Avaya IP Office 4.0
Customer Configuration Guide
SIP Trunking Configuration
For Use with Cbeyond's
BeyondVoice with SIPconnect Service

Issue 2.2
06/25/2007

Table of contents

List of Figures

History

Version	Date	Review
1.0	01/27/2007	Cbeyond Internal
2.0	03/02/2007	Bob Bellinger's review
2.1	06/08/2007	Bob Bellinger's review
2.2	06/25/2007	Philippe du Fou's and Greg Rothman's review

1 Introduction

This document provides a configuration guide to assist administrators in connecting Avaya IP Office Communication System to Cbeyond's BeyondVoice with SIPconnect service.

2 Special Notes

Fax is Not Supported

IP Office does not support fax transmission using SIP.

In order for Cbeyond BeyondVoice with SIPconnect customers to have business grade fax service, they can use the analog ports provided on the Integrated Access Device (IAD) that Cbeyond deploys at their premise. Two analog ports are provisioned at no charge. Up to fourteen other ports can be provisioned for $10 per port per month. Note that an analog port is not extra call capacity, but just another connection sharing the same total capacity. For example,if a SIPconnect customer has 2 fax lines, 10 DIDs, and 6 SIP trunks, only 4 SIP trunks are available if 2 fax machines are currently in use.

2.1 Connectivity Issues of VoIP

SIP protocol uses IP addresses embedded into its messages. This issue creates a problem while performing NAT transversal.

Network Address Translator (NAT), is a network element that creates a binding between a private IP address and transport port and global ones. As a result the IP address and transport embedded in SIP message embedded in SIP message can be those of a private network. Once SIP Server will receive them, either it will be able to spot the difference between the IP headers and SIP messages, (for instance using a Session Border Controller), or may fail to successfully establish the call. NAT functionality is embedded in most of DSL routers therefore its unique deserves characterization.

RFC 3489, defines a protocol STUN protocol (Simple Transversal of UDP through NAT) to solve the problem of SIP and NAT.

The aim of STUN in to assess the nature of network connectivity the SIP User Agent views is seeing. Based on a number of tests that protocol runs using external servers, the results can be classified as:

1. Open Internet: no NAT or firewall present
2. Symmetric Firewall: SDP unchanged but ports need to be opened and kept open with keep-alive
3. Full Cone NAT: SDP needs to be mapped to the NAT address and port; any Host in the Internet can call in on the Open Port
4. Symmetric NAT: SDP needs to be mapped but STUN will not provide the correct info unless the IP Address on the STUN server is the same as the ITSP Host.
5. Restricted Cone NAT: SDP needs to be mapped. Responses from Hosts are restricted to those that a packet has been sent to.
6. Port Restricted Cone NAT: SDP needs to be mapped. Keep-alive must be sent to all ports that will be the source of a packet for each ITSP Host IP Address

If IP Office sits behind ***Symmetric NATs*** and ***Port Restricted NATs*** there might be problems in establishing connection with SIP. IP Office *Network Topology Discovery* under *System* tab allows instructing IP Office to run STUN discovery and obtaining information on the type of connectivity the system has been provided. Please see section 4.5 for more information.

2.1 Examples of common network topology

ITSP with Session Border Controller

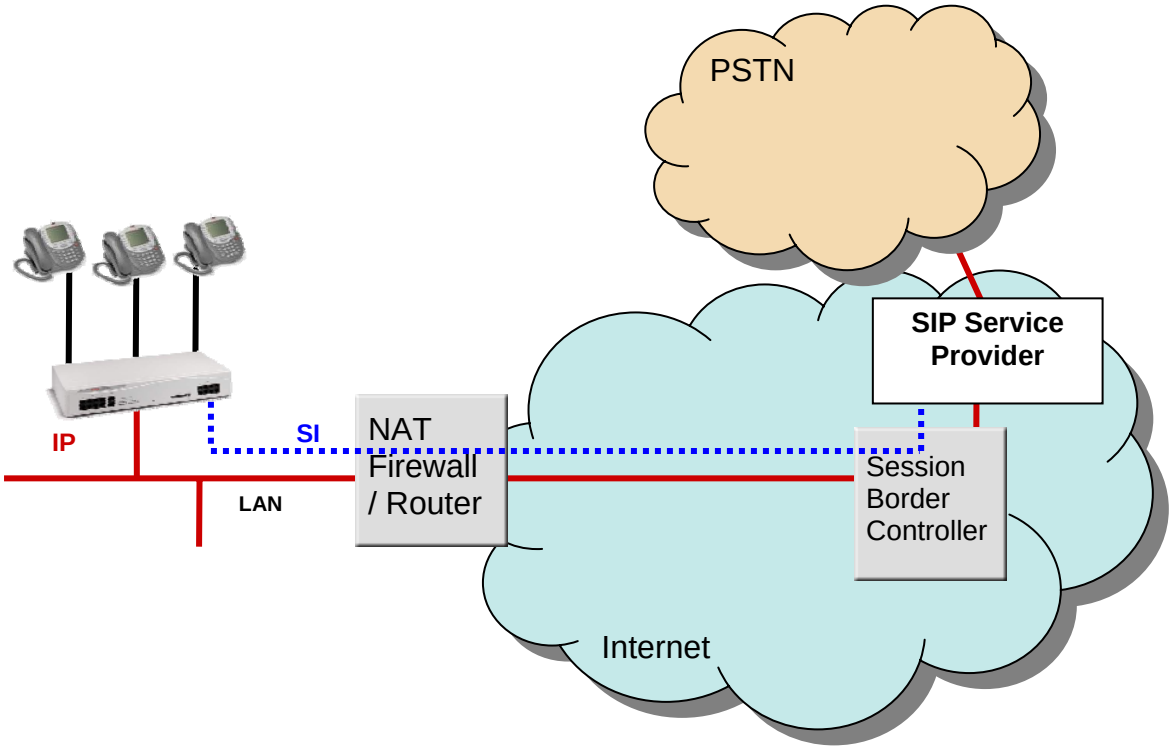

Figure 1: ITSP with SBC

Figure 1 depicts a common scenario where ITSP equipment is provisioned with Session Border Controller (SBC) to filter any inconsistency between IP header and SIP messages deriving from NAT transversal. In such configuration running STUN is not necessary, as ITSP network will take responsibility of any packet filtering.

ITSP Connection Using STUN Server

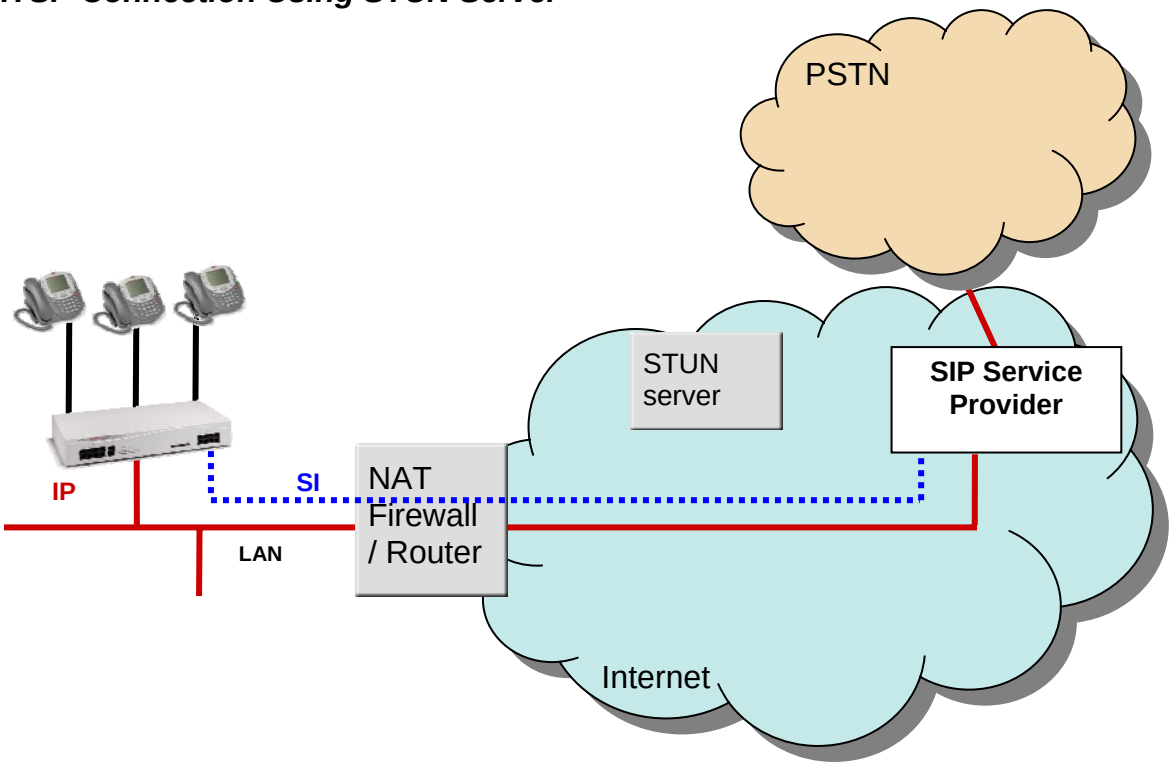

Figure 2: ITSP Connection Using STUN

Figure 2 depicts a scenario where ITSP network has no infrastructure to support NAT transversal, therefore STUN must be employed to support both signaling and media paths. Network Topology Discovery shall be employed and used for each trunks configured.

ITSP Connection Using Demilitarised Zone (DMZ)

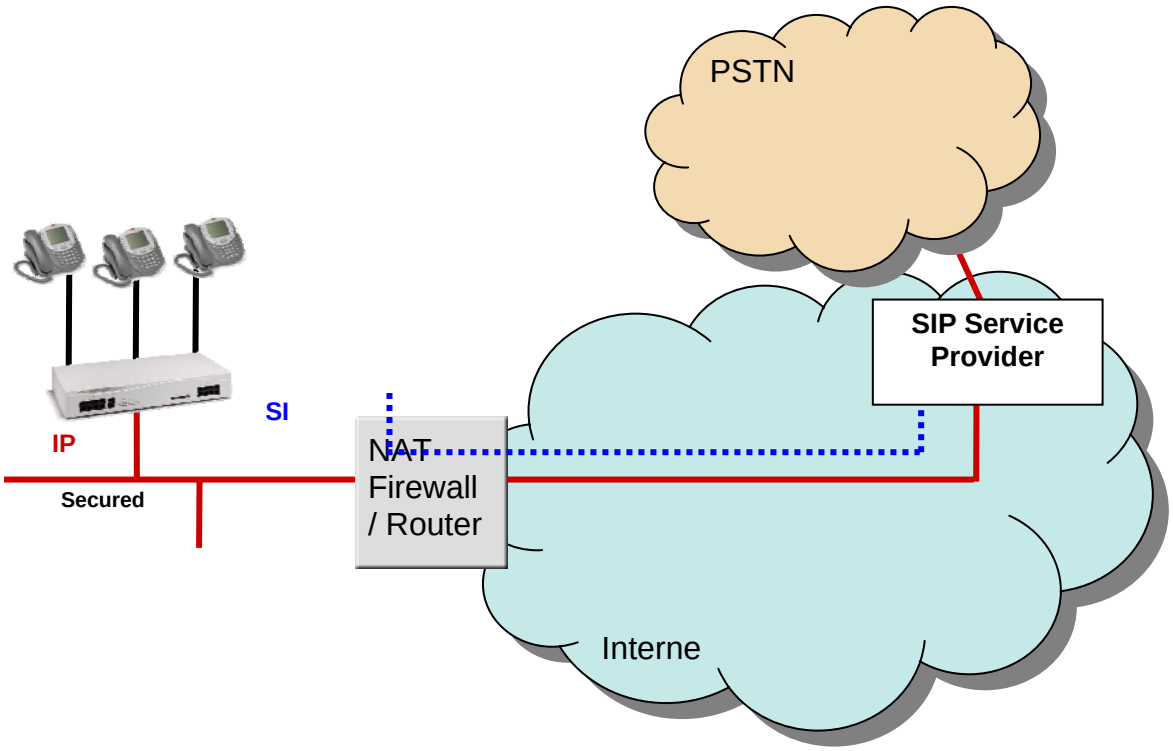

Figure 3: ITSP connection via DMZ

Figure 3 depict a case where STUN discovery has been run, but unfortunately has resolved into the discovery of a NAT that is not SIP friendly and does not allow complete call establishment. If such kind of NAT is discovered, a ***warning will be issued at the end of STUN discovery***.
Setting up a demilitarized zone requires having to network interfaces, one to be dedicated to direct Internet connection that bypasses the NAT/ Firewall that is used for all other types of media.

3 SIP Trunks in IP Office

3.1 Supported Platforms

SIP trunks are supported in the following platforms:

- Small Office Edition
- IP406v2
- IP412
- IP500

3.2 Supported Phone Types

A list of supported phone is provided below:

2400/5400 series digital
3600 series WiFi (wireless IP)
4600/5600 series IP
6400 series digital
T3 (IP and digital) –excluding Small Office
3701/3711 (IP DECT)
Analogue phone

3.3 Voice Coders Supported (VCM) per platform

- IP Office Communication System Small Office Edition: either VCM 3 or VCM 16.
- IP406v2 supports a single VCM chosen among the following types: VCM4, VCM 5, VCM 8, VCM 10, VCM 16, VCM 20, VCM 24 and VCM 30.
- IP412 supports any two cards VCM's of the following types; VCM4, VCM 5, VCM 8, VCM 10, VCM 16, VCM 20, VCM 24 and VCM 30.
- IP500 supports two variants: First is legacy VCM cards in number of two selected between the following options: VCM4, VCM 8, VCM 16, VCM 24 and VCM 30. Second option is new VCM cards in number of two from any VCM 32 and 64.

The number of calls supported on the VCM card is specified by the VCM card number (i.e. VCM 5 supports 5 calls, etc).

4 Customer Configuration Guide

This configuration guide specifies the Avaya IP Office Communication System screens that must be configured and updated to support the Cbeyond Voice over Managed Services.

In order to enable SIP communication you will need a valid SIP trunking license and IP Office with VCM cards.

4.1 How to identify you are running version 4.0

Users can identify the version number they are running by to looking at the top line of their manager screen and identify the Manager and Core version.
An example is given in Figure 1.

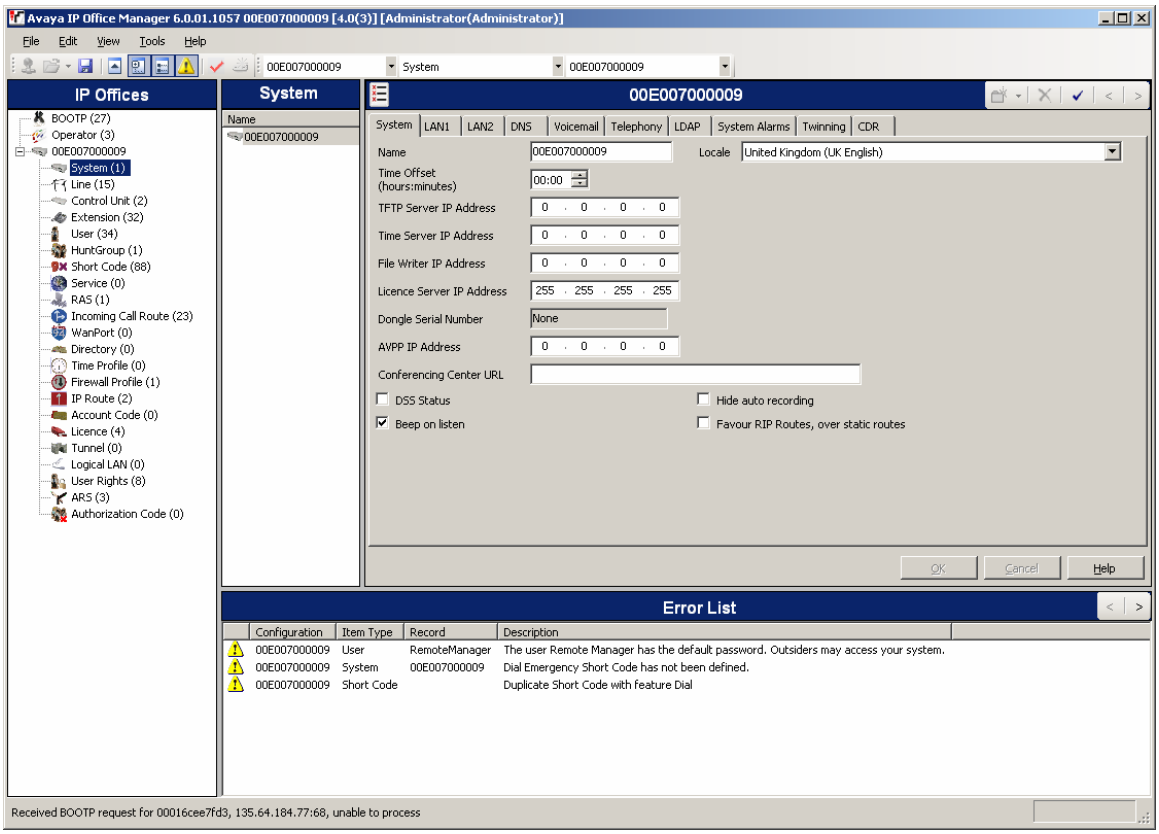

Figure 4: Example of Manager Screen Shot

In the example of Figure 4, the Manager Version 6.0.01.1057, and the IP Office Core software version is 4.0 (3).

4.2 How to check for SIP Trunking Licenses

To make calls using SIP you must have a valid license that can be purchased through Avaya business partners, in the number of 1, 5, 10, 20 or a combination of all the above up to 128 instances of the same license. Avaya will provide a license that will need to be inserted into license form. An example is provided in Figure 5. License can be shared among different SIP trunks; the number of instances represents the maximum number of calls that can be dialed or received at the same time by IP Office using any of its SIP trunks.

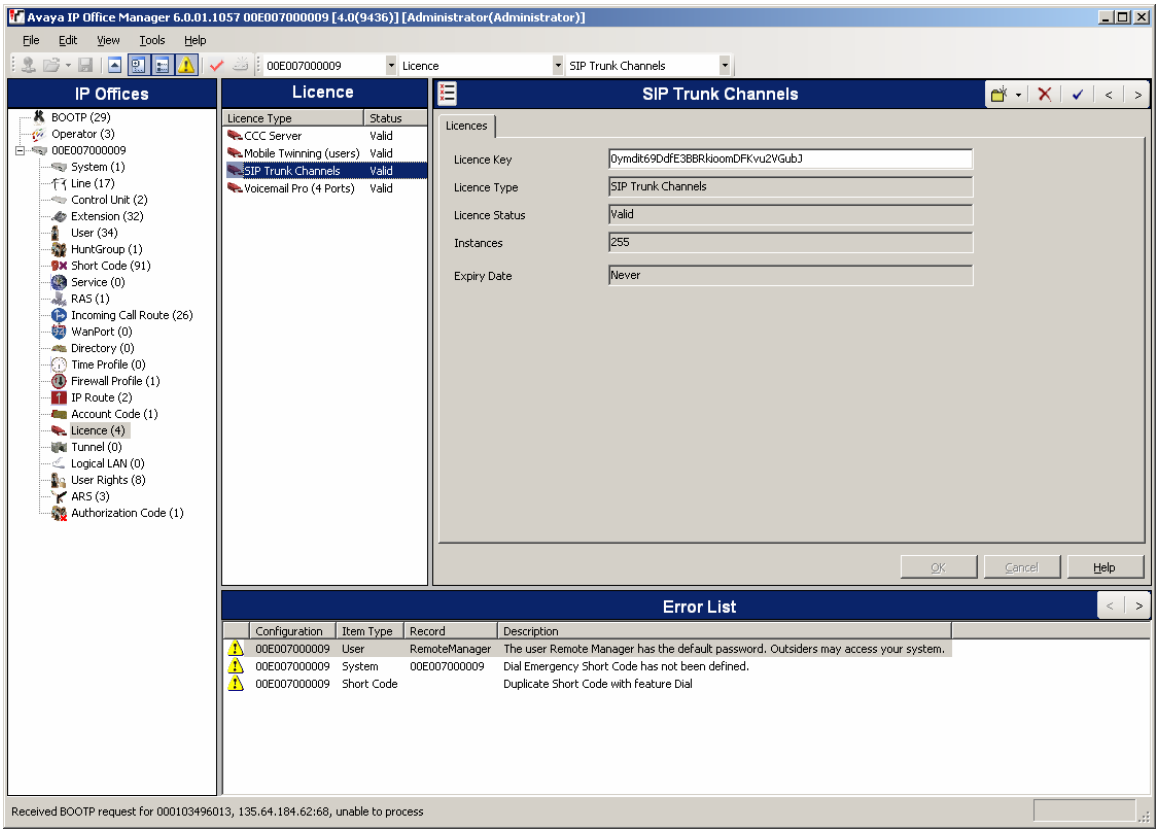

Figure 5: License Form with Valid SIP license

License Key is the license identifier that will be provided by Avaya business partners.

License Type must be set to *SIP Trunk Channel*.

License Status should be set to *Valid*, if the acquired license is a valid one.

Instances, will display the number of license instance that have been purchased.

Expiry Date will indicate the expiration of the license

4.3 Setting Up IP Route to Cbeyond IP Network

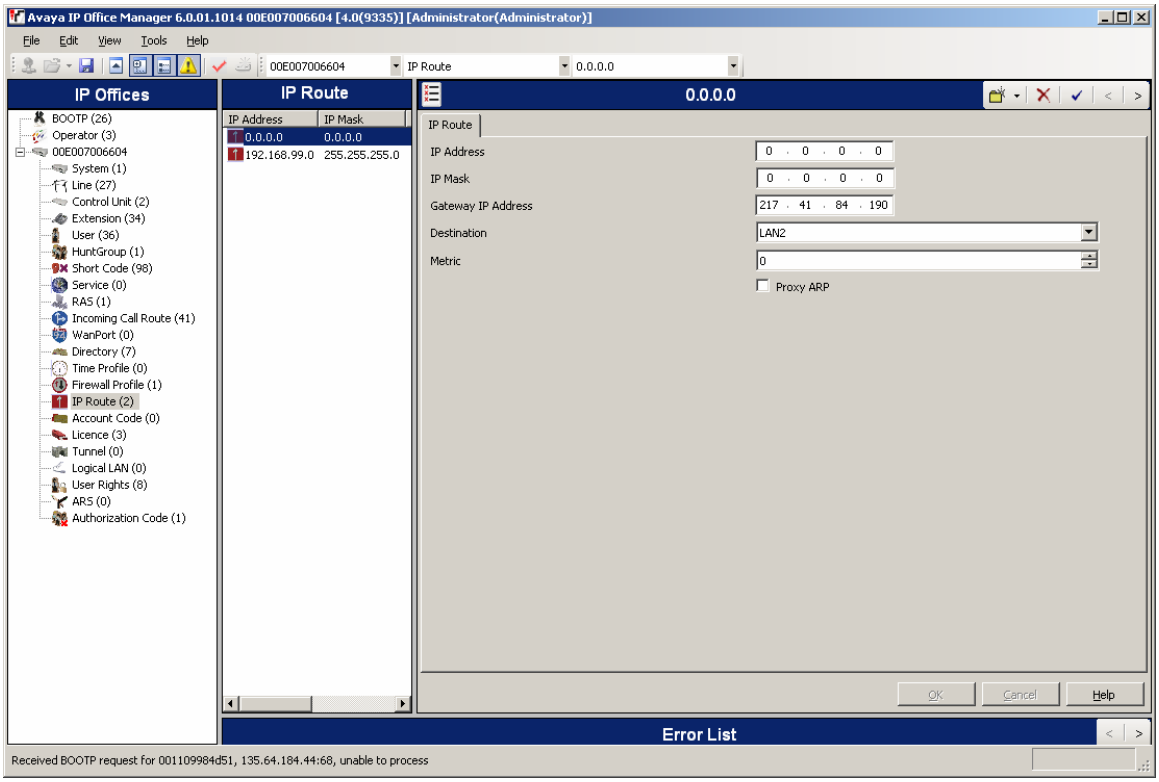

Figure 6: Setting IP Route to Managed Router at Customer Site

An example of how to set IP Route to Managed Router at Customer Site is depicted in Figure 6, where a fictitious IP address has been used.

4.4 Check that TOS settings are correct default values

TOS settings can be checked for the interface that is going to be connected to Cbeyond through the Managed Router at Customer Site. An example configuration is depicted in Figure 5

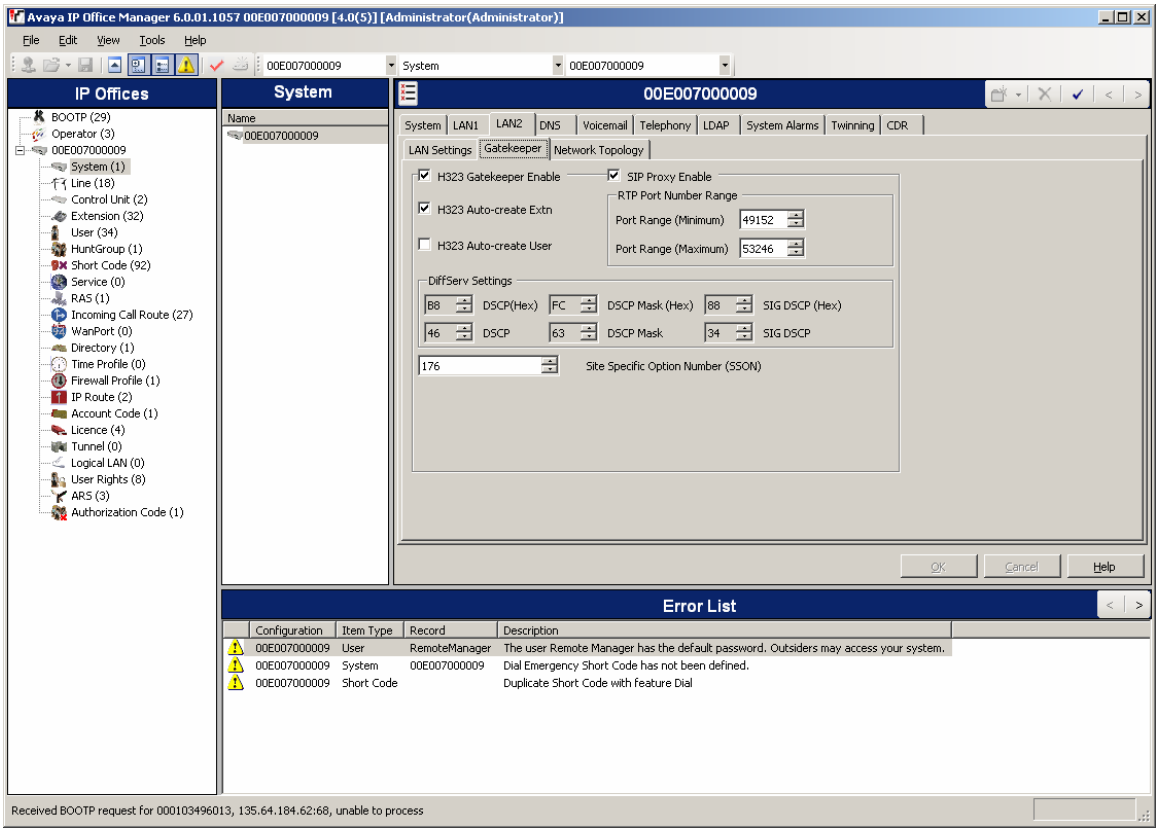

Figure 7 : TOS settings on LAN interface connected to Cbeyond network

It is important to note that for each field in Figure 7, DSCP, DSCP Mask and SIG DSCP, the decimal and hexadecimal field needs to be set individually.

4.5 SIP Main Line

This section deals with SIP Line configuration, starting with its main tab.

IP Office does not support DNS, *ITSP IP Address* will be filled with the IP address of Outbound Proxy provided by service provider. This may, or may not coincide with *ITSP Domain Name*.

Registration Required if checked, after re-booting the trunk will attempt to register using the information enclosed in the fields *ITSP Domain Name* and authentication account.

IP Office Rel 4.0 allows using two different authentication names on the same trunk. It is not possible to create two different trunks with the same *ITSP IP Address* to increase such number.

Each authentication account (primary and secondary) has three fields: *Name*, *Password* and *Expiry*. *Name* is the name of the account, *password* its password and *expiry* is the registration expiry of such registration, expressed in minutes. After each registration interval has expired, SIP trunks will attempt to register again.
In Service allows inhibiting the trunk from making and receiving phone calls, but does not prevent it from registering and probing for media capability.

If *Use Tel URI* is checked, the FROM Header will take the form of TEL URI. Given the early status of adoption of such URIs, it is strongly recommended to check with the ITSP for their support before using it.

VoIP Silence Suppression allows turning on silence suppression for that particular trunk.

Re-Invite Supported allows IP Office generating re-Invite when the target of an incoming call or a transfer does not support the vocoder negotiated for a given trunk. However, two issues may arise with the use of Re-Invites. First not all ITSP accepts them, and more importantly, negotiation problems may appear. This is why such options can become risky. The safer alternative is to un-tick it, but the security may come at the cost of using two codecs for the same call.

Compression Mode indicates the favorite codec that SIP trunk is going to offer for outbound call, and it is likely to accept for inbound.

Layer 4 Protocol is the transport protocol that is going to be used for SIP to convey message to ISP network. Two options are available: TCP and UDP.

Listen Port indicates the local Transport Layer port where SIP messages are received. Default is 5060, and the field is grayed out if *LAN1* of *LAN2* network profiles are selected in *Use Network Topology* Field. This is because STUN discoveries are run only on port 5060.

Use Network Topology Info is a field of great importance for SIP trunks, as it instructs IP Office firmware about which IP address and Transport Port to embed into SIP message. This is a particularly hot topic for NAT transversal, where the IP address and transport port that are being used for SIP messages can be made inconsistent with Global IP and Port information by NAT transversal.

Three options are available: *LAN1*, *LAN2*, and *None*.
LAN1 forces IP Office firmware to embed into SIP messages the IP Address and Port of *System->LAN1->Network Topology ->Public Address* and *Port*.

Send Port indicates the remote Transport Layer port where SIP messages will be sent. Default is 5060.

LAN2 forces IP Office firmware to embed into SIP messages the IP Address and Port of *System->LAN2->Network Topology ->Public Address* and *Port*.

None forces IP Office firmware to embed into SIP messages IP address obtained through Routing Information and Port set in the *Listen Port* field.

Selection of "Use Network Topology Info"

It is important to discuss the selection of this field, recalling the network connectivity scenarios of Section 2.1.

The options available here are *LAN1, LAN2* and *None*. Choosing *None* will force SIP trunk to derive the IP address to embed in SIP messages from Routing Information, **that needs to be set separately by creating a static route**. *Listen* and *Send* port will be set by homonymous fields in *SIP Line* form.

Choosing *LAN1/2* will force SIP trunk to derive the IP address and port to embed in its messages using *System->Lan1/2->Network Topology*. The profile correspondent to the interface that is **connected to the internet must be selected**.
Table 1 gives an example about how best select the field given the connectivity available.

Network Topology	*Use Network Topology Info*
ITSP with Session Border	*LANx* or *None*.

Controller	*LANx* may be necessary to keep firewall open by sending binding refresh
ITSP Connection Using STUN Server	*LANx*
ITSP Connection Using Demilitarized Zone (DMZ)	*None*, since the DMZ zone goes around NAT/firewall.

Table 1

Guideline for Cbeyond specific configuration of each field

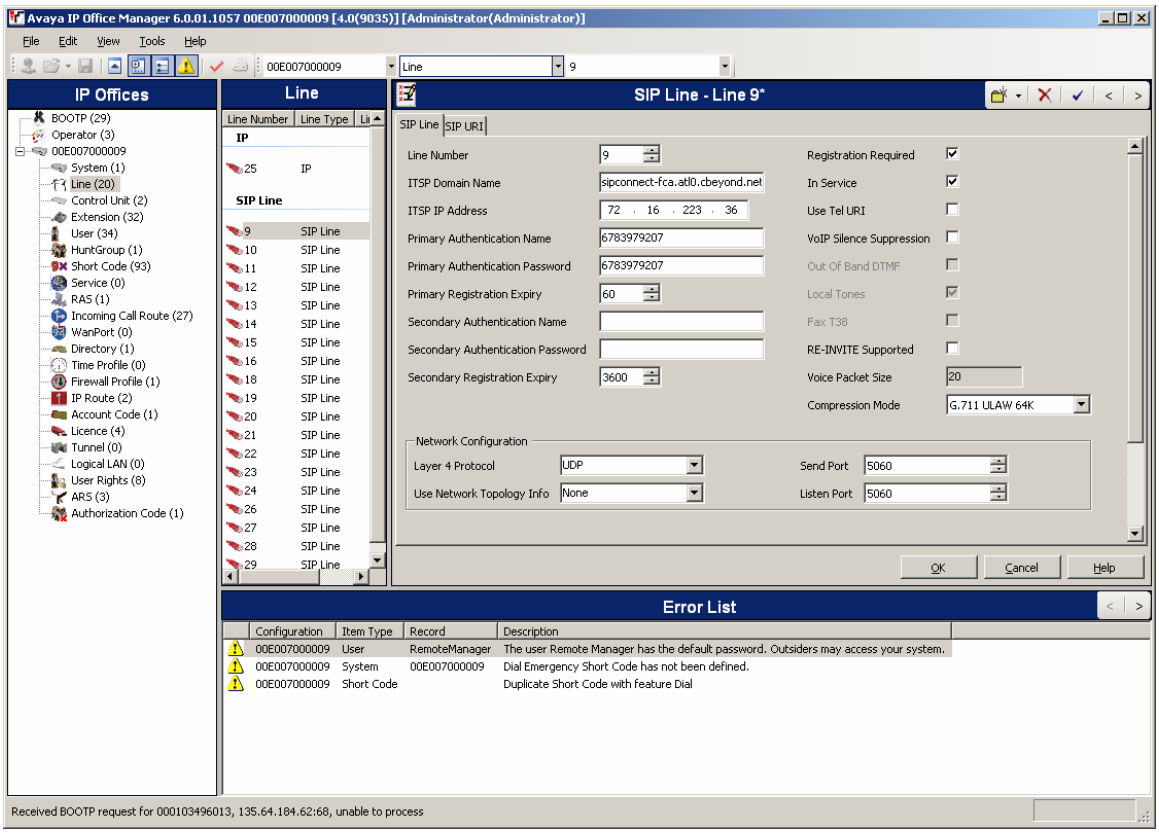

Figure 8: SIP Main Line

- Line number is automatically assigned by Manager in an incremental manner.
- ITSP Domain Name. In the example of Figure 8 set to “sipconnect-fca.atl0.Cbeyond.net”. In general should be set using *SIPconnect Settings* section of *the Install Profile* under the *SIPconnect Domain*. The Install Profile is supplied by Cbeyond prior to install.

- Registration Required, shall be checked.
- In Service shall be checked.
- ITSP IP Address shall be set to Cbeyond border element. In this instance, it has been set by resolving “sipconnect-fca.atl0.Cbeyond.net” using ping. In Figure 8, it resulted into 72.16.223.36. In general should be set using *SIPconnect Settings* section of *the Install Profile* under the *SIPconnect Domain*. The Install Profile is supplied by Cbeyond prior to install by the Cbeyond Service Coordinator.
- Primary Authentication Name shall be set to Cbeyond PBX username.
- Primary Authentication Password shall be to Cbeyond PBX password.
- Primary Registration Expiry, expressed in minutes. In case of Cbeyond, should be left as default.
- Secondary Authentication Name can be left blank, or used for a second authentication name.
- Secondary Authentication Password can be left blank, or used for a second authentication password.
- Secondary Registration Expiry, expressed in minutes. In case of Cbeyond, should be left as default.
- In Service shall be checked
- Use TEL URI shall be left un-checked
- Re-INVITE Supported shall be left un-checked
- Compression mode should be set to G.711 U-Law 64k
- Send Port shall be set to 5060 (default)
- Listen Port shall be set to 5060 (default)

4.6 SIP Line: SIP URI tab

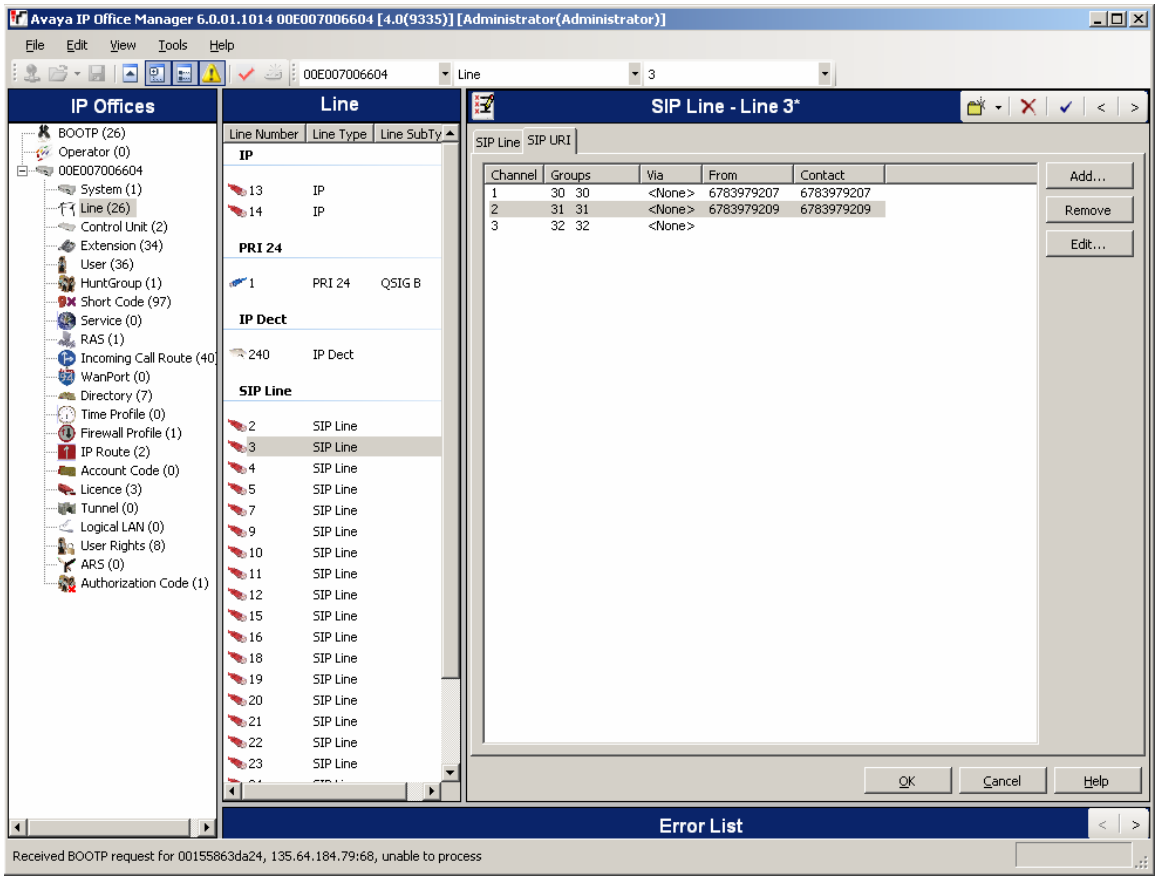

Figure 9: SIP URI tab

For each DID that is assigned to a specific user, a correspondent *SIP URI* needs to be created. Figure 9 depicts a scenario where three fictitious DIDs, have been assigned. Each *SIP URI* has a number of fields to set.

Each SIP URI has its own Incoming and Outgoing Group ID. Though it is not necessary it is strongly recommended to use a different Group ID for each SIP URI (and each type of Trunk also). Outgoing Group ID allows selecting using short code, which SIP URI to use to make outbound calls.
Incoming Group ID allows routing of incoming calls to a specific route, if a match between the target of the call and Local URI is produced.

The fields which characterize each URI are Local URI, Contact, and Display Name. Such fields are used to set SIP message headers for both outgoing calls and Incoming calls.

- Local URI acts as user part of FROM header for outbound calls, and it is the field used to match user part of TO header from incoming calls
- Contact sets user part of CONTACT field in SIP messages
- Display Name sets the homonymous field in FROM header for outbound calls

Local URI can be set in two different modes for this configuration type:

1. By setting the URI to “Use Authentication Name” (Figure 8). This mode allows using the authentication name as an identifier for Local URI.
2. By editing each field individually (Figure 9). This mode allows setting each SIP URI to coincide with a given DID assigned by ITSP. With this mode, SIP URI settings are common for all users in the system.
3. By setting in to Use User Data (Figure 10). This setting allows differentiating each SIP URI to a given user in the system. The fields will be filled in using SIP tab in User form.

The number of simultaneous calls may also dependent on the number of calls supported on the VCM cards.

4.6.1 Using Authentication Name

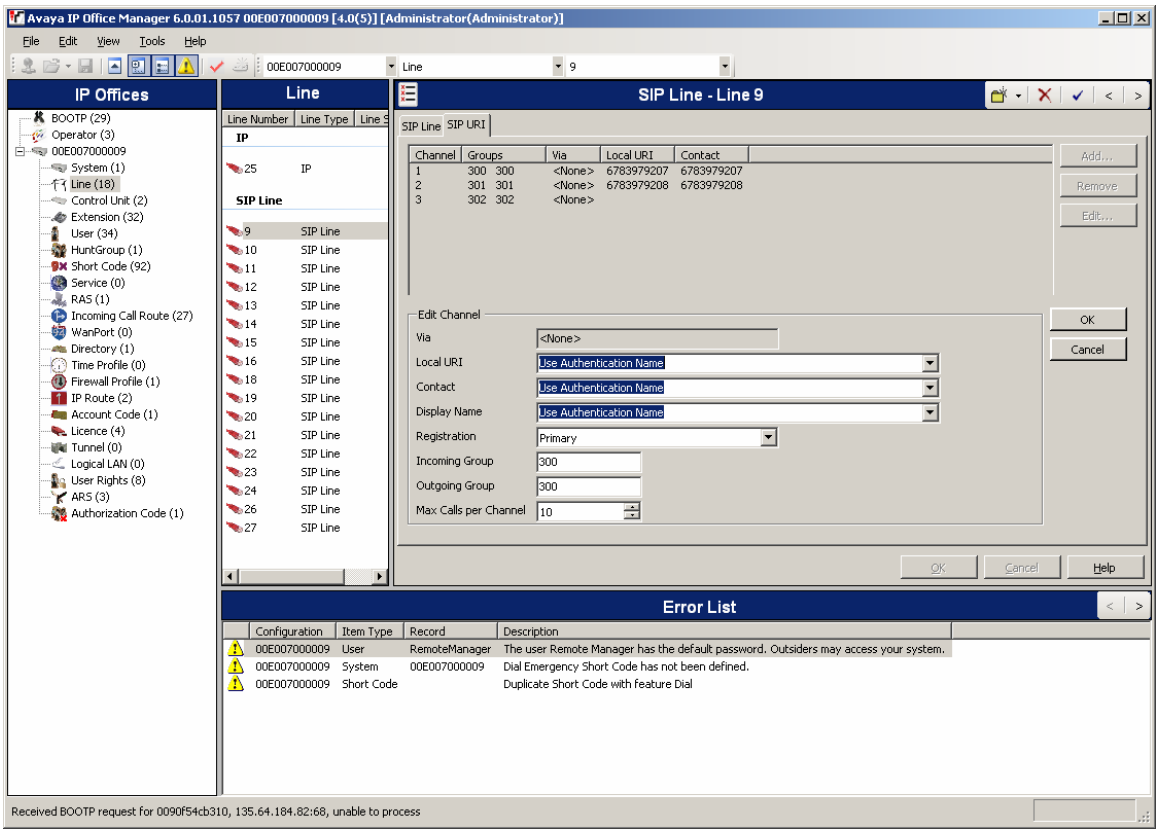

Figure 10: URI using Authentication Name

Figure 10 depicts a URI configuration where the authentication is used to set *Local URI* field. Outbound call will have the user portion on FROM field set accordingly to *Local URI* field, and incoming call will have the user part of TO field matched against *Local URI* field.

4.6.2 URI configuration using an assigned DID

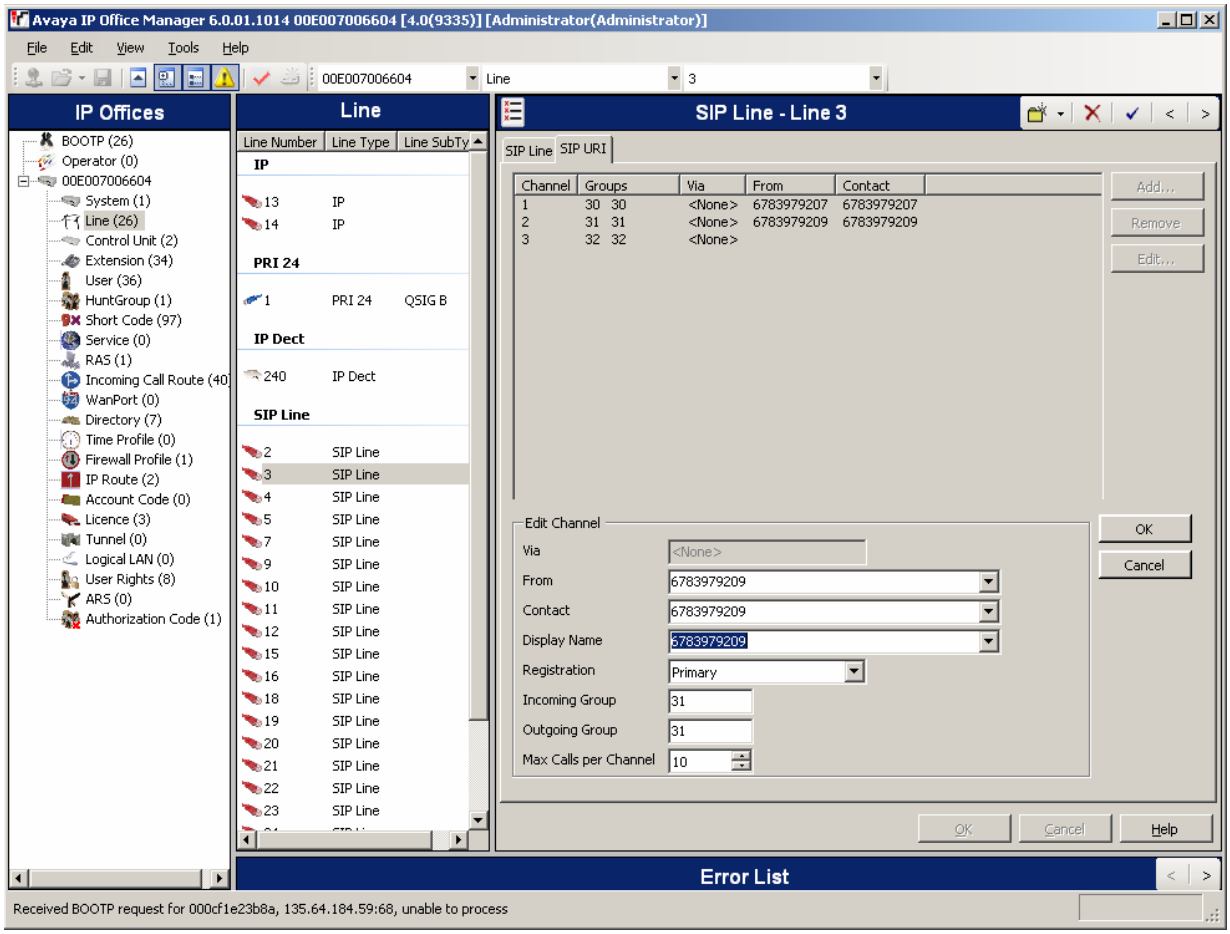

Figure 11: URI using assigned DID

Figure 11 depicts SIP URI configuration where an assigned DID is used to identify the destination of an incoming call and the originator of an outbound call.

It is a quite common case in SIP trunking configuration, to have one account with authentication name and password, but more DIDs associated with it. Such authentication name and password may or may not coincide with one of associated DIDs.

It is important to realize that using an assigned DID can still required authentication. For such purpose *Registration* field is provided.

4.6.3 URI configuration using assigned DID under User Data

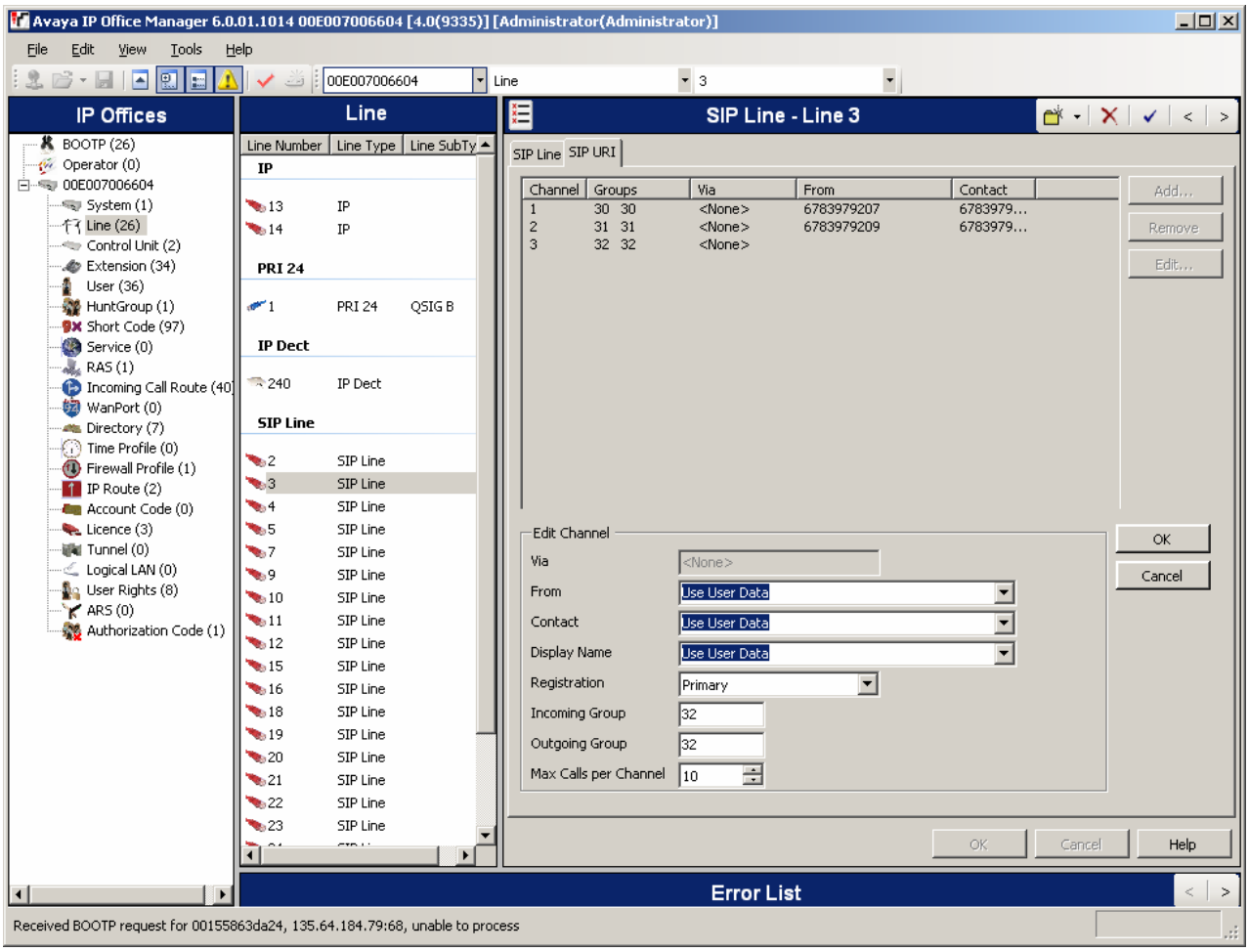

Figure 12: URI using assigned DID, configured through Use User Data

Figure 12 depicts a variant of SIP URI configuration using an assigned DID where the DID is not shared by all users of IP Office, but rather is limited to a given user.

To set up such DID, it is needed to fill in *User->SIP* tab in a manner exemplified by Figure 13.

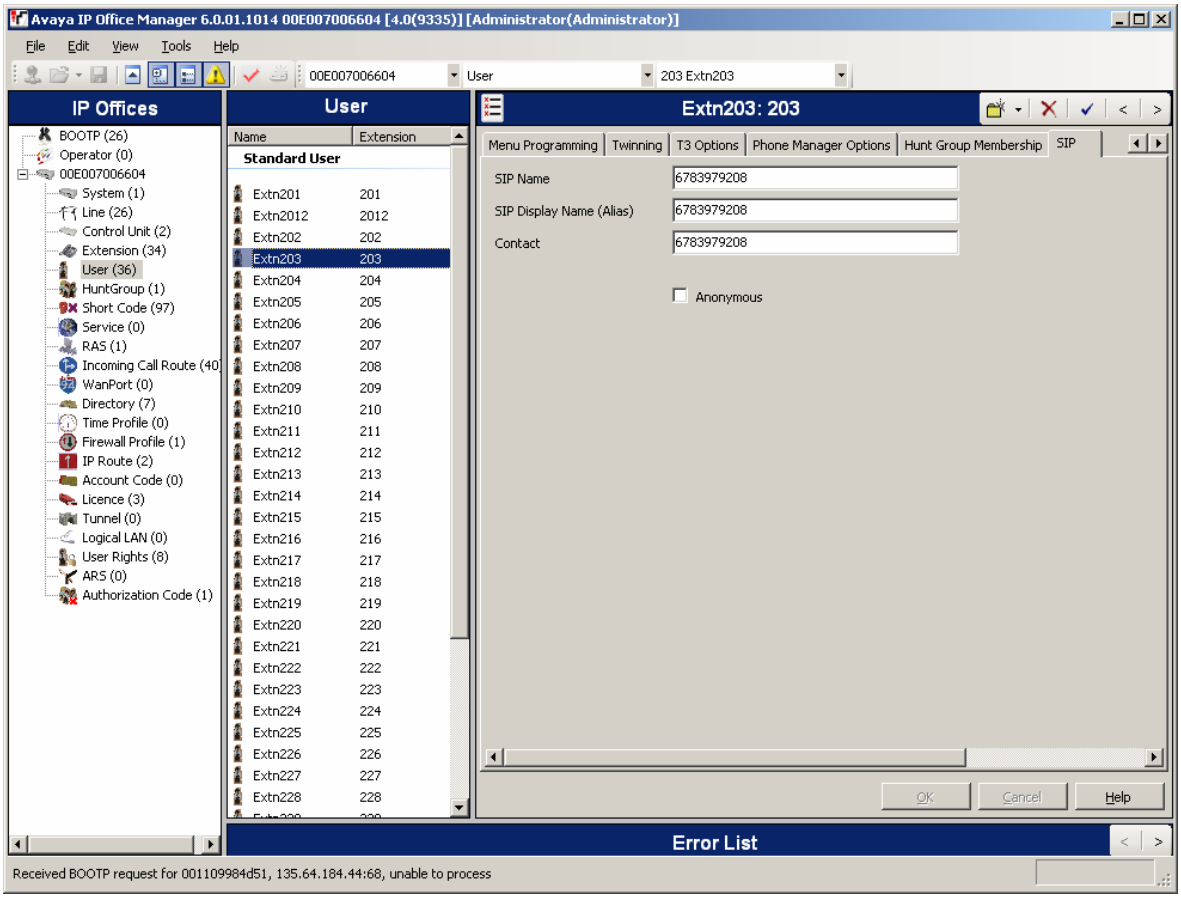

Figure 13: SIP tab in User Setting

SIP Name corresponds to *SIP URI From* field and will be used to make matching and routing decision of incoming calls, and will represent the caller number for outbound calls. *Display Name* will fill the homonymous field in FROM header, and *Contact* will fill the user part of CONTACT header. *SIP Name*, *Display Name* and *Contact* can be alphanumeric characters.

Anonymous allows enabling Privacy Mechanism for outbound calls according to RFC 3323.

4.7 Routing Calls to Cbeyond

This section describes the IP Office configuration required for sending calls to the Cbeyond.

4.7.1 Calling Plan

The usual system of SHORT CODE object can be used to direct calls to the Cbeyond network. The screen shot of Figure 14 gives an example in a fictitious IP Address.

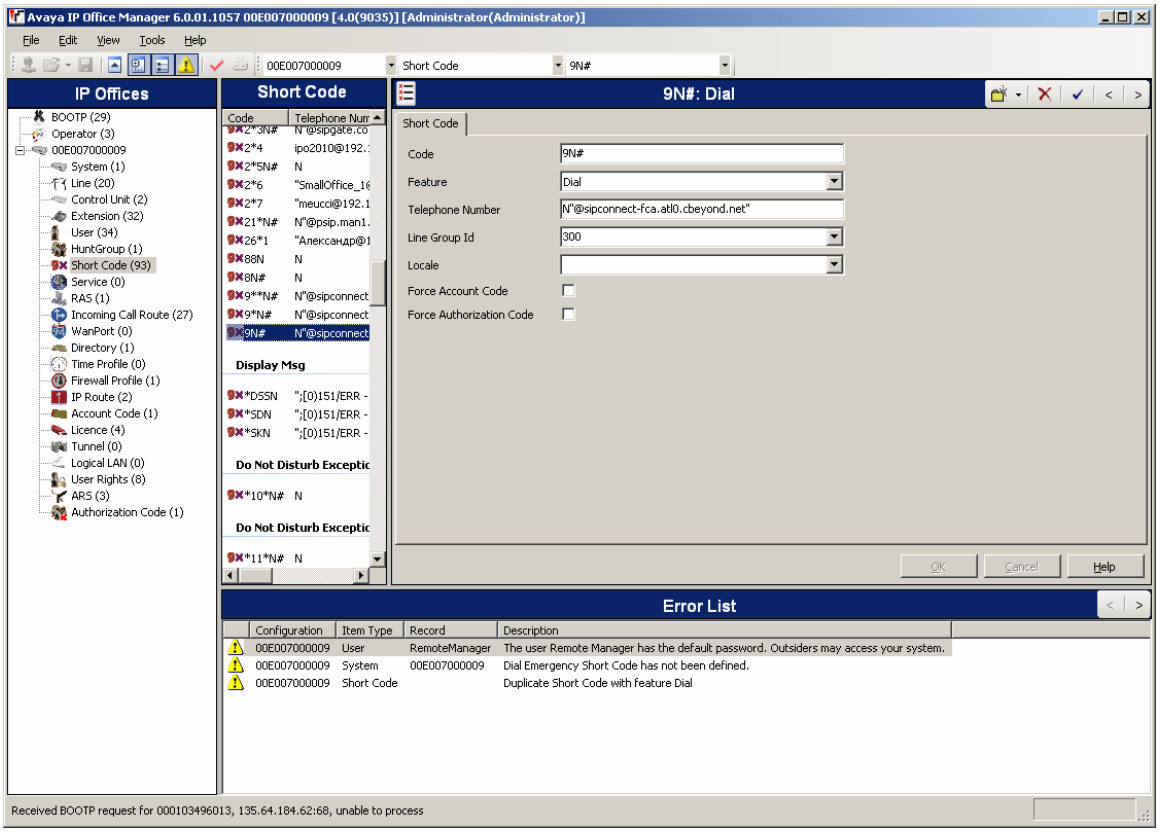

Figure 14: Setting Calling Plan

The fields are populated as follows.

- *Short code* – This field is set to “<trunk identifier>N#”.<trunk identifier> is a series of number or characters that uniquely identify while dialing out. The character “#” is used to terminate the string.
- *Line Group ID* – Set this field to the SIP *URI Outgoing Group* ID that it is used to connect to the Cbeyond network. A subsequent section will

describe how to configure IP Office to route to the 2 Cbeyond Border Elements in a primary / secondary arrangement.

- *Feature* – Set this field to “Dial”.
- *Telephone number* - is set to “N@<Cbeyond SIP Server FQDN>”. Beware that appending IP address of remote server is necessary to select a SIP URI rather than a TEL URI.

4.7.2 Routing to a Primary and Secondary Cbeyond Border Element

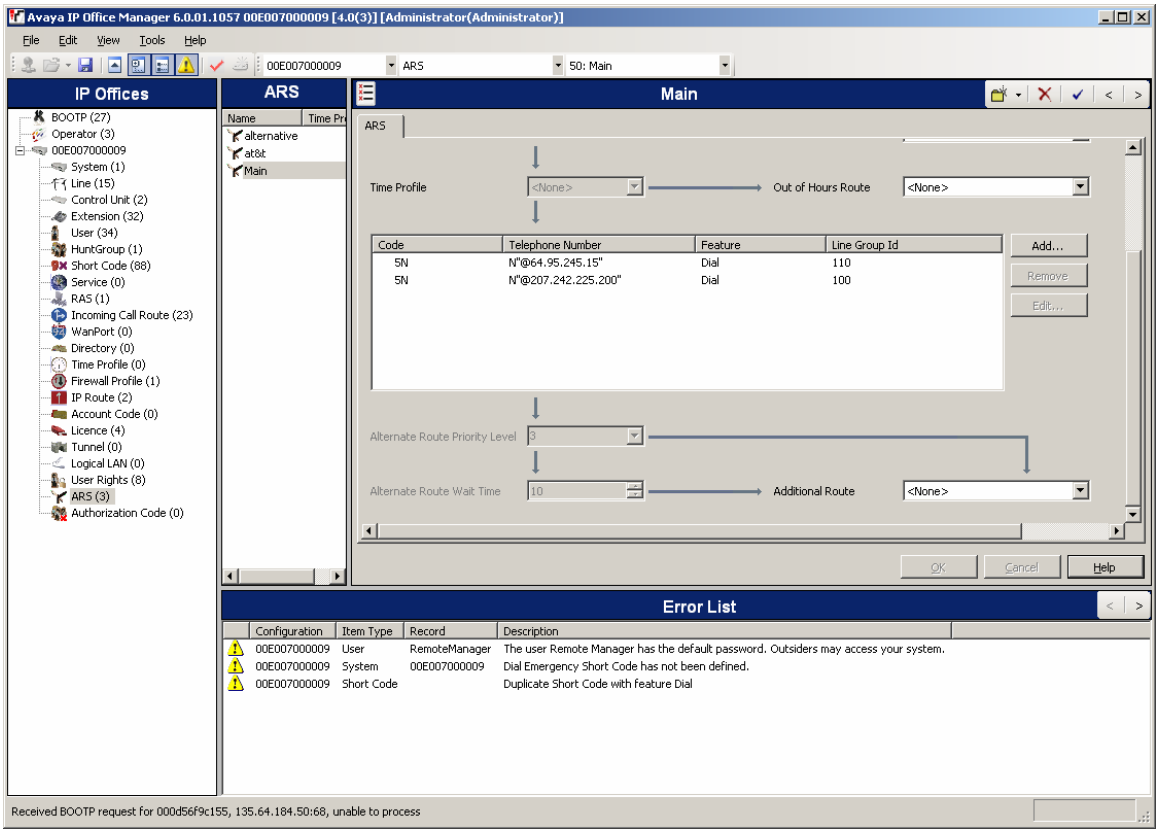

Figure 15: ARS form

Figure 15 depicts an example of Alternate Route Selection (ARS) that can be used to try different target for the same number.

Each ARS for is entered using a short-code, like that of Figure 16.

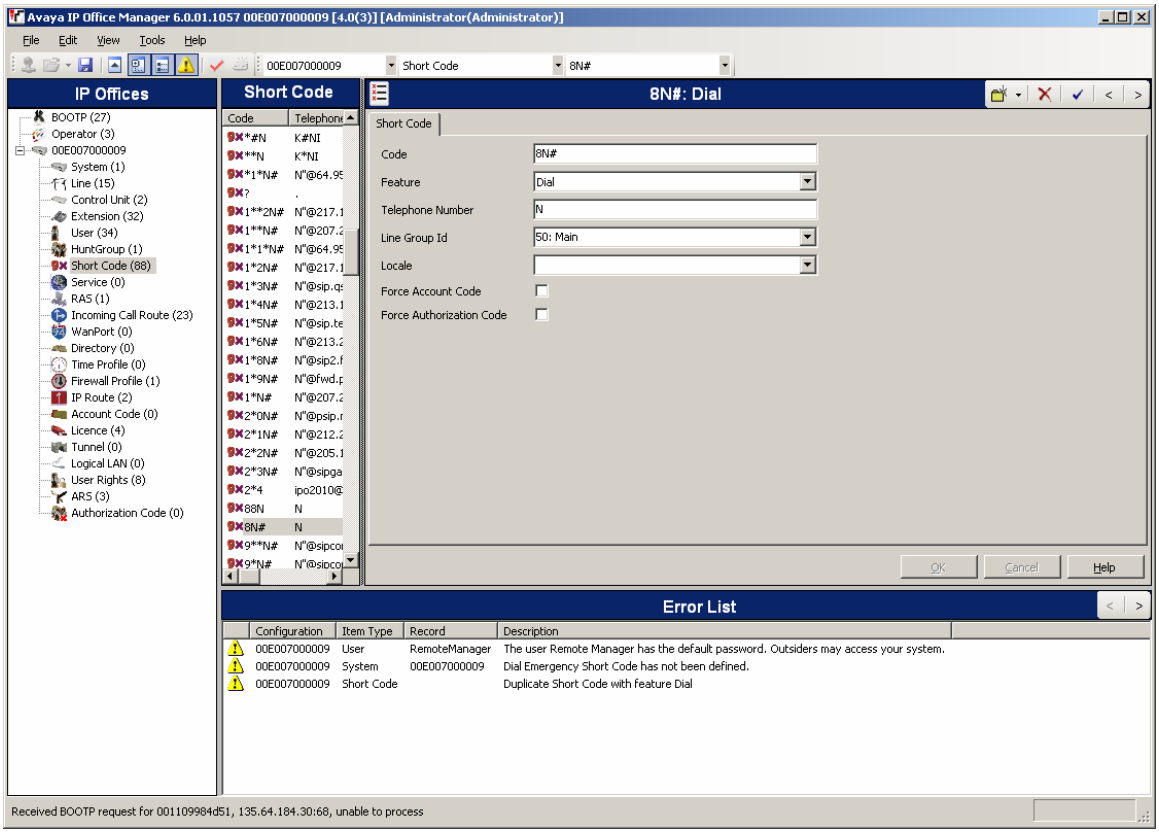

Figure 16: Short Code Setting to Dial ARS

Each target listed in Figure 15 is attempted from bottom to top, and Invite Timeout is fixed to approximately 32 seconds.

4.8 Receiving Calls from Cbeyond

4.8.1Called Number Translation (Local)

The translation of each DID to an IP Office extension is done using ICR call route field, as depicted in Figure 17.

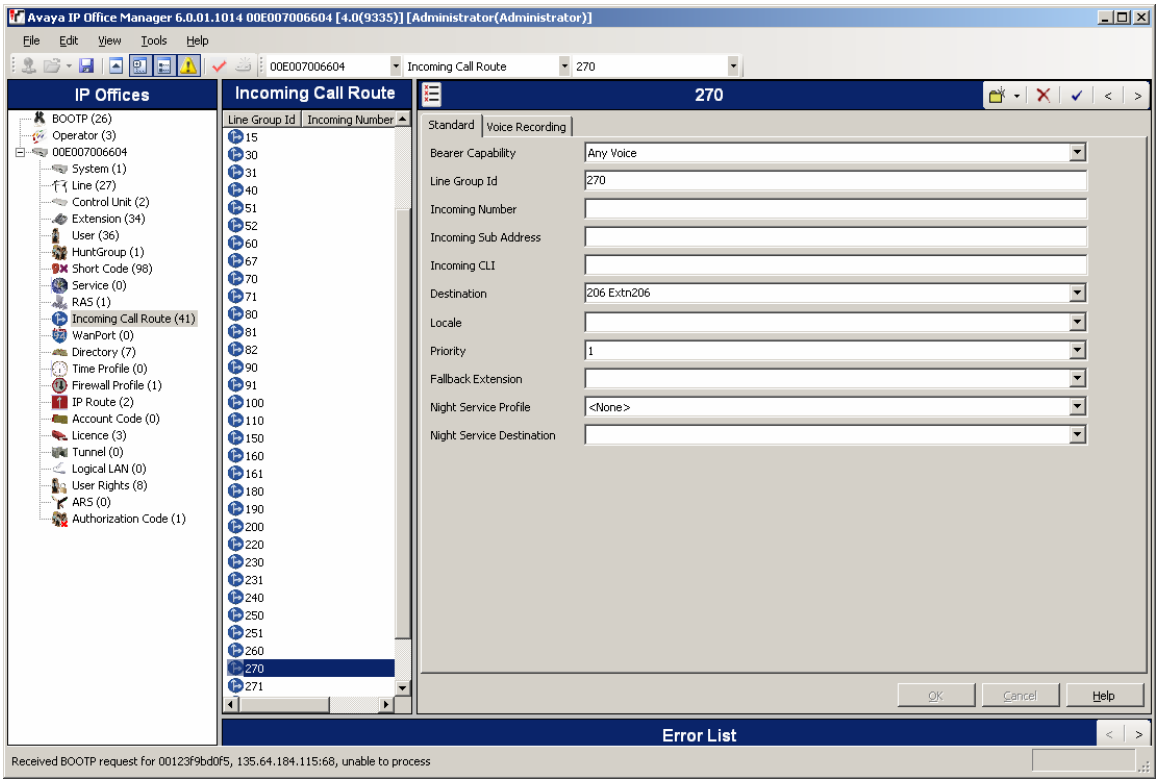

Figure 17: Incoming Call Route

The fields are populated as follows:

Bearer Capability shall be set to *Any Voice.*
Line Group Id shall be set to the *Incoming Group ID* of the *SIP URI* that is used to receive external phone calls.

Destination shall be set to the desired target of incoming calls that can be an extension or hunt-group.

4.9 IP Phone Configuration

An example of IP phone configuration is given in Figure 15. *Enable Fast Start for non Avaya phones* is enabled, and *Allow Direct Media Path* can be left checked or un-checked depending on user preference. SIP trunks will always use relay.

To minimize the number of voice coder employed, it is recommended to set *Compression Mode* to G.711.

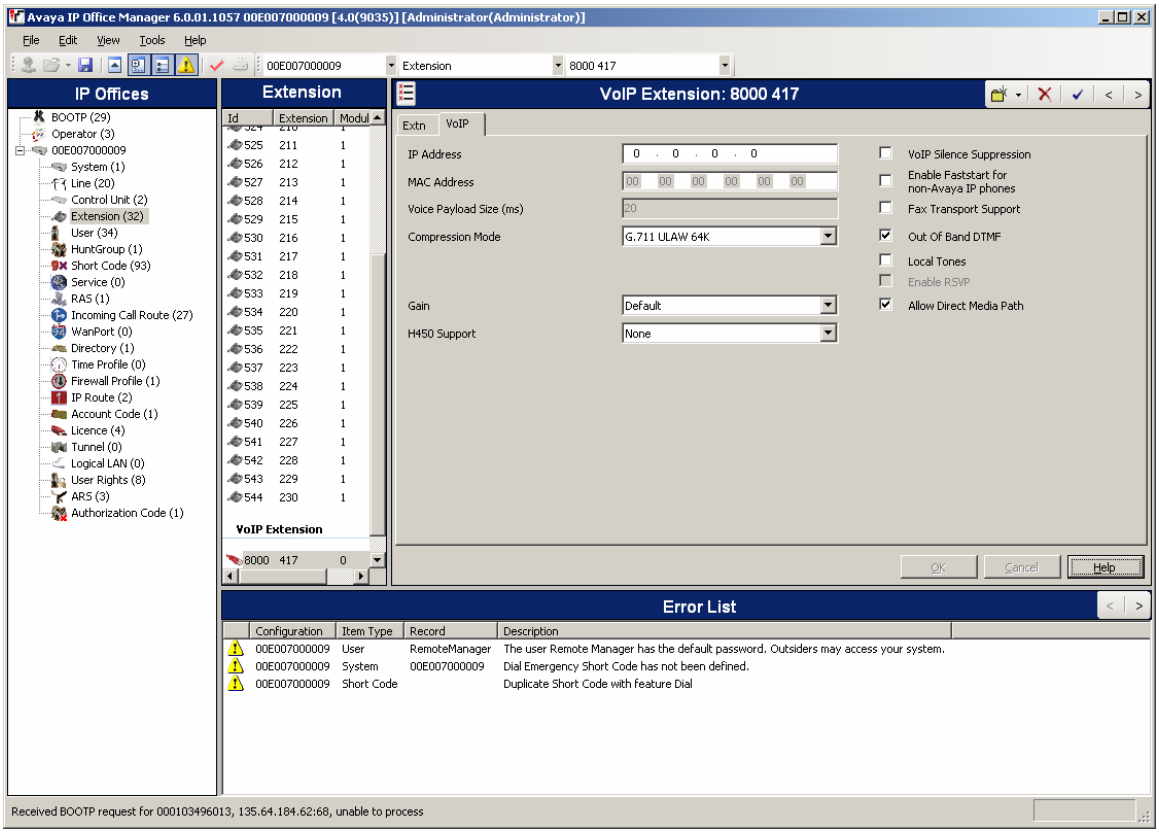

Figure 18: IP Phone Configuration

4.10 Troubleshooting using STUN Discovery and Monitor Traces

This section aims at helping customers to configure their SIP trunks and individuated any problem that could prevent the successful SIP call establishment to be achieved. Troubleshooting can be done by using both STUN discovery mechanism and Monitor tracing. STUN discovery is a useful tool that allows users to know the nature of their internet connectivity. A run discovery can be run at boot-up is always recommended, and can be repeated at any moment, using the RUN STUN button in Network Topology Form of the selected interface. Monitor traces can be turned on for SIP. Three flags are crucial for debugging purposes:

1. STUN info: enables the tracing concerning STUN.
2. SIP Trunk Traffic: displays the messages exchanges through SIP trunks.
3. Sip Debug Info (advanced) displays useful debugging information for traces collection in case you need to contact Avaya Tier3/4 Engineers.
4. SIP TX: same as SIP trunk Traffic, but only for Transmitted messages.
5. SIP RX: same as SIP trunk Traffic, but only for Received messages.

Here is a list of most common configuration mistakes and their recommended remedy.

Problems with outbound calls

If you are sending an INVITE and we get no reply from SIP Servers

There a few reasons why IP Office would not get an answer to an INVITE. The advice would be the following:

1. Check your IP Office is physically connected to your network modem
2. Check an IP Route is set to your network modem.
3. If your SIP line is using Network Topology Info, make sure that you have selected the right interface.
4. Check ITSP IP address is set correctly.

If you are sending an INVITE and we get a negative reply from SIP Servers

In this case many things could have wrong. Here is a list of most common problems.

1. Check with ITSP about what is the dial plan that must be used.
2. Check you have configured the short code for the right purpose. Most of ISP support SIP URI only, therefore please make sure that you Short code

is that of Figure 14. A short code like the one in Figure 19, will use TEL URI.

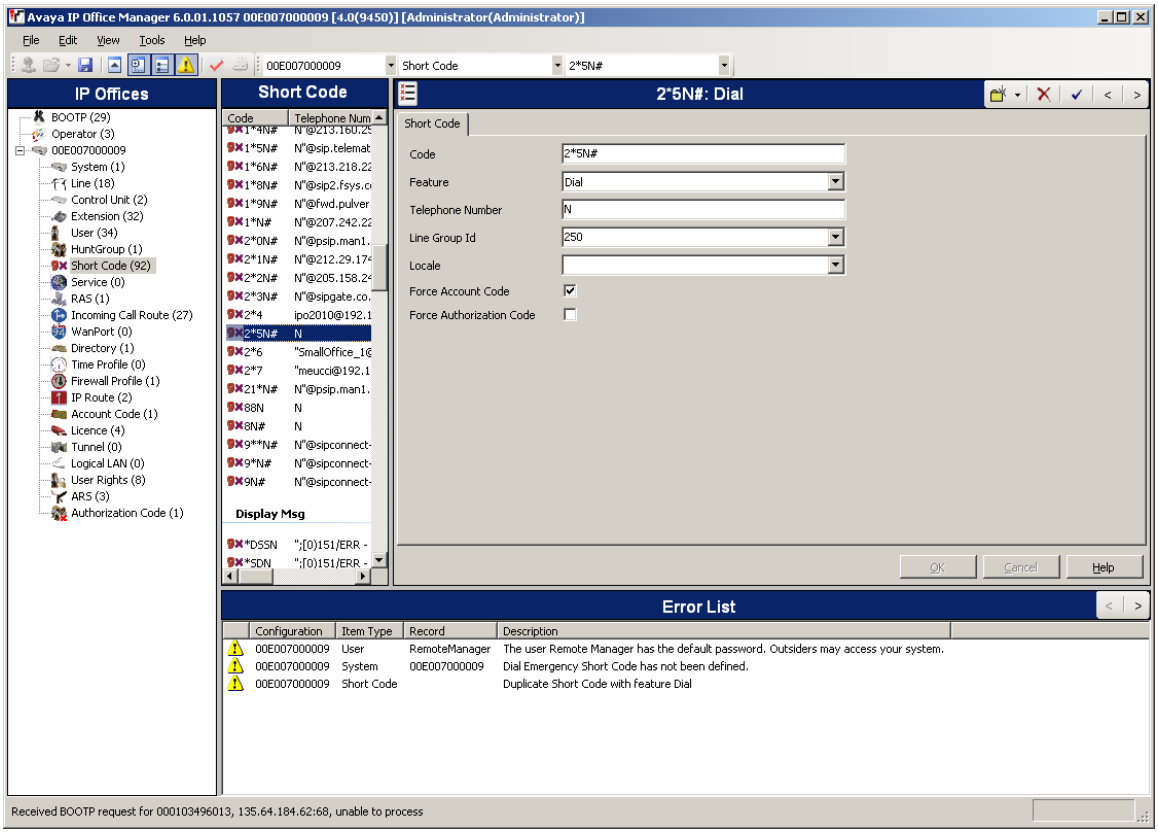

Figure 19: Wrong Short Code Setting

Will produce an INVITE send out of Trace 8, that is using TEL-URI (marked in black).Unless this is expected and supported by ITSP, in general may cause a problem in call establishment.

```
    65145mS SIP Trunk: 11:Tx
                    INVITE Tel:+17325308100 SIP/2.0
                    Via: SIP/2.0/UDP
217.41.84.186:5060;rport;branch=z9hG4bK726cc0cd3741855d8a36b8a8fd56126a
                    From: 12134551358
<sip:12134551358@217.41.84.186>;tag=f9023fc0ee53bbd1
                    To: Tel:+17325308100
                    Call-ID: 3fe2a6900d0e7b7c71dabf6c3f1b37f3@217.41.84.186
                    CSeq: 771361749 INVITE
                    Contact: 12134551358
<sip:12134551358@217.41.84.186:5060;transport=udp>
                    Max-Forwards: 70
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
                    Content-Type: application/sdp
                    Content-Length: 303
```

```
                    v=0
                    o=UserA 3697612515 4264844916 IN IP4 217.41.84.186
                    s=Session SDP
                    c=IN IP4 217.41.84.186
                    t=0 0
                    m=audio 49152 RTP/AVP 18 4 8 0 101
                    a=rtpmap:18 G729/8000
                    a=rtpmap:4 G723/8000
                    a=rtpmap:8 PCMA/8000
                    a=rtpmap:0 PCMU/8000
                    a=fmtp:18 annexb = no
                    a=rtpmap:101 telephone-event/8000
                    a=fmtp:101 0-15
```

Trace 1: Invite with mistaken TEL-URI use

3. There might be an authentication problem that only occurs if you have failed to register. An example is depicted in Trace 2. It can bee seen that after the first 401 challenge to INVITE, the response is acknowledge (using ACK method) and another INVITE with challenge response is sent. But in this scenario, being a problem with authentication account, the challenge response is rejected with another 401.

```
    39497mS SIP Trunk: 9:Tx
                    INVITE sip:17325308100@sipconnect-fca.atl0.Cbeyond.net
SIP/2.0
                    Via: SIP/2.0/UDP
217.41.84.186:5060;rport;branch=z9hG4bKbbc6051c74bf6d2ef00b04374b2e6b9a
                    From: 6783979207 <sip:6783979207@sipconnect-
fca.atl0.Cbeyond.net>;tag=9564653dc79736fb
                    To: <sip:17325308100@sipconnect-fca.atl0.Cbeyond.net>
                    Call-ID: 7a0e46537c3bf1cc34dcef9476d67a42@217.41.84.186
                    CSeq: 1100436280 INVITE
                    Contact: 6783979207
<sip:6783979207@217.41.84.186:5060;transport=udp>
                    Max-Forwards: 70
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
                    Content-Type: application/sdp
                    Content-Length: 302

                    v=0
                    o=UserA 2385045156 658699819 IN IP4 217.41.84.186
                    s=Session SDP
                    c=IN IP4 217.41.84.186
                    t=0 0
                    m=audio 49152 RTP/AVP 0 18 4 8 101
                    a=rtpmap:0 PCMU/8000
                    a=rtpmap:18 G729/8000
                    a=rtpmap:4 G723/8000
                    a=rtpmap:8 PCMA/8000
                    a=fmtp:18 annexb = no
                    a=rtpmap:101 telephone-event/8000
                    a=fmtp:101 0-15

     39716mS SIP Trunk: 9:Rx
                    SIP/2.0 401 Unauthorized
                    Via:SIP/2.0/UDP
```

```
217.41.84.186:5060;branch=z9hG4bKbbc6051c74bf6d2ef00b04374b2e6b9a;rport
                    From:"6783979207"<sip:6783979207@sipconnect-
fca.atl0.Cbeyond.net>;tag=9564653dc79736fb
                    To:<sip:17325308100@sipconnect-
fca.atl0.Cbeyond.net>;tag=142089592-1172067317469
                    Call-ID:7a0e46537c3bf1cc34dcef9476d67a42@217.41.84.186
                    CSeq:1100436280 INVITE
                    WWW-Authenticate:DIGEST
realm="BroadWorks",qop="auth",algorithm=MD5,nonce="BroadWorksXeyfuma59TwlewaxBW
"
                    Content-Length:0


     39725mS SIP Trunk: 9:Tx
                    ACK sip:17325308100@sipconnect-fca.atl0.Cbeyond.net SIP/2.0
                    Via: SIP/2.0/UDP
217.41.84.186:5060;rport;branch=z9hG4bKbbc6051c74bf6d2ef00b04374b2e6b9a
                    From: 6783979207 <sip:6783979207@sipconnect-
fca.atl0.Cbeyond.net>;tag=9564653dc79736fb
                    To: <sip:17325308100@sipconnect-
fca.atl0.Cbeyond.net>;tag=142089592-1172067317469
                    Call-ID: 7a0e46537c3bf1cc34dcef9476d67a42@217.41.84.186
                    CSeq: 1100436280 ACK
                    Max-Forwards: 70
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
                    Content-Length: 0


     39730mS SIP Trunk: 9:Tx
                    INVITE sip:17325308100@sipconnect-fca.atl0.Cbeyond.net
SIP/2.0
                    Via: SIP/2.0/UDP
217.41.84.186:5060;rport;branch=z9hG4bKed6df0d4b80d5e36cbb3172c1352fc3b
                    From: 6783979207 <sip:6783979207@sipconnect-
fca.atl0.Cbeyond.net>;tag=9564653dc79736fb
                    To: <sip:17325308100@sipconnect-fca.atl0.Cbeyond.net>
                    Call-ID: 7a0e46537c3bf1cc34dcef9476d67a42@217.41.84.186
                    CSeq: 1100436281 INVITE
                    Contact: 6783979207
<sip:6783979207@217.41.84.186:5060;transport=udp>
                    Max-Forwards: 70
                    Authorization: Digest
username="6783979207",realm="BroadWorks",nonce="BroadWorksXeyfuma59TwlewaxBW",r
esponse="a81dbb71c28733b672b8b00cd960d613",uri="sip:17325308100@sipconnect-
fca.atl0.Cbeyond.net"
                    Content-Type: application/sdp
                    Content-Length: 302

                    v=0
                    o=UserA 2385045156 658699820 IN IP4 217.41.84.186
                    s=Session SDP
                    c=IN IP4 217.41.84.186
                    t=0 0
                    m=audio 49152 RTP/AVP 0 18 4 8 101
                    a=rtpmap:0 PCMU/8000
                    a=rtpmap:18 G729/8000
                    a=rtpmap:4 G723/8000
                    a=rtpmap:8 PCMA/8000
                    a=fmtp:18 annexb = no
                    a=rtpmap:101 telephone-event/8000
```

```
                    a=fmtp:101 0-15

     39954mS SIP Trunk: 9:Rx
                    SIP/2.0 401 Unauthorized
                    Via:SIP/2.0/UDP
217.41.84.186:5060;branch=z9hG4bKed6df0d4b80d5e36cbb3172c1352fc3b;rport
                    From:"6783979207"<sip:6783979207@sipconnect-
fca.atl0.Cbeyond.net>;tag=9564653dc79736fb
                    To:<sip:17325308100@sipconnect-
fca.atl0.Cbeyond.net>;tag=1305376958-1172067317716
                    Call-ID:7a0e46537c3bf1cc34dcef9476d67a42@217.41.84.186
                    CSeq:1100436281 INVITE
                    WWW-Authenticate:DIGEST
realm="BroadWorks",qop="auth",algorithm=MD5,nonce="BroadWorksXeyfumac4Tu37yg9BW
"
                    Content-Length:0
```

Trace 2: INVITE with Failed Authentication

4. Make sure you appear to the ITSP world the way you are expected to. Some ITSP have strict rules about the format of the calling number. In the example of Trace 2, the calling number is identifiable in the FROM field, as being "6783979207@sipconnect-fca.atl0.Cbeyond.net" . In order to use such URI, the SIP URI tab *Local URI* used should be "6783979207".

5. Make sure you are dialing using a plan that is supported by your ITSP. Requirements about dialing plan can significantly vary from one ISP to another. Area and country codes might be needed and there might be also dialing restriction on some number, for instance, international.

Problems with Inbound Calls

If you are receiving an INVITE but your responses are not reaching SIP servers

In this case it is almost invariantly a problem with default IP route to your modem.

If you are receiving an INVITE but IP Office seems unable to route the call

This is one of the most common scenarios of failure for inbound calls:

1. You have not set properly the Incoming URI for the given number. This case happens often when only IP address is used authenticate calls. The inbound call does contains the DID assigned by ITSP to your site. Here is an example of incoming call traces

```
  165251mS SIP Trunk: 10:Rx
                    INVITE sip:7324209231@217.41.84.186:5060 SIP/2.0
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0osknm10bon11c42i0g1.1
                    From: Unavailable
<sip:1441707299900@127.16.21.179;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDl467d01-1172066614-828461172149460-11
                    To: <sip:7324209231@200.123.200.123;user=phone>
                    CSeq: 9192 INVITE
                    Contact: <sip:1441707299900@200.123.200.123:5060;att=AJAY2-
n4hi26am5t17b;transport=udp>
                    Call-ID: SDl467d01-f1a930b070d8b0491d80d36fd4f7f1cc-vjvtfv3
                    Max-Forwards: 68
                    Content-Type: application/sdp
                    Content-Length: 251
                    Accept: application/sdp, application/isup,
application/dtmf, application/dtmf-relay, multipart/mixed
                    Accept-Language: en; q=0.0
                    Allow: INVITE, ACK, CANCEL, BYE, REGISTER, REFER, INFO,
SUBSCRIBE, NOTIFY, PRACK, UPDATE

                    v=0
                    o=Sonus_UAC 23948 189 IN IP4 200.123.200.123
                    s=SIP Media Capabilities
                    c=IN IP4 200.123.200.123
                    t=0 0
                    m=audio 26732 RTP/AVP 18 0 127
                    a=rtpmap:18 G729/8000
                    a=rtpmap:0 PCMU/8000
                    a=rtpmap:127 telephone-event/8000
                    a=fmtp:127 0-15
                    a=sendrecv


    165264mS SIP Trunk: 10:Tx
                    SIP/2.0 100 Trying
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0osknm10bon11c42i0g1.1
                    From: Unavailable
<sip:1441707299900@127.16.21.179;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDl467d01-1172066614-828461172149460-11
                    To:
<sip:7324209231@200.123.200.123;user=phone>;tag=766328382d3efc1f
                    Call-ID: SDl467d01-f1a930b070d8b0491d80d36fd4f7f1cc-vjvtfv3
                    CSeq: 9192 INVITE
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
                    Content-Length: 0


    165271mS SIP Trunk: 10:Tx
                    SIP/2.0 404 Not Found
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0osknm10bon11c42i0g1.1
                    From: Unavailable
<sip:1441707299900@127.16.21.179;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDl467d01-1172066614-828461172149460-11
                    To:
<sip:7324209231@200.123.200.123;user=phone>;tag=766328382d3efc1f
                    Call-ID: SDl467d01-f1a930b070d8b0491d80d36fd4f7f1cc-vjvtfv3
                    CSeq: 9192 INVITE
```

```
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
                    Content-Length: 0


    165410mS SIP Trunk: 10:Rx
                    ACK sip:7324209231@217.41.84.186:5060 SIP/2.0
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0osknm10bon11c42i0g1.1
                    CSeq: 9192 ACK
                    From: Unavailable
<sip:1441707299900@172.16.22.1:1559;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDl467d01-1172066614-828461172149460-11
                    To:
<sip:7324209231@200.123.200.123;user=phone>;tag=766328382d3efc1f
                    Call-ID: SDl467d01-f1a930b070d8b0491d80d36fd4f7f1cc-vjvtfv3
                    Max-Forwards: 68
                    Content-Length: 0
```

Trace 3: INIVTE Received but no SIP URI available

The number the incoming call is trying to dial is “7324209231”, unfortunately the SIP URI available is depicted in Figure 20.

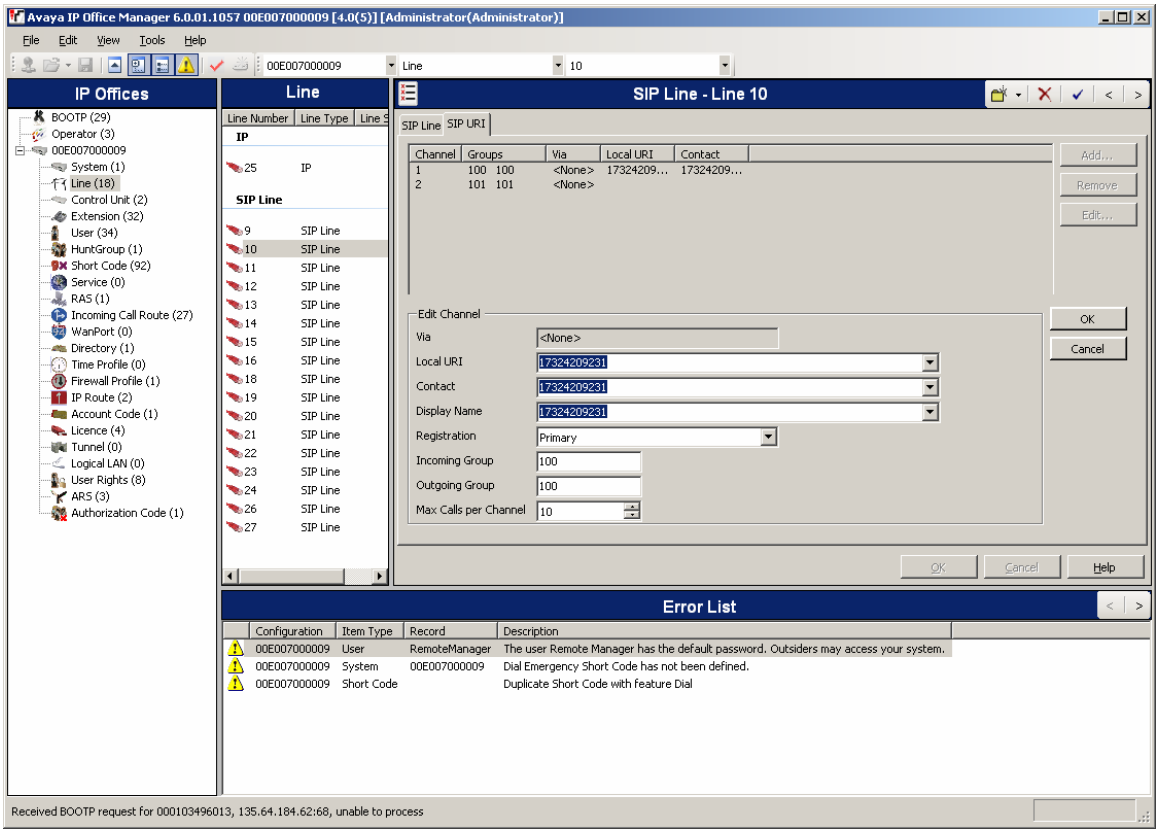

Figure 20: Example of Wrong SIP URI setting

The incoming number is not matching the URI selected because its local URI field has one digit more, a digit “1” in front of the number that is target of the call of Trace 3.

2. Another common error is to forget to set the Incoming Call Route for a given SIP URI. Here is an example. This time the URI of Figure 20 as been correctly configured, in Figure 21

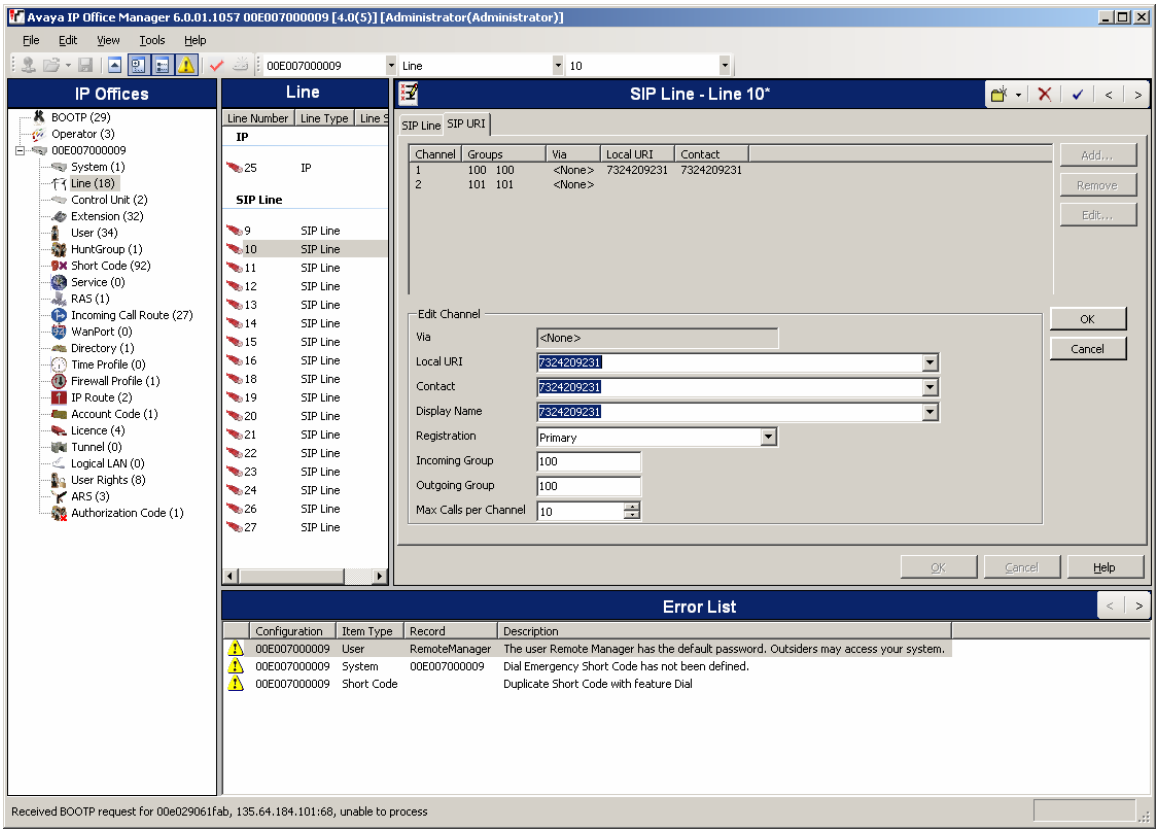

Figure 21: Correct Version of SIP URI of Figure 20

Unfortunately no Incoming Call Route has been set for Incoming Group 100 (not displayed in Figure 26). The result is a failure of incoming call, documented in Trace 4 as reported below:

```
     40719mS SIP Trunk: 10:Rx
                    INVITE sip:7324209231@217.41.84.186:5060 SIP/2.0
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0oso78307861lbsvo0k0.1
                    From: Unavailable
<sip:1441707299900@127.16.21.179;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDucmtb01-1172067223-1491271172216350-11
                    To: <sip:7324209231@200.123.200.123;user=phone>
                    CSeq: 5608 INVITE
                    Contact: <sip:1441707299900@200.123.200.123:5060;att=AJAY2-
n4hi26am5t17b;transport=udp>
                    Call-ID: SDucmtb01-2fc380b1c3ed02e3b7cbf66831754c2d-vjvtfv3
                    Max-Forwards: 68
                    Content-Type: application/sdp
                    Content-Length: 253
                    Accept: application/sdp, application/isup,
application/dtmf, application/dtmf-relay, multipart/mixed
                    Accept-Language: en; q=0.0
```

```
                    Allow: INVITE, ACK, CANCEL, BYE, REGISTER, REFER, INFO,
SUBSCRIBE, NOTIFY, PRACK, UPDATE

                    v=0
                    o=Sonus_UAC 28793 21060 IN IP4 200.123.200.123
                    s=SIP Media Capabilities
                    c=IN IP4 200.123.200.123
                    t=0 0
                    m=audio 26734 RTP/AVP 18 0 127
                    a=rtpmap:18 G729/8000
                    a=rtpmap:0 PCMU/8000
                    a=rtpmap:127 telephone-event/8000
                    a=fmtp:127 0-15
                    a=sendrecv


     40732mS SIP Trunk: 10:Tx
                    SIP/2.0 100 Trying
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0oso78307861lbsvo0k0.1
                    From: Unavailable
<sip:1441707299900@127.16.21.179;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDucmtb01-1172067223-1491271172216350-11
                    To:
<sip:7324209231@200.123.200.123;user=phone>;tag=906a1d2e68dd38ba
                    Call-ID: SDucmtb01-2fc380b1c3ed02e3b7cbf66831754c2d-vjvtfv3
                    CSeq: 5608 INVITE
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
                    Content-Length: 0


     40744mS CMExtnCutEvt: 0.1014.2 1 SIPTrunk Endpoint: SetLocalTone
CMLocalToneNone->CMLocalToneCutThru
     40745mS CMExtnCutEvt: 0.1014.2 1 SIPTrunk Endpoint: AudioConnectionChange
current=CMLocalToneCutThru new=CMLocalToneUnCut active=CMLocalToneNone
     40746mS MH  : 0.1014.2 1 SIPTrunk Endpoint LCMH Tone
CMLocalToneNone(CMLocalToneNone)->CMLocalToneUnCut, other side's media handler
is not changed (not lcmh) renego 0
     40746mS MH  : 0.1014.2 1 SIPTrunk Endpoint LCMH PlayLocalTone
CMLocalToneUnCut (current CMLocalToneUnCut, prev CMLocalToneNone) in parent
state CMCSIdle action 1 renegotiate 0 voip_negotiator->processing_inbound 0
     40747mS MH  : 0.1014.2 1 SIPTrunk Endpoint ProcessInboundMsg, set
incoming_leg to true
     40747mS CD: CALL: 0.1014.2 State=0 Cut=1 Music=0.0 Aend="Line 10" (0.0)
Bend="" [] (0.0) CalledNum=7324209231 () CallingNum=1441707299900@127.16.21.179
(Unavailable) Internal=0 Time=5 AState=0
     40749mS CMTARGET:     0.1014.2 1 SIPTrunk Endpoint: LOOKUP CALL ROUTE:
type=0 called_party=7324209231 sub= calling=1441707299900@127.16.21.179 in=1
complete=1
     40749mS PRN: BasicFindBestInCallRouteMatch returns(0)
     40751mS CMLOGGING:
CALL:2007/02/2114:13,00:00:00,000,1441707299900@127.16.21.179,I,7324209231,7324
209231,Unavailable,,,1,,""n/a,0
     40751mS CD: CALL: 0.1014.2 State=0 Cut=0 Music=0.0 Aend="Line 10" (0.0)
Bend="" [] (0.0) CalledNum=7324209231 () CallingNum=1441707299900@127.16.21.179
(Unavailable) Internal=0 Time=9 AState=7
     40753mS CD: CALL: 0.1014.2 Deleted
     40753mS CMTARGET:     0.1014.2 -1 SIPTrunk Endpoint: ~CMTargetHandler
     40753mS SipDebugInfo:  Terminating dialog 1ce94b8, state 10 for cause 1
     40754mS SipDebugInfo:  Sending code 404 to method INVITE
```

```
     40754mS SipDebugInfo:  SendSIPResponse, Number of Tag Count, 1
     40755mS SipDebugInfo: Sip_sendToNetwork packet of length 445
     40756mS SipDebugInfo: SIPTrunk SendToTarget  cff2e1c8, 5060
     40756mS SIP Trunk: 10:Tx
                    SIP/2.0 404 Not Found
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0oso78307861lbsvo0k0.1
                    From: Unavailable
<sip:1441707299900@127.16.21.179;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDucmtb01-1172067223-1491271172216350-11
                    To:
<sip:7324209231@200.123.200.123;user=phone>;tag=906a1d2e68dd38ba
                    Call-ID: SDucmtb01-2fc380b1c3ed02e3b7cbf66831754c2d-vjvtfv3
                    CSeq: 5608 INVITE
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
                    Content-Length: 0



     41376mS SIP Trunk: 10:Rx
                    ACK sip:7324209231@217.41.84.186:5060 SIP/2.0
                    Via: SIP/2.0/UDP
200.123.200.123:5060;branch=z9hG4bK0oso78307861lbsvo0k0.1
                    CSeq: 5608 ACK
                    From: Unavailable
<sip:1441707299900@172.16.22.1:1700;user=phone;att=AJAY2-
0dj4jaenrcebe>;tag=SDucmtb01-1172067223-1491271172216350-11
                    To:
<sip:7324209231@200.123.200.123;user=phone>;tag=906a1d2e68dd38ba
                    Call-ID: SDucmtb01-2fc380b1c3ed02e3b7cbf66831754c2d-vjvtfv3
                    Max-Forwards: 68
                    Content-Length: 0
```

Trace 4: Incoming INVITE, but Incoming Call Route is found for that SIP URI

As it is reported in Trace 11, the log marked in red "BasicFindBestInCallRouteMatch returns(0)", highlights that a valid SIP URI existed, but the route correspective to such URI was inexistent.

If you are capable of making outbound calls, but not of receiving inbound calls

In case outbound calls are successful, but inbound fails, these are some areas of investigation:

1. Check with ITSP if the inbound number is assigned to your SIP account.
2. Check if an INVITE reaches your modem. It might be that there is some form of firewall, may be coupled with NAT functionality, that allows methods inbound only if there has been some outbound on the same port to keep the binding alive.

   In that case there are two feasible way to proceed:

One is to open permanently port 5060 to allow inbound calls to reach IP Office. The other is to set a non-zero Binding Refresh time in the Network Topology Discovery of the LAN interface used as Network Topology Profile. That will trigger the transmission of OPTIONS method on port 5060 that will allow keeping the firewall binding open.

If you are behind a Symmetric Firewall

Depending on the type of configuration, you may need to open some hole in the firewall to communicate with SIP. This concerns both port 5060 and RTP range. If you plan to run STUN discovery and port 3478 is not open, you may actually end up having as a result of discovery a UDP BLOCKED topology.