaya Aura Communication Manager (CM) 7.0 using either SIP, H.323 or SIPS/SRTP protocols. See Fax over IP Integration for the exact versions required.

This version of Avaya CM (7.0) has been certified in the Avaya's certification lab and there are three application notes written by Avaya which describe both types of the integrations – the H.323, SIP, and SIP/TLS/SRTP as well.

H.323 (T.38 ECM and Pass-through)

https://www.devconnectprogram.com/fileMedia/download/ed25feca-41d2-4f98-83e7-3e67ac78c604

SIP (T.38 ECM and Pass-through)

https://www.devconnectprogram.com/fileMedia/download/bcf81346-5eee-4782-a5ed-a86d3e138efa

SIP/TLS/SRTP (Pass-through)

https://www.devconnectprogram.com/fileMedia/download/abd8a96f-febe-429a-b531-b406442cb975

Avaya Aura Communication Manager 7.0.1

KCS FoIP 3.26.11 or later can be integrated with Avaya Aura Communication Manager (CM) 7.0.1 using either SIP, H.323 or SIPS/SRTP protocols. See Fax over IP Integration for the exact versions required.

This version of Avaya CM (7.0.1) has been certified in the Avaya's certification lab and there are three application notes written by Avaya which describe both types of the integrations – the H.323, SIP, and SIP/TLS/SRTP as well.

H.323 (T.38 ECM and Pass-through)

https://www.devconnectprogram.com/fileMedia/download/4a42fa87-c714-497c-82d0-eac8216cefb0

SIP (T.38 ECM and Pass-through)

https://www.devconnectprogram.com/fileMedia/download/6a71638a-9dff-484f-bb15-26296c956700

SIP/TLS/SRTP (Pass-through)

https://www.devconnectprogram.com/fileMedia/download/a353a515-02da-4a57-93f8-5a9bc762d6d0

Microsoft Lync Server 2013

KCS FoIP 3.17.04 or later can be integrated with Microsoft Lync Server 2013. The integration into earlier versions of Microsoft Lync Server is not supported. Compatibility with other devices can be found on Microsoft Lync Server Interop Program page: http://technet.microsoft.com/en-us/lync/gg131938.aspx

Integration as SIP Trunk Without Encryption

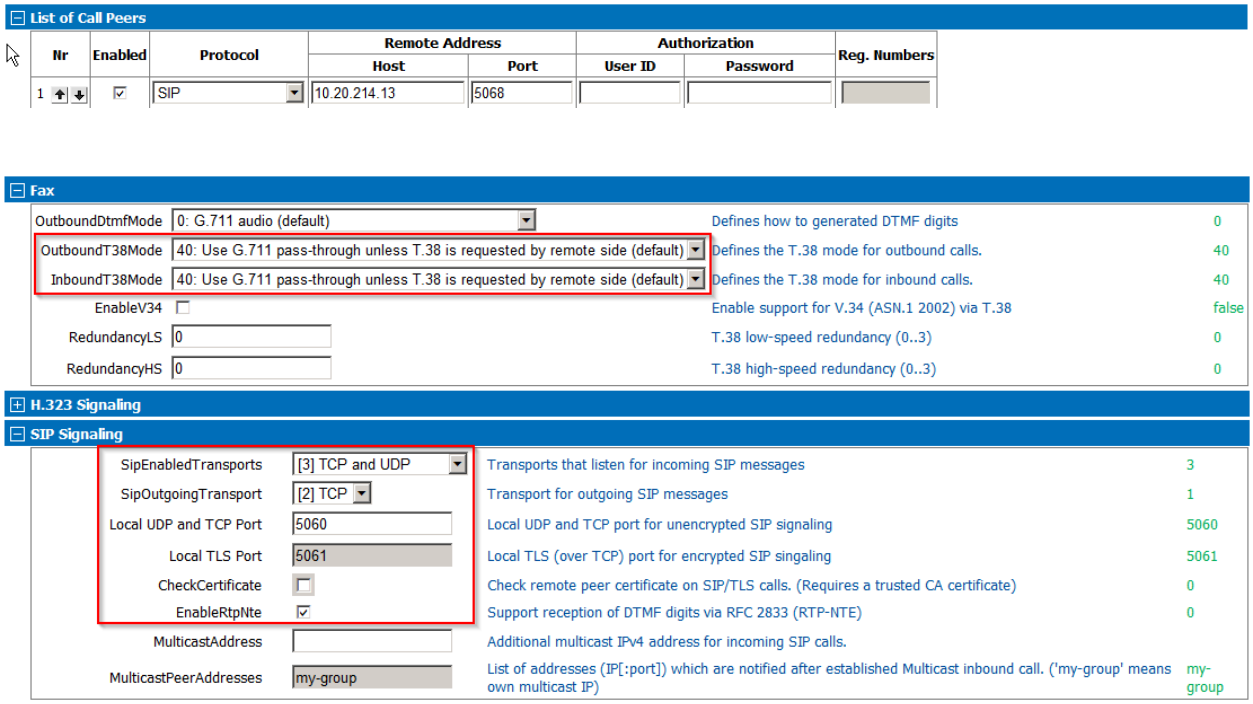
This chapter describes the basic integration of KCS FoIP as SIP trunk without encryption. It is strongly recommended to perform this step also in cases where encryption is required in order to simplify troubleshooting.

FoIP Configuration

The FoIP Configuration is very simple.

1. Configure the IP and port of the mediation server in the used call-peer.
2. Set to T.38 mode in the fax section to 40 (Use G.711 pass-through unless T.38 is requested by remote side). The EnableV.34 check-box will be ignored because is not supported with G.711 pass-through mode.

3. Set the Sip transport for outgoing calls to TCP and enable reception of DTMF digits via RFC2833. Here is a screen shot from a sample configuration:



Lync Server 2013 Configuration

Note that the Lync Server supports by user/pool/side specific configuration parameters. In order to keep things as simple as possible only the default identity “Global” is use within this chapter. An example with screen shots can be found in chapter Example Configuration with Lync Server 2013.

A high-level summary of the KCS FoIP integration (which is like an integration of a SIP Gateway) is listed below:

1. Run the Lync Server Topology Builder.
   a. Take care that the TCP listener is enabled in the Mediation Server(s).
   b. Add KCS FoIP as SIP Gateway (using TCP transport).
   c. Publish the modified Topology.
   d. Close the **Topology Builder**.
2. Run the Lync Server Deployment Wizard.
   a. Run **Install or Update Lync Server System**.
   b. Execute Step 2: Setup or Remove **Lync Server Components**.
   c. Execute Step 4: **Start Services**.
   d. Close the Deployment Wizard.

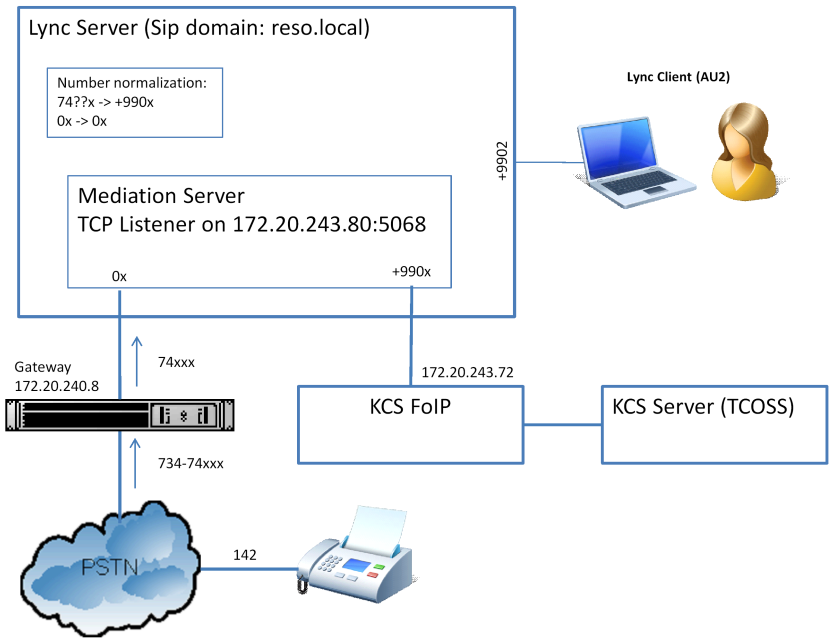
3. Configure a voice route to KCS FoIP and set the correct trunk configuration:
   a. Run the **Lync Server Control Panel**.
   b. Open **Voice Routing** > **Voice Policy** > **Global**.
   c. Select the Associated PSTN usage (such as “Internal”).
   d. Create a new Route to KCS FoIP (associate starting digits with the gateway IP of KCS FoIP).
   e. Open **Voice Routing** > **Trunk Configuration** > **Global**.
   f. Set **Encryption support level** to **Optional**.
   g. Commit all changes.
   h. Open the **Lync Server Management Shell**.
   i. Disable RTCP time-outs and enable session timers in the trunk configuration.

```
Set-CsTrunkConfiguration -Identity Global -RTCPActiveCalls
    $false
Set-CsTrunkConfiguration -Identity Global -RTCPCallsOnHold $false
Set-CsTrunkConfiguration -Identity Global -EnableSessionTimer $true
```

4. If you want to use Fax over IP, media bypass must be enabled in the network configuration:
   a. Run the Lync Server Control Panel.
   b. Open **Voice Routing** > **Trunk Configuration** > **Global**.
   c. Set **Enable media bypass**.
   d. Save and commit changes.
   e. Open **Network Configuration** > **Global**.
   f. Select **Enable media** > **always bypass**.
5. Optionally, you can enable enterprise Voice in any Lync Client in order to support calls between KCS FoIP and the Lync Client as described below:
   a. Run the Lync Server Control Panel.
   b. Search and open the Lync user you want to enable from **Users** > **User Search**.
   c. Set Telephony to Enterprise Voice and assign a telephone number in the field Line URI.
   d. Commit changes.

Example Configuration with Lync Server 2013

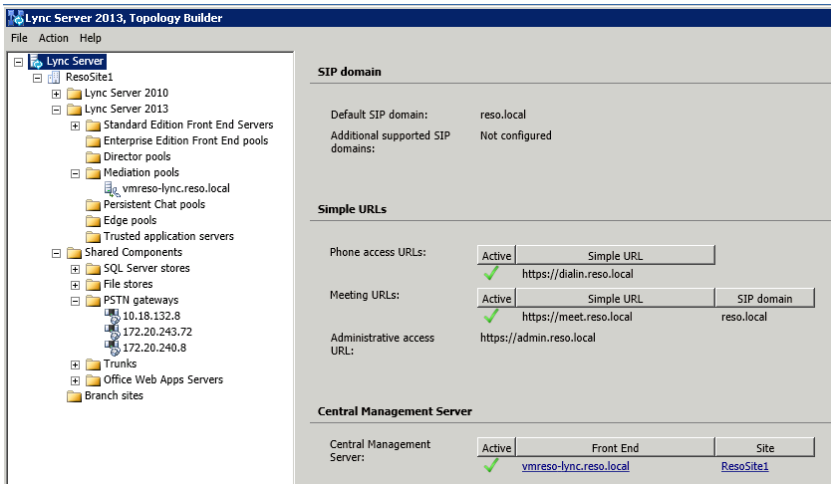
The chapter shows an example configuration with Lync Server 2013, KCS FoIP, and PSTN Gateway and a Lync user.

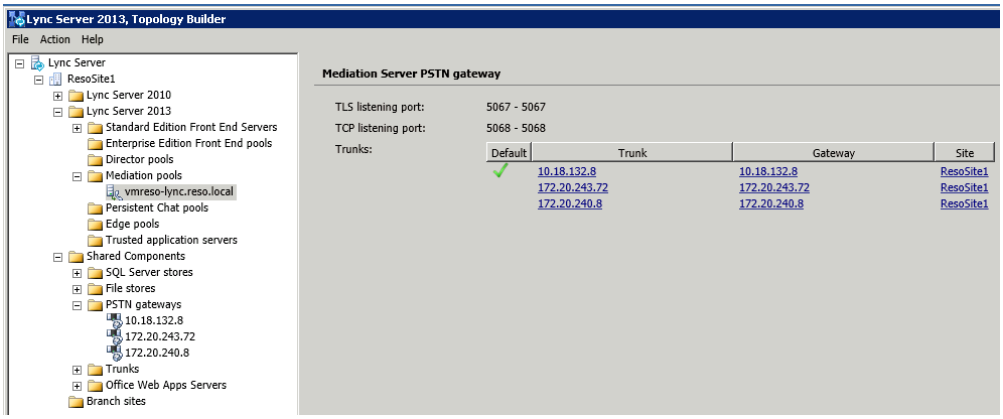


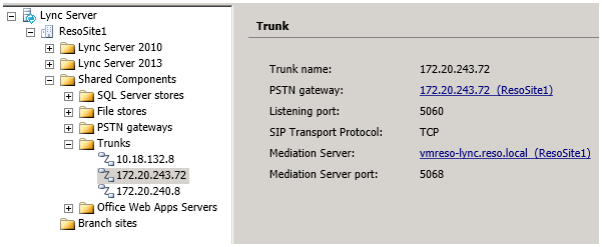
Configuration Description

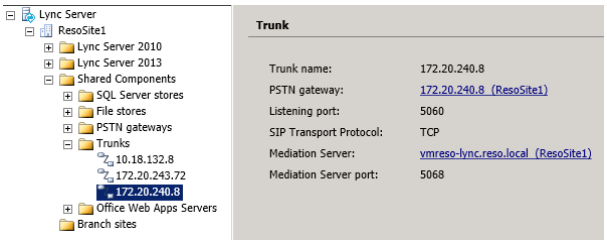
The KCS FoIP configuration is the same as already shown in FoIP Configuration.

The Lync Server Topology Builder defines the SIP domain and the connections to the Gateways.

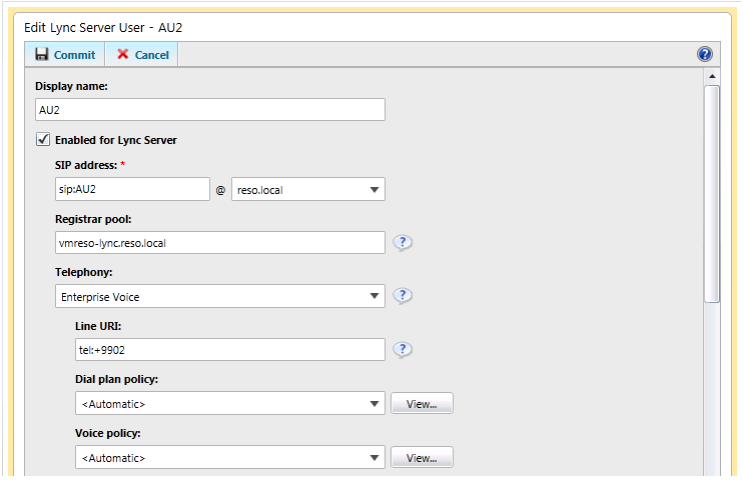








The Lync Server Control Panel User settings for “AU2“

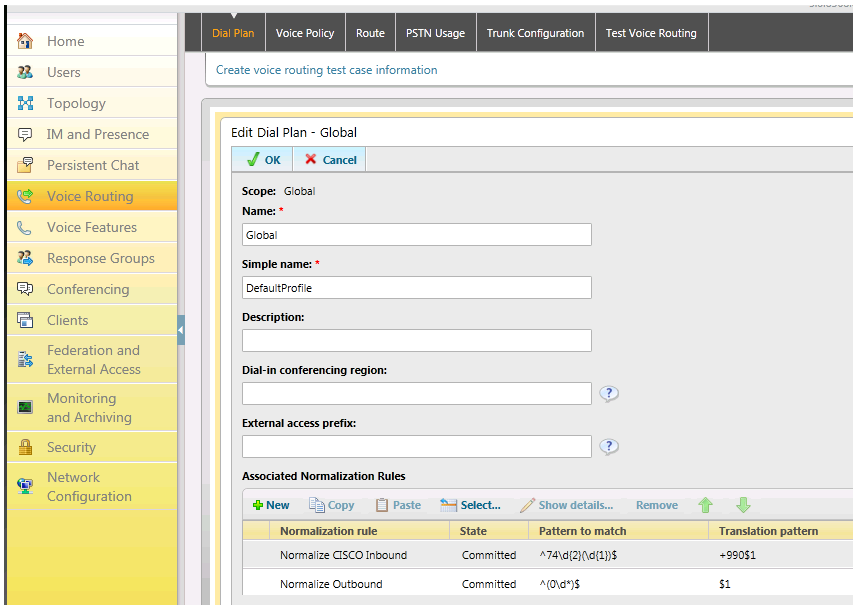


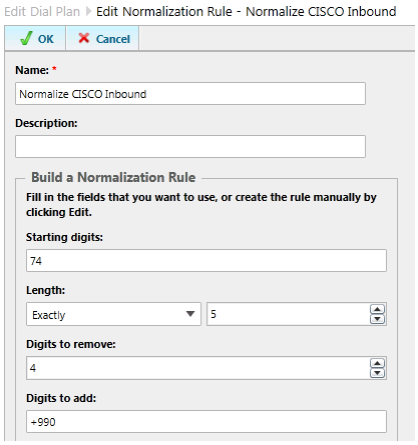
All other values are set to <Automatic>

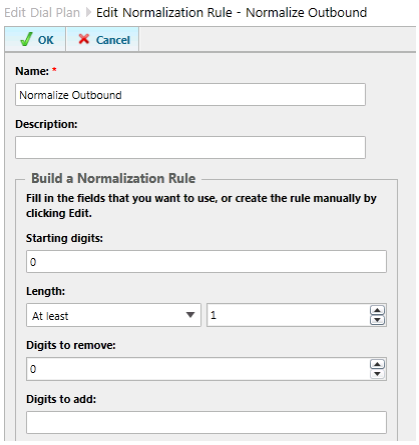
Lync Server Control Panel, Voice Routing, Dial Plan, “Global”

The associated Normalization Rules are used for the following number conversions:

Dialed number	Converted number	Description
74??x	+990x	Normalize inbound numbers from Gateway
0x	0x	Normalization rule for outbound calls (it does not change the number but it must exist to allow outbound calls)

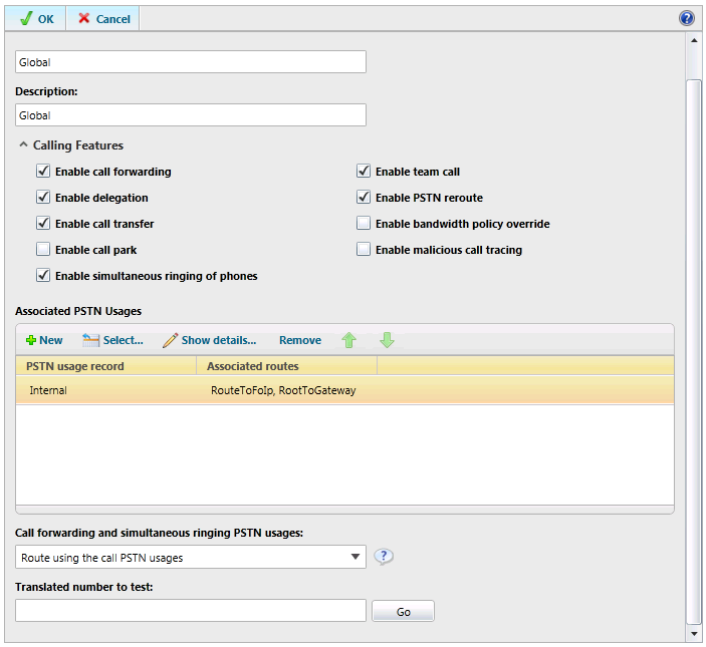




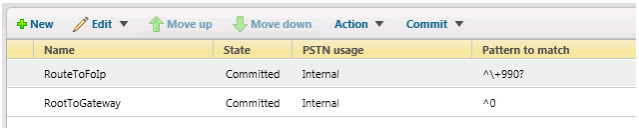


Lync Server Control Panel, Voice Routing, Voice Policy, “Global”

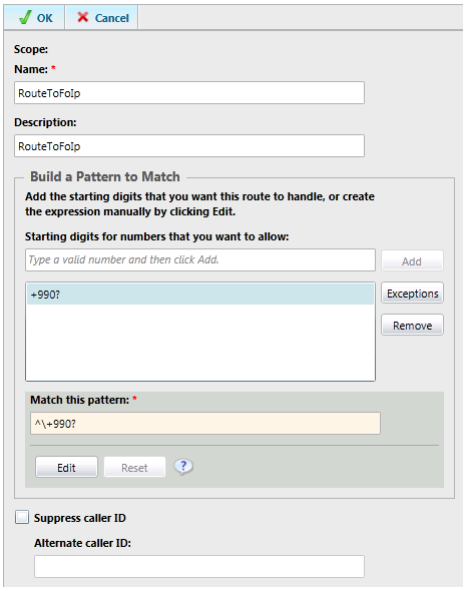
Edit Voice Policy - Global



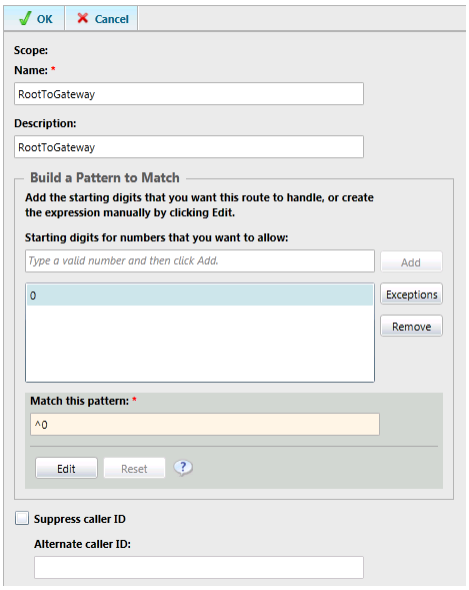
Lync Server Control Panel, Voice Routing, Voice Policy, Route

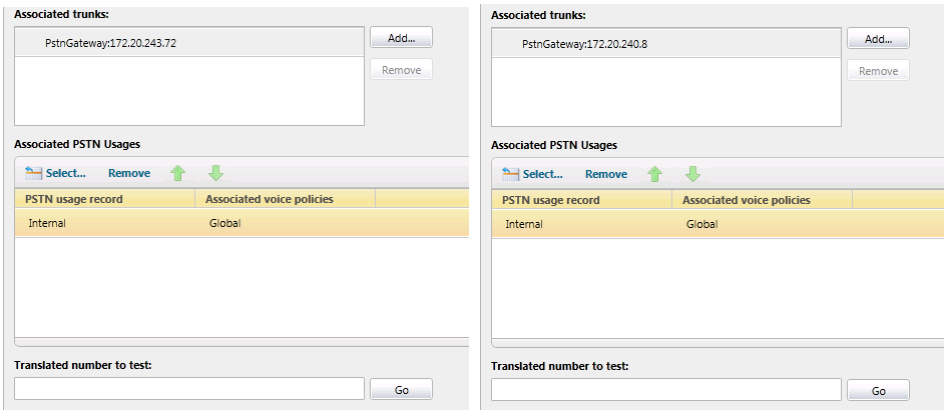


Edit Voice Route - RouteToFoIp

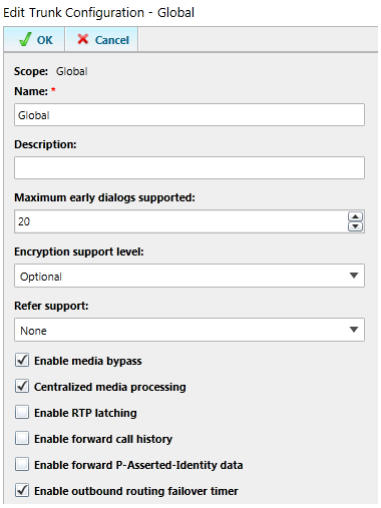


Edit Voice Route - RootToGateway

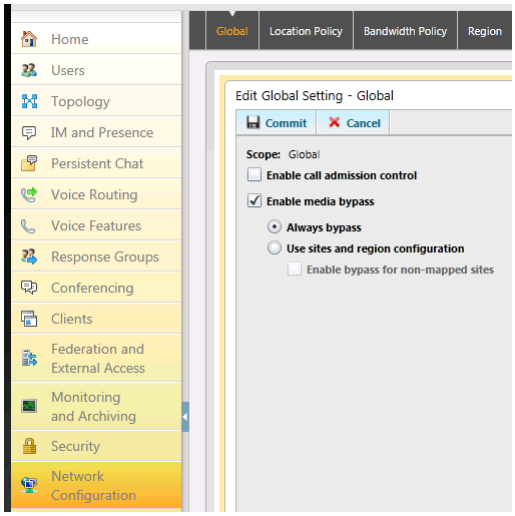




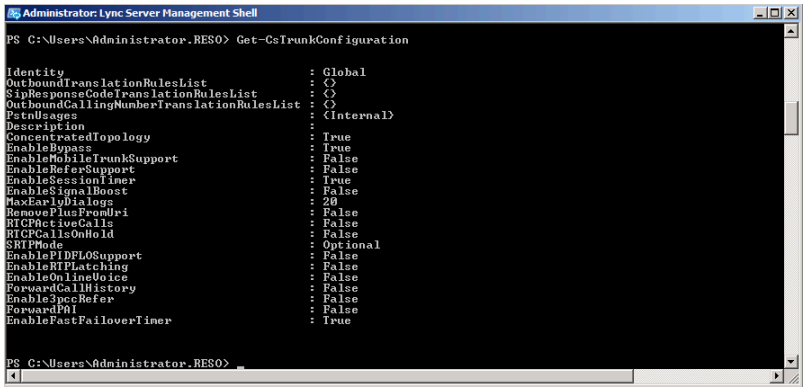
Lync Server Control Panel, Voice Routing, Voice Policy, Trunk Configuration, “Global”



Lync Server Control Panel, Network Configuration, Global, “Global”



Lync Server Control Panel, Trunk Configuration



Use Cases

1. Internal call from KCS FoIP to Lync User “AU2” (such as, Voice Player)
   a. KCS FoIP calls the number +9902
   b. Lync user “AU2” gets the call
2. Internal call from Lync User “AU2” to KCS FoIP (such as, Voice-mailbox access)
   a. The Lync user “AU2” calls the number +9901
   b. KCS FoIP (+9901) get the calls
3. Inbound call from telephone/fax via PSTN Gateway to Lync user “Tester03”
   a. Telephone calls 734-74002
   b. The Mediation server gets the incoming call with extension 74002 and normalizes the number to +9902
   c. Lync user “AU2” has the telephone number +9902 and it gets the call.

4. Inbound fax from fax via PSTN Gateway to KCS FoIP
   a. The fax calls 734-7401
   b. The Mediation server gets the incoming call with extension 7401 and normalizes the number to +9901.
   c. KCS FoIP (+9901) gets the inbound call.
5. Outbound call from Lync User via PSTN Gateway to external telephone or fax.
   a. The Lync user “AU2” calls the number 0142
   b. The call is routed via PSTN Gateway to the telephone/fax at 0142
6. Outbound call from KCS FoIP via PSTN Gateway to external telephone or fax.
   a. KCS FoIP calls the number 0142
   b. The call is routed via PSTN Gateway to the telephone/fax at 0142

Enable Encryption of SIP Messages

The description in this chapter assumes that you have a working integration as SIP trunk without security as described in Integration as SIP Trunk Without Encryption above.

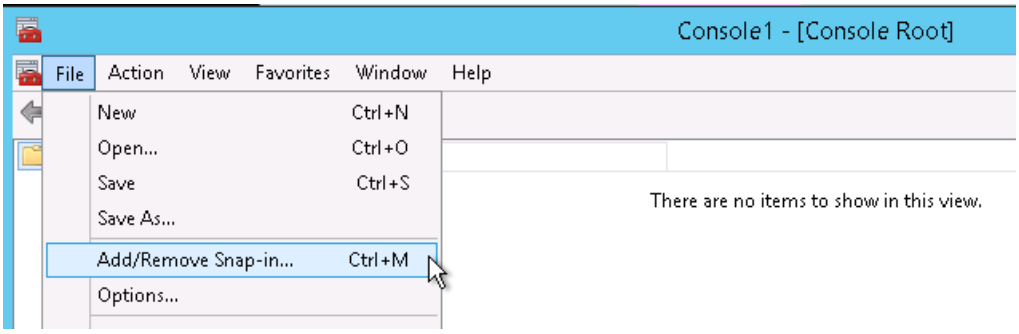
Create SSL Key for FoIP Using the Windows Domain Controller

This section describes how to get an SSL key as PEM format using the Windows Domain controller certification authority. You can also use any other Certification Authority to generate an SSL key as described in the KCS Web Services (TWS) for KCS manual.

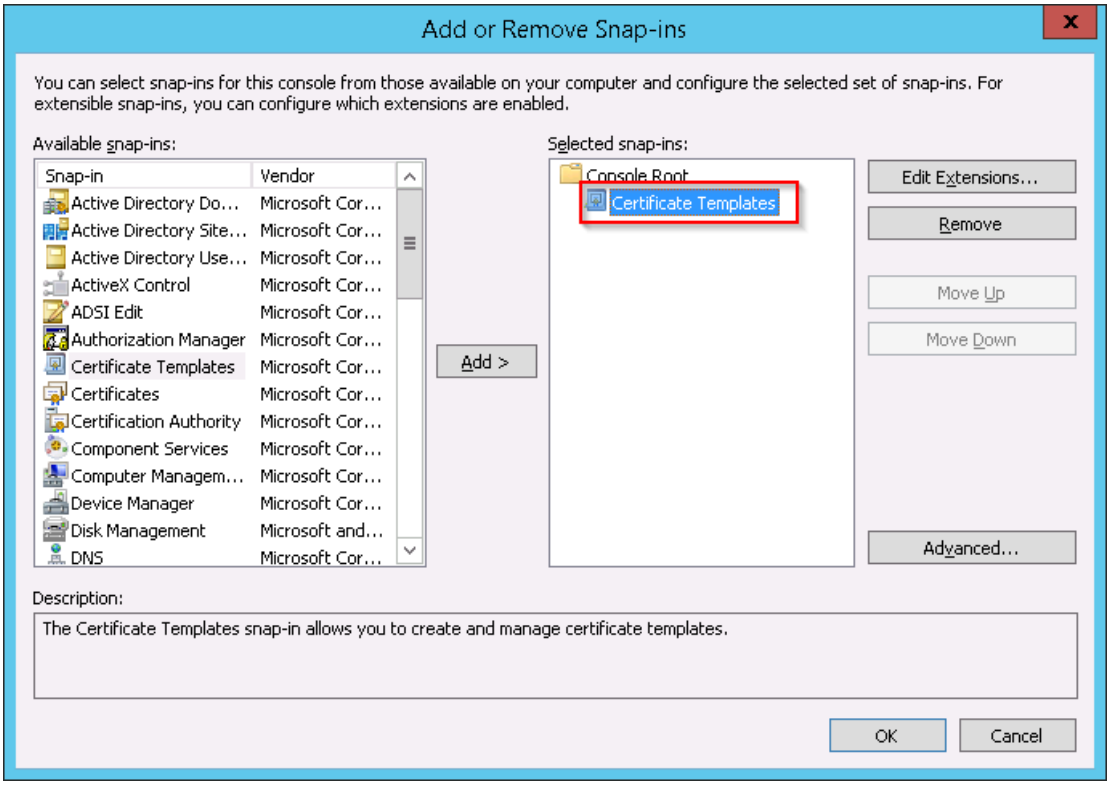
Part 1: Create a Web Service Certification Template with exportable keys

This part has to be done once on the domain controller. If you already have an appropriate template, you can re-use it. This description assumes that the template is called “Web Server 2”.

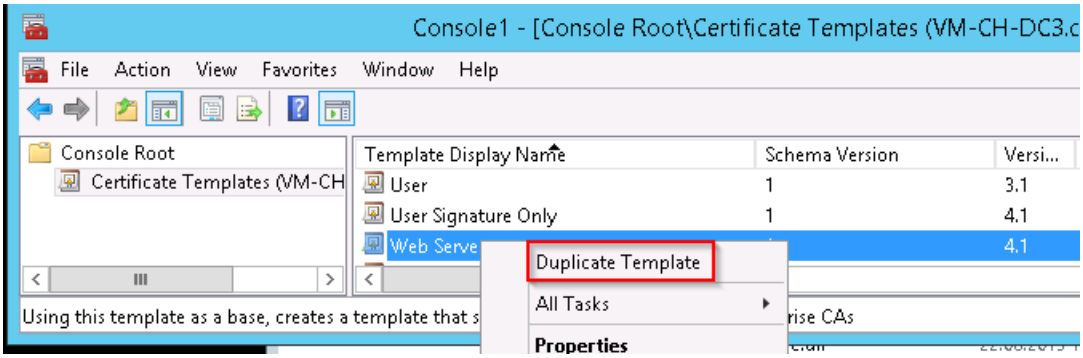
1. Log in to the domain controller (as domain admin) and run mmc.exe to open the Windows Management Console. Select File -> Add/Remove Snap-in.



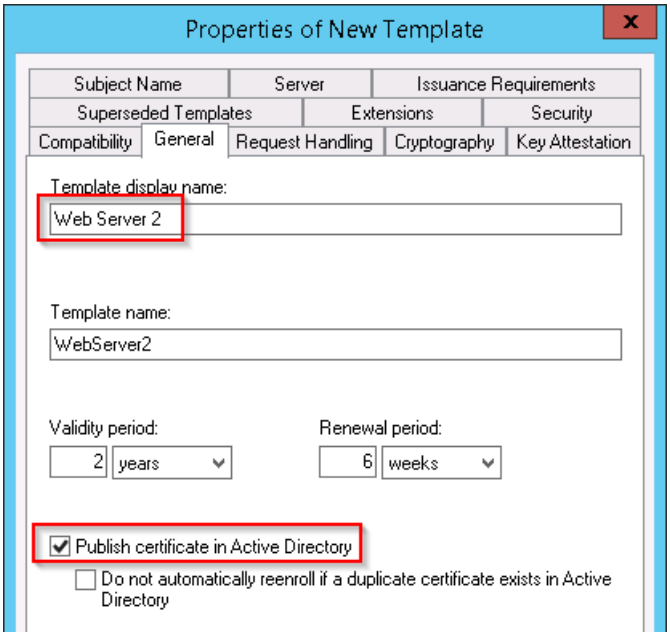
2. Ensure that the snap-in for Certificate Templates is enabled.



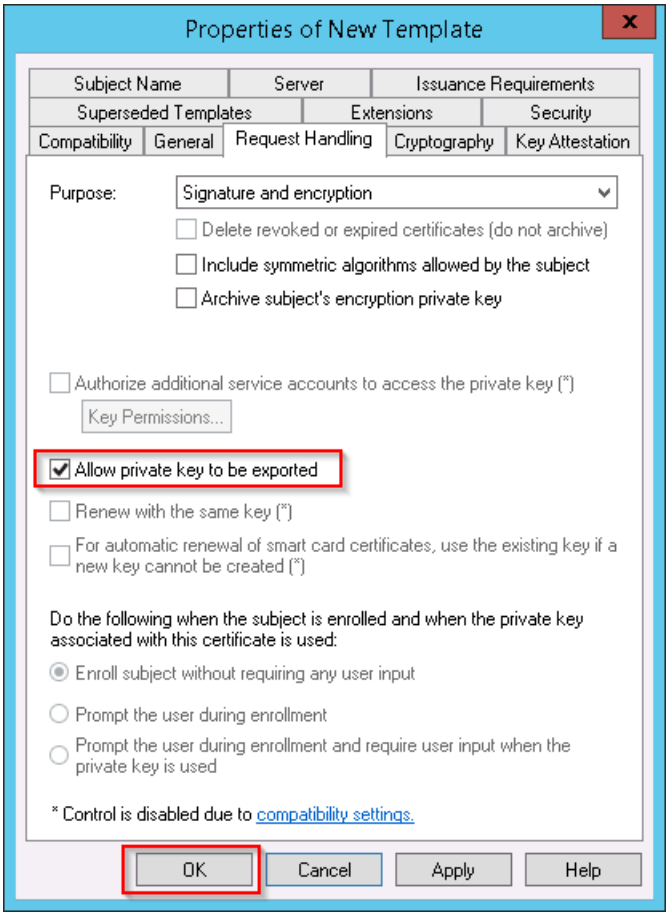
3. Activate “Certificate Templates”, select the template “Web Server” and start the action “Duplicate Template”



4. Select a display name for the template and enable publish certificate in Active Directory. Optionally change the validity period.

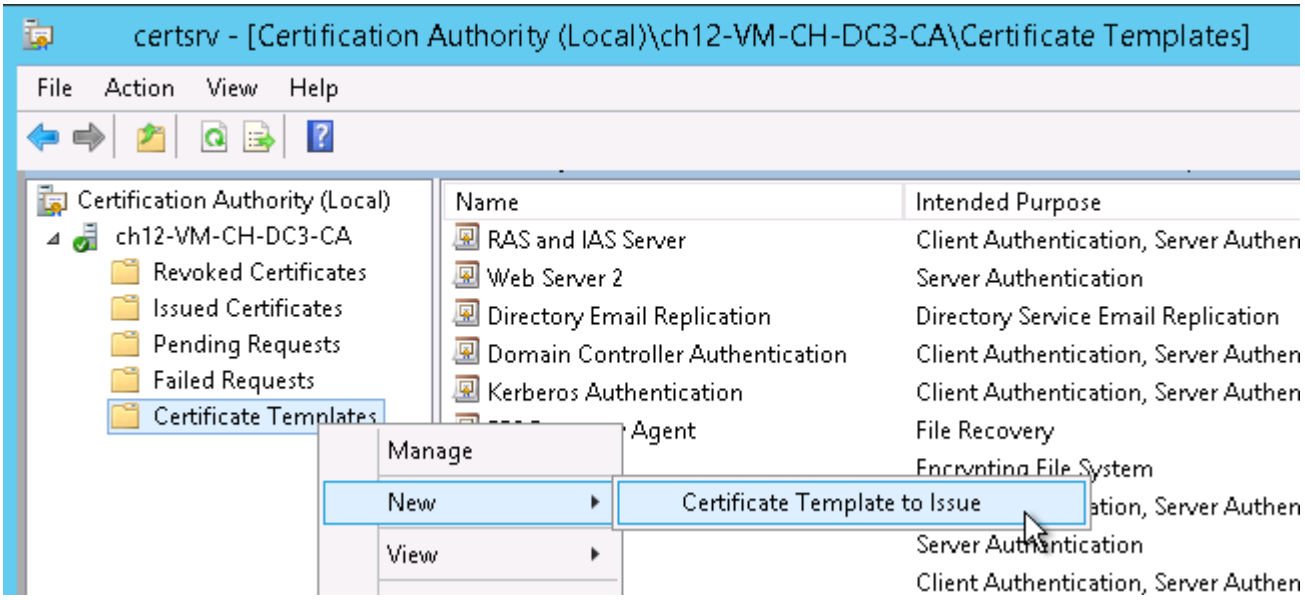


5. Allow export of private keys and then click OK to save the template.

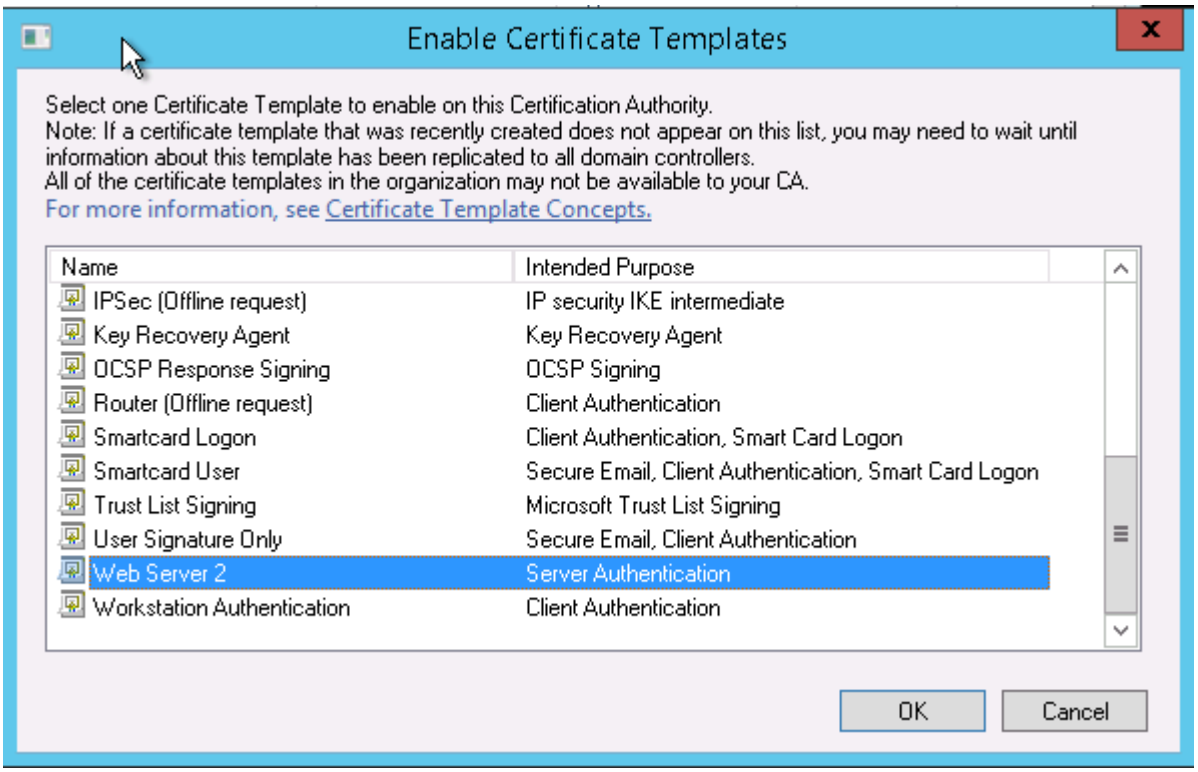


6. Close the management console. It is not required to save the console settings.

7. Open **Administrative Tools** > **Certification Authority** > **Certification Templates**. Select **New** > **Certificate Template**to Issue

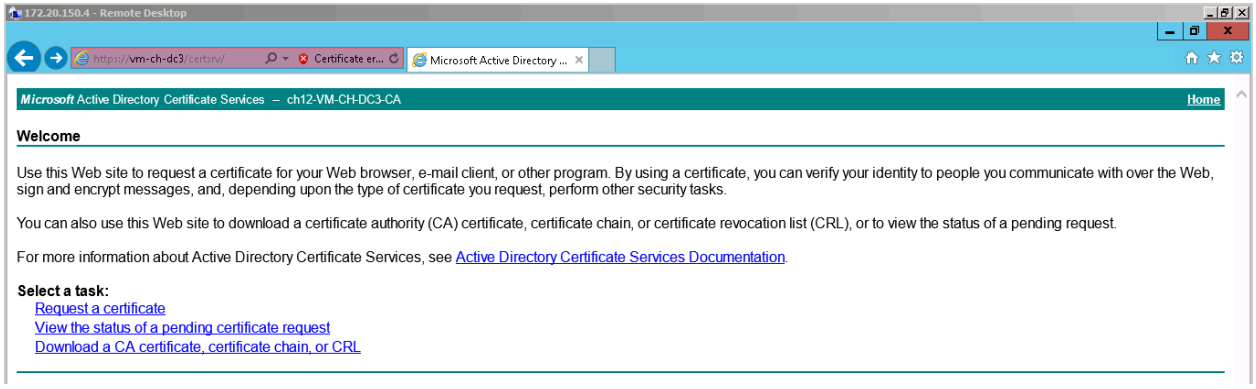


8. Select “Web Server 2“:

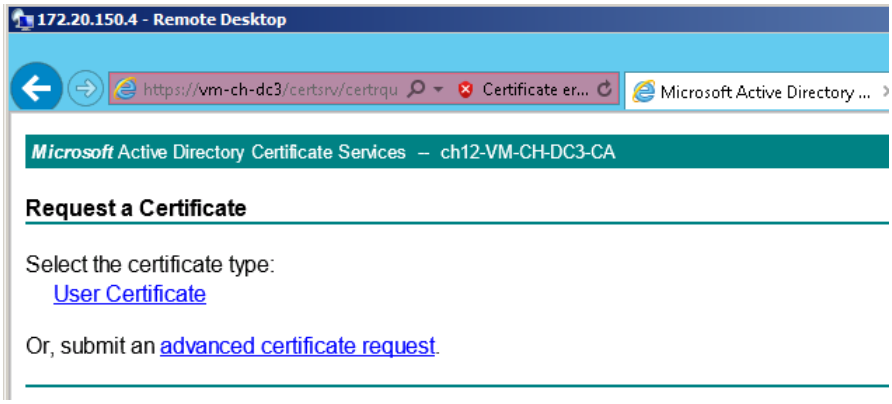


Part 2: Generate a new key as PEM Format

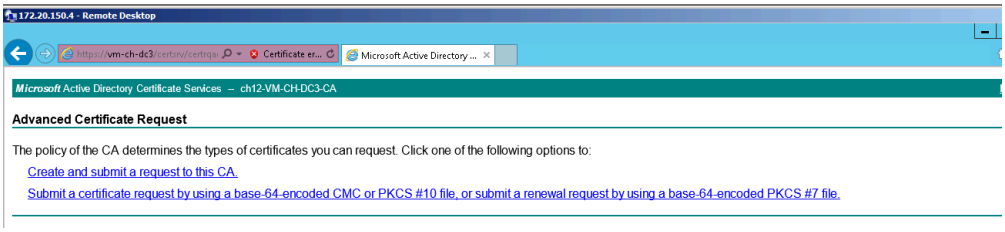
1. Open the Active Directory Certificate Server with url https://{Domain-Controller}/certsrv:



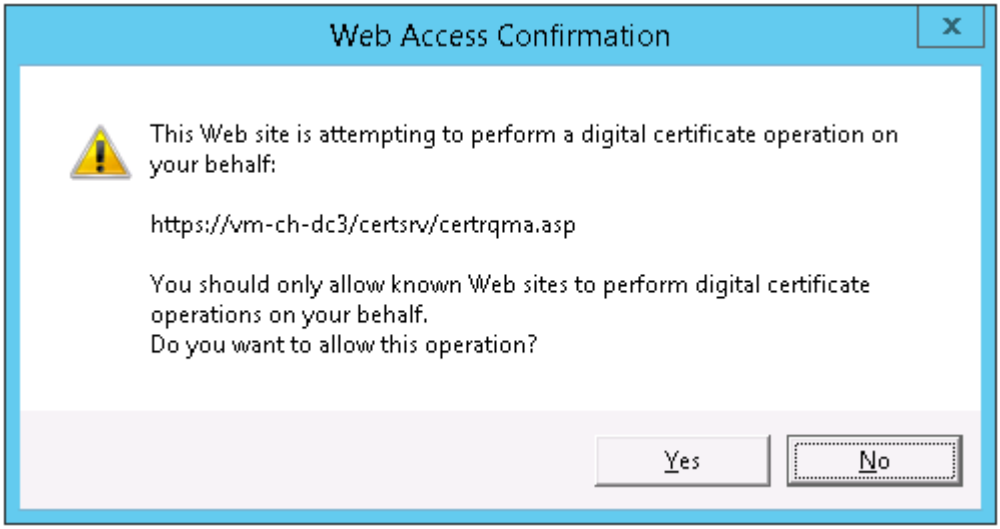
2. Select “Request a certificate”



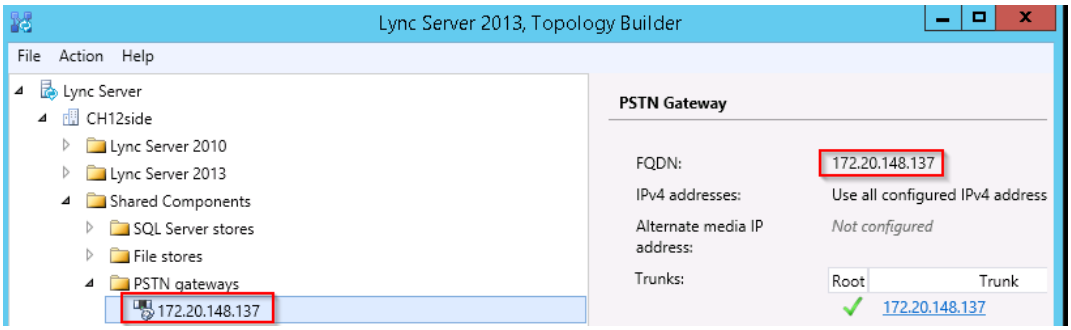
3. Select “advanced certificate request”

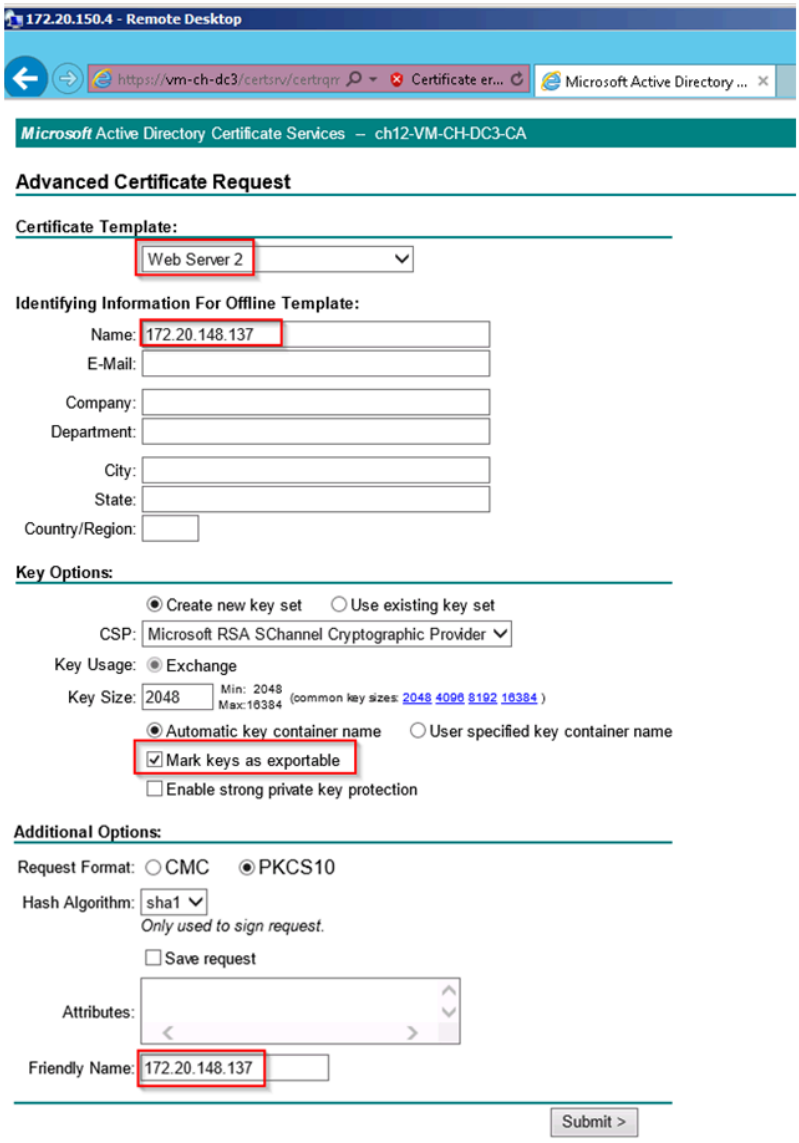


4. Select “Create and submit a request to this CA” and confirm the following operation:



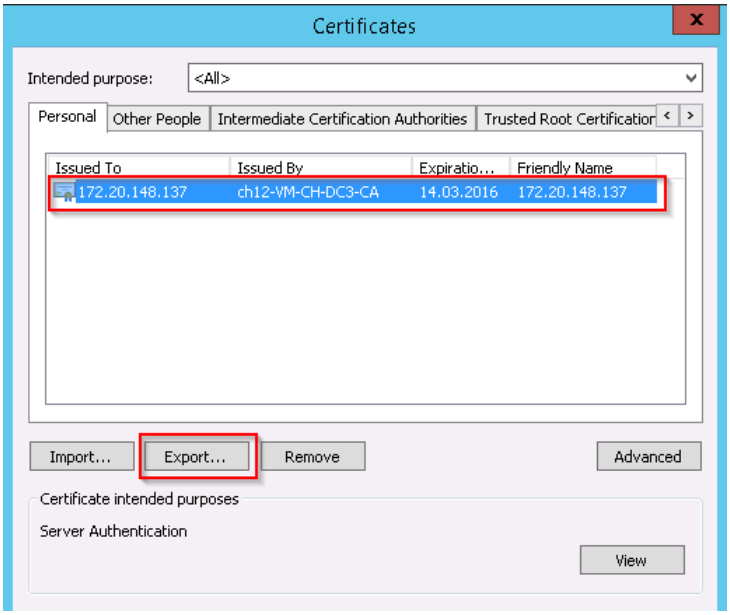
5. Fill out the certificate request as shown below. Take care that template “Web Server 2” is used and that the Name matches both with Host/IP of KCS FoIP and the configured gateway name in the Lync Topology Manager. Finish input with the “Submit” button:





6. You get the issued certificate. Click “Install this certificate”

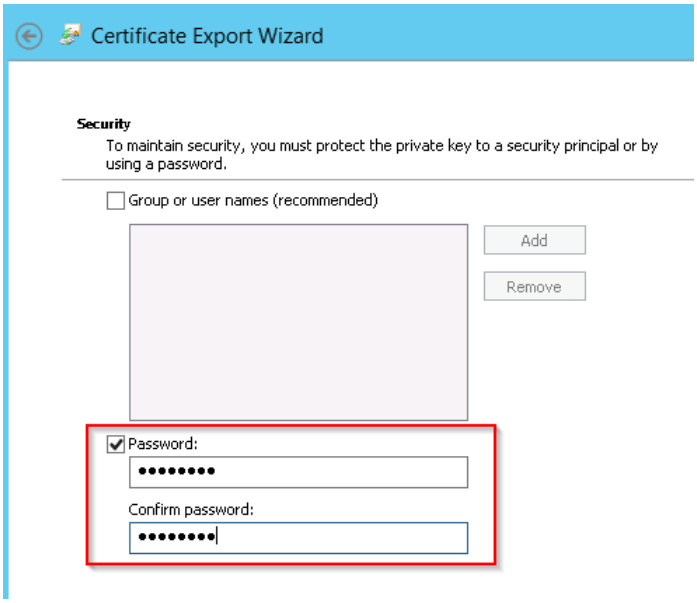
7. Open **Internet Options** > **Content** > **Certificates**. Select the installed certificate and then click Export:



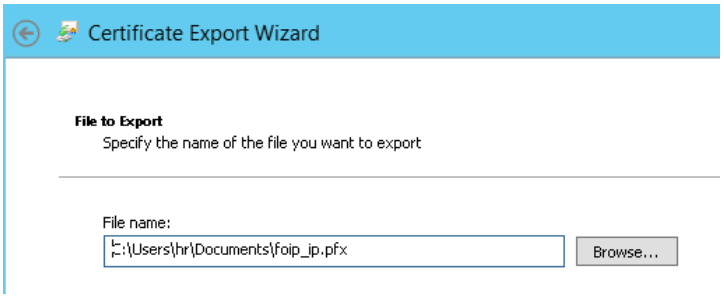
8. On the 2nd page of the export wizard, select to include the private key.

9. On the 3rd page select PKCS#12 format as shown below:

10. Protect the key with a password.



11. Save the certificate is .pfx file



12. Confirm to finish the export:

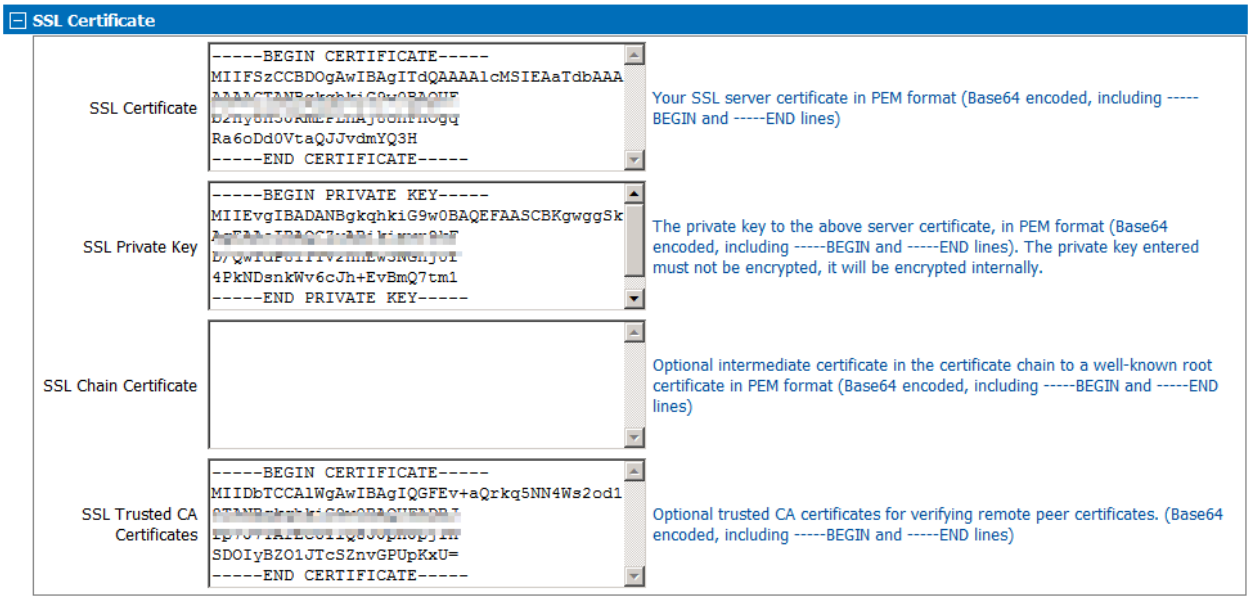
13. Convert the generated file foip_ip.pfx with the openssl command-line
openssl pkcs12 -in foip_ip.pfx -out foip_ip.pem -nodes
Into a PEM file foip_ip.pem. You will be prompted for the password used in step 10 above.

The resulting PEM file is required in the FoIP Configuration as described in the next chapter.

Configure the SSL key in KCS FoIP

This description assumes that you have created an SSL key as PEM format as described in the previous chapter. The keys and certificates insides this PEM files must be saved in the KCS FoIP configuration section as shown in the screen shots below:

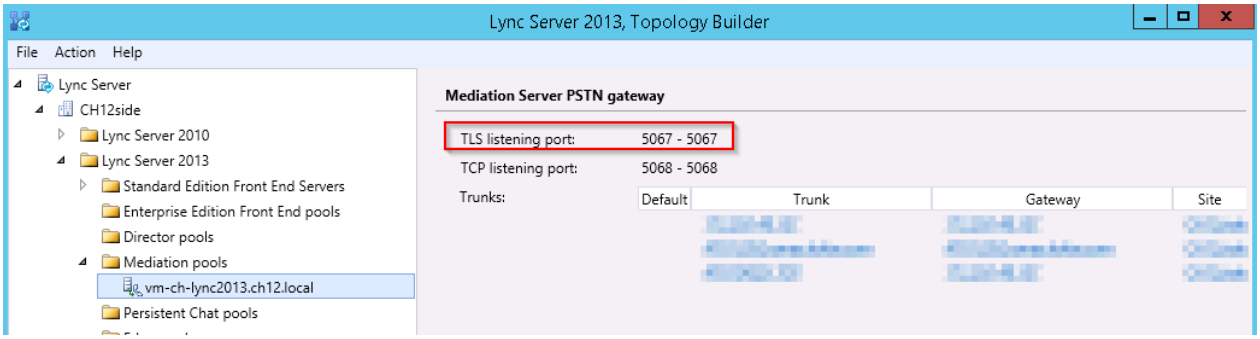

```
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: le-b0fe5308-bf16-4da5-a5c0-1c1a3466a038
    Microsoft CSP Name: Microsoft RSA SChannel Cryptographic Provider
Key Attributes
    X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCZyABikixwr9kF
FOYpoMN3/eoYVRd6MeeLLx7kZMbng3FLwYlxngnOx92qiLOuYcgrYAul3puTpHupP
XwWQjx2agIPBRI8I2zyRMe5dKmezsX1urudXkIGBfqN8FwoZrQW1nd77MKD4HDeP
R6xAy/W4VhY3i4K/sBVAZPbnE/kScnOptUJ1zwXiD/QwTdP81TYV2nhEw3NGnjOf
4PkNDsnkWv6cJh+EvBmQ7tm1
-----END PRIVATE KEY-----
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: 172.20.148.137
subject=/CN=172.20.148.137
issuer=/DC=local/DC=ch12/CN=ch12-VM-CH-DC3-CA
-----BEGIN CERTIFICATE-----
MIIFSzCCBDOgAwIBAgITdQAAAAlcMSIEAaTdbAAAAAAACTANBgkqhkiG9w0BAQUF
ADBJMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRjaDEw
y2uZQ6u+jKb7VGzFoVEQN42XhmKjSxJ+cgbHLnwQOj/RgrdaIy8YszCc8gB62bNb
kjBIs4R5merEU6ddQkE/uTUGOUXvADmzsV1TC7M1b2ny8H5JRmEPLnAj8ohFhOgq
Ra6oDdOVtaQJJvdmYQ3H
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/DC=local/DC=ch12/CN=ch12-VM-CH-DC3-CA
issuer=/DC=local/DC=ch12/CN=ch12-VM-CH-DC3-CA
-----BEGIN CERTIFICATE-----
MIIDbTCCAlWgAwIBAgIQGFEv+aQrkq5NN4Ws2od18TANBgkqhkiG9w0BAQUFADBJ
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRjaDEwMRcw
fK9hbIEGZbTOjZAOqhuTOB9Zw1OwRIs2IyYmKMQOIp787YAIEC0TIQ8O0pHOpjIn
SDOIyBZO1JTcSZnvGPUpKxU=
-----END CERTIFICATE-----
```



Note The “SSL Trusted CA Certificates” are only required if the certificate check is enabled in the SIP section of the FoIP configuration.

Enable SIP via TSL in the Lync Mediation Server

1. Open the Lync Server 2013 Topology builder, download the current topology and ensure that at least one TLS listener port is enabled in the used Mediation server.



2. Publish the topology if you made some changes.

Change Trunk Configuration from SIP/TCP to SIP/TSL

This section assumes that you have completed all steps as described in sections Create SSL Key for FoIP Using the Windows Domain Controller through Configure the SSL key in KCSFoIP. It is recommended that you verify that your installation is still working with TCP before you do the changes described in this section.

KCS FoIP Configuration Changes

1. Change the remote port in the used call-peer to the TLS listener of the used mediation server (see Enable SIP via TSL in the Lync Mediation Server)

2. Enable SIP via TSL in the SIP signaling.

Note

- The enabled transports may include SIP/UDP and SIP/TCP in addition to SIP/TSL.
- The outgoing sip transport must be set to SIP/TSL.

Lync Server Topology Changes

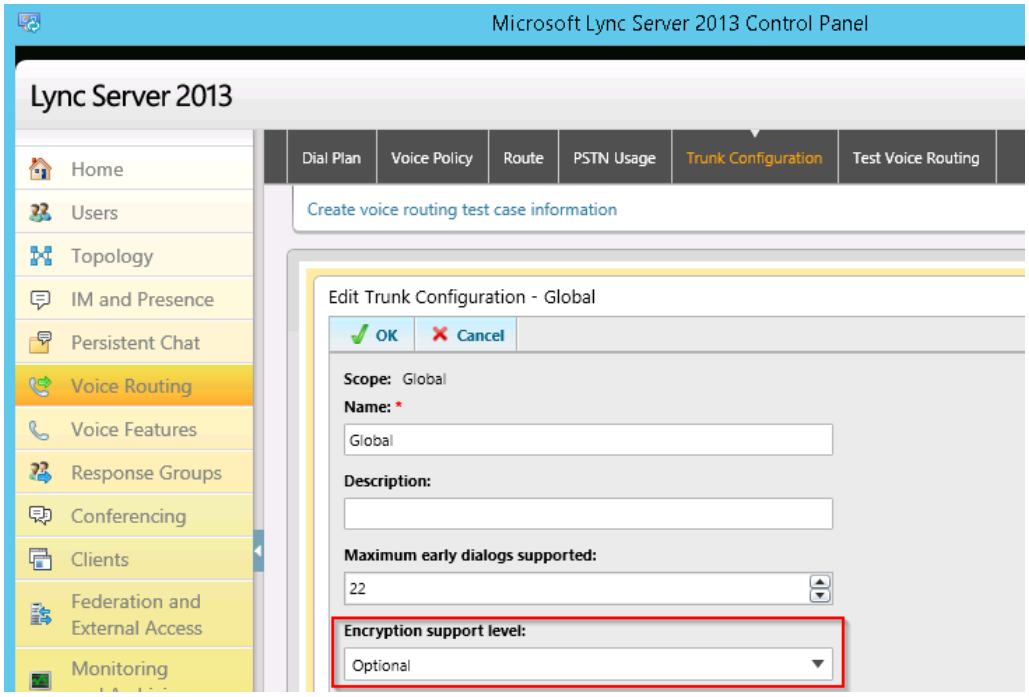
1. Open the Lync Server 2013 Topology builder und download the current topology.
2. Open the properties of the used Trunk and change the SIP transport protocol to TLS. Set the “Listening port for IP/PSTN gateway” to the “Local sips port” configured in KCS FoIP. Set the “Associated Mediation Server” port to mediation server TLS listener that is also used as remote port in the FoIP call-peer.

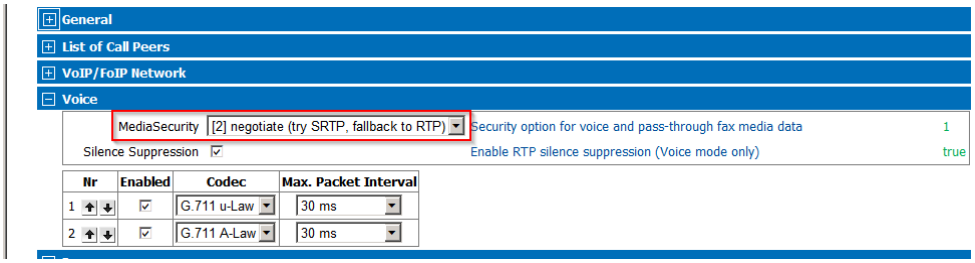
3. Publish the modified topology.

Enable Media Encryption (SRTP)

The media encryption mode can be configured both in KCS FoIP (configuration value Voice -> Media Security) and the Lync Server (**Lync Server Control Panel** > **Voice Routing** > **Trunk Configuration** > **Encryption support level**).

It is recommended to set the Lync Trunk encryption level to "Optional" and the FoIP Media Security to "Negotiate" as you can see in the screen shots below. Such a configuration will automatically use media security if SIP via TSL is used.





All supported values are shown in the table below:

SIP Transport	Lync Server Trunk encryption level			FoIP Media Security				Media
	Not Supp.	Optional	Required	Disabled	Negotiate	Always		Encryption
TCP	#	#	-	#	#	-		No
TSL	#	#	-	#	-	-		No
TSL	#	-	-	#	#	-		No
TSL	-	#	#	-	#	#		Yes

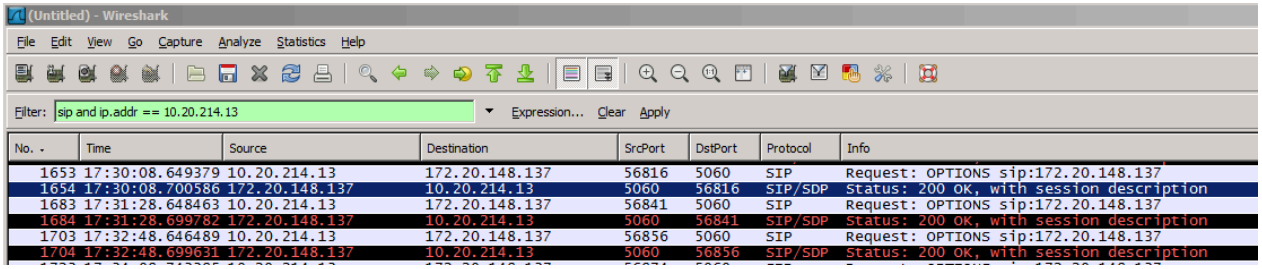
Note The Media Bypass is ignored if media encryption is supported by one side of the call only. In that case, the media data is always transferred via mediation server which uses RTAudio compression that prevents reliable fax transmission!

Troubleshooting and Hints

Here are some Lync Server specific hints. See also Hints for general hints.

Verify SIP Connection Between FoIP and Mediation Server

After FoIP is configured as gateway, the Lync Mediation starts sending SIP OPTIONS requests approximately once in 80 seconds. You can see the OPTIONS requests as SIP messages in the network trace.



If do not have any network trace you can also check the FoIP trace for GetServerState messages (from sip to fx7)

28/12:25:11.510 (3c2c/390c/08d8) Dump-Req: Message 'GetServerState' (203 byte) from 1(sip) ---> 3(fx7) 28/12:26:31.494 (3c2c/38a0/08da) Dump-Req: Message 'GetServerState' (203 byte) from 1(sip) ---> 3(fx7) 28/12:27:51.489 (3c2c/1500/08dc) Dump-Req: Message 'GetServerState' (203 byte) from 1(sip) ---> 3(fx7)

Call Failure with SIP Status 488

Microsoft Lync Server expects that the Gateway has the DTMF capability enabled. Otherwise, calls fail with Sip Status “488 Invalid incoming Gateway SDP: Gateway ParseSdpOffer Error: No DTMF support on Gateway side”.

If you see this problem, ensure that the configuration option EnableRtpNte is enabled in the SIP section of the FoIP configuration.

Call Failure with SIP Status 404

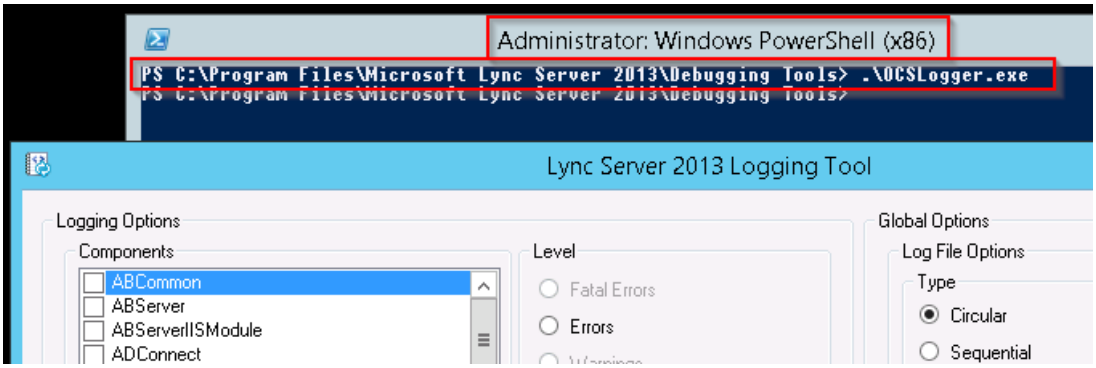
Sip status 404 indicates that the dialed number is invalid. Here are some troubleshooting hints:

- Open the **Lync Server Control Panel** > **Voice Routing** > **Test Voice Routing**.
- Create a Test with the used number and verify the expected number translation, PSTN usage and route.
- Check associated trunks in the used route.

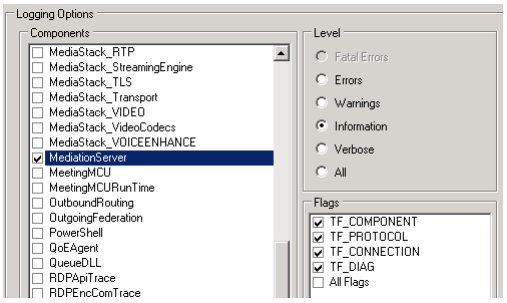
Using the Lync Server Logging Tool

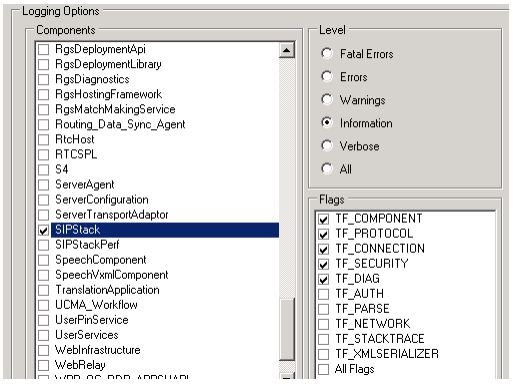
In some cases it is helpful to get more details about a failed call from the Lync Server logs as described below.

1. Install the Microsoft Lync Server 2013 Debugging Tools (can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=35453).
2. Open a power-shell as an Admin.
3. Change to the debugging tools installation folder and run OCSLogger.exe. After a few seconds you should see the “Lync Server 2013 Logging Tool” window.



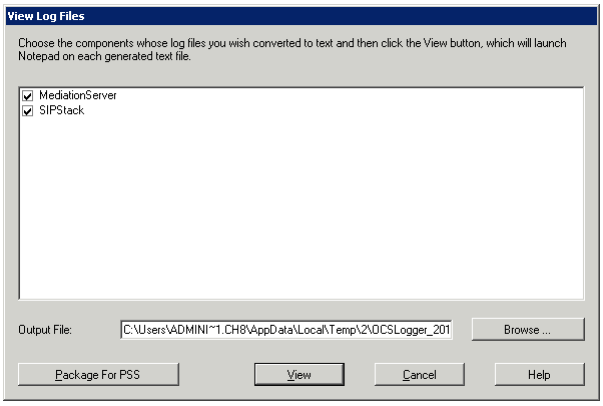
4. Enable logging in the Mediation Server and SIP Stack as shown the following screen shots:



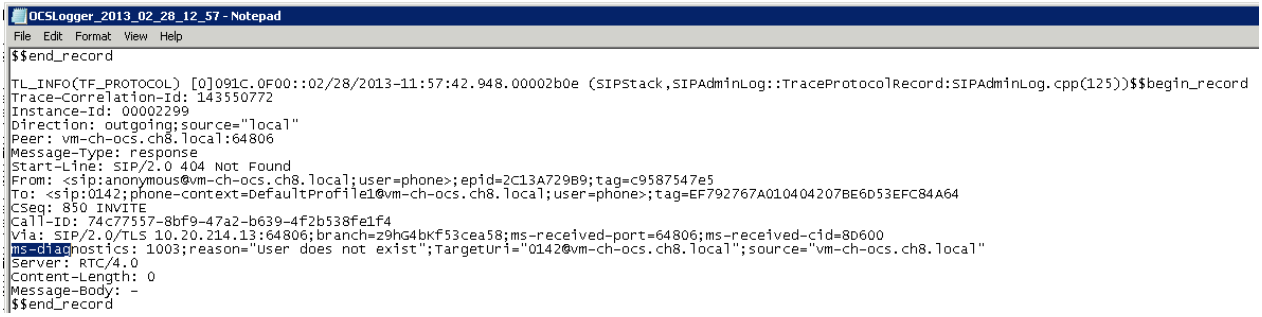


5. Click “Start Logging” to start generation of log data.
6. Click “Stop Logging” to stop generation of log data.

7. Click “View Log Files” and then “View” in order open the log data in a text editor.



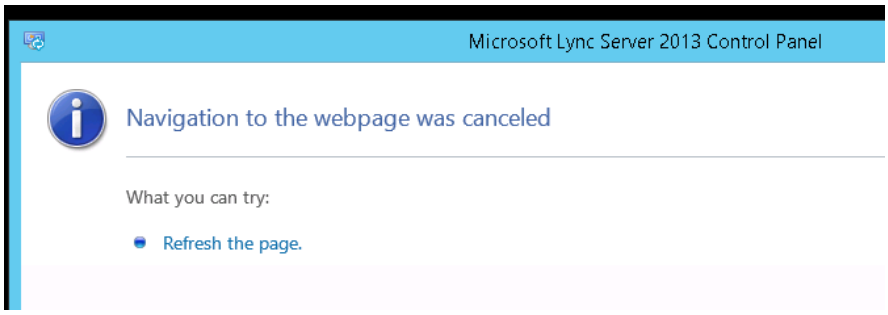
8. In many case you will get a good hint for the failure when searching for lines with “ms-diagnostics”. See example below:



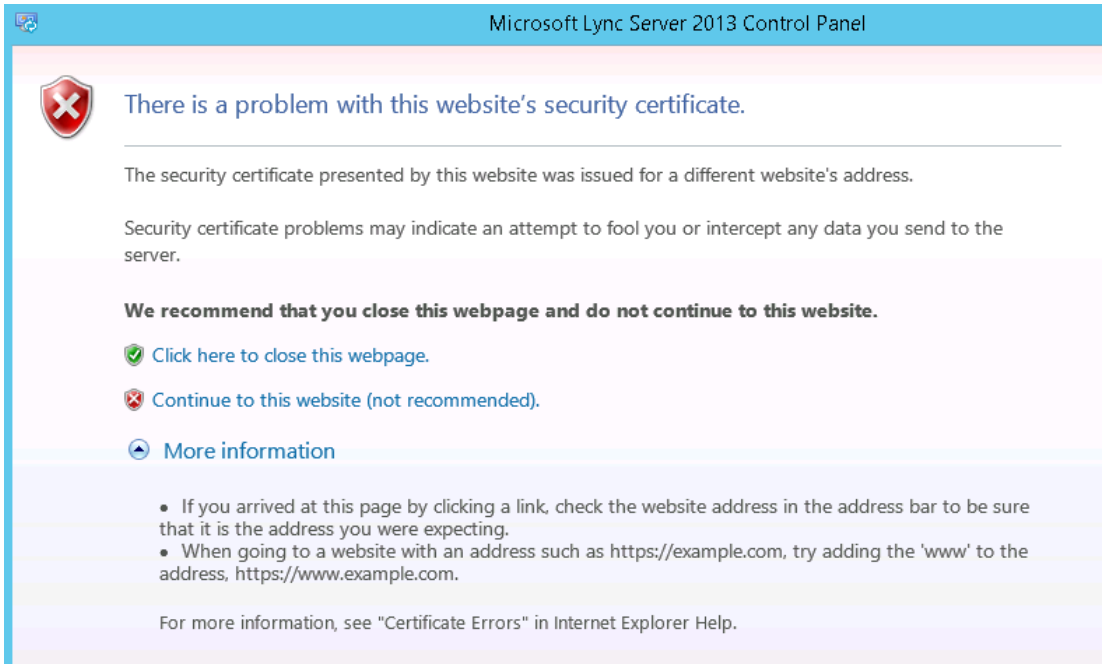
Some Lync Services Fail to Start

For some unknown reasons it may happen that the Lync Services do not start anymore due to any issue with the Lync Server certificates. In that case you will see the following symptoms:

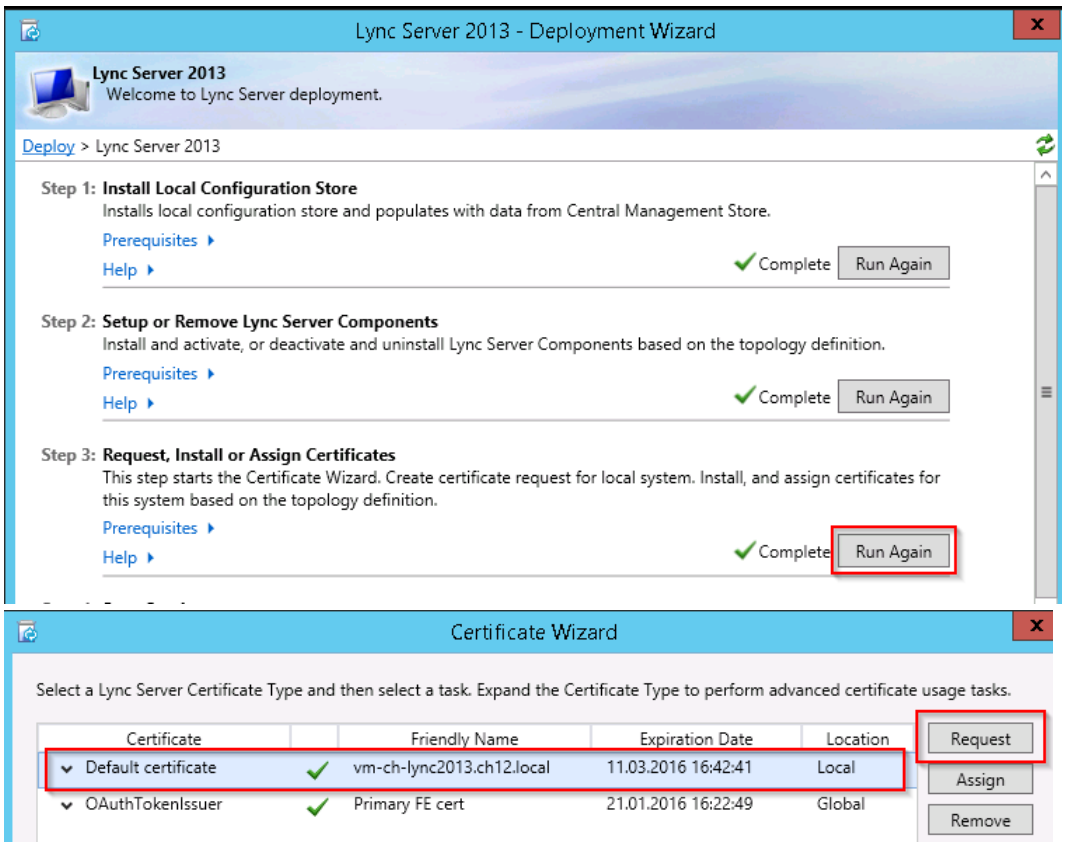
- Important services like “Lync Server Mediation” and “Lync Server Front-End” fail to start up.
- When you open the Lync Server Control Panel you will get a security warning as shown in the screen shots below.



After Refresh you get the following certificate warning:



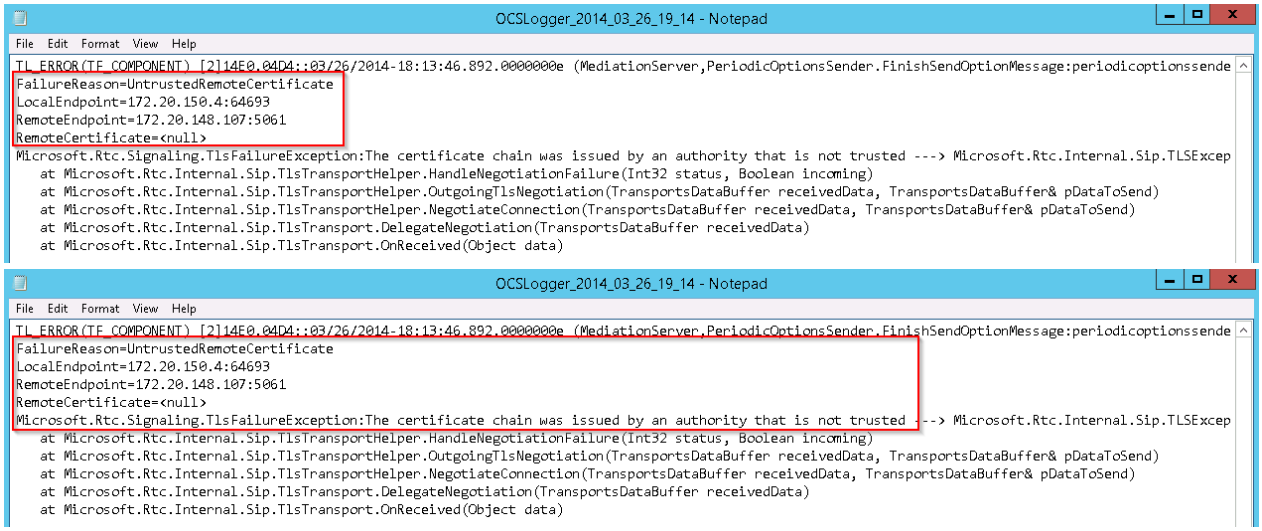
This problem can be fixed by rerunning step 3 of the Lync Server – Deployment Wizard.



Sip Trunk via TSL Does Not Work

If your TSL connection is not working it is recommend to search for “TlsFailure” in the Lync Server trace.

An example trace output when using an SSL key that is not trusted by the Lync server is shown in the screen shot below:



Configure a valid SSL key as described in Configure the SSL key in KCS FoIP.

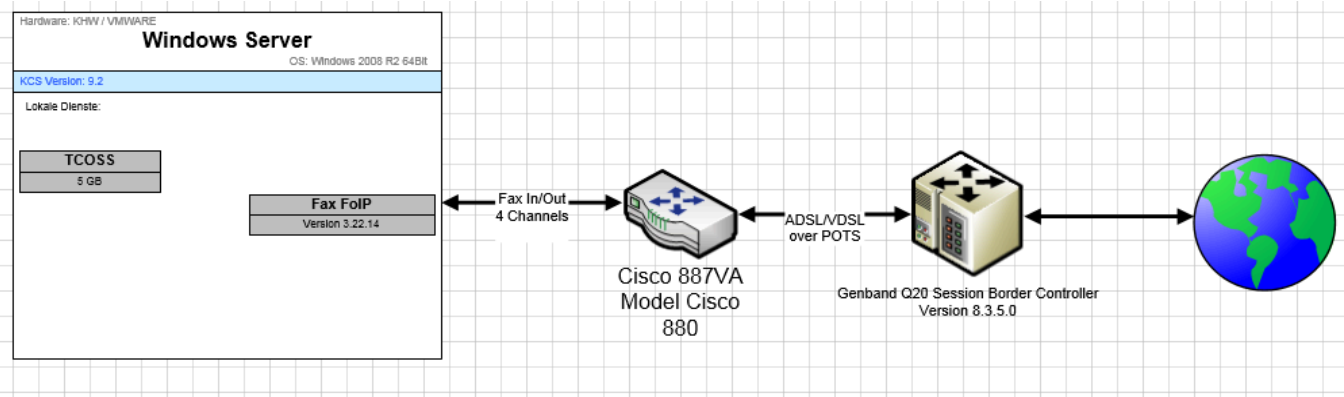
Chapter 4

Integration with SIP Providers

This section describes integration with SIP providers.

Swisscom SIP Trunk

The integration with Swisscom SIP trunks will be supported with FoIP for KCS 10.0 or higher. It has been certified using the following system overview:



Used 3rd party software/hardware versions:

- Genband Session Border Controller 8.3.5.0
- Aastra 415, Aastra 430, Aastra 470 Release 3.0 Software-Version 8428b1

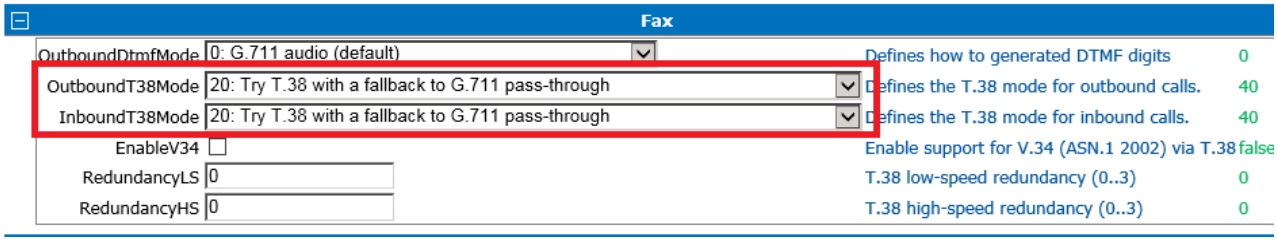
FoIP Configuration

1. Configure the SIP trunk the Genband Session Border Controller:

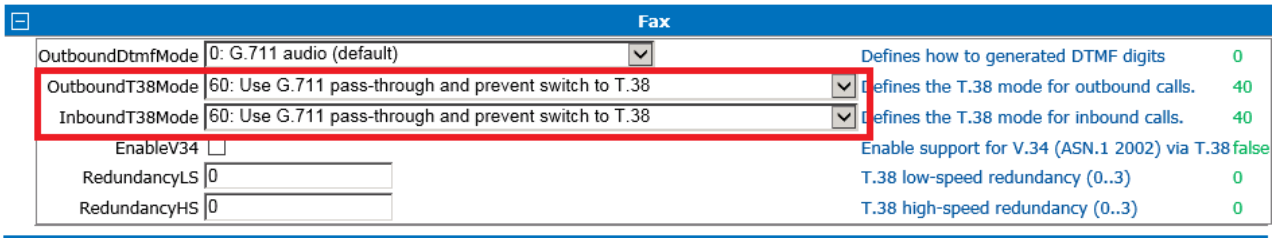
List of Call Peers

Nr	Enabled	Protocol	Remote Address		Authorization		Reg. Numbers
			Host	Port	User ID	Password	
1	☑	SIP	195.176.152.148				

2. Change the fax inbound/outbound mode to 20 (for T.38 mode) or 60 (for pass-through mode):

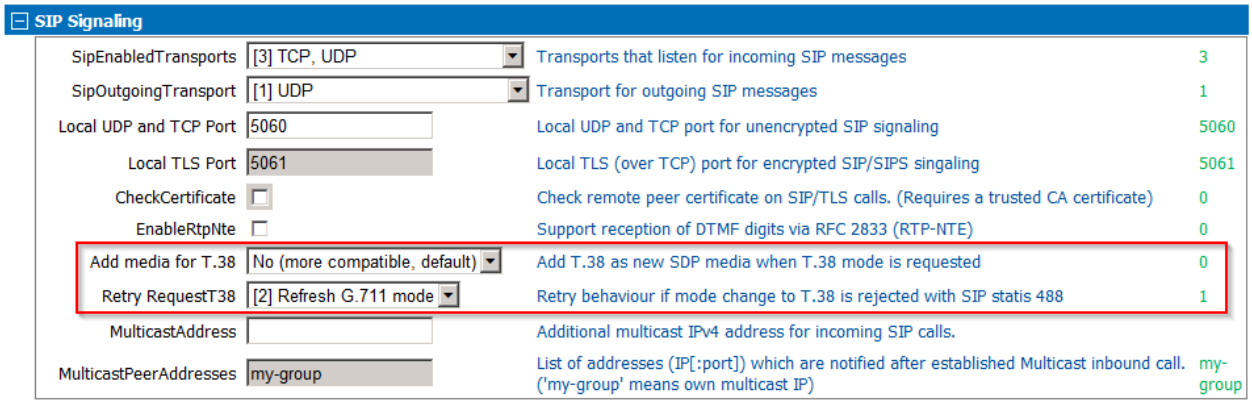


or



3. Change the SIP parameters “Add media for T.38” and “Retry RequestT38” as shown in the screen shot below:

Note Option “Add media for T.38” will be set to “Yes”, if a Swisscom SIP trunk installation with KCS FoIP 10.0.1 is updated. It is recommended to change this value to “No” in order to fix bug 672110.



4. Set the own telephone number (caller–id) in the Fax over IP channel configuration as described in the TCOSS system manual chaper “Cost Center Parameter, Caller ID”. An example with number 0123456789 in configuration lines 276 to 279 is shown below:

```
'8*~=0123456789%TI~ ,     276
   '80~=0123456789%0~  ,     277
   '8I~=0123456789%I~  ,     278
   '8~=0123456789%~    ,     279
```

Chapter 5

Recommended Tools and Hints

This section describes recommended tools and hints.

Tools

This section describes recommended tools.

MyPhone (H.323 Telephone Software)

MyPhone is a freeware application (available from http://myphone.sourceforge.net). It can be used to test a H.323 connection. This section describes how to test a direct connection to a gateway using H.323 with MyPhone.

Prerequisites

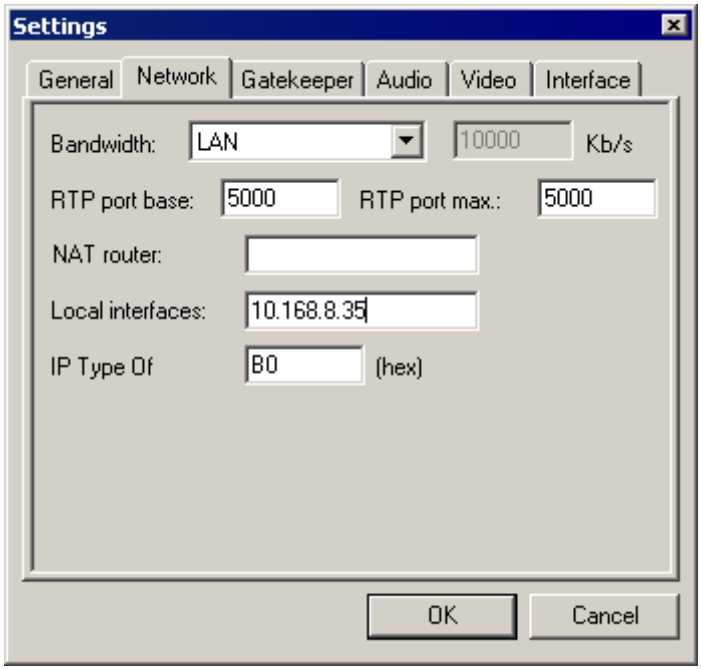
- Make sure that MyPhone 0.2b12 or higher is running on the Windows machine.
- LAN connection between the gateway and the Windows machine must be allowed with the following ports and protocols in both directions (check firewall configuration)

Port	Type	Purpose
1720	TCP	H.323 call setup
1024 – 65535	Dynamic TCP	H.245 (call parameters)
1024 – 65535	Dynamic UDP	RTP (audio and fax stream data) RTCP (control information)

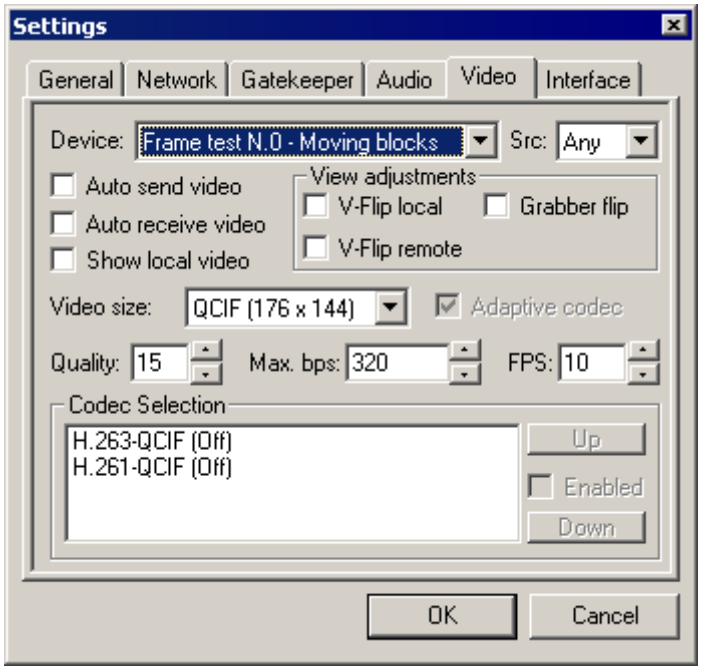
MyPhone Configuration

If MyPhone issues an error on startup like "Could not open H.323 listener interface <local-ip>", another process may be running which listens on one of the ports listed in *Prerequisites* (probably port 1720). You can use the Windows command line tool netstat to find that out (see *Check for Open H.323 Listeners on the Local Interfaces*).

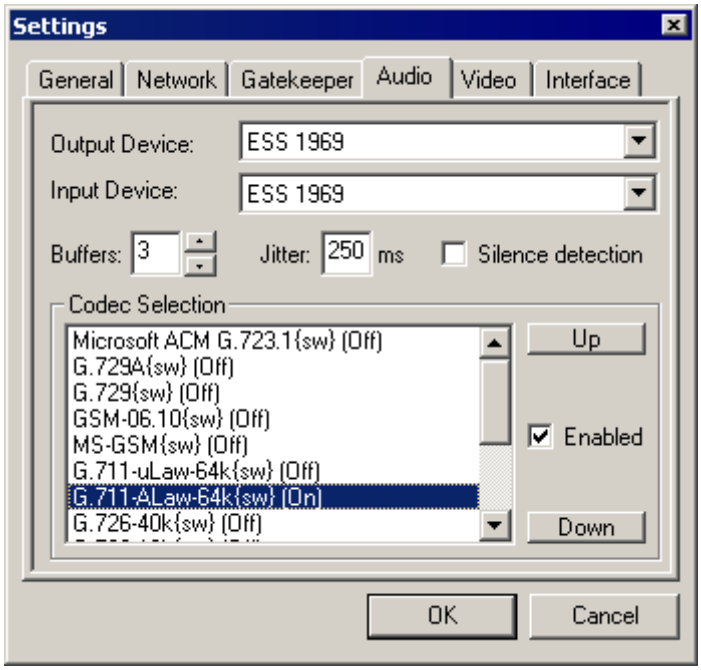
Another reason for the problem can be that the local IP address of the machine has to be entered in MyPhone's network settings. This looks as follows if you have 10.168.8.35 as IP address.



Be careful to have all video options deactivated in MyPhone. If MyPhone signals any video capabilities in a H.323 session, a call over our Cisco gateway will not work.

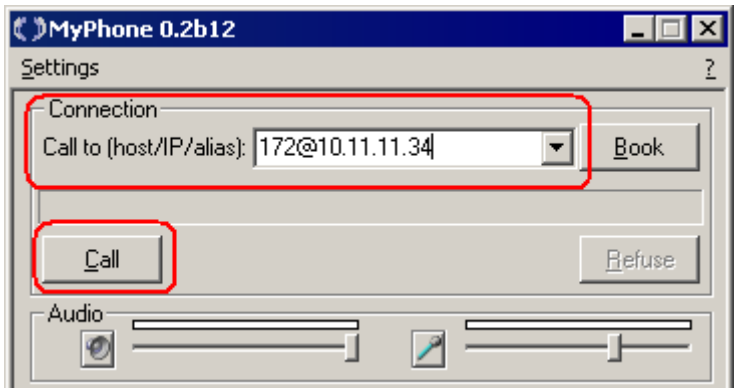


You should also take care that only the audio codecs that you have activated on the gateway are enabled in MyPhone. In our case this is only G.711 Alaw.

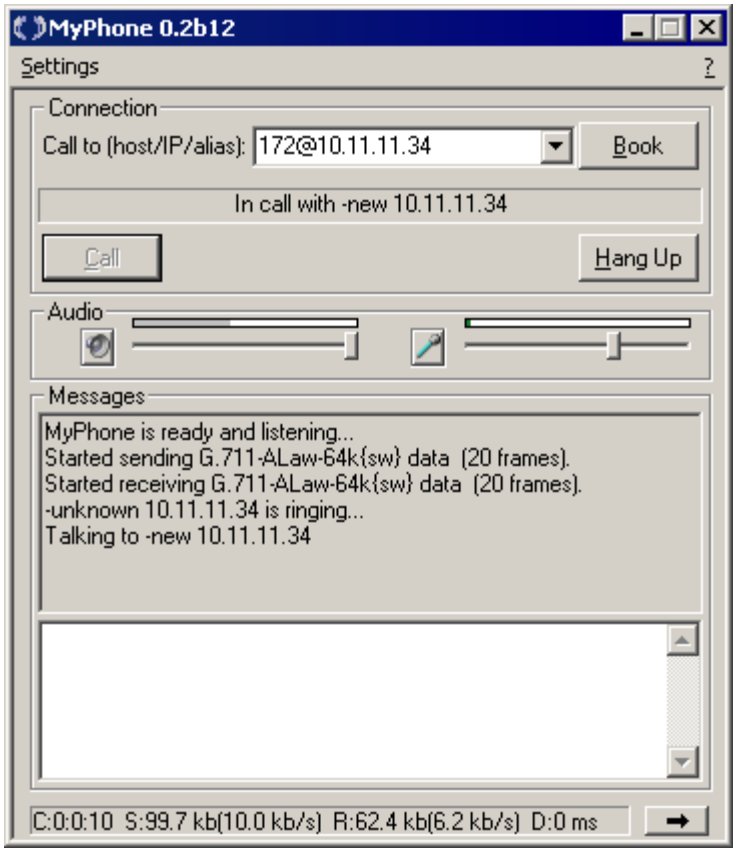


Test Outgoing Connections (IP to ISDN)

Enter the number to call and gateway's IP address in MyPhone's **Call to (host/IP/alias)** field in the format <number-to-call>@<gateway-IP-address> and click **Call**.



The telephone with the number 172 must be ringing now. If you pick up, the call is established and MyPhone should look like this.



Test Incoming Connections (ISDN to IP)

Dial a number configured in the range of the dial-peer on a PBX telephone. MyPhone indicates an incoming call on the user interface by displaying 10.11.11.34 is calling in the status field. When you click **Answer**, the call is established.

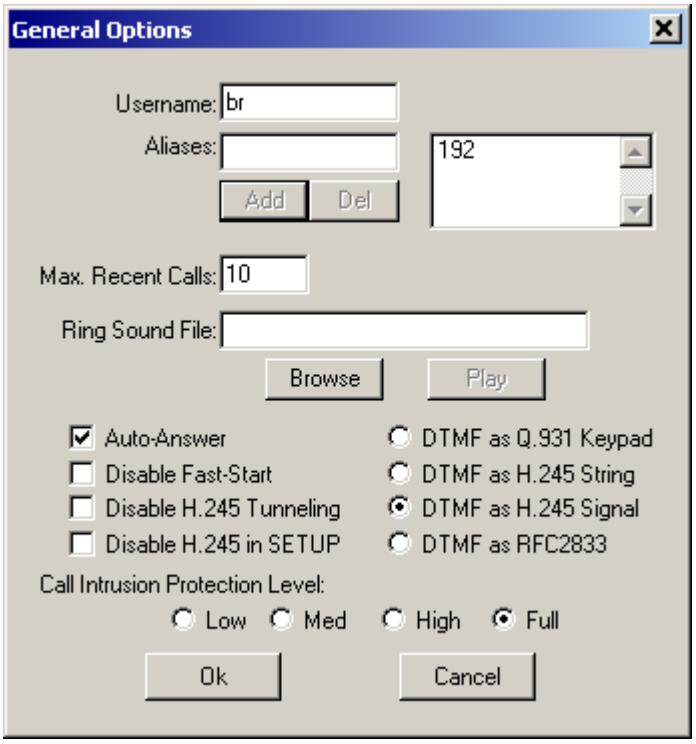
OpenPhone (H.323 Telephone Software)

It is not recommended to install OpenPhone on the KCS Voice Server for the following two reasons.

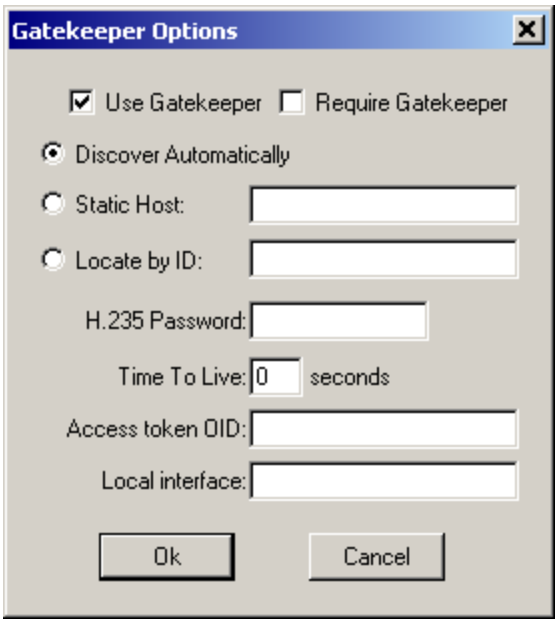
- There are "compatibility problems" between the OpenH323 libraries used by OpenPhone and the ones, which are installed into `c:\topcall\shared` by KCS Voice Server setup. If you want to run OpenPhone on the same machine make sure that the appropriate versions of the DLLs (pwlib.dll, ptlib.dll and openh323.dll) are in the same directory as openphone.exe.
- The second reason is the restriction that "only one H.323 listener per machine" is allowed. If it is required to run OpenPhone on the same machine you have to set its listener port to any other free port than 1720. You can make it listen on port 1721 by entering “127.0.0.1:1721” in the field “Local interfaces” in OpenPhone’s networking options.

1. Download executables for OpenPhone 1.7.0 or later from http://openh323.sourceforge.net/ (openphone.exe, openh323.dll, pwlib.dll and ptlib.dll); copy them into dedicated directory like OpenPhone.
2. Start openphone.exe.

3. In the **General Options**, type your alias number, such as 192.

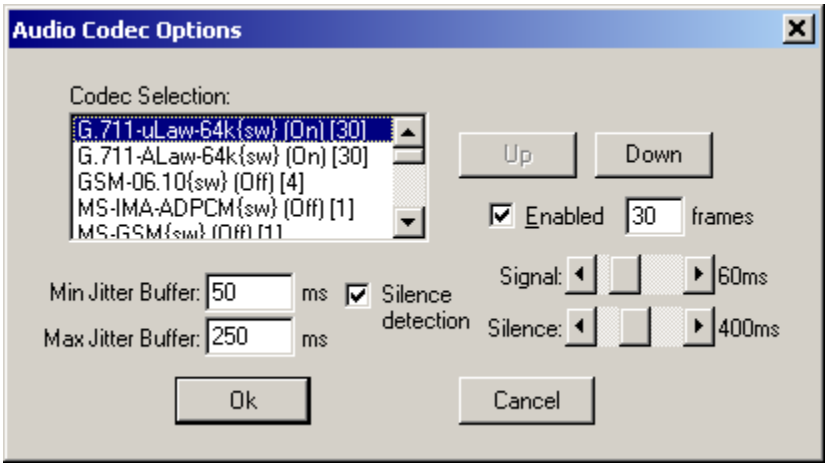


4. In the **Gatekeeper Options**, select **Use Gatekeeper** and **Discover Automatically**.

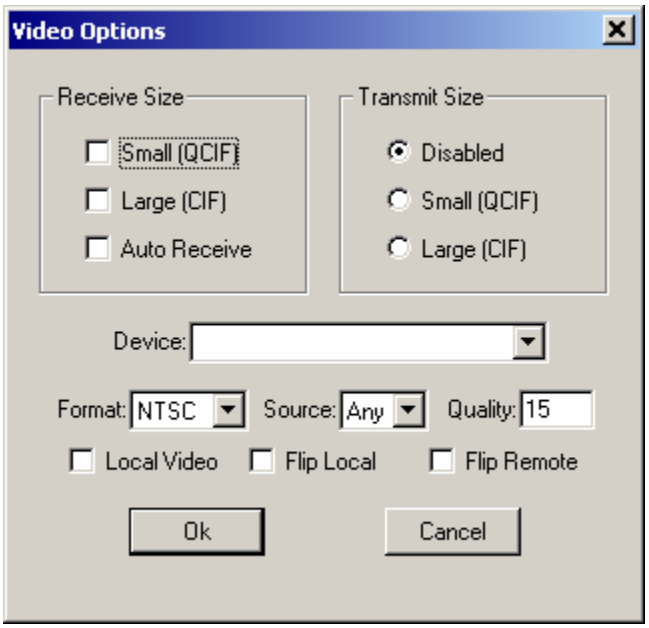


Note If you have several gatekeepers running in your network, it would be better not to use automatic discovery, but type the IP address of the GNUGk directly as Static Host!

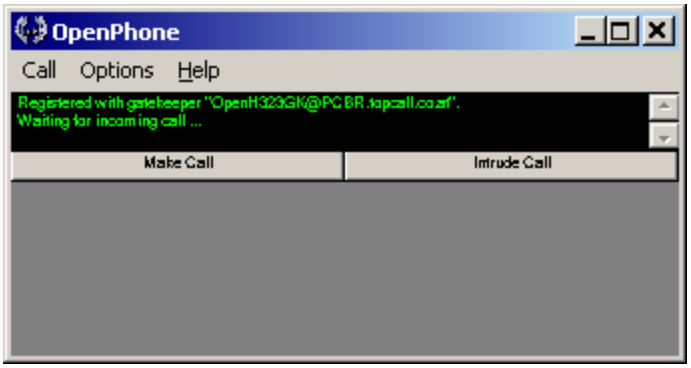
5. In **Audio Codec Options**, verify that **G.711 u-law** and **A-law** codecs are enabled.



6. In the **Video Options**, disable everything what you can.



7. Restart OpenPhone and you should see the following screen informing you on the successful gatekeeper registration.



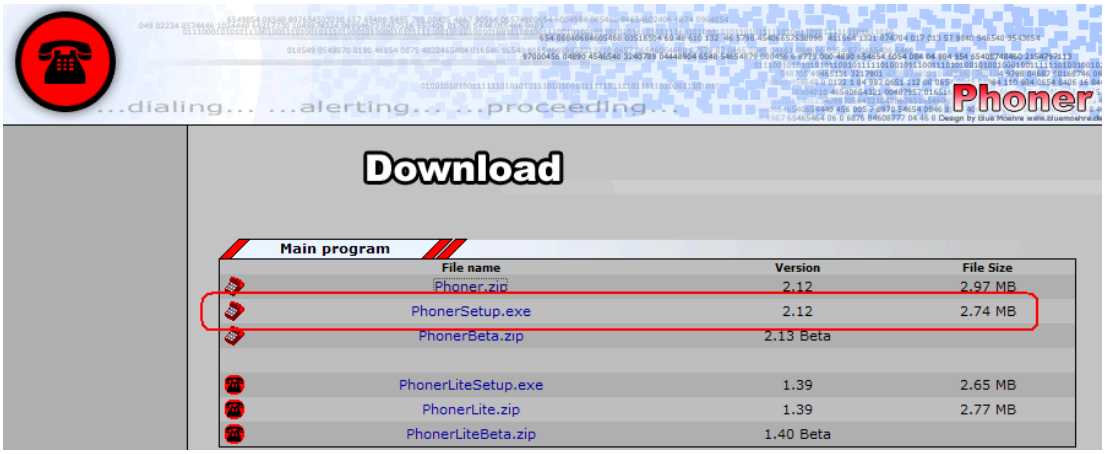
Now if you dial any number starting with digit 9, the call will be routed towards KCS Voice server.

SIP SoftPhone

Sometimes it can be useful to test the SIP connectivity between KCS server and the SIP gateway with a software phone.

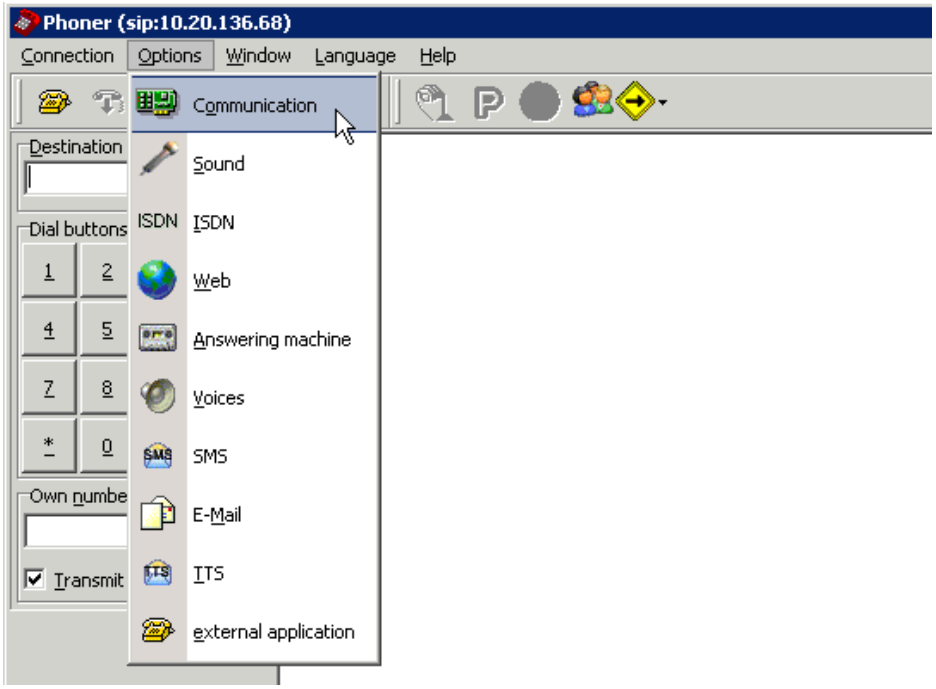
For example, it can be done with the free “Phoner” as follows:

1. Download Phoner Setup application from http://phoner.de/download_en.htm

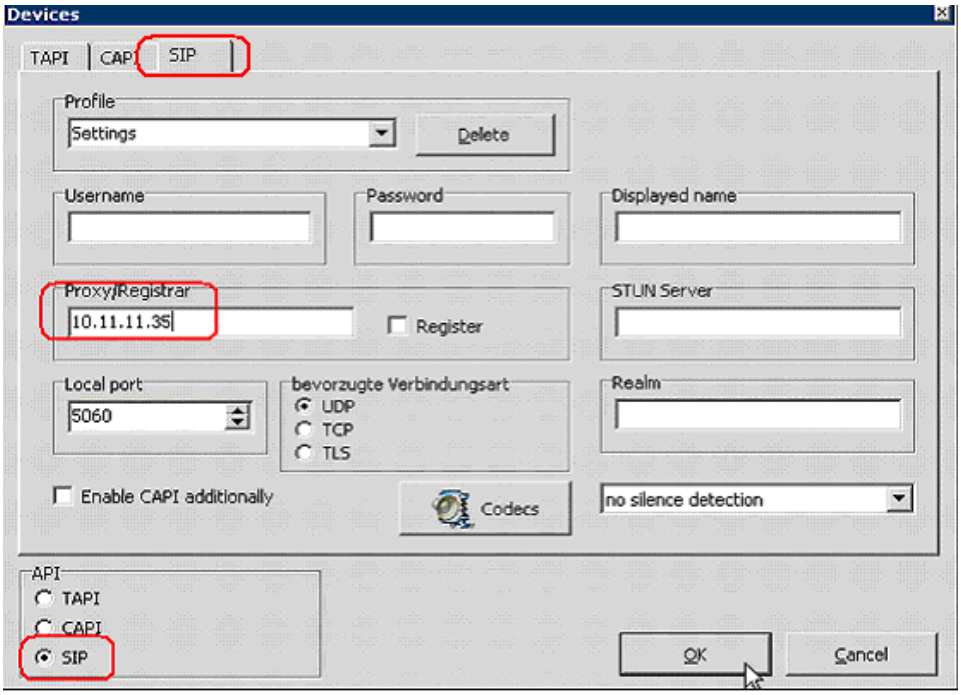


2. Start the Phoner setup and install it with default settings.

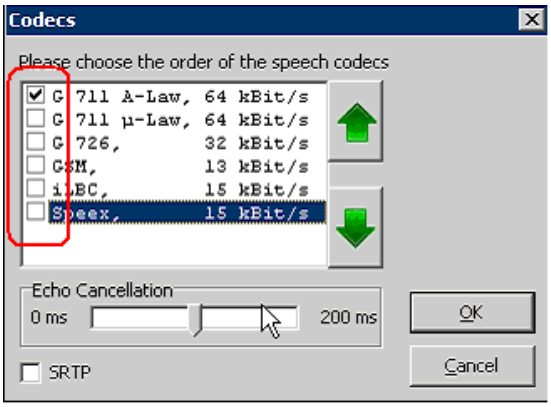
3. Start Phoner application and go to Options | Communication.



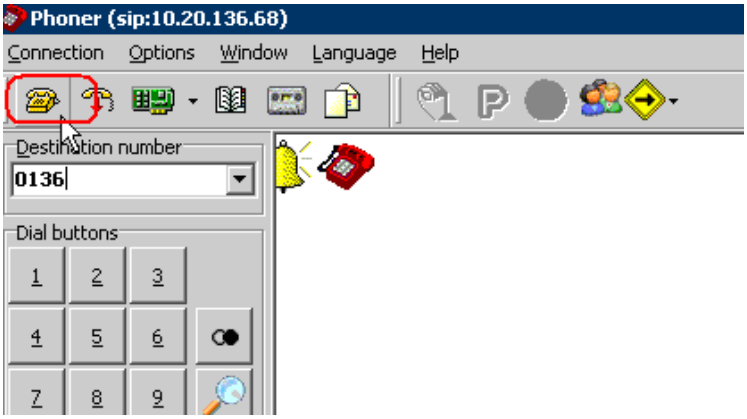
4. In the SIP tab, set the API checkbox to SIP and type the IP address of the gateway in the field Proxy/Registrar. Click the Codecs button.



5. Disable all codecs except G.711 A-law (or G.711 mu-law)

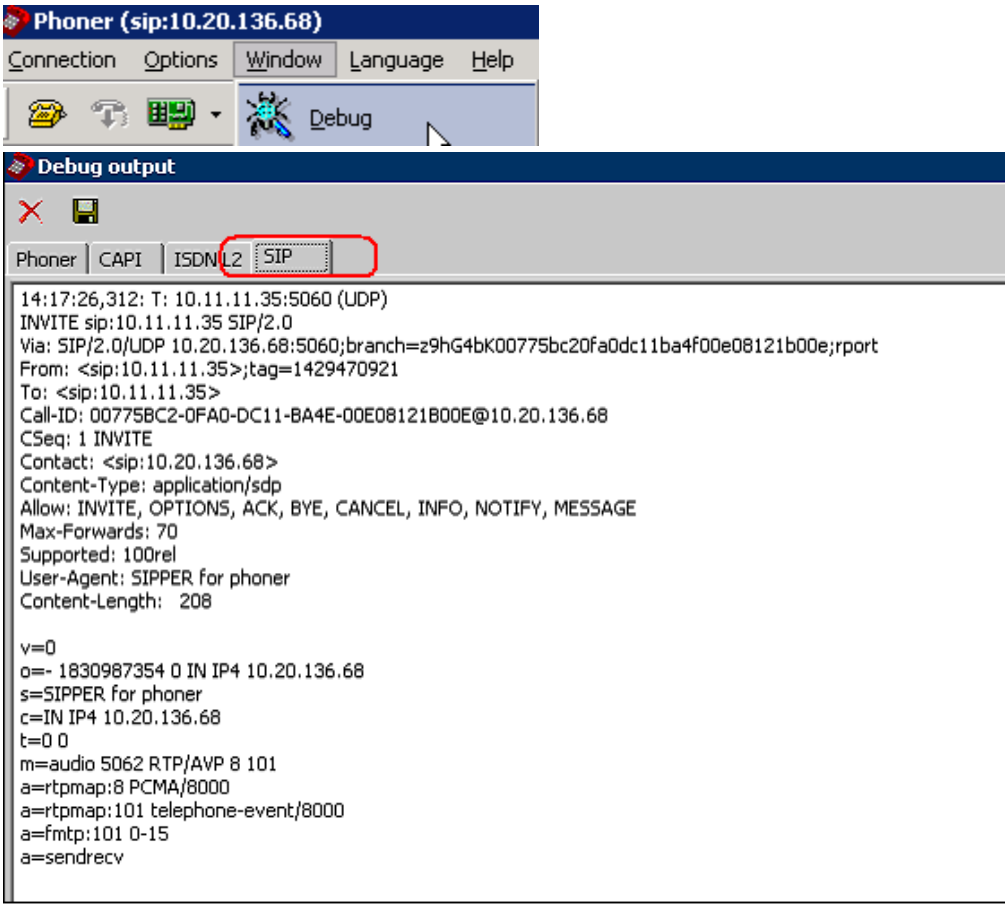


6. Type the phone number to be dialed and click the telephone icon.



7. The destination phone should be ringing now. Pick up the phone; you should have the voice channels connected through.

8. Go to Window | Debug to see the debug output for the SIP session

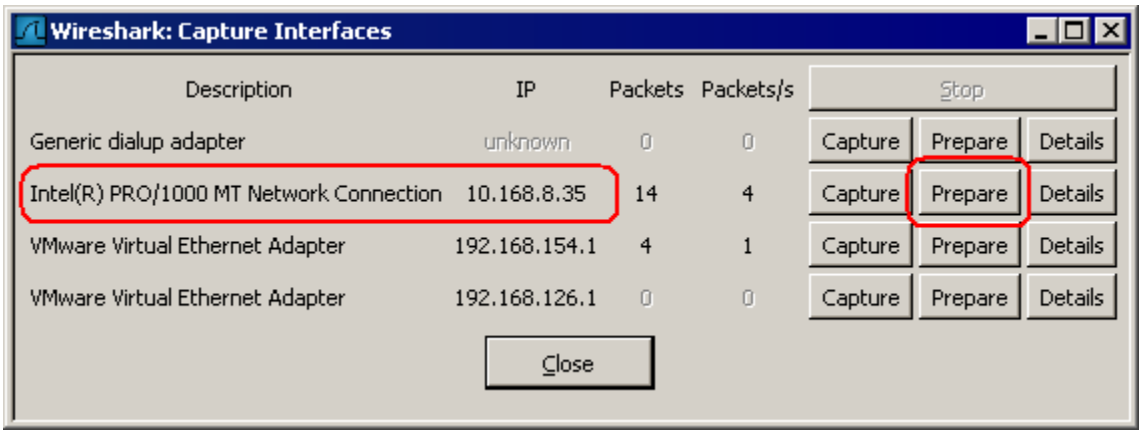


Wireshark

Wireshark (formerly known as Ethereal) is an IP sniffer with support of extensive VoIP and FoIP protocol analysis. IP sniffers are programs that can capture the IP traffic in a network and analyze the packets according to the used protocols. This helps to find problems and their reasons.

Wireshark can be used free of charge and is available from http://www.wireshark.org. We use version 0.99.2 in this manual.

1. To start capturing, select **Capture | Interfaces** from the menu. Pick your local interface used for FoIP by clicking the **Prepare** button on the right.



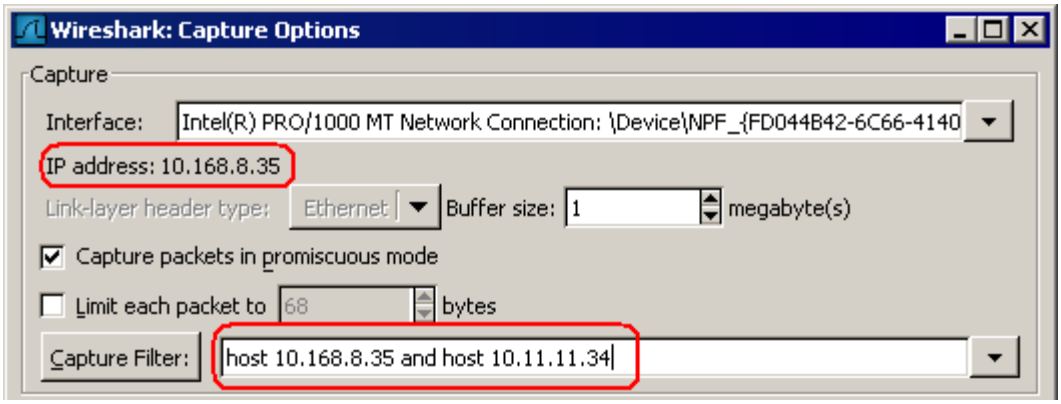
2. The following window appears. You should again check if the correct local interface is selected.

   If there is a lot of IP traffic you should limit the amount of data by setting a filter, which captures only the traffic between the gateway and the Windows machine where the VoIP/FoIP application is running. You can use logical operators like and/or/not in the filters. A filter rule to capture the whole traffic between our windows machine and the gateway would look like this.

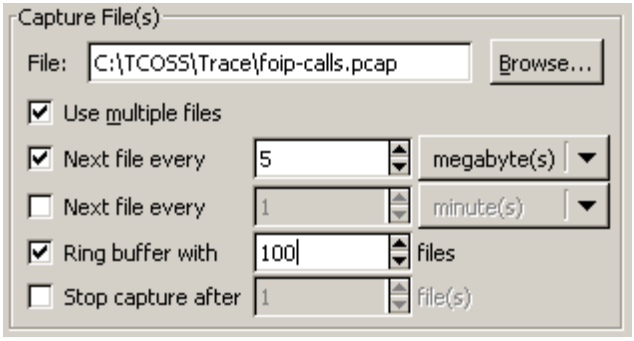
```
host 10.168.8.35 and host 10.11.11.34
```

   If you also have a CallManager or an H.323 gatekeeper involved, your capture filter must also include those IP addresses.

   Refer to Wireshark help for more information on the filter syntax.

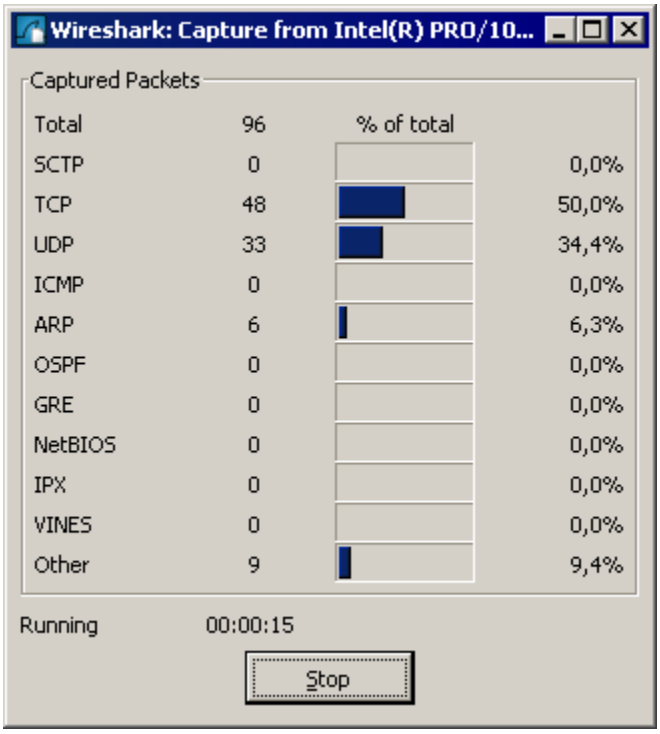


3. In the same dialog it is possible to write the captured traffic immediately into one or more files with limited size and cyclic overwriting as you know it from the KCS traces. Here is an example with max. 100 files with max. size 5 MB.



If you do not enter anything here your capture is only in the memory and can be saved later by selecting **File – Save** from the menu. You should in any case use .pcap as extension for files created with Wireshark.

4. Click **Start** to start capturing. While this is active you will see the following live statistics.



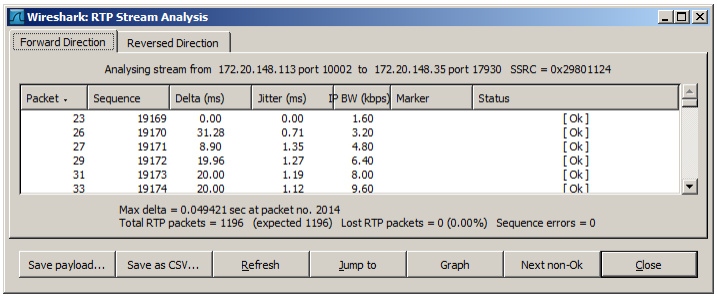
5. Click **Stop** to end capturing and see the captured traffic.

Note For information how to analyze and troubleshoot FoIP problems with Wireshark, refer to the *T.38 Fax over IP Trace Analysis Guide* that comes with TC/SP.

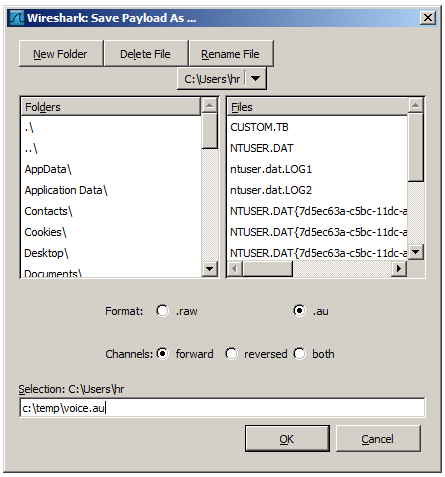
Extract Voice data from a network trace

This section explains how the extract voice data from a network trace.

1. Mark any UDP Packet of the voice stream that should be extracted and then select function **Statistics -> RTP -> Stream Analysis**. You will get a new window as shown in the screen shot below:



2. Click **Save payload** and save the forward channel as .au file (such as `C:\temp\voice.au`).



The saved file can be opened with Audacity (see Extract Voice data from a network trace).

Audacity

Audacity® is free, open source software for recording and editing sounds. It can be downloaded from the following address: http://audacity.sourceforge.net/

Hints

This section describes hints.

Check for Open H.323 Listeners on the Local Interfaces

The Windows command line tool netstat you can display all open IP listeners on the system. If no inbound call (from ISDN to MyPhone) is possible or if MyPhone starts with an error message that it failed to open the listener, you should check all listeners open. Probably the H.323 signaling protocol is already used by any other application.

Here is an example of how the output of netstat should look after you started MyPhone.

```
C:\Documents and Settings\CHKA>netstat -a -b -n
Active Connections
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1500
  RpcSs
  [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  [System]
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       1120
  [lsass.exe]
  TCP    10.168.8.35:1720       0.0.0.0:0              LISTENING       5008
  [MyPhone.exe]
  ...
```

If here is a different application that uses port 1720 (or any of the required) you have to stop it.

Check the LAN Connections

Ping the gateway from the Windows machine. The gateway must respond.

```
C:\>ping 10.11.11.34
Pinging 10.11.11.34 with 32 bytes of data:
Reply from 10.11.11.34: bytes=32 time<10ms TTL=255
Reply from 10.11.11.34: bytes=32 time<10ms TTL=255
Reply from 10.11.11.34: bytes=32 time<10ms TTL=255
Reply from 10.11.11.34: bytes=32 time<10ms TTL=255
Ping statistics for 10.11.11.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Ping the Windows machine from the gateways standard prompt. The Windows machine must respond.

```
Cisco2620>ping 10.168.8.35
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.168.8.35, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Cisco2620>
```

It must be guaranteed that no firewall between the gateway and the Windows machine denies connections on any of the required ports and protocols.

Do not forget to make sure that no other listeners (except OpenPhone) are active on the required ports on the Windows machine. You can use netstat for this purpose.

Set Caller ID for Outgoing Calls

On incoming calls the dial-peer is chosen by the dialed number (called party number). For outgoing calls the dial-peer is selected by the calling party number, which FoIPv3 sets in H.323 information elements. If the calling party number matches to a dial-peers destination pattern, then the configuration of that dial-peer is applied for the outgoing call. If no dial-peer matches, the global gateway configuration is applied (defined in voice service VoIP etc.). If the global configuration is different from the KCS configuration, problems can occur, so it is highly recommended to set the calling party number for outgoing calls.

The calling party number can be set fixed for the channel (with a number conversion rule) or user dependent (with a ++CID line in the users template or by the cost center parameter and an entry in Arr99). Refer to the *TCOSS System Manual* for details on that.

This is an example for setting the calling party number to 8000 for all outgoing calls in the TCOSS channel configuration.

```
‘8I~=I8000%~                    ,254
‘8~=8000%~                      ,255
```

To check if you are sending the calling party number to the gateway correctly, enable ISDN debug on the gateway by entering “debug isdn q931” (Cisco-specific) in the enabled mode and make an outgoing call. Some traces like this appear where the calling and the called party number among other ISDN information is visible.

```
Cisco2620#debug isdn q931
debug isdn q931 is               ON.
Cisco2620#
Cisco2620#
19:05:14: ISDN BR1/0 Q931: TX -> SETUP pd = 8  callref = 0x14
        Bearer Capability i = 0x9090A3
                Standard = CCITT
                Transer Capability = 3.1kHz Audio
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0x83
        Display i = '8000'
        Calling Party Number i = 0x80, '8000'
                Plan:Unknown, Type:Unknown
        Called Party Number i = 0x81, '08172'
                Plan:ISDN, Type:Unknown
        Sending Complete
        Channel ID i = 0x89
        Progress Ind i = 0x8188 - In-band info or appropriate now available
        Date/Time i = 0x030B040B0A
        Connected Number i = 0x018038313732
19:05:15: ISDN BR1/0 Q931: TX -> CONNECT_ACK pd = 8  callref = 0x14
```

To check if the right dial-peer is associated with your outgoing call, you can use “debug voip dialpeer all” (Cisco specific) and then make an outgoing call.

SIP Protocol Basics and Examples

SIP is an application-layer protocol that can establish, modify and terminate multimedia session such as telephony or fax calls. SIP messages are text encoded and use the UTF-8 character set. Much of the SIP’s message and header syntax is identical to HTTP/1.1 protocol.

SIP is being developed by the SIP Working Group within the Internet Engineering Task Force (IETF); the protocol is published as RFC 3261.

From the functional / call control point of view, SIP protocol could be compared with H.323 protocol stack, but it is simpler and uses fewer messages – requests and corresponding responses.

SIP protocol is transaction oriented, as in the fact each SIP request starts a separate transaction.

Most important SIP requests/transactions are:

- **INVITE**: initiates a call (equivalent to H.323/Setup) and changes call parameters (“RE-INVITE”) (in the case of T.38 fax call, RE-INVITE is being used to switch from the voice mode into the T.38 mode, equivalent with H.323/RequestChangeMode)
- **ACK**: confirmation for final response to INVITE
- **BYE**: Disconnects the call

SIP responses are partly based on HTTP protocol responses; there are two main types of them:

- **Provisional (1XX class)**: Used by the servers to indicate call progress (like CallProceeding, Alerting with H.323) but do not terminate SIP transactions
  For example, 100 stands for Trying (equivalent to H.323/CallProc) 180 stands for Ringing (equivalent to H.323/Alerting)
- **Final (2XX, 3XX. 4XX, 5XX, 6XX classes)**: Used by the servers to terminate SIP transactions.
  For example, 200 stands for OK (equivalent with H.323/Connect in the case of the INVITE transaction and with H.323 ReleaseComplete in the case of BYE transaction)

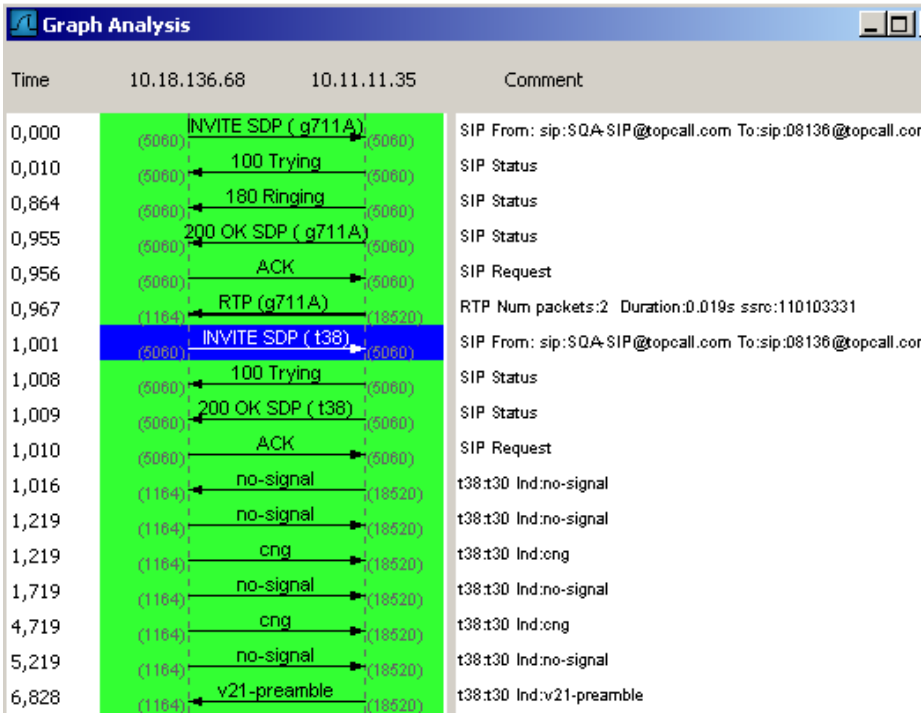
Example of an outgoing T.38 fax call from KCS towards gateway

(10.18.136.68 is the KCS server, 10.11.11.35 the gateway):

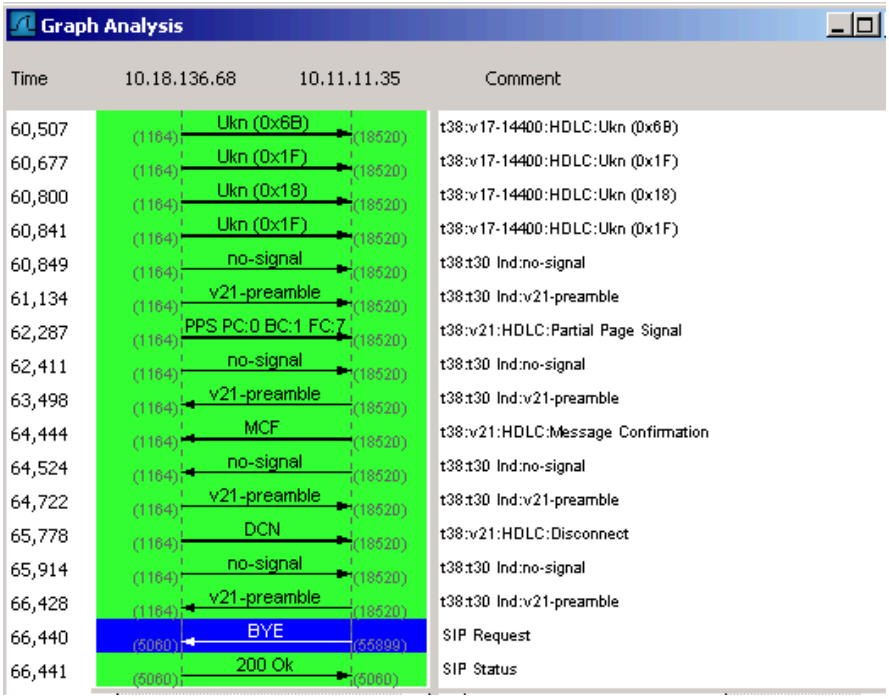
1. KCS starts the call establishment by sending the INVITE, and the gateway responds with 100 Trying (“CallProc”), 180 Ringing (“Alerting”) and finally 200 OK (“Connect”).

   This final response from gateway is acknowledged by sending ACK request and voice media channels are established.

   Then KCS enforces the T.38 mode by sending the “(RE-)INVITE” (marked in blue below) and the gateway responds with 100 Trying and 200 OK. The T.38 communication can start now:



2. Once the T.38 communication has finished, KCS disconnects the call by sending BYE and the gateway responds by the 200 OK:



For further information on SIP, refer to the SIP documentation available on the Internet. For example:

- http://www.ietf.org/rfc/rfc3261.txt (RFC that defines the SIP protocol).
  Refer to the *Overview of Operation*) for a good introduction.
- http://www.sipforum.org
  In the white paper section, there are some good papers providing introduction on SIP protocol.

Concurrent Operation with KCS H.323 Integration for Voice on the Same Machine

FoIPv3 can be installed on the same machine as the *H.323 Integration for Voice (tce_h323)*. This requires at least H.323 Engine for Voice (tce_h323) 1.02.06 included in TC/SP 7.59.06 and higher.

The necessary steps to install and configure both systems on one machine are described in the *H.323 Voice Integration documentation* under *Concurrent Operation with T.38 Fax over IP (TC/FoIP)*.

Check the ISDN Line Synchronization Up to the CISCO Gateway (BERT)

It is often necessary to verify the quality of the local PBX or PTT interconnection of the T.38 gateways due to different stability issues (like alarm conditions, slip errors, or too much of different analog fax errors like XT, XV, XT etc. that may indicate poor line quality).

The easiest method how to verify the quality of the line (even remotely) is to perform so called *Bit Error Rate Testing* (BERT). All what we need is an ISDN test equipment capable of doing BERT testing.

The basic principle is simple: the ISDN tester (Test generator) sends a pseudo-random digital test pattern towards the Device under Test (DUT) that loops the received data transparently back (via the same B-channel). The tester compares the sent and received data for a defined time and makes the test verdict in terms of error ratio (number of bit errors per 1000 bits, for example 1.10-6). This method is often being used with the Kofax lineservers and requires only one B channel between the ISDN tested and the DUT.

In order to test the line quality towards the T.38 gateway, it is possible to use the same ISDN tester as both Test generator and DUT as well like following:

1. Connect the ISDN Tester to the available BRI/PRI line
2. Make a call to the T.38 gateway through its ISDN line and use the special extension
3. Configure the gateway so that upon receiving this special extension, the gateway establishes the 2nd call with the ISDN tester and answer the call on the tester
4. Setup one of the calls into the LOOP mode on the tester and start the BERT test on another one
5. In this way, the test patterns would proceed from the tester to the gateway, would be looped to the 2nd call towards the tester, there they would be looped back to the gateway and finally would be sent back to the tester like this:

Configuration Example for BERT on the Cisco 28xx Gateway

Assume there is a CISCO gateway 2821 connected to one E1 line and the ISDN Aurora tester connected to the public ISDN line with the number 8658927. The Cisco gateways is connected to the PBX reachable through the public number 8658929-79xxx, the escape digit for the public line in the PBX is 0. We define a special extension 098 so that if we dial the number 8658929-79098 from the tester the gateway would establish the 2nd call to the number 8658927 and connect both calls together.

The leading 0 in the special extension would force the gateway to route the 2nd call through the POTS dial-peer with the destination pattern 0T, but then, prior to dialing out, the gateway would perform the number translation due to

translate-outgoing called command so that the number 08658927 would be dialed instead of 098:

Excerpt from the Cisco gateway configuration:

```
!
translation-rule 98
 Rule 0 ^098 08658927
!
!
dial-peer voice 1 pots
destination-pattern 0T
progress_ind alert enable 8
progress_ind progress enable 8
progress_ind connect enable 8
translate-outgoing called 98
direct-inward-dial
```

```
port 0/2/0:15
!
```

Bad Fax Quality Due to RTP-NTE

We have recognized a fax quality issue with CISCO UCM and CISCO Gateways in the following case:

1. FoIP is connected as SIP trunk
2. The SIP option EnableRtpNte (Support reception of DTMF digits via RFC 2833) is enabled.
3. The initial connection will be created between FoIP and any CISCO softphone. The call is then transferred to a gateway.

In that case it may happen that the media data of the transferred call is routed via CISCO UCM which may cause a very bad fax quality.

If you have a similar use case, it is recommended to check the IP address of the actual used media connection in the Peer parameter of the FoIP trace as shown in the example below:

```
Inbound Call: CallerId=@4630, TSI= EC= (), Peer=10.20.30.40:19140
Outbound Call: Number=I4602 -> 4602, CallerId=, CSI=, EC=  (), Peer=10.20.30.40:18414
```

Outgoing Secure SIP Call Fails with Error Code 12700

If an outgoing SIP call via TLS fails with error code 12700, there may be a TLS authentication issue. Check the FoIP traces for “Could not connect TLS connection”. The example below shows an error case where the Certificate Check was enabled in the SIP configuration parameters but they remote server does not use a key that was issued by an computer using a certification configured in “SSL Trusted CA Certificates”.

```
13/15:34:54.924 (2a08/2fd8/0007) {"SipTcpConnList" 0x1cdf47c} Could not connect TLS
 connection, rhost=::ffff:172.20.150.4, rport=5067: Error 586157578: SSL verify error
 20 unable to get local issuer certificate
```

Change to FoIP Configuration to either use a correct “SSL Trusted CA Certificate” or disable the certificate check.