Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking between Metaswitch MetaSphere CFS 7.4 with Metaswitch Perimeta Session Border Controller 3.1.0 and Avaya IP Office 8.0(18) - Issue 1.0

Abstract

These application notes describe the steps required to configure Session Initiation Protocol (SIP) trunking between a Metaswitch MetaSphere Call Feature Server (CFS) solution with a Metaswitch Perimeta Session Border Controller (SBC) and an Avaya IP Office telephony solution

This is not a replacement of Service Provider SIP Trunk service compliance test. To verify the SIP Trunk service for a particular Service Provider, a test needs to be requested by the Service Provider.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps required to configure Session Initiation Protocol (SIP) trunking between a Metaswitch MetaSphere Call Feature Server (CFS) with a Metaswitch Perimeta Session Border Controller (SBC) solution and an Avaya IP Office telephony solution. The Avaya solution consists of Avaya IP Office, and Avaya H.323, digital and analog endpoints

SIP is a standards-based communications approach designed to provide a common framework to support multimedia communication. RFC 3261 is the primary specification governing this protocol. SIP manages the establishment and termination of connections and the transfer of related information such as the desired codec, calling party identity, etc. Within these Application Notes, SIP is used as the signaling protocol between Avaya IP Office and the Metaswitch MetaSphere CFS solution.

MetaSphere is a broad suite of telephony applications. MetaSphere applications may be deployed individually or in combination to deliver the full spectrum of legacy and next-generation voice services.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to a Metaswitch CFS via SIP Trunking. This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify SIP trunking interoperability between the Metaswitch MetaSphere CFS solution and the Avaya IP Office solution.

The following areas are covered in the test:

- Response to SIP OPTIONS queries
- Incoming calls to various phone types from Metaswitch CommPortal softclient registered to Metaswitch CFS. Phone types included SIP, H.323, digital, and analog telephones at the enterprise.

- Outgoing DID calls from various phone types. Phone types included SIP, H.323, digital, and analog telephones at the enterprise. All outbound DID calls were routed from the enterprise across the SIP trunk to Metaswitch CFS
- Inbound and outbound calls to/from the Avaya one-X® Communicator-softclient
- Inbound and outbound long hold time call stability
- Codec G.711 A-LAW, G.711 U-LAW and G.729 (a)
- Caller number/ID presentation
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls
- DTMF transmission using RFC 2833
- Voicemail navigation for inbound and outbound calls
- T.38 Fax Support
- Telephony features such as hold and resume, transfer, and conference
- Call forwarding

The following areas are not covered in the test:

- Various PSTN call types including: local, long distance, international, outbound toll-free, operator service and directory assistance. Due to limitation of Metaswitch lab environment

2.2. Test Results

Interoperability testing of Metaswitch SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below:

- Inbound/Outbound PSTN calls were not tested as part of this compliance test. The Metaswitch lab environment did not support PSTN testing.
- Metaswitch CommPortal does not support G.729. Only G.711 could be tested with it. G.711 and G.729 were tested from Avaya DID to Avaya DID traversing the SIP trunk to Metaswitch CFS.
- Outgoing call from Metaswitch CommPortal to Avaya endpoint, when placing the call on hold from Metaswitch CommPortal side, the call is dropped. Note this was successfully tested with a 3rd party softphone registered to the CFS.
- Call from Metaswitch CommPortal to Avaya H.323 endpoint, when pressing digits on CommPortal side they could not be heard on the H.323 side.
- Incoming call from Metaswitch CommPortal to Avaya endpoint. When the call is placed on hold from the Avaya endpoint side the CommPortal sends a re-invite to the Avaya endpoint and rings the line until the call is resumed.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on Metaswitch SIP Trunking contact Metaswitch at www.metaswitch.com.

3. Reference Configuration

Figure 1 illustrates an example Avaya IP telephony solution connected to Metaswitch that was utilized for compliance testing. Located at the enterprise site is an Avaya IP Office 500v2 with the COMBO6210/ATM4 expansion card which provides connections for 6 digital stations, 2 analog stations, 4 analog trunks as well as 10-channel VCM (Voice Compression Module) for supporting VoIP codecs. The LAN port of Avaya IP Office is connected to the enterprise LAN while the WAN (LAN2) port is connected to the public IP network. Located at Metaswitch's site, is a Metaswitch MetaSphere CFS and a Metaswitch Perimeta SBC. For security purposes, the real public IP addresses used in the compliance test were changed to 192.168.x.x in these Application Notes.

The site also has a Windows Server (not shown) running Avaya Voicemail Pro for providing voice messaging service to the Avaya IP Office users. A separate Windows PC (not shown) runs Avaya IP Office Manager to configure and administer the Avaya IP Office system.

Avaya IP telephony solution comprised of the following endpoints used to simulate a customer site:

- Avaya 96x0 IP Telephone (H.323 protocol)
- Avaya 96x1 IP Telephone (H.323 protocol)
- Avaya 96x0 IP Telephone (SIP protocol)
- Avaya 96x1 IP Telephone (SIP protocol)
- Avaya 1416 Digital Telephone
- Avaya 5420 Digital Telephone
- Avaya 9508 Digital Telephone
- Avaya one-X Communicator
- Generic Analog Telephone
- Generic Fax Machines

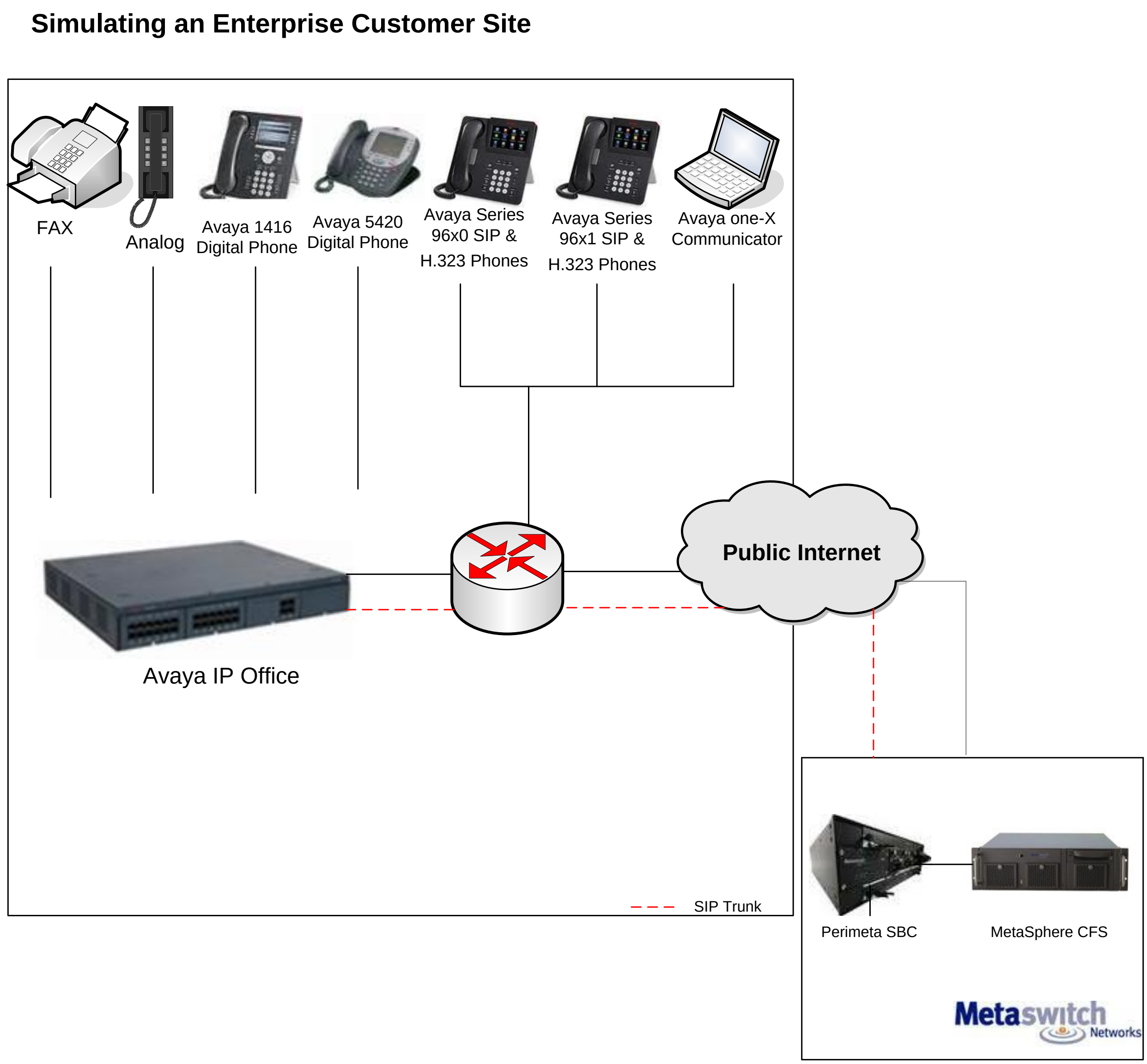


Figure 1: Avaya IP Telephony Network connected to Metaswitch

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

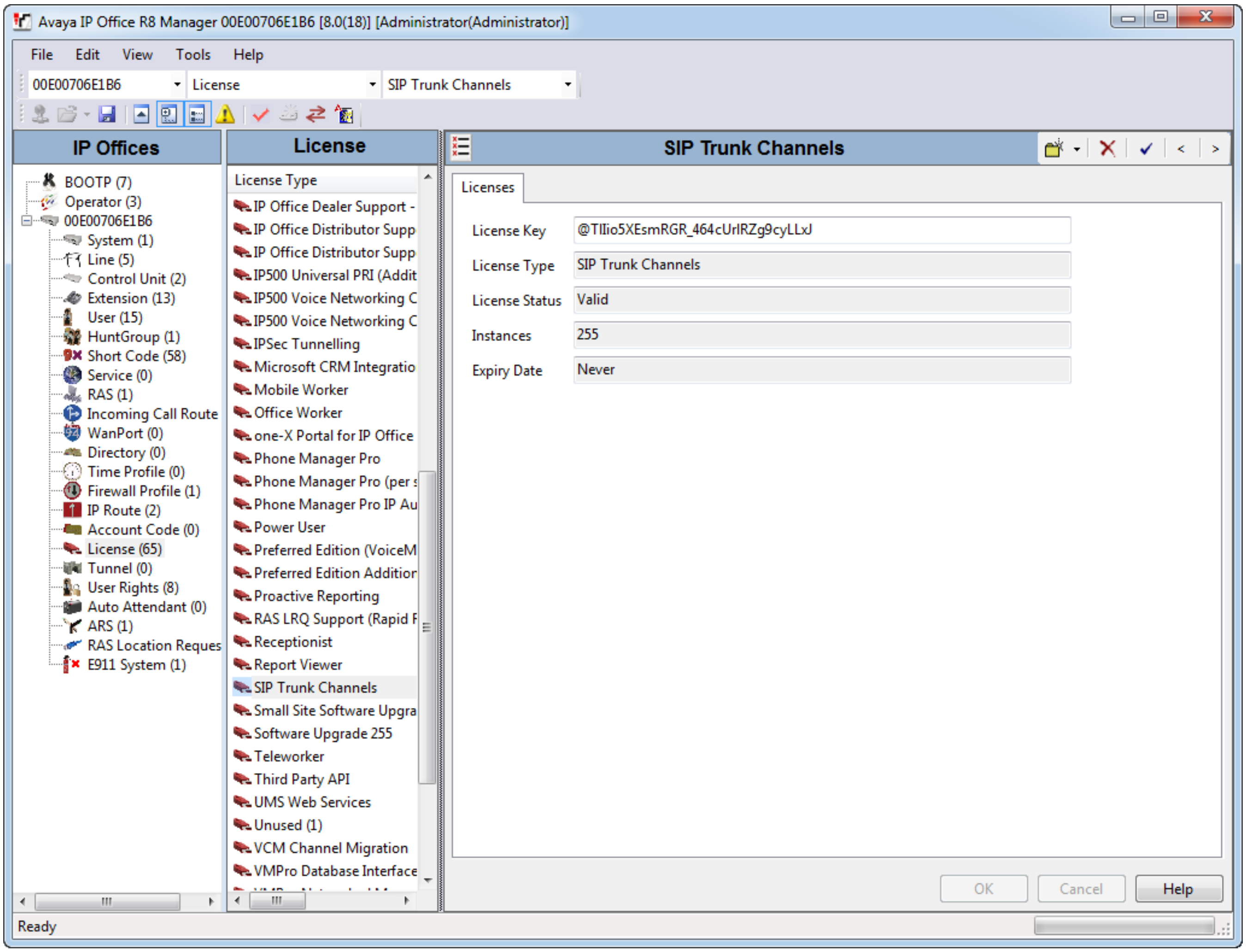
Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya IP Office	8.0 (18)
Avaya IP Office COMBO6210/ATM4 Module	8.0 (18)
Avaya IP Office Manager	10.0 (18)
Avaya 96x0 Series (H.323)	3.1-SP3
Avaya 96x1 Series (H.323)	6.2
Avaya 96x0 Series (SIP)	2.6-SP7
Avaya 96x1 Series (SIP)	6.0-SP3
Avaya 1416 Digital Telephone	N/A
Avaya 5420 Digital Telephone	N/A
Avaya 9508 Digital Telephone	N/A
Generic Analog Phone	N/A
Generic Fax Machines	N/A
Avaya one-X Communicator	6.1.3.09-SP3
Metaswitch Solution Components	
Metaswitch MetaSphere CFS	7.4
Metaswitch Perimeta SBC	3.1.0
CommPortal Communicator	1.2.2

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration necessary to support connectivity to Metaswitch SIP Trunking service. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start→ Programs → IP Office→ Manager** to launch the application. Navigate to **File → Open** Configuration, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one shown in the next section. The appearance of the IP Office Manager can be customized using the View menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center, and the Details pane on the right side. These panes will be referenced throughout the Avaya IP Office configuration.

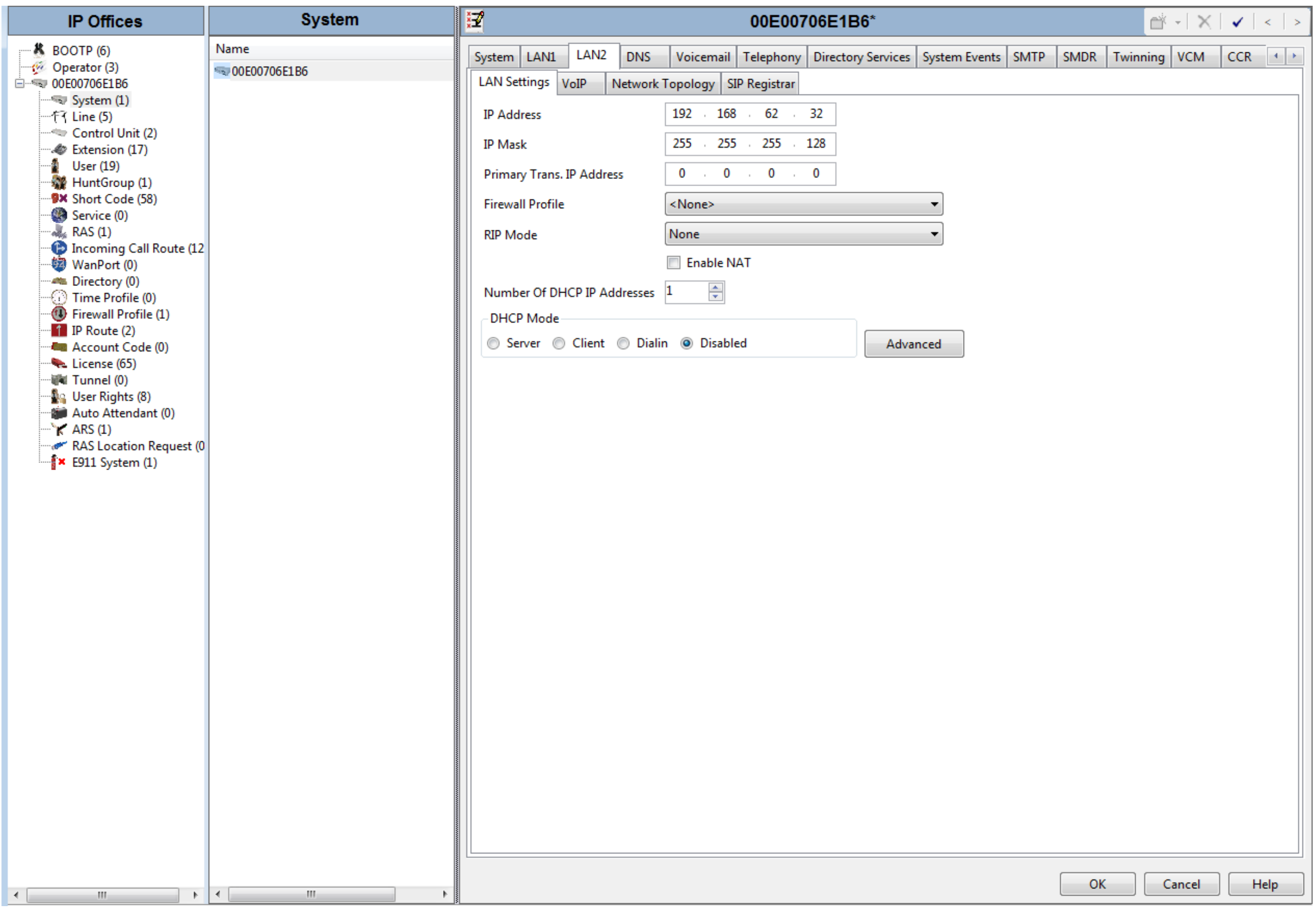
5.1. Verify IP Office License

Click on **License** in the left panel. Confirm that there is a valid **SIP Trunk Channels** entry. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

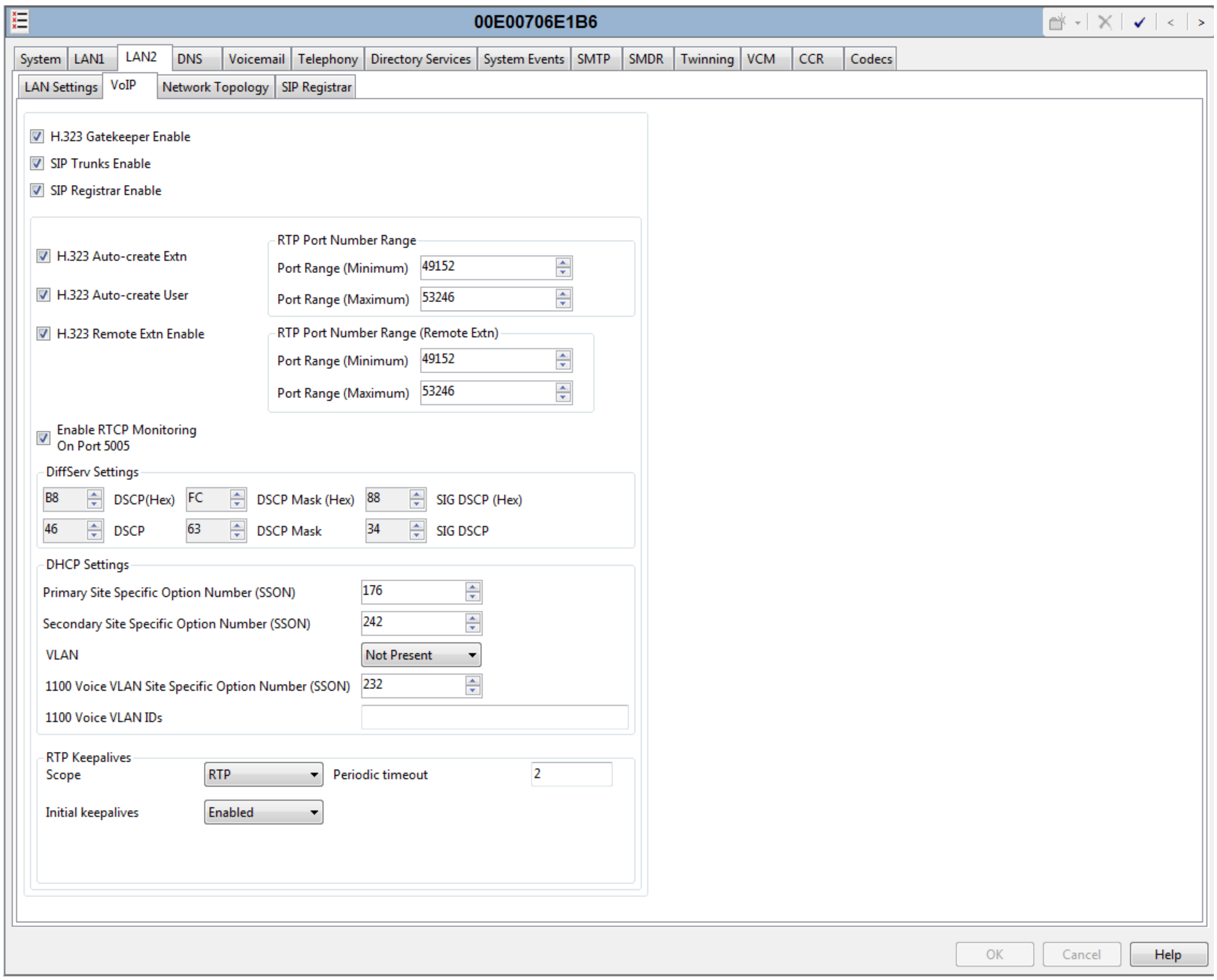


5.2. LAN2 Settings

In the sample configuration, the MAC address 00E00706E1B6 was used as the system name and the WAN port (LAN2) was used to connect the Avaya IP Office to the public network. The LAN2 settings correspond to the WAN port on the Avaya IP Office system. To access the LAN2 settings, first navigate to **System (1) → 00E00706E1B6** in the Navigation and Group Panes respectively, and then navigate to the **LAN2→ LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office WAN port. Set the **IP Mask** field to the mask used on the public network. All other parameters should be set according to customer requirements. Click **"OK"** when finished and Save the configuration.
Describe the configuration of each Avaya device used.

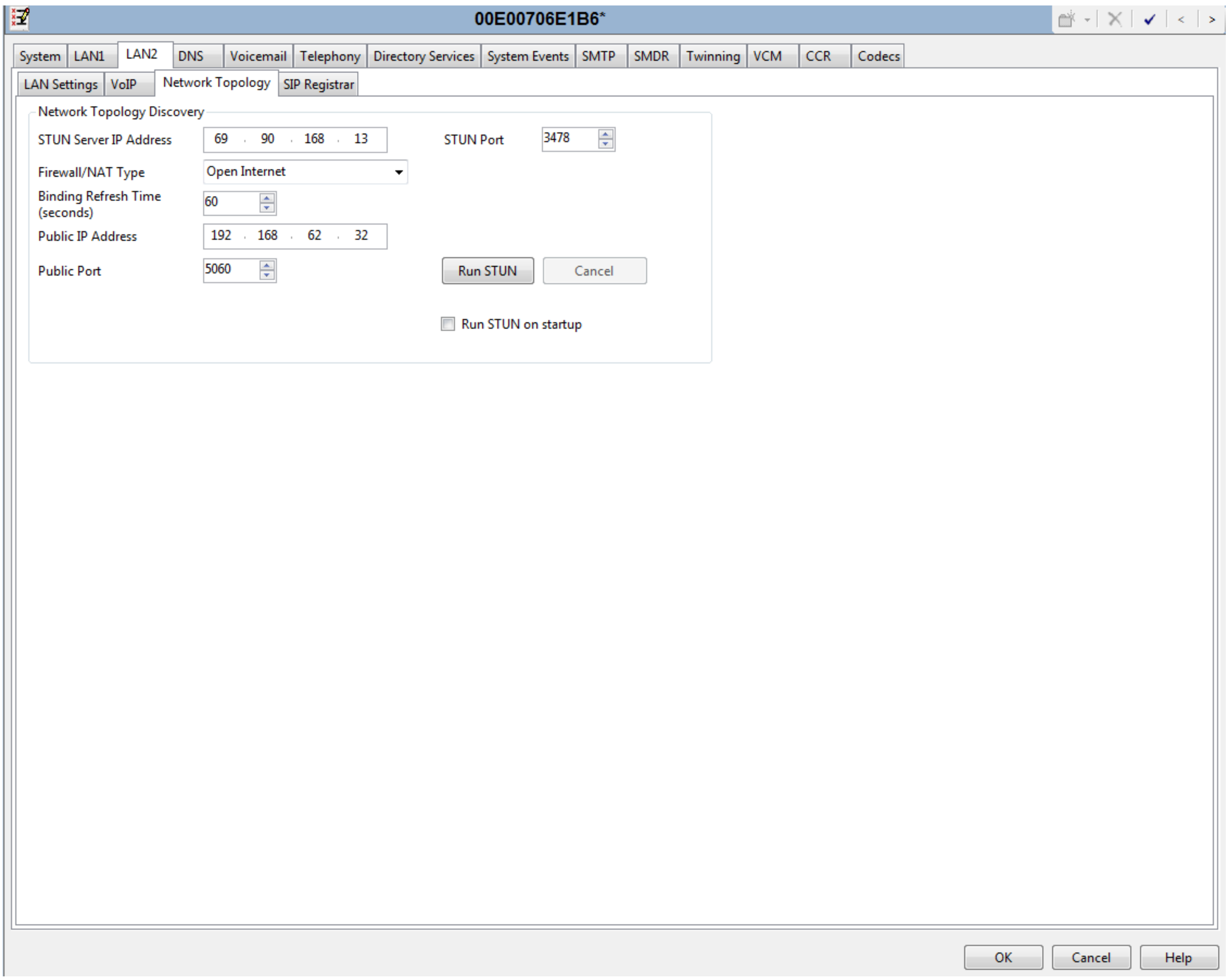


Select the **VoIP** tab as shown in the following screen.   The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Metaswitch. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range for calls using LAN2. Avaya IP Office can also be configured to mark the **Differentiated Services Code Point (DSCP)** in the IP Header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. To prevent possible loss of audio path during some call forward off-net scenarios, it is recommended to set the following fields under **RTP Keepalives:** Set **Scope** to **RTP**, **Initial keepalives** to **Enable** and an appropriate **Periodic timeout** from **1** to **180** seconds. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements.



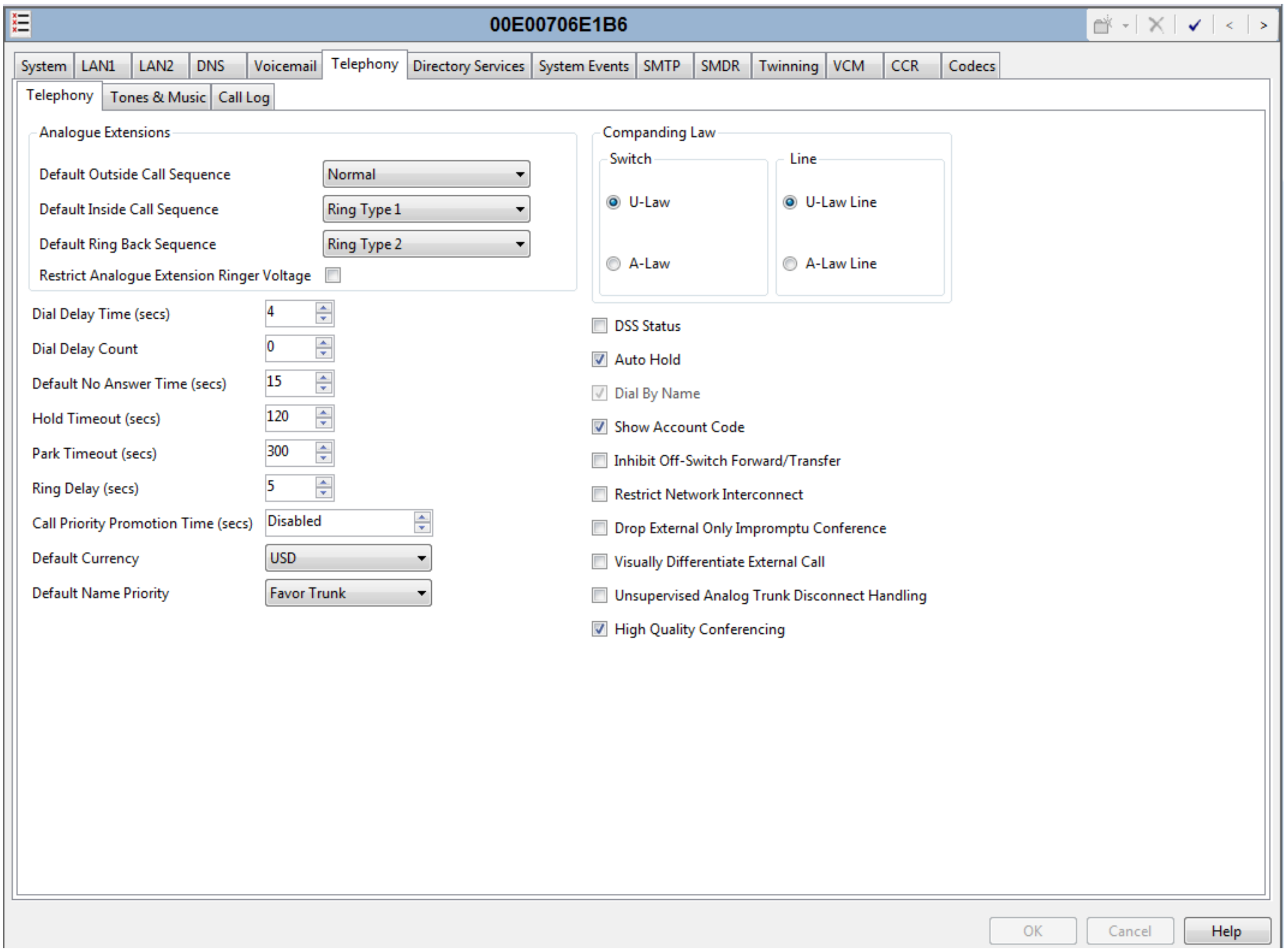
On the **Network Topology** tab in the Details Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test, so the parameter was set to **Open Internet**. With this configuration, STUN will not be used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used as one input to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to Metaswitch. See Section **5.9** for more details.
- Set **Public IP Address** to the IP address of the Avaya IP Office WAN port.
- All other parameters should be set according to customer requirements.
- Click **"OK"** when finished and Save the configuration



5.3. System Telephony Settings

Navigate to the **Telephony** → **Telephony** Tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. For North America, **ULAW** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer across the SIP trunk.



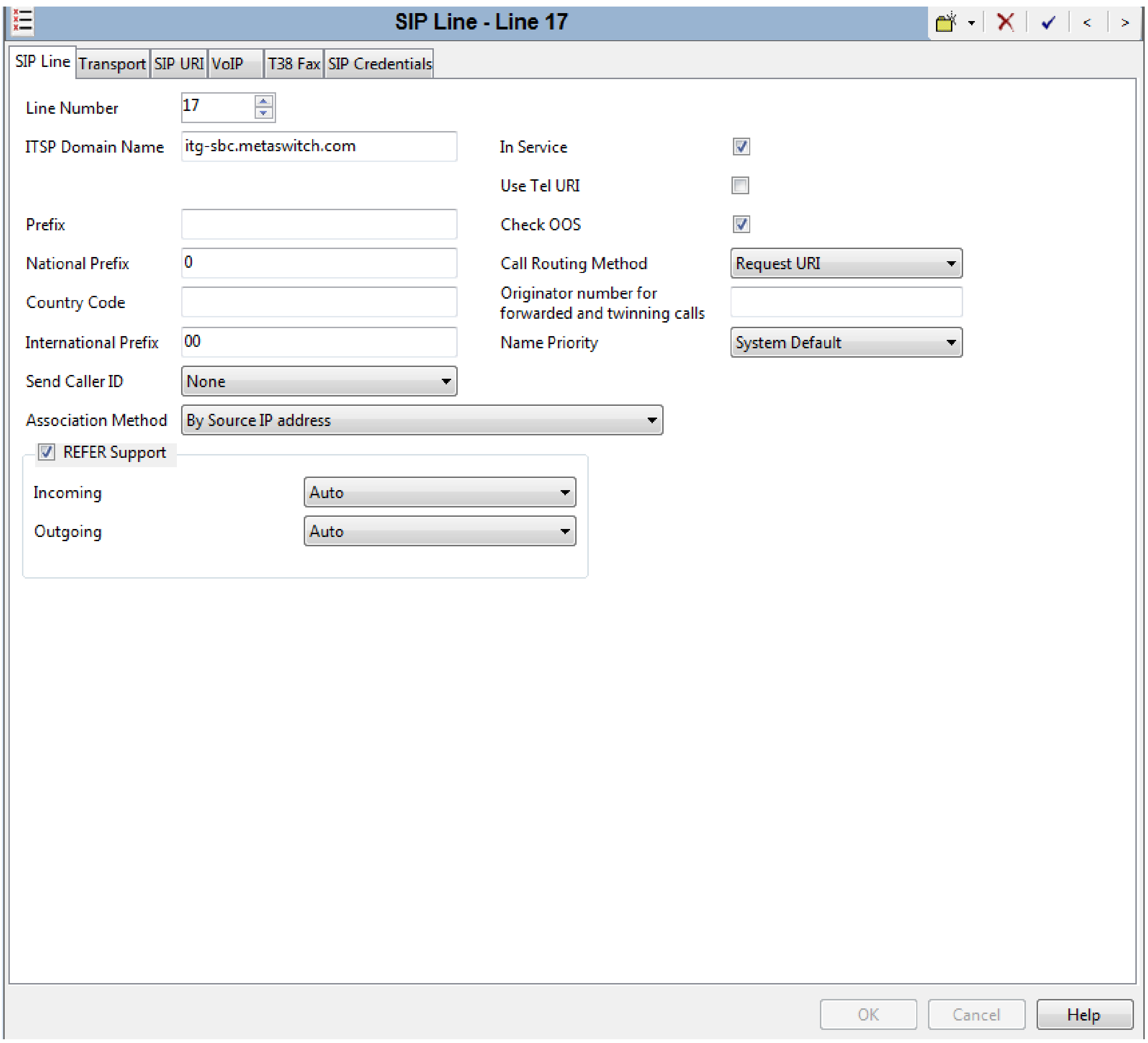
5.4. Administering SIP Line

A SIP Line needs to be established between Avaya IP Office and Metaswitch MetaSphere CFS. To create a SIP line, begin by navigating to Line in the left Navigation Pane, then right-click in the Group Pane and select **New**→ **SIP Line**. On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

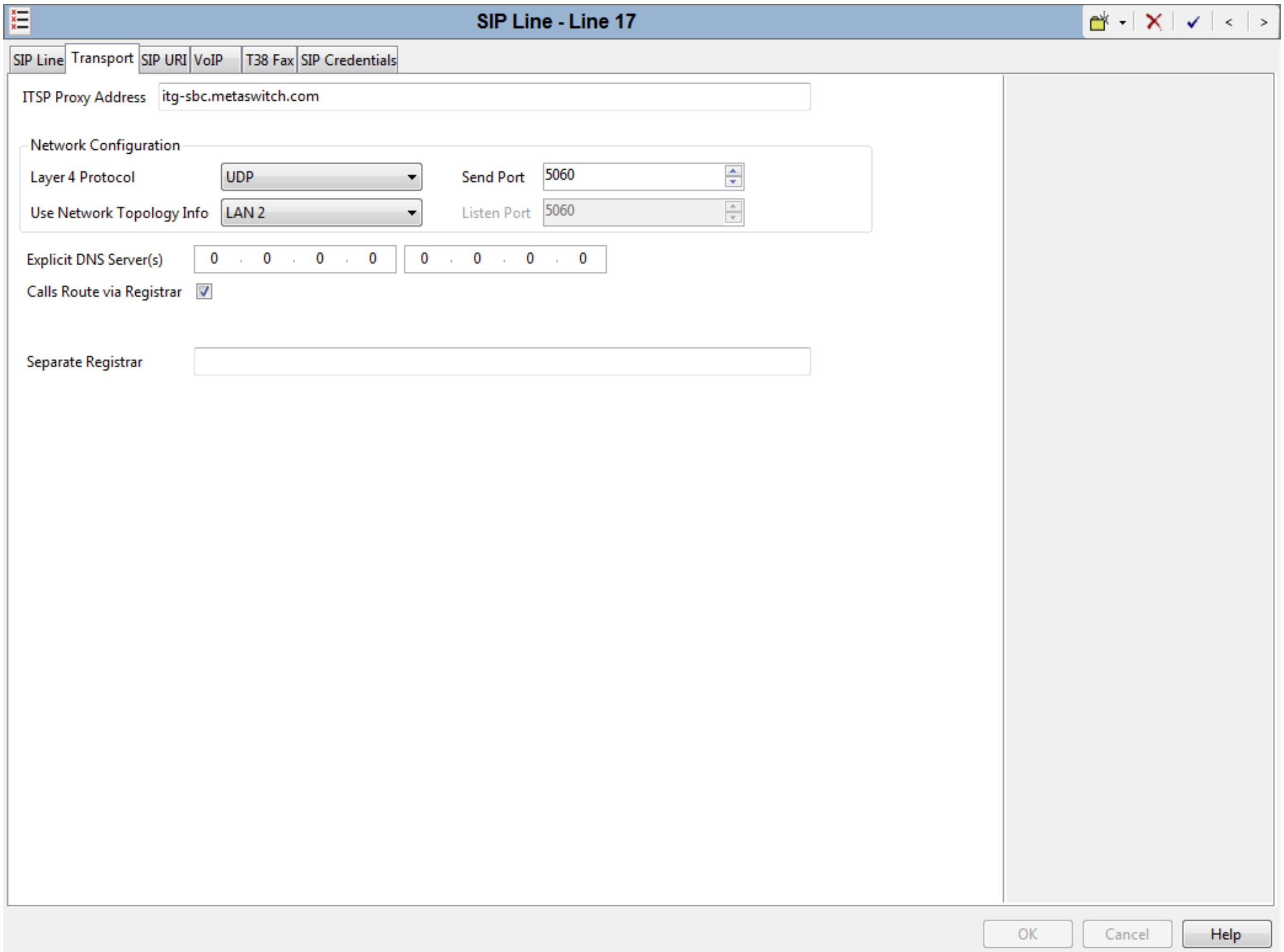
- Set the **ITSP Domain Name** to the required FQDN provided by Metaswitch. IP Office will use this field for the host portion of SIP headers such as the From header
- Check the **In Service** box

- Check the **Check OOS** box. With this option selected, Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line
- Default values may be used for all other parameters

In the following screen, the default automatic determination **of REFER Support** is shown. Alternatively, the default can be overridden with "Never" to explicitly disable use of REFER, or "Always" to explicitly enable use of REFER. The **Association Method** parameter was introduced in IP Office Release 7.0 and the screen below shows the default value, which is sufficient in the sample configuration. The various alternatives for **the Association Method** may be useful when multiple SIP Trunks with different SIP domains resolve to a single IP Address. The default option associates incoming requests with SIP Lines by comparing the source IP Address and port of the incoming message against the configured far-end of the SIP Line.

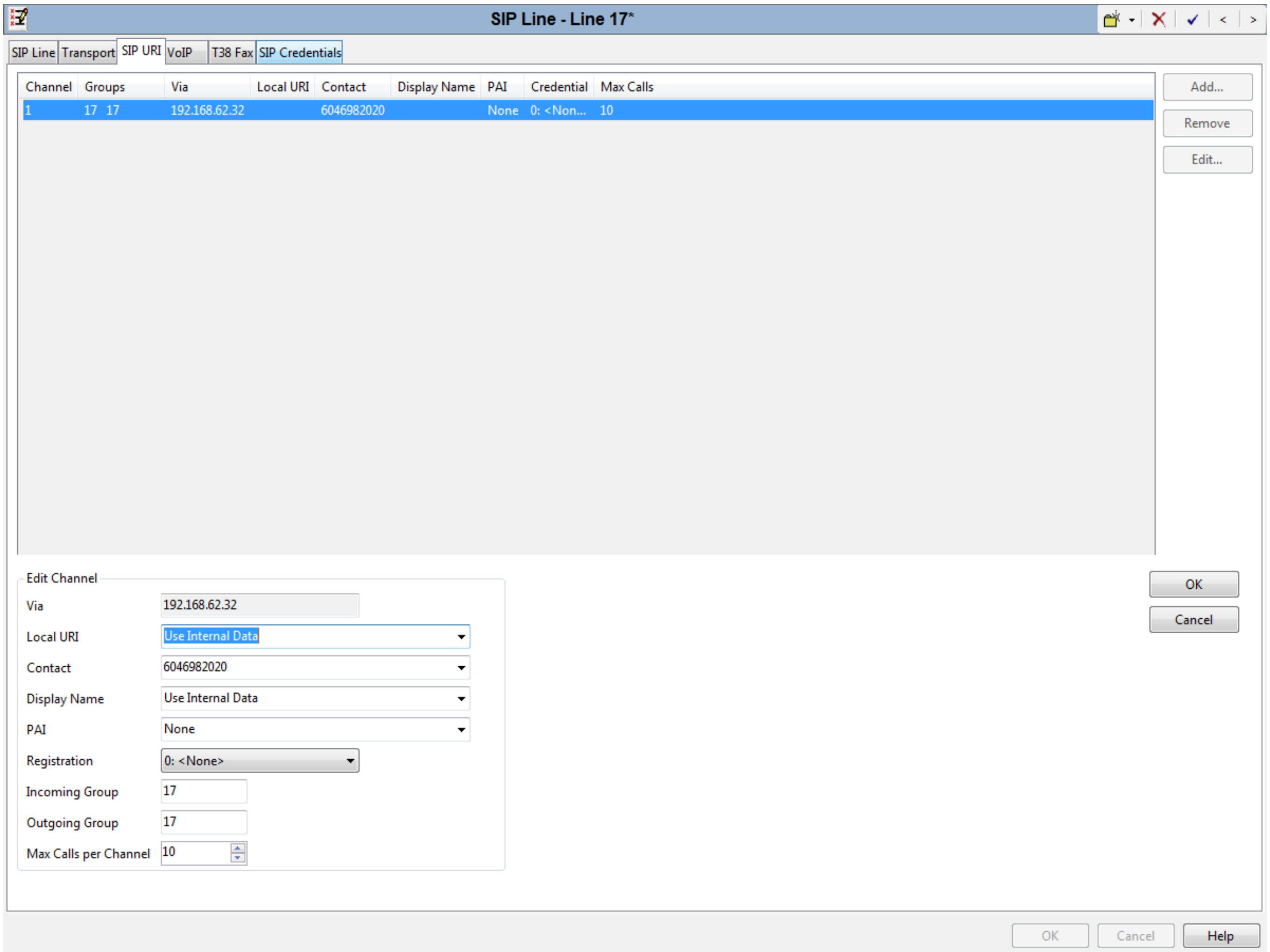


Select the **Transport** tab. Set the **ITSP Proxy Address** to the required FQDN provided by Metaswitch. In **the Network Configuration** area, **UDP** is selected as the **Layer 4 Protocol**, and the **Send Port** is set to the port number provided by Metaswitch. The **Use Network Topology Info** parameter is set to **LAN 2**. This associates the SIP Line with the parameters in the **System → LAN2 → Network Topology tab**. Other parameters retain default values in the screen below.



A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab; click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. In the example screen below, a previously configured entry is edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

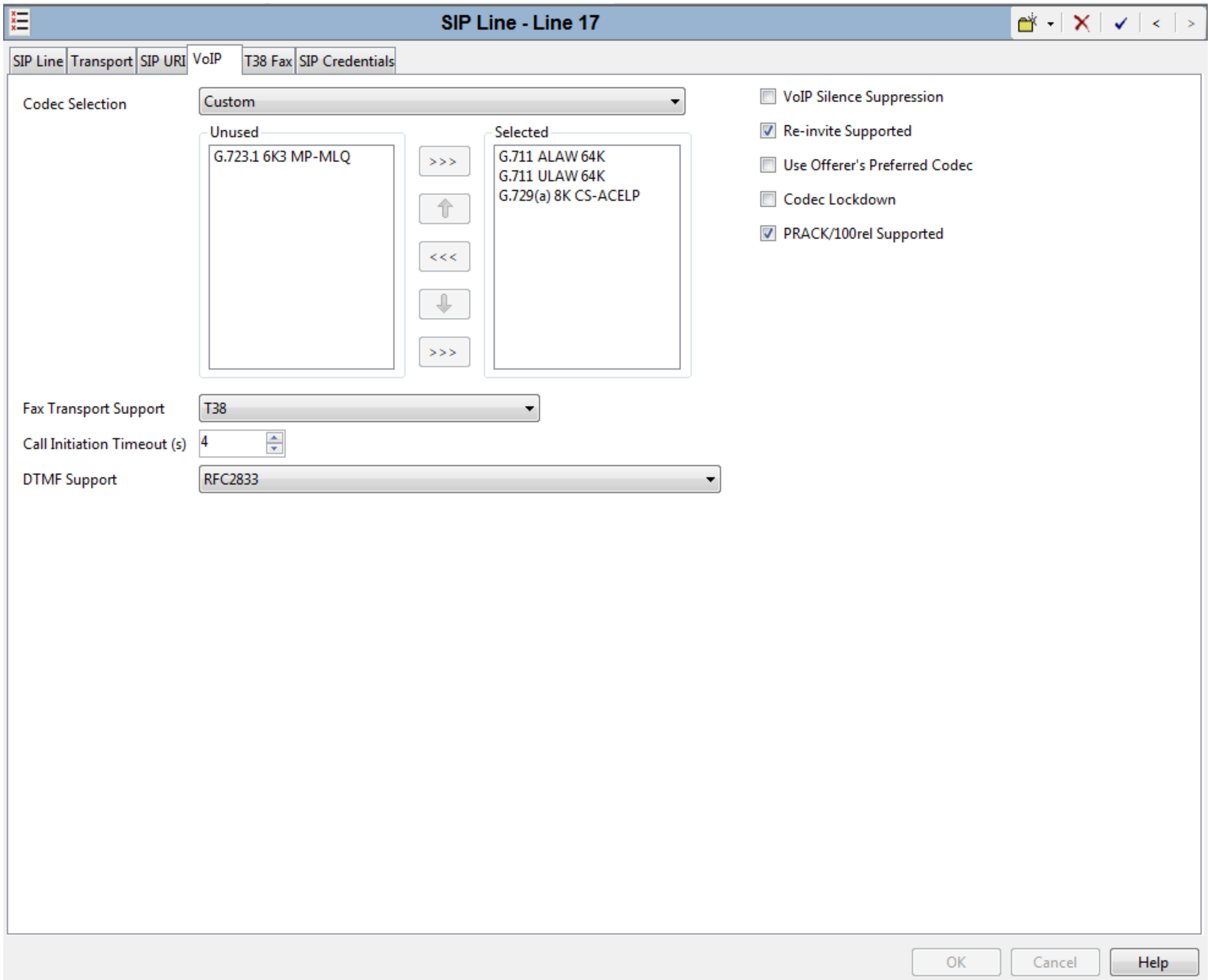
- **Set Local URI and Display Name** to **Use Internal Data**. Metaswitch required the **Contact** to be set to the pilot number of the trunk. These setting allow calls on this line for SIP URIs that match the number set in the **SIP** tab of any **User** as shown in **Section 5.6.**
- Set **PAI** to **None** for this test. The **Source Number**s field was set to **SIP_USE_PAI_FOR_PRIVACY** in **section 5.8** for privacy/anonymous calls.
- For **Registration**, select **None** since Metaswitch didn’t require Registration for this testing. If Registration was required, then the account credentials would have been configured on the line's **SIP Credentials** tab would be entered here.
- Associate this line with an incoming line group in **the Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, a new incoming and outgoing line group **17** was defined.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



SIP Line - Line 17*
SIP Line
Transport
SIP URI
VoIP
T38 Fax
SIP Credentials
Channel
Groups
Via
Local URI
Contact
Display Name
PAI
Credential
Max Calls
1
17 17
192.168.62.32
6046982020
None
0: <Non...
10
Add...
Remove
Edit...
Edit Channel
Via
192.168.62.32
Local URI
Use Internal Data
Contact
6046982020
Display Name
Use Internal Data
PAI
None
Registration
0: <None>
Incoming Group
17
Outgoing Group
17
Max Calls per Channel
10
OK
Cancel
OK
Cancel
Help

Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

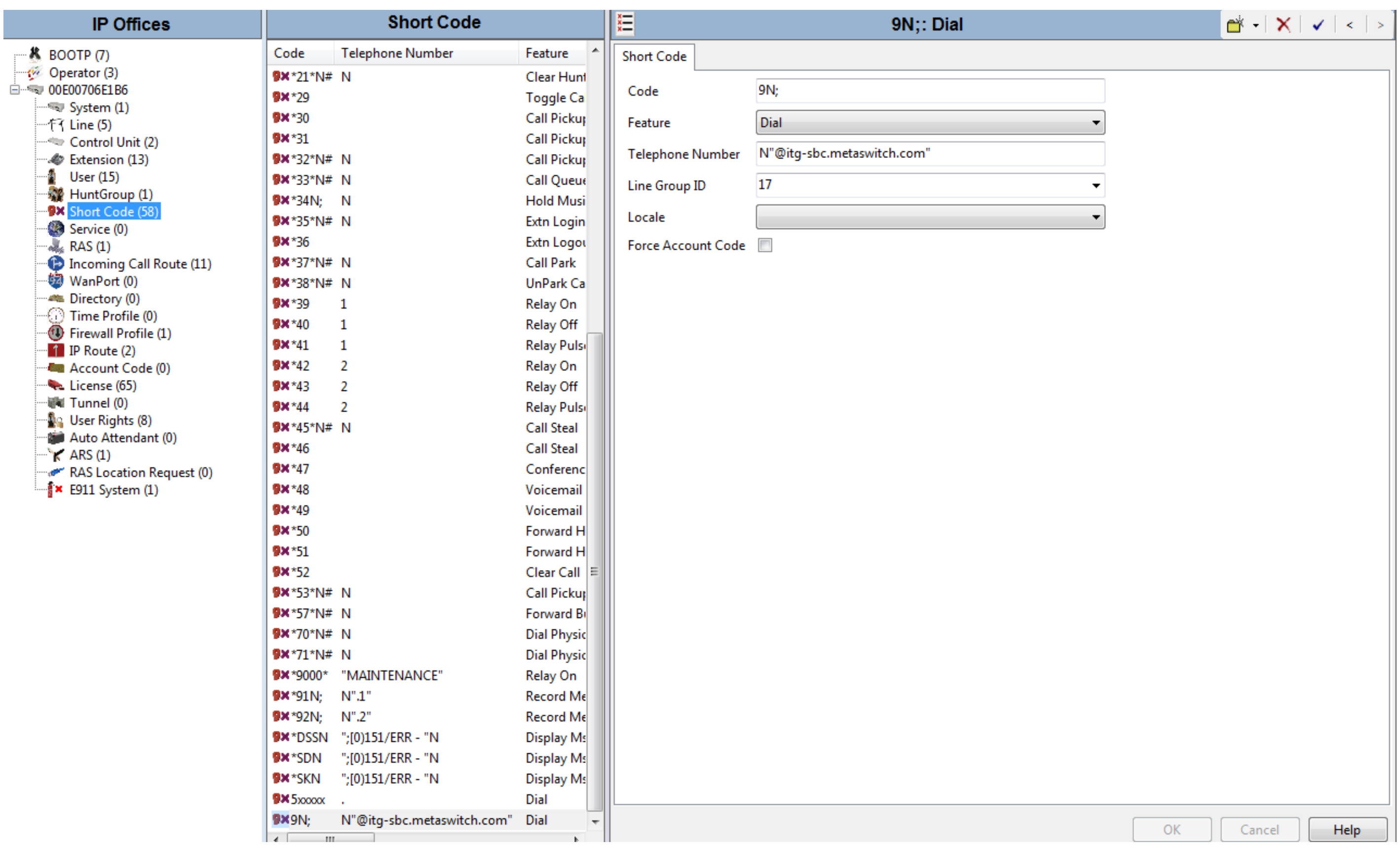
- The **Codec Selection** was configured using the **Custom** option, allowing an explicit ordered list of codecs to be specified These can easily be **Selected** or moved to **Unused** while testing different codecs
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP event messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box. By unchecking the VoIP Silence Suppression box, calls can be established with the G.729 codec but without silence suppression.
- Select **T.38** for **Fax Transport Support**. T.38 faxing is supported by Metaswitch and was successfully tested.
- Check **PRACK/100rel Supported** (default is unchecked). This is new to IP Office 8. SIP trunks can be configured to support early media by adding “100rel to Supported” header in the INVITE. This option sets whether Provisional Reliable Acknowledgement (PRACK) and 100rel are enabled. 100rel allows SDP negotiation to be completed while the call is in ringing state and allows further media changes for announcements or progress tones before a call is actually answered.
- Check the **Re-invite Supported** box.
- Default values may be used for all other parameters.


SIP Line - Line 17
SIP Line
Transport
SIP URI
VoIP
T38 Fax
SIP Credentials
Codec Selection
Custom
Unused
G.723.1 6K3 MP-MLQ
Selected
G.711 ALAW 64K
G.711 ULAW 64K
G.729(a) 8K CS-ACELP
VoIP Silence Suppression
Re-invite Supported
Use Offerer's Preferred Codec
Codec Lockdown
PRACK/100rel Supported
Fax Transport Support
T38
Call Initiation Timeout (s)
4
DTMF Support
RFC2833
OK
Cancel
Help

5.5. Short Code

Define a short code to route outbound traffic to the SIP line. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered **"9N;"** short code used in the test configuration.

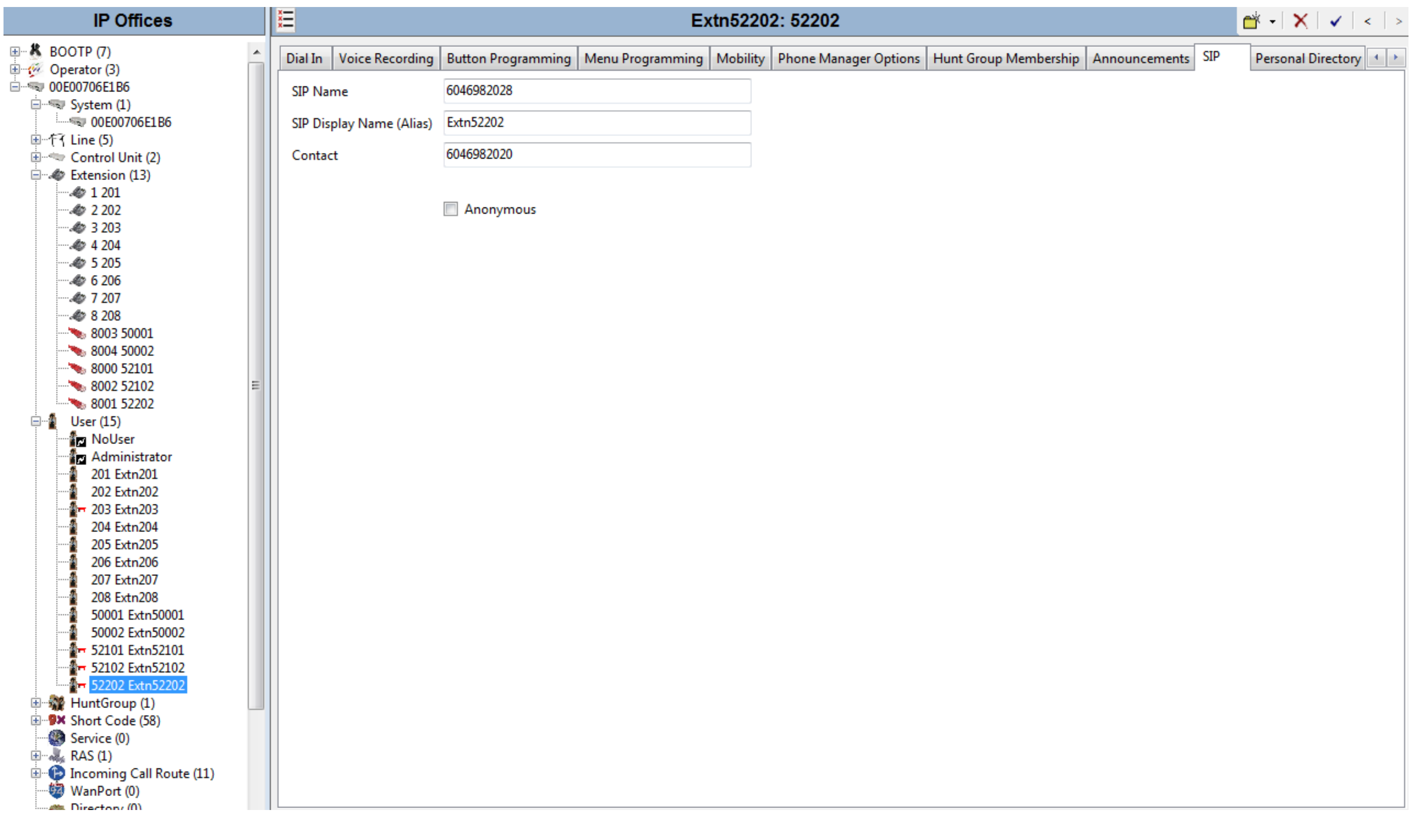
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semicolon. In this case, **9N;.** This short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N"@itg-sbc.metaswitch.com".** This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value N represents the number dialed by the user.
- Set the **Line Group ID** to the outgoing line group number defined on the SIP URI tab on the **SIP Line** in **Section 5.4**. This short code will use this line group when placing the outbound call.



5.6. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line. To configure these settings, first select **User** in the left Navigation Pane. In the example below, the name of the user is **"Extn52202"**. Select the **SIP** tab in the Details Pane.

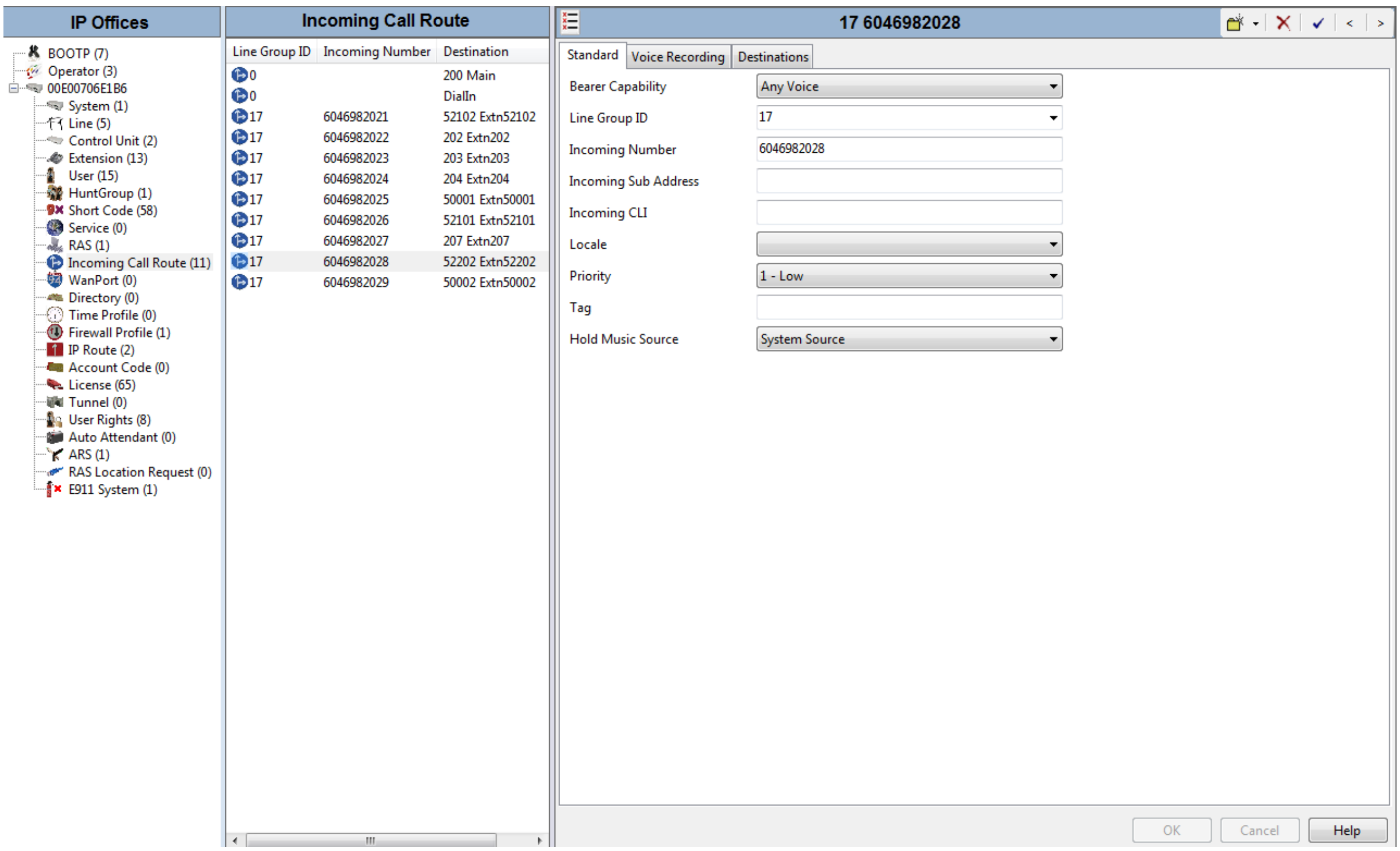
The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. The **SIP Name** is set to one of the DID numbers assigned to the enterprise and the **Contact** is the pilot number, both provided by Metaswitch. This is the same pilot number configure on the **SIP URI** in **Section 5.4**. The **SIP Display Name** (Alias) parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.



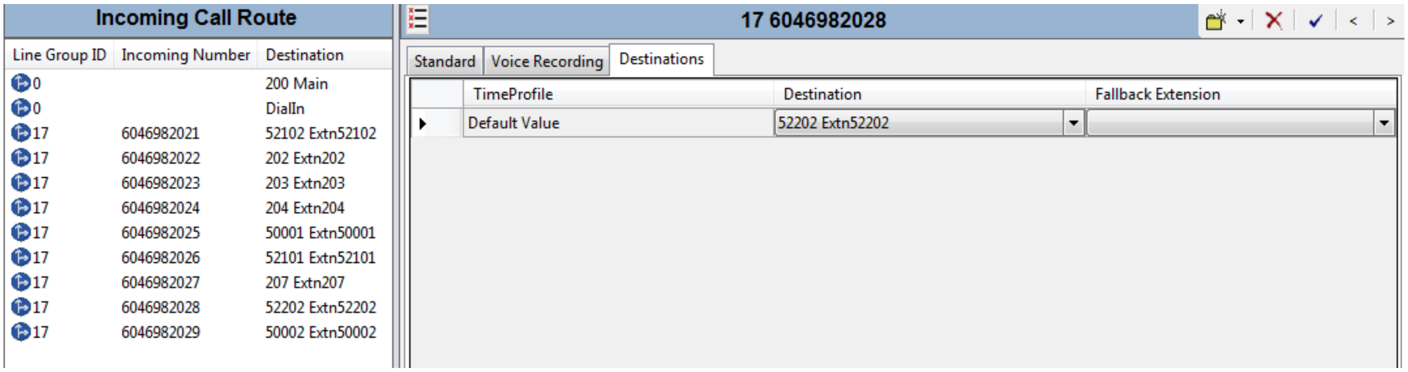
5.7. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by Metaswitch. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right click in the center Group Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Default values can be used for all other fields.



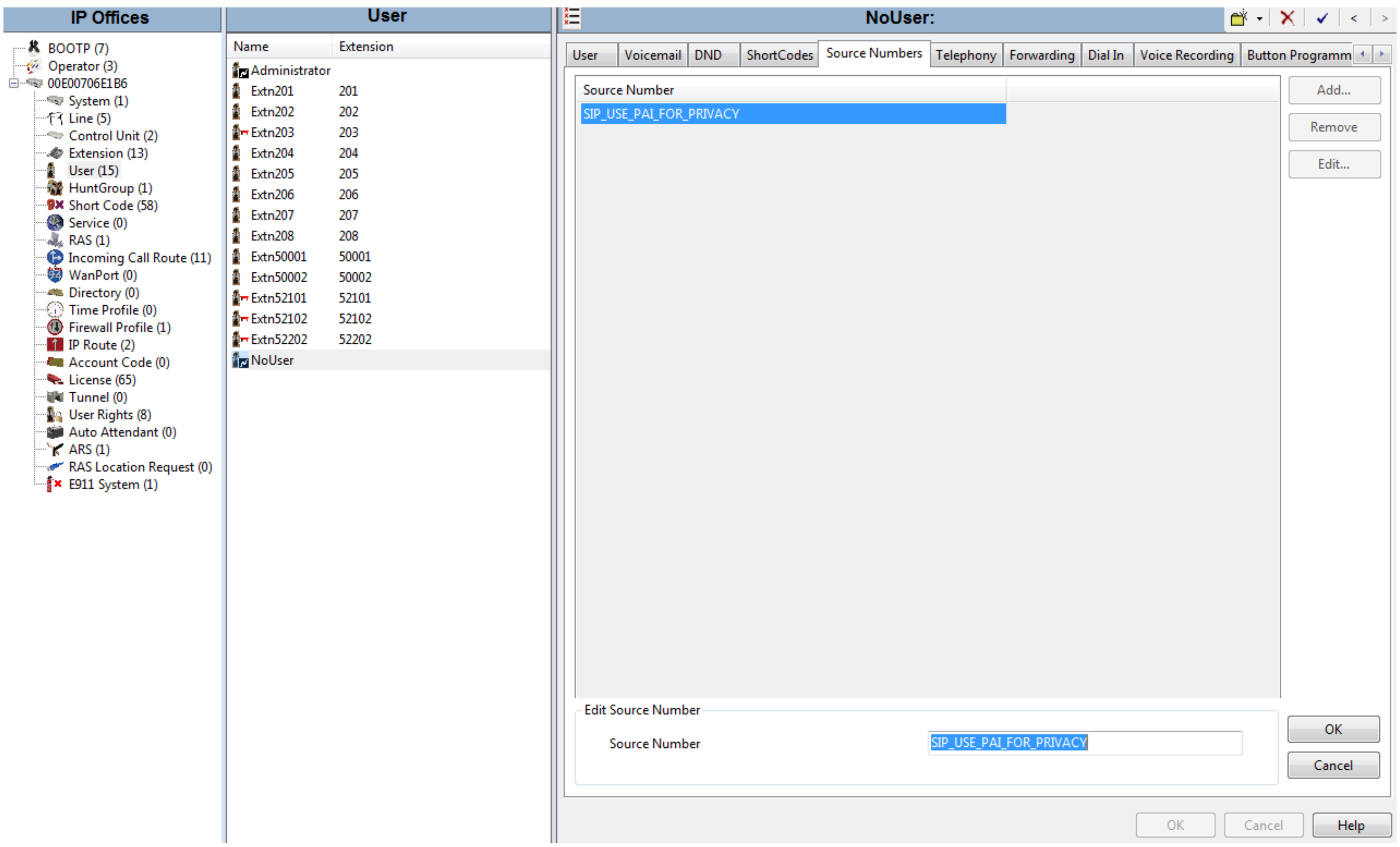
On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to 6046982028 on line 17 are routed to user 52202 Extn52202.



5.8. Privacy/Anonymous Calls

For outbound calls with privacy (anonymous) enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with "restricted" and "anonymous" respectively. Avaya IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI) header to pass the actual calling party information for authentication and billing. For the compliance test, PAI was used for the purposes of privacy. To configure Avaya IP Office to use PAI for privacy calls, navigate to **User** → **NoUser** in the Navigation / Group Panes. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.

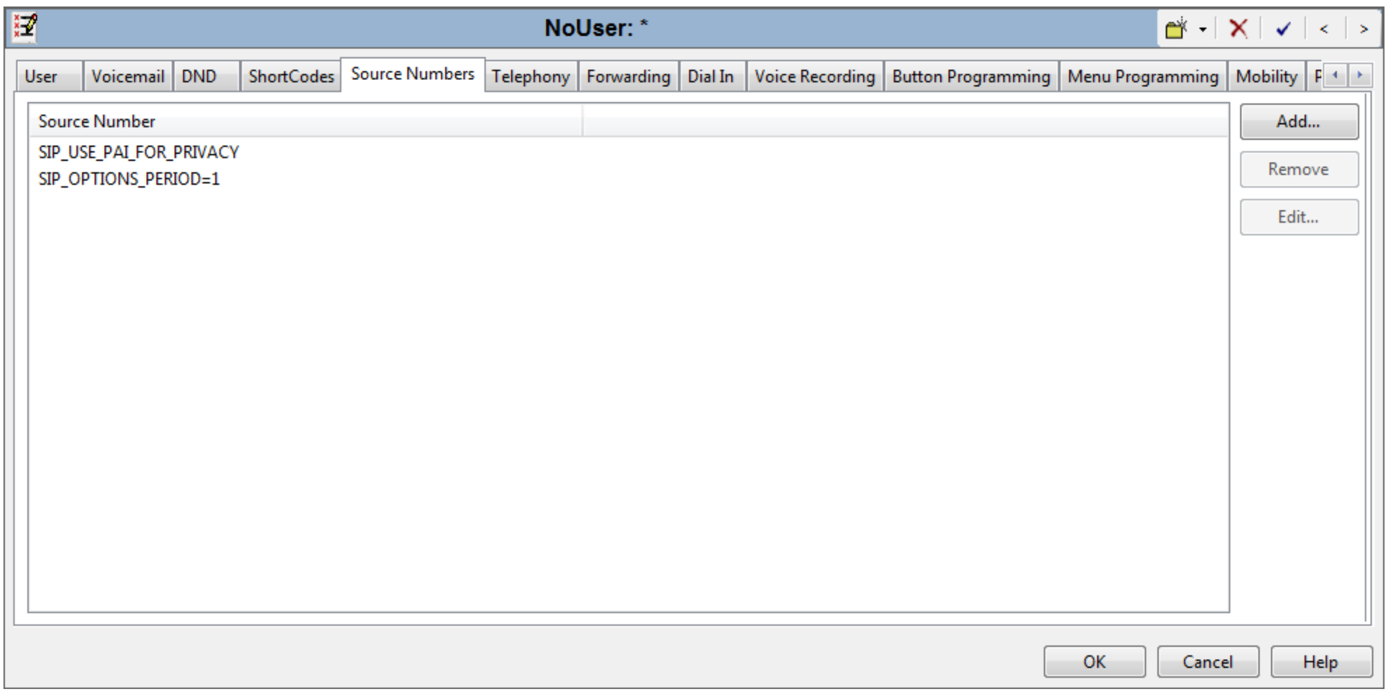
At the bottom of the Details Pane, the Source Number field will appear. Enter **SIP_USE_PAI_FOR_PRIVACY**. Click **OK**.



5.9. SIP Options Frequency

Avaya IP Office sends **SIP OPTIONS** messages periodically to determine if the SIP connection is active. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set on the **Network Topology** tab in **Section 5.2** and the **SIP_OPTIONS_PERIOD** parameter (in minutes) that can be set on the Source Number tab of the **NoUse**r user.

To configure the **SIP_OPTIONS_PERIOD** parameter, navigate to **User → NoUser** in the Navigation / Group Panes. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button. In the Source Number field shown below, type **SIP_OPTIONS_PERIOD=X**. X is a value (in minutes) representing a longer time than the interval configured (in seconds) in the **Binding Refresh Time**. In the sample configuration, the value used for X was 1 minute. Click **OK**.



5.10. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections

6. Configure Metaswitch

During the test effort, the Metaswitch network was protected by Metaswitch Perimeta Session Border Controller. The session border controller is not required as part of the solution. Basic configuration is provided below. If a Perimeta Session Border controller is used between the MetaSphere CFS solution and the Avaya IP Office solution, contact a Metaswitch Networks support representative for additional configuration details.

6.1. Media Gateway Model

A truncated text dump of the Remote Media Gateway Model used for the Avaya IP Office testing is shown below. For an importable version, contact a Metaswitch customer service representative.

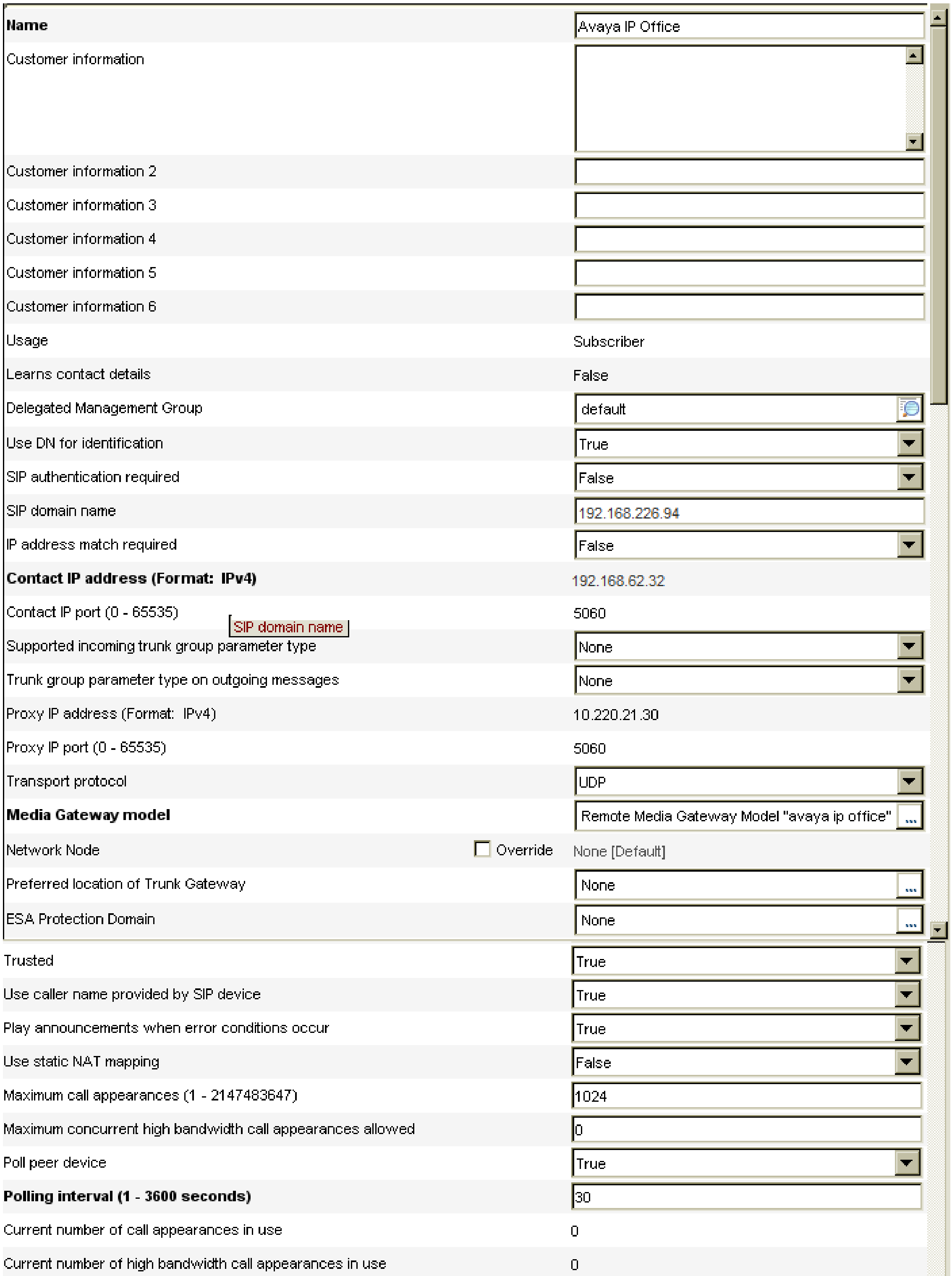
begin MediaGatewayModel // Remote Media Gateway Model "avaya ip office"

Category	SIP
ModelName	avaya ip office
ControlProtocol	SIP
DefaultModel	False
AlertInfoStringsForDistinctiveRingingHeading	Alert-Info strings for Distinctive Ringing
SignalingSettingsHeading	Signaling settings
SupportedHighBandwidthMediaFormats	{G.711 u-law,G.711 A-law}
LowBandwidthVoiceCodecsSupportedAsStandard	{G.726 32kbps,G.729 (A/AB)}
AdvancedVoiceCodecsPermitted	Any codecs
VideoCodecsPermitted	Any codecs
OrderOfPreferenceForSupportedCodecs	G726-32/8000|G729/8000
PacketizationInterval	0
SilenceSuppressionAllowed	False
MaximumSimultaneousTransactionsOutstanding	100
DigitOverhangTime	250
FixBitsMGCPMeGaCoSIPMSML	{Cannot be hub,Simple contexts,Cannot play ringback,Cannot control endpoint connectivity,Cannot move contexts,Connections always receive,Cannot report detection of call-type discrimination tones,T.38 supported}
DynamicFixBitsMGCPMeGaCoSIPMSML	{}
FixBitsSIP	{Supports SDP connectivity requests,Supports receiving INVITEs with no SDP,Supports receiving SIP Reason header over tandem trunk calls}
FixBitsSIP2	{}
SIPResponseCodeForESAFailure	503
ReferenceCount	1
UpToDateCount	1
ExportHeading	Export
StatusHeading	Status
RequestedStatus	Enabled

end //MediaGatewayModel

6.2. Configured SIP Bindings

The connection to Avaya IP Office is modeled as a configured SIP binding. During compliance testing, the configured SIP Binding was configured as shown below.



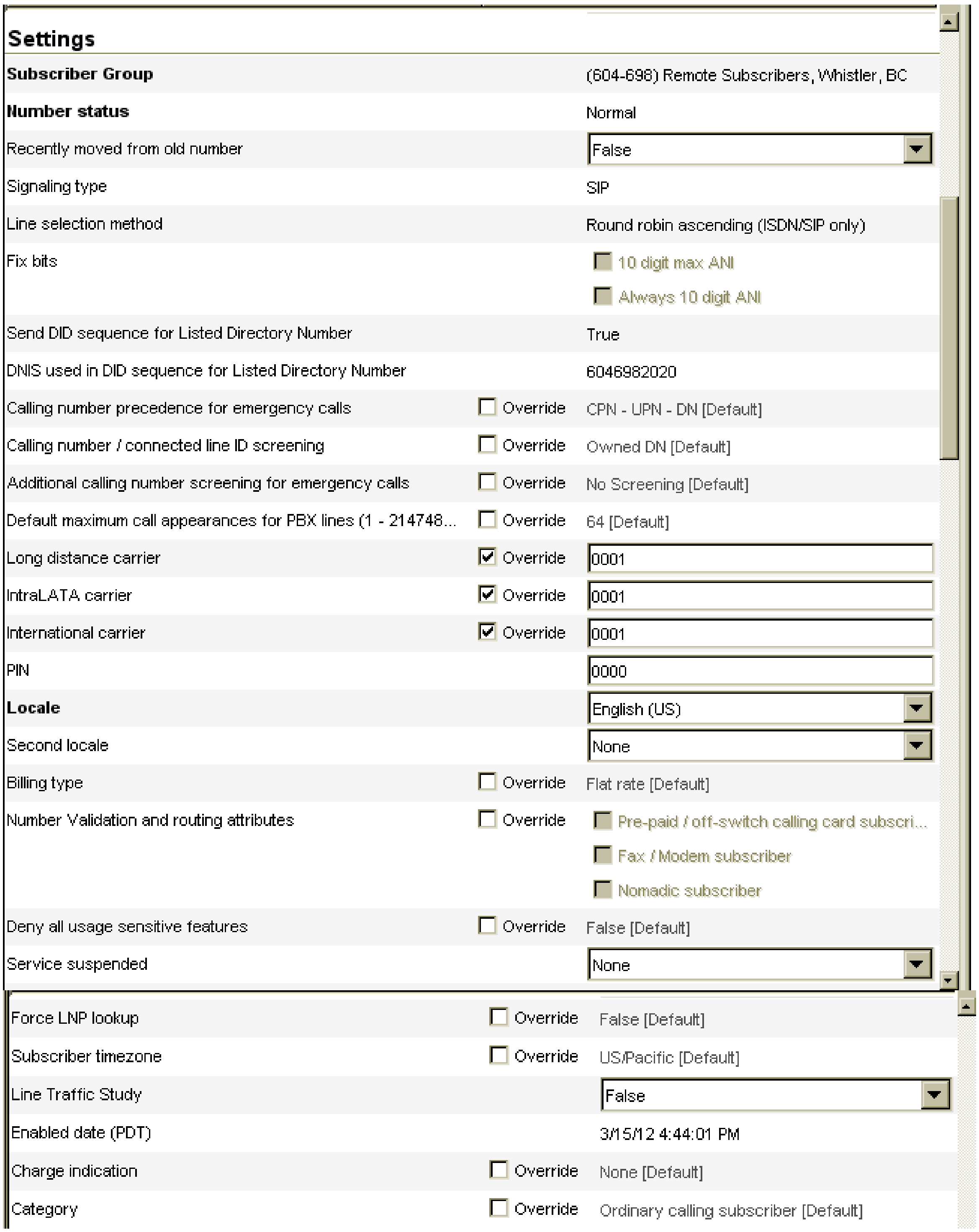
Name	Avaya IP Office
Customer information	
Customer information 2	
Customer information 3	
Customer information 4	
Customer information 5	
Customer information 6	
Usage	Subscriber
Learns contact details	False
Delegated Management Group	default
Use DN for identification	True
SIP authentication required	False
SIP domain name	192.168.226.94
IP address match required	False
Contact IP address (Format: IPv4)	192.168.62.32
Contact IP port (0 - 65535)	5060
Supported incoming trunk group parameter type	None
Trunk group parameter type on outgoing messages	None
Proxy IP address (Format: IPv4)	10.220.21.30
Proxy IP port (0 - 65535)	5060
Transport protocol	UDP
Media Gateway model	Remote Media Gateway Model "avaya ip office"
Network Node ☐ Override	None [Default]
Preferred location of Trunk Gateway	None
ESA Protection Domain	None
Trusted	True
Use caller name provided by SIP device	True
Play announcements when error conditions occur	True
Use static NAT mapping	False
Maximum call appearances (1 - 2147483647)	1024
Maximum concurrent high bandwidth call appearances allowed	0
Poll peer device	True
Polling interval (1 - 3600 seconds)	30
Current number of call appearances in use	0
Current number of high bandwidth call appearances in use	0

SIP domain name

6.3. PBX Object Configuration

The Avaya IP Office is modeled in MetaView as a PBX. The settings used during compliance testing are shown in the sections below.

6.3.1. PBX Object



Settings

Subscriber Group		(604-698) Remote Subscribers, Whistler, BC
Number status		Normal
Recently moved from old number		False
Signaling type		SIP
Line selection method		Round robin ascending (ISDN/SIP only)
Fix bits		☐ 10 digit max ANI ☐ Always 10 digit ANI
Send DID sequence for Listed Directory Number		True
DNIS used in DID sequence for Listed Directory Number		6046982020
Calling number precedence for emergency calls	☐ Override	CPN - UPN - DN [Default]
Calling number / connected line ID screening	☐ Override	Owned DN [Default]
Additional calling number screening for emergency calls	☐ Override	No Screening [Default]
Default maximum call appearances for PBX lines (1 - 214748...	☐ Override	64 [Default]
Long distance carrier	☑ Override	0001
IntraLATA carrier	☑ Override	0001
International carrier	☑ Override	0001
PIN		0000
Locale		English (US)
Second locale		None
Billing type	☐ Override	Flat rate [Default]
Number Validation and routing attributes	☐ Override	☐ Pre-paid / off-switch calling card subscri... ☐ Fax / Modem subscriber ☐ Nomadic subscriber
Deny all usage sensitive features	☐ Override	False [Default]
Service suspended		None
Force LNP lookup	☐ Override	False [Default]
Subscriber timezone	☐ Override	US/Pacific [Default]
Line Traffic Study		False
Enabled date (PDT)		3/15/12 4:44:01 PM
Charge indication	☐ Override	None [Default]
Category	☐ Override	Ordinary calling subscriber [Default]

6.3.2. PBX Line Object

Settings		
Configured SIP Binding		Avaya IP Office
Maximum call appearances (1 - 2147483647)	☑ Override	10
Call burst threshold (0 - 2147483647)		0
Line usage		Voice and fax
PBX plays ringback		False

6.3.3. DID Objects

Type	DID range
Description	normal
Range size (1 - 1000000000)	9
(First) Directory number	6046982021
Last Directory number	6046982029
First code	6046982021
Last code	6046982029

6.3.4. Perimeta SBC Configuration

Adding a Trusted Device (e.g. PBX, Proxy, and Application Server) into the Perimeta SBC:

- Login into Perimeta and enter the defcraft menu as shown below

```
SUMMARY
-------
Tue Apr 10 00:24:09 BST 2012 = Mon Apr 9 23:24:09 UTC 2012
This is processor B.
Processor B is the primary processor

Process  RunningTime
ethmgr   14-03:10:07
vpcn      5-21:54:11
vpsi      5-21:54:07


CPU2:ITG-PerimetaB:~# su - defcraft

--------------------------------------------------------------------------------

                                                     10-Apr-2012 00:24:31 +0100
Perimeta ISC ITG-Perimeta is running
WARNING: System running on an unsupported hardware configuration for role.
This is processor-blade B; processor-blade A is contactable;
Session Controller is partnered; processor-blade B is primary
[Main] [=]
  Select a command group or command
  Press ENTER to refresh
0   Exit        < Log off the craft menu
1   CLI           Command Line Interface
2   Admin       > Administrator Function
3   Software    > Update Perimeta Session Controller Software
4   Diagnostics > Retrieve Diagnostic Information
:
```

- Enter the CLI interface.
- Go into Configuration Mode and navigate to the trusted sources section as follows:
  - System -> ip-access-control ->trusted-sources

```
--------------------------------------------------------------------------------

% Warning: this system is not licensed.  Enter your license key using the
apply-license command or contact your sales representative to acquire a valid
license key.
ITG-Perimeta#config
ITG-Perimeta(config)#system
ITG-Perimeta(system)#ip-access
ITG-Perimeta(ip-access-ctrl)#trusted-sources
```

- Add in the appropriate ip addresses of the trusted devices as follows:
  - **Prompt>** permit-peer service-network 1 ipv4 <***ip-address***>

```
ITG-Perimeta(trusted-src)#?
  end                                  Return to top level mode
  exit                                 Exit the current CLI mode
  no                                   Remove object or set config to default
  permit-peer                          Configure a trusted IP device
ITG-Perimeta(trusted-src)#permit-peer service-network 1 ipv4 123456789012
```

- Type **exit** until out of the CLI command tree (e.g. system > ip-access-control > trusted-sources > permit-peer > service-network 1)

7. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP line of interest from the left pane. On the Status tab in the right pane, verify that the Current State is **Idle** for each channel (assuming no active calls at present time).
- The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start →Programs →IP Office →Monitor**. This application allows the monitored information to be customized. To customize, select **Filters →Trace Options**.
- Verify that the H.323, SIP, Digital and Analog endpoints on the enterprise site can place calls terminating over the SIP trunk and the call can remain active for more than 35 seconds.
- Verify that the endpoints at the enterprise site can receive calls from the CommPortal registered to Metaswitch CFS and can remain active for more than 35 seconds.
- Verify that the CommPortal can terminate an active call by hanging up.
- Verify that an endpoint at the enterprise site can terminate an active call by hanging up.

8. Conclusion

Metaswitch SIP Trunking passed compliance testing. These Application Notes describe the procedures required to configure the SIP trunk connection between Avaya IP Office and the Metaswitch SIP Trunking service as shown in **Figure 1**. Please refer to **Section 2.2** above for Test Results and any Limitations that were observed.

9. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

(1) IP Office 8.0 Manager 10.0, Document number 15-601011, May 21, 2012

(2) IP Office 8.0 IP Office Basic Edition, Quick Mode Installation, Document number 5-601042, April 27, 2012

(3) IP Office System Status Application, Document number15-601758, November 12, 2011.

(4) RFC 3261 SIP: Session Initiation Protocol

Additional IP Office documentation can be found at http://marketingtools.avaya.com/knowledgebase

Product documentation for Metaswitch SIP Trunking is available from Metaswitch.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.