Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Ingate SIParator with Avaya SIP Enablement Services and Avaya Communication Manager to Support Remote SIP Endpoints - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Ingate SIParator with Avaya SIP Enablement Services and Avaya Communication Manager.

The Ingate SIParator is a SIP session border controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints connected to an enterprise site across an untrusted network.

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 procedures for configuring the Ingate SIParator with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

The Ingate SIParator is a SIP session border controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints connected to an enterprise site across an untrusted network.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows various remote SIP endpoints connected to an enterprise site across an untrusted network. The main site has a Juniper Networks Netscreen-50 firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise. Also connected to the edge of the main site is a SIParator SBC. The public side of the SIParator is connected to the untrusted network and the private side is connected to the trusted corporate LAN. The SIParator could also reside in the demilitarized zone (DMZ) of the enterprise but this configuration was not tested.

All SIP traffic between the remote endpoints and the enterprise site flows through the SIParator. In this manner, the SIParator can protect the main site's infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams. All non-SIP traffic bypasses the SIParator and flows directly between the untrusted network and the private LAN of the enterprise if permitted by the data firewall.

Connected to the corporate LAN at the main site is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Both SIP and non-SIP endpoints are included. An ISDN-PRI trunk connects the media gateway to the PSTN.

Remote SIP endpoints include Avaya 4600 Series IP Telephones running SIP firmware. Some of the telephones were located behind a router/firewall performing network address translation (NAT) while others were not. The remote SIP endpoints use the SIParator as their call server. The SIParator in turn registers to the Avaya SES on behalf of the remote endpoints using its own private IP address. Thus, the SIParator appears to the Avaya SES as a set of SIP endpoints. All SIP endpoints both internal and remote use the same SIP domain: ***business.com***. All IP endpoints use the main enterprise site's TFTP/HTTP server to obtain their configuration files.

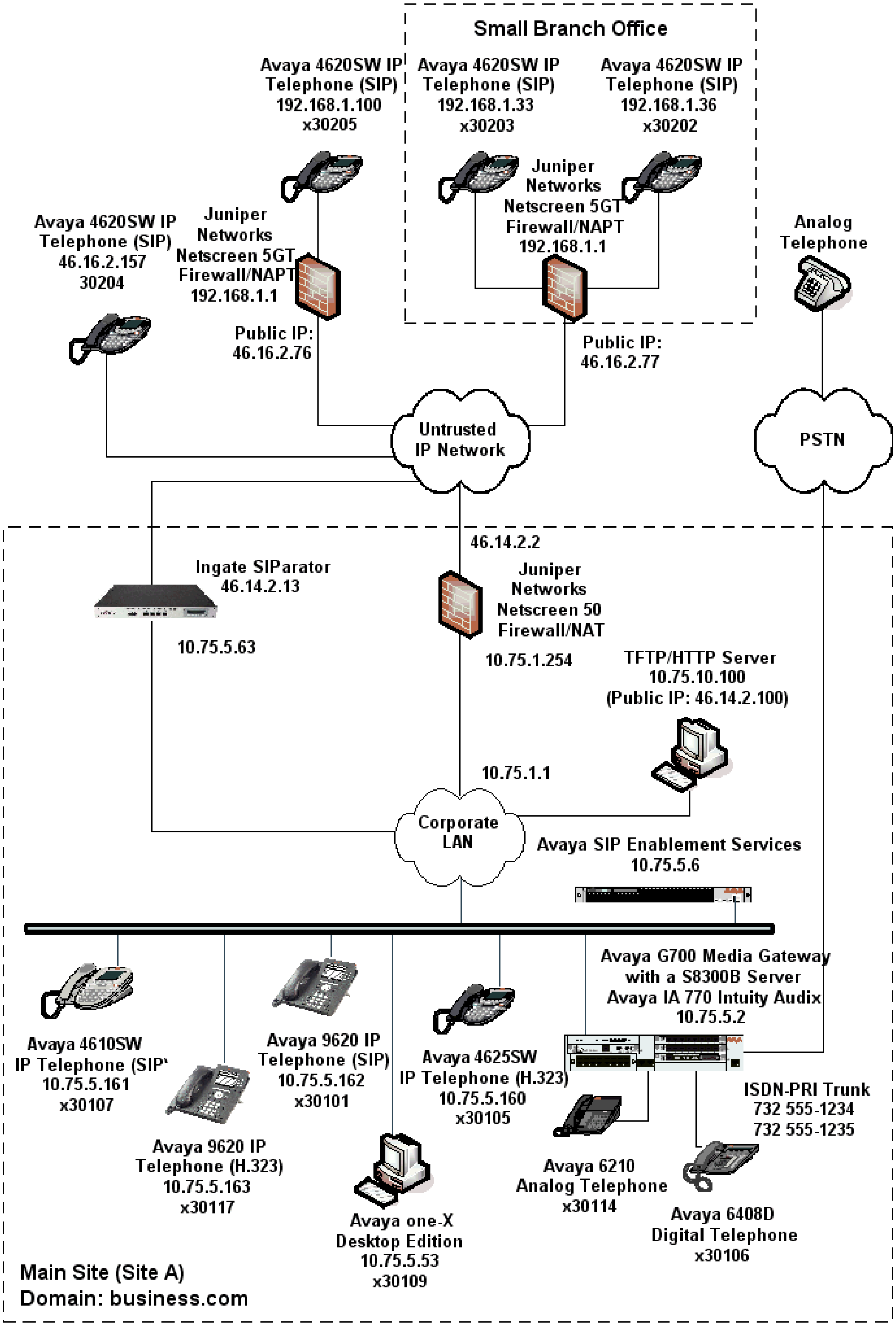

Small Branch Office
Avaya 4620SW IP Telephone (SIP) 192.168.1.100 x30205
Avaya 4620SW IP Telephone (SIP) 192.168.1.33 x30203
Avaya 4620SW IP Telephone (SIP) 192.168.1.36 x30202
Juniper Networks Netscreen 5GT Firewall/NAPT 192.168.1.1
Avaya 4620SW IP Telephone (SIP) 46.16.2.157 30204
Juniper Networks Netscreen 5GT Firewall/NAPT 192.168.1.1
Analog Telephone
Public IP: 46.16.2.76
Public IP: 46.16.2.77
Untrusted IP Network
PSTN
46.14.2.2
Ingate SIParator 46.14.2.13
Juniper Networks Netscreen 50 Firewall/NAT
10.75.5.63
10.75.1.254
TFTP/HTTP Server 10.75.10.100 (Public IP: 46.14.2.100)
10.75.1.1
Corporate LAN
Avaya SIP Enablement Services 10.75.5.6
Avaya G700 Media Gateway with a S8300B Server Avaya IA 770 Intuity Audix 10.75.5.2
Avaya 4610SW IP Telephone (SIP' 10.75.5.161 x30107
Avaya 9620 IP Telephone (SIP) 10.75.5.162 x30101
Avaya 4625SW IP Telephone (H.323) 10.75.5.160 x30105
ISDN-PRI Trunk 732 555-1234 732 555-1235
Avaya 9620 IP Telephone (H.323) 10.75.5.163 x30117
Avaya 6210 Analog Telephone x30114
Avaya one-X Desktop Edition 10.75.5.53 x30109
Avaya 6408D Digital Telephone x30106
Main Site (Site A)
Domain: business.com

Figure 1: SIP Remote Access Test Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300B Server with Avaya G700 Media Gateway Avaya IA 770 Intuity Audix	Avaya Communication Manager 5.0 Service Pack (R015x.00.0.825.4-15175)
Avaya S8500 Server	Avaya SIP Enablement Services 5.0
Avaya 4625SW IP Telephones (H.323)	H.323 version 2.8.3
Avaya 4610SW IP Telephone (SIP) Avaya 4620SW IP Telephones (SIP)	SIP version 2.2.2
Avaya 9620 IP Telephones (H.323)	Avaya one-X Deskphone Edition 1.5
Avaya 9620 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.0.3
Avaya one-X Desktop Edition (SIP)	2.1 Service Pack 2
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (TFTP/HTTP Server)	Windows XP Professional SP 2
Juniper Networks Netscreen-50	5.4.0r9.0
Ingate SIParator QoS Module (optional)	4.6.2 with patch ig-patch-4-6-2-media_stream_linger_2.fup

3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration at the main site to support the network shown in **Figure 1**. It assumes the procedures necessary to support SIP and connectivity to Avaya SES have been performed as described in [3]. It also assumes that an off-PBX station (OPS) has been configured on Avaya Communication Manager for each internal SIP endpoint in the configuration as described in [3] and [4]. The configuration of the remote SIP endpoints is shown in **Section 3.2**.

This section is divided into two parts. **Section 3.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

Section 3.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with the SIParator. This includes the configuration of the remote SIP endpoints.

The configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

3.1. Summary of Initial SIP Installation

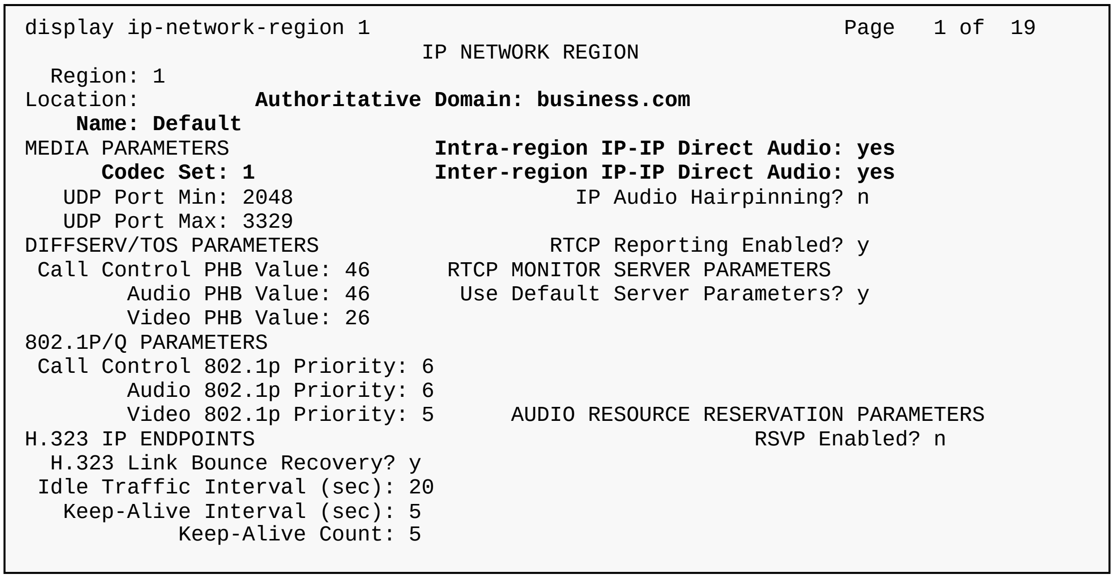
This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

IP network region

The Avaya S8300 Server, Avaya SES and IP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test.

- **Authoritative Domain**: ***business.com*** This field was configured to match the domain name configured on Avaya SES. This name will appear in the "From" header of SIP messages originating from this IP region.
- **Name**: ***Default*** Any descriptive name may be used.
- **Intra-region IP-IP Direct Audio**: ***yes***
Inter-region IP-IP Direct Audio: ***yes***
By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the **Signaling Group** form.
- **Codec Set**: ***1*** The codec set contains the set of codecs available for calls within this IP network region. This includes SIP calls since all necessary components are within the same region.



```
display ip-network-region 1                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: business.com
    Name: Default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td><b>Codecs</b>
IP codec set 1 was used for the compliance test. Multiple codecs were listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The list includes the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test. It should be noted that when testing the use of each individual codec, only the codec under test was included in the list.
<pre>
display ip-codec-set 1   Page   1 of   2

                          IP Codec Set

    Codec Set: 1

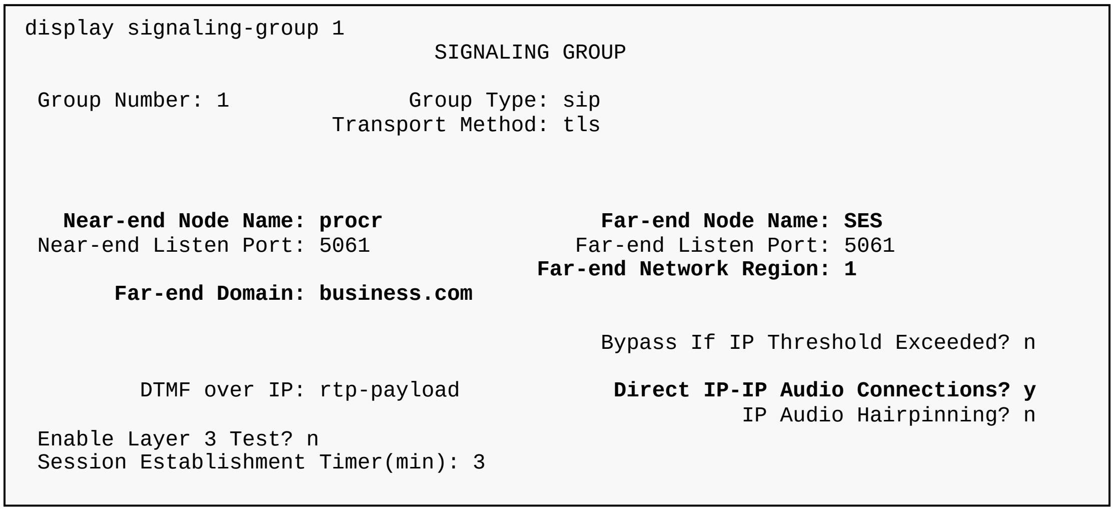
    Audio   Silence   Frames   Packet
    Codec   Suppression Per Pkt Size(ms)
 1: G.711MU   n   2   20
 2: G.729AB   n   2   20
 3:
</pre></td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Signaling Group

For the compliance test, signaling group 1 was used for the signaling group associated with the SIP trunk group between Avaya Communication Manager and Avaya SES. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as described in [3].

- **Near-end Node Name**: ***procr*** This node name maps to the IP address of the Avaya S8300 Server. Node names are defined using the **change node-names ip** command.
- **Far-end Node Name**: ***SES*** This node name maps to the IP address of Avaya SES.
- **Far-end Network Region**: ***1*** This defines the IP network region which contains Avaya SES.
- **Far-end Domain**: ***business.com*** This domain is sent in the “To” header of SIP messages of calls using this signaling group.
- **Direct IP-IP Audio Connections**: ***y*** This field must be set to ***y*** to enable media shuffling on the SIP trunk.



```
display signaling-group 1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
                        Transport Method: tls



   Near-end Node Name: procr                 Far-end Node Name: SES
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
       Far-end Domain: business.com

                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? n
 Enable Layer 3 Test? n
 Session Establishment Timer(min): 3
```

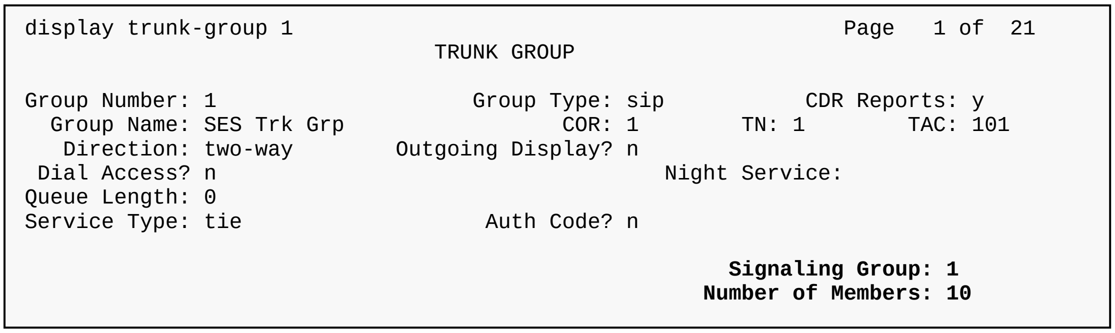
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

Trunk Group

For the compliance test, trunk group 1 was used for the SIP trunk group between Avaya Communication Manager and Avaya SES. Trunk group 1 was configured using the parameters highlighted below. All other fields were set as described in [3].

- **Signaling Group**: ***1*** This field is set to the signaling group shown in the previous step.
- **Number of Members: *10*** This field represents the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.



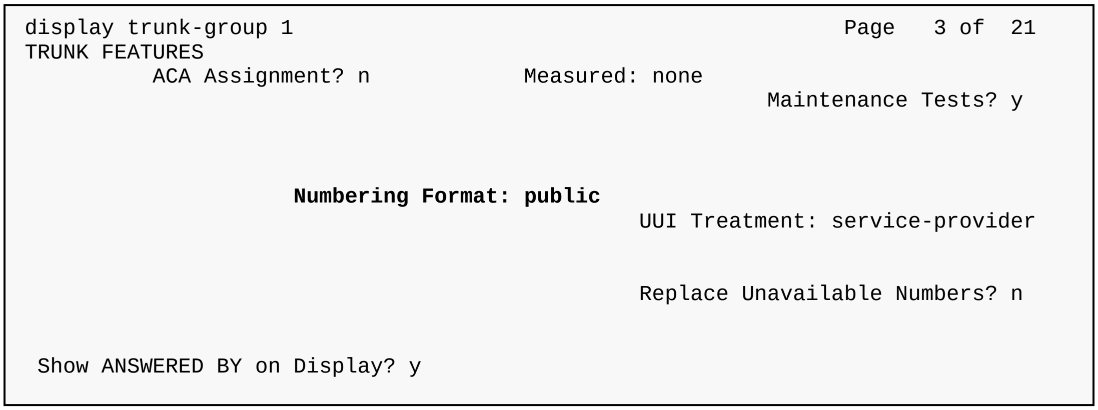
```
display trunk-group 1                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SES Trk Grp                 COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 1
                                                     Number of Members: 10
```

</td></tr>
<tr><td>5.</td><td>

Trunk Group – continued

On **Page 3**:

- Verify the **Numbering Format** field is set to ***public***. This field specifies the format of the calling party number sent to the far-end.
- The default values may be retained for the other fields.



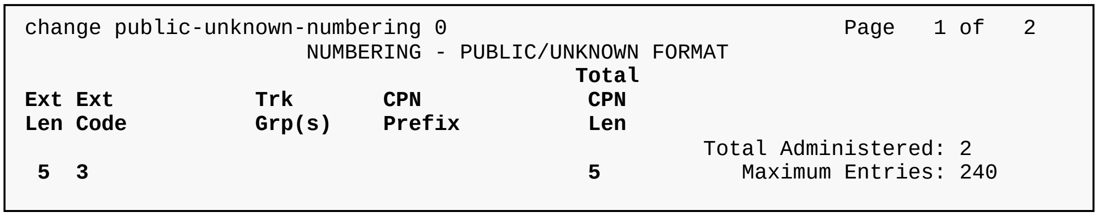
```
display trunk-group 1                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider


                                                Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>

Public Unknown Numbering

Public unknown numbering defines the calling party number to be sent to the far-end. An entry was created for the trunk group defined in **Step 4**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across any trunk group (**Trk Grp** column is blank) will be sent as a 5 digit calling number. This calling party number is sent to the far-end in the SIP “From” header.



```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 2
 5  3                                       5           Maximum Entries: 240
```

</td></tr>
</table>

3.2. Configure SIParator Specific Configuration

This section describes the specific procedures necessary for interfacing to the SIParator to support remote endpoints. This involves the creation of OPS stations on Avaya Communication Manager for each remote endpoint supported by the SIParator. For interoperability, IP-IP Direct Audio (media shuffling) must be disabled for calls passing through the SIParator. This section will describe how to configure Avaya Communication Manager so that media shuffling will only be disabled on calls to the SIParator.

Step — **Description**

1. **IP Network Region For Remote Users**
A separate IP network region was created for the remote endpoints. It is configured the same as the IP network region described in **Section 3.1**, **Step 1**, except a different descriptive name is used for the **Name** field and both **Intra-region** and **Inter-region IP-IP Direct Audio** is set to ***no***.

```
change ip-network-region 3                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 3
Location:         Authoritative Domain: business.com
    Name: Remote Users
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

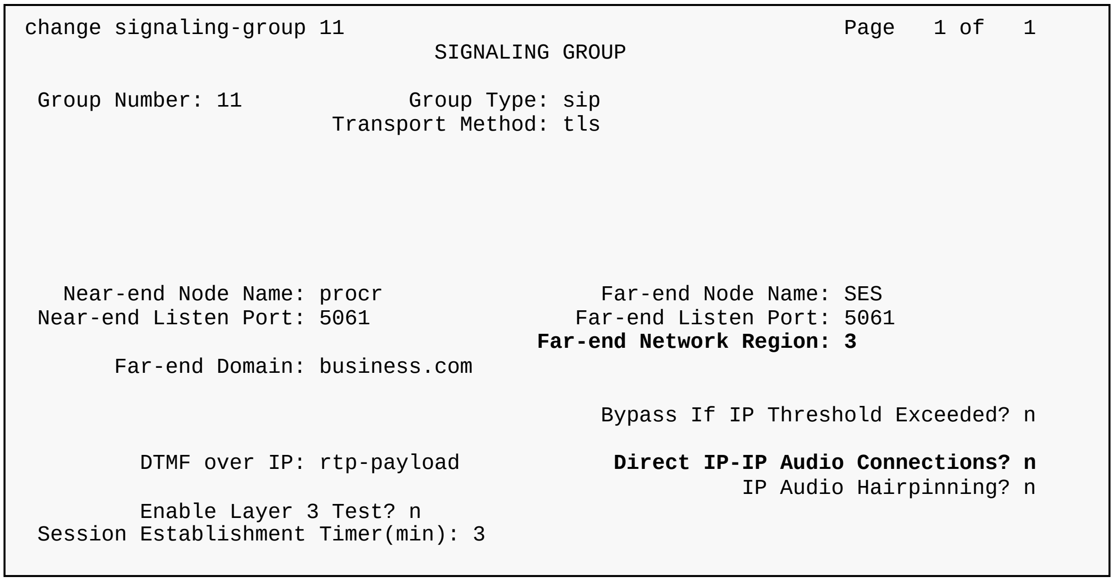
2. **IP Network Region For Remote Users - Continued**
On **Page 3**, the codec set used between region 3 and region 1 was selected to be codec set 1. Default values were used for all other parameters. This is the same codec set used for intra-region calls in both regions 3 and 1 (See **Section 3.1**, **Step 1**). Optionally, a different codec set could have been chosen for inter-region calls.

```
change ip-network-region 3                                      Page   3 of  19

                   Inter Network Region Connection Management

 src dst codec direct   WAN-BW-limits   Video                        Dyn
 rgn rgn  set   WAN  Units    Total Norm  Prio Shr Intervening-regions  CAC IGAR
 3   1    1     y    NoLimit                                                 n
 3   2
 3   3    1
 3   4
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Signaling Group

A second signaling group was created for the remote endpoints. It has the same properties as the signaling group described in **Section 3.1**, **Step 3**, except the **Far-end Network Region** is set to ***3*** and the **Direct IP-IP Audio Connections** field is set to ***no***.

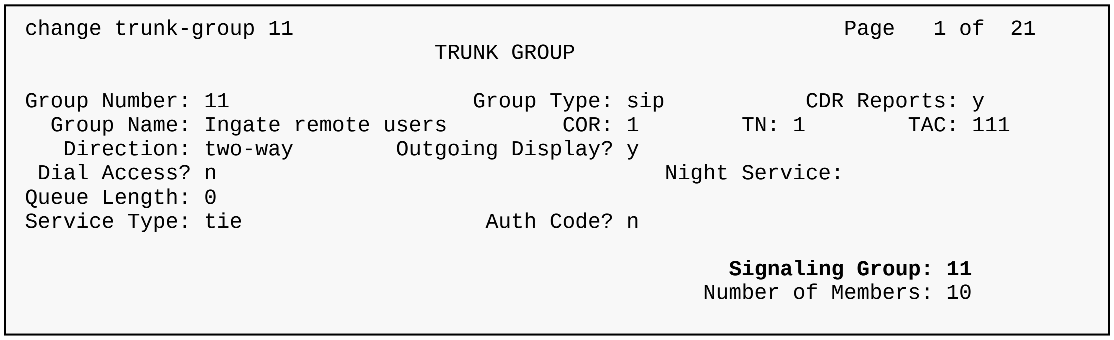


```
change signaling-group 11                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 11             Group Type: sip
                        Transport Method: tls







   Near-end Node Name: procr                 Far-end Node Name: SES
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 3
       Far-end Domain: business.com

                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? n
                                                        IP Audio Hairpinning? n
         Enable Layer 3 Test? n
 Session Establishment Timer(min): 3
```

</td></tr>
<tr><td>4.</td><td>

Trunk Group

A second trunk group was created for the remote endpoints. It has the same properties as the trunk group described in **Section 3.1**, **Step 4**, except the **Signaling Group** field is set to ***11***. In **Step 8**, the remote SIP endpoints will be mapped to use this trunk group which has media shuffling disabled.



```
change trunk-group 11                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 11                   Group Type: sip           CDR Reports: y
  Group Name: Ingate remote users         COR: 1        TN: 1        TAC: 111
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 11
                                                     Number of Members: 10
```

</td></tr>
</table>

Step	Description
5.	**Stations** Each remote endpoint must have a station created for it in the same manner as an internal enterprise endpoint. The example below shows the creation of one of the remote endpoints – extension 30204. The **Type** field was set to match the type of telephone used - ***4620***. The **Port** field was set to ***IP***. The **Name** field can be set to any descriptive name. The remote endpoints had **Coverage Path 1** set to ***1***. This coverage path pointed to voicemail. The configuration of the coverage path and voicemail are beyond the scope of these Application Notes.

```
add station 30204                                              Page   1 of   5
                                     STATION

Extension: 30204                           Lock Messages? n               BCC: 0
     Type: 4620                            Security Code:                  TN: 1
     Port: IP                            Coverage Path 1: 1               COR: 1
     Name: Remote SIP3                   Coverage Path 2:                 COS: 1
                                         Hunt-to Station:
STATION OPTIONS
                                             Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                   Message Lamp Ext: 30204
            Speakerphone: 2-way                 Mute Button Enabled? y
        Display Language: english                  Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n


                                                Customizable Labels? y
```

Step	Description

6.

Stations - Continued

On **Page 2**, the **Bridged Call Alerting** field was set to ***y***. This will allow this endpoint to ring on a bridged call for another endpoint. The **Restrict Last Appearance** field was set to ***n***, so that the last call appearance can be used for either an inbound or outbound call.

```
add station 30204                                              Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
             CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? y                       Restrict Last Appearance? n
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: enhanced
    MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name:                      Select Last Used Appearance? n
                                                 Coverage After Forwarding? s

                                               Direct IP-IP Audio Connections? y
  Emergency Location Ext: 30204         Always Use? n IP Audio Hairpinning? n
```

7.

Stations - Continued

On **Page 4**, under BUTTON ASSIGNMENTS, three call appearances (**call-appr**) were created. In addition, some features tested during the compliance test require button assignments on the station form. This included Conference On Answer (**no-hld-cnf**) and Automatic Callback (**auto-cback**).

```
add station 30204                                              Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                              Headset? n
       Jack:                                              Speaker? n
      Cable:                                             Mounting: d
      Floor:                                          Cord Length: 0
   Building:                                            Set Color:

ABBREVIATED DIALING
     List1:                   List2:                   List3:


BUTTON ASSIGNMENTS
 1: call-appr                           5: no-hld-cnf
 2: call-appr                           6: auto-cback
 3: call-appr                           7:
 4:                                     8:
```

Step **Description**

8. **Off-PBX station mapping**

All SIP endpoints, including the remote SIP endpoints, are configured as OPS stations on Avaya Communication Manager. Thus, they require a mapping between the station extension and the **Phone Number** and **Trunk** used to reach the SES. In the example below, the station extension 30204 is listed as an OPS station that is mapped to phone number 30204 via trunk 11. (The phone number in this case refers to the user name defined on the Avaya SES **– Section 4.2**, **Step 1**). The remote endpoints are mapped to trunk group 11 because media shuffling has been disabled on this trunk group. Default values are used for all other fields.

```
change off-pbx-telephone station-mapping 30204                  Page   1 of   2
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station        Application Dial   CC  Phone Number      Trunk       Config
 Extension                  Prefix                       Selection   Set
 30204             OPS           -     30204              11         1
```

9. **Off-PBX station mapping - Continued**

On **Page 2**, station extension 30204 has a **Call Limit** set to ***3*** to match the number of call appearances in **Step 7**. **Mapping Mode** and **Bridged Calls** are set to ***both*** to receive both incoming and outgoing calls. Default values are used for all other fields.

```
change off-pbx-telephone station-mapping 30204                  Page   2 of   2
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Call      Mapping      Calls       Bridged        Location
 Extension     Limit     Mode         Allowed     Calls
 30204          3      both           all         both
```

4. Configure Avaya SIP Enablement Services

This section covers the configuration of Avaya SES at the main site. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure Avaya SES. For additional information on these installation tasks, refer to [5].

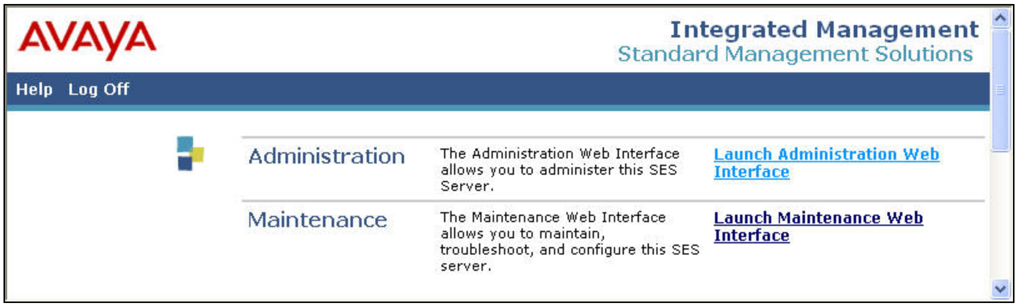
Each SIP endpoint used in the compliance test that registers with Avaya SES requires that a user and media server extension be created on Avaya SES. The creation of users and media server extensions for the internal enterprise SIP endpoints are not covered here. These procedures are covered in [5]. The creation of users and media server extensions for the remote SIP endpoints are covered in **Section 4.2**.

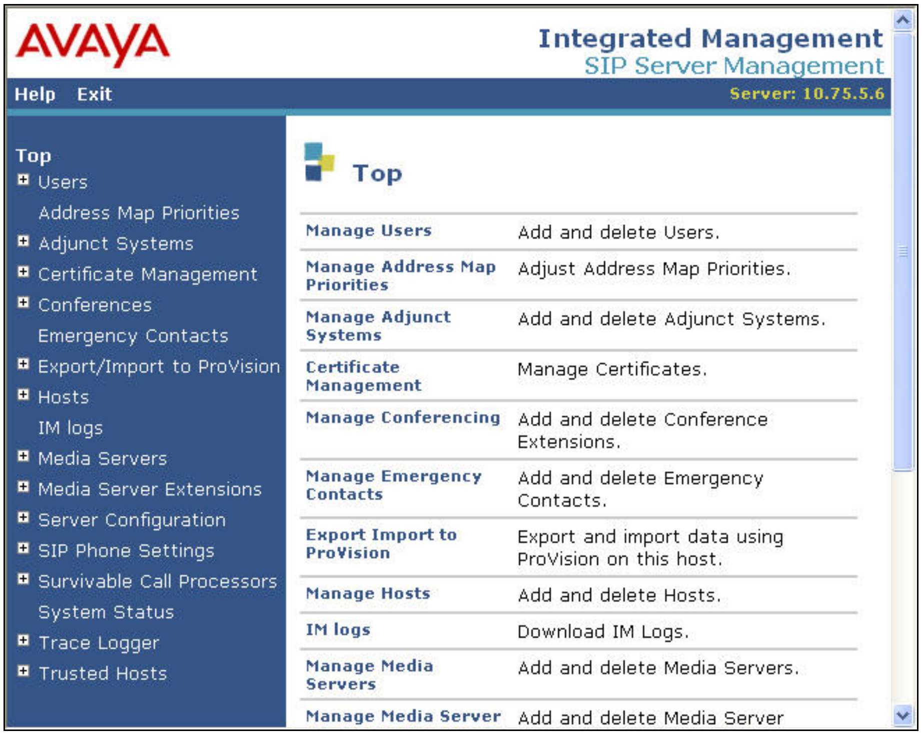
This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

Section 4.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with the SIParator. This includes configuration of the remote SIP endpoints.

4.1. Summary of Initial Configuration Parameters

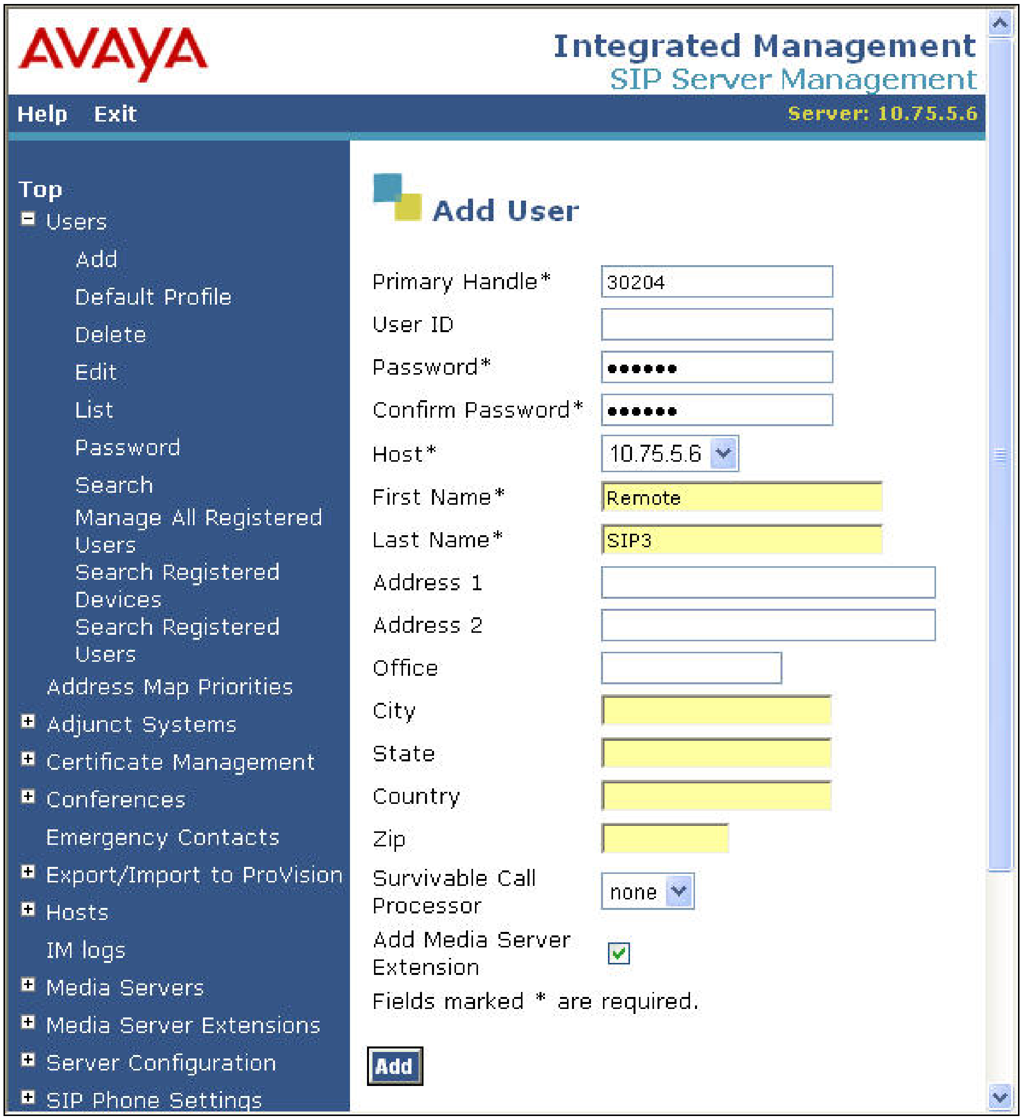
This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	**Login** Access the Avaya SES administration web interface by entering http://<*ip-addr*>/admin as the URL in an Internet browser, where <*ip-addr*> is the IP address of the Avaya SES server. Log in with the appropriate credentials and then select the **Launch Administration Web Interface** link from the main page as shown below.  AVAYA Integrated Management Standard Management Solutions Help Log Off Administration – The Administration Web Interface allows you to administer this SES Server. – Launch Administration Web Interface Maintenance – The Maintenance Web Interface allows you to maintain, troubleshoot, and configure this SES server. – Launch Maintenance Web Interface

Step	Description
2.	**Top Page** The Avaya SES **Top** page will be displayed as shown below.  AVAYA Integrated Management SIP Server Management Help Exit Server: 10.75.5.6 Top Users Address Map Priorities Adjunct Systems Certificate Management Conferences Emergency Contacts Export/Import to ProVision Hosts IM logs Media Servers Media Server Extensions Server Configuration SIP Phone Settings Survivable Call Processors System Status Trace Logger Trusted Hosts Top Manage Users — Add and delete Users. Manage Address Map Priorities — Adjust Address Map Priorities. Manage Adjunct Systems — Add and delete Adjunct Systems. Certificate Management — Manage Certificates. Manage Conferencing — Add and delete Conference Extensions. Manage Emergency Contacts — Add and delete Emergency Contacts. Export Import to ProVision — Export and import data using ProVision on this host. Manage Hosts — Add and delete Hosts. IM logs — Download IM Logs. Manage Media Servers — Add and delete Media Servers. Manage Media Server — Add and delete Media Server
3.	**Initial Configuration Parameters** As part of the Avaya SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the Avaya SES administration home page shown in the previous step. • SIP Domain: ***business.com*** (To view, navigate to **Server Configuration→System Parameters**) • Host IP Address (SES IP address): ***10.75.5.6*** • Host Type: ***SES combined home-edge*** (To view, navigate to **Host→List**; click **Edit**) • Media Server (Avaya Communication Manager) Interface Name: ***CMeast*** • SIP Trunk Link Type: ***TLS*** • SIP Trunk IP Address (Avaya S8300 Server IP address): ***10.75.5.2*** (To view, navigate to **Media Server→List**; click **Edit**)

4.2. SIParator Specific Configuration

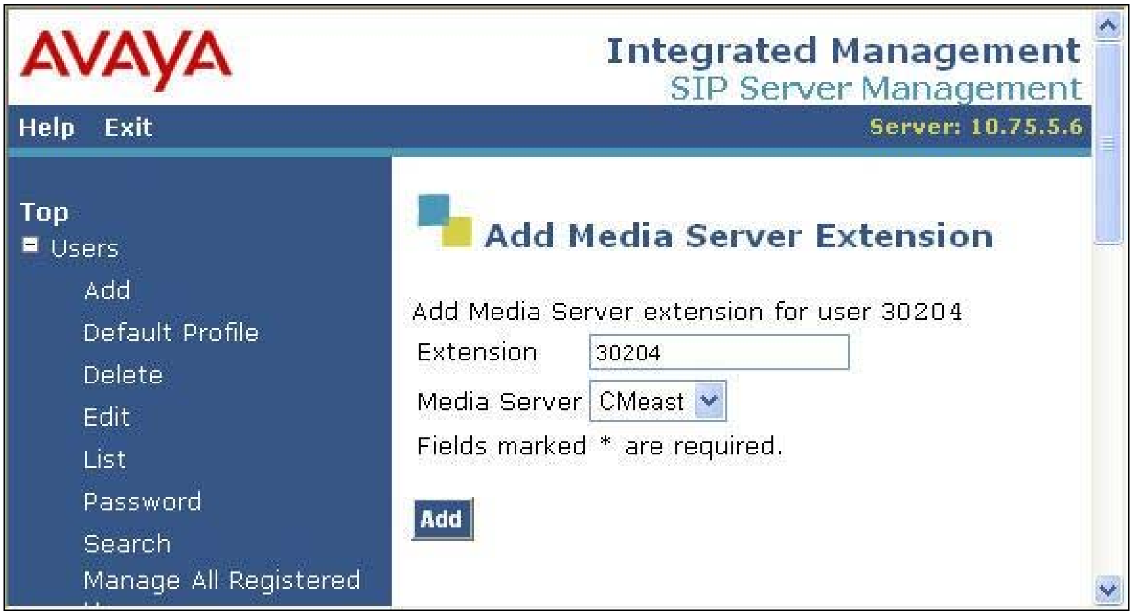
This section describes additional Avaya SES configuration necessary for interoperating with the SIParator. In particular, this section describes the configuration of a user and media server extension for each of the remote SIP endpoints that will be registered to the Avaya SES by the SIParator.

Step	Description
1.	**Users** Each remote SIP endpoint must have a user created for it on the Avaya SES in the same manner as an internal enterprise endpoint. The example below shows the creation of user 30204. The **Primary Handle** is set to the station extension created in **Section 3.2**, **Step 5**. Enter a password to be used to authenticate this user. Enter any descriptive name for the **First Name** and **Last Name** fields. Check the box **Add Media Server Extension**. 

Add User

Primary Handle*	30204
User ID	
Password*	••••••
Confirm Password*	••••••
Host*	10.75.5.6
First Name*	Remote
Last Name*	SIP3
Address 1	
Address 2	
Office	
City	
State	
Country	
Zip	
Survivable Call Processor	none
Add Media Server Extension	☑

Fields marked * are required.

Step	Description
2.	**Media Server Extension** After a confirmation screen (not shown), the following screen appears. In the extension field, enter the Avaya Communication Manager extension created in **Section 3.2**, **Step 5**.  AVAYA Integrated Management SIP Server Management Help Exit Server: 10.75.5.6 Top Users Add Default Profile Delete Edit List Password Search Manage All Registered Add Media Server Extension Add Add Media Server extension for user 30204 Extension 30204 Media Server CMeast Fields marked * are required.
3.	Repeat **Steps 1 – 2** for all remote SIP endpoints.

5. Configure the Avaya SIP Telephones

The SIP telephones at the enterprise site will use the local Avaya SES as the call server. The remote SIP endpoints will use the public IP address of the SIParator. The table below shows an example of the SIP telephone network settings for different types of endpoints.

	Main Site	**Remote Endpoint without NAT**	**Remote Endpoint with NAT**
Extension	30107	30204	30203
IP Address	10.75.5.161	46.16.2.157	192.168.1.33
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Router	10.75.5.1	46.16.2.1	192.168.1.1
File Server	10.75.10.100	46.14.2.100	46.14.2.100
DNS Server	0.0.0.0	0.0.0.0	0.0.0.0
SIP Domain	business.com	business.com	business.com
Call Server or SIP Proxy Server	10.75.5.6	46.14.2.13	46.14.2.13

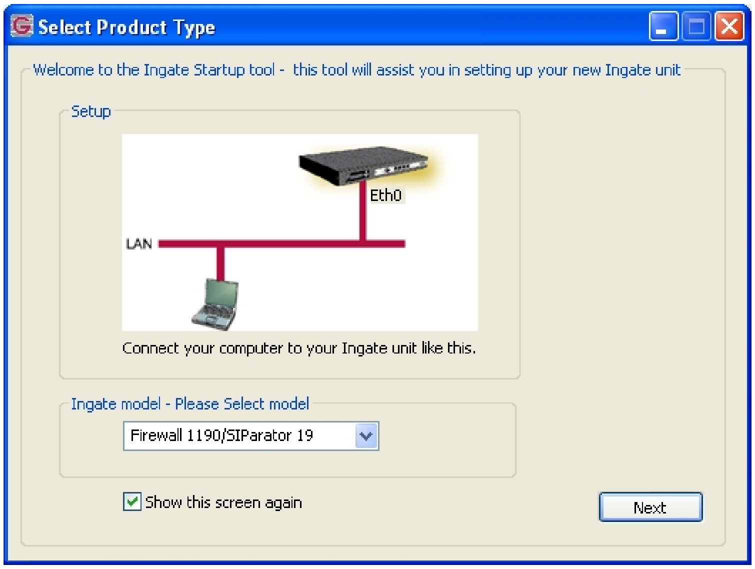
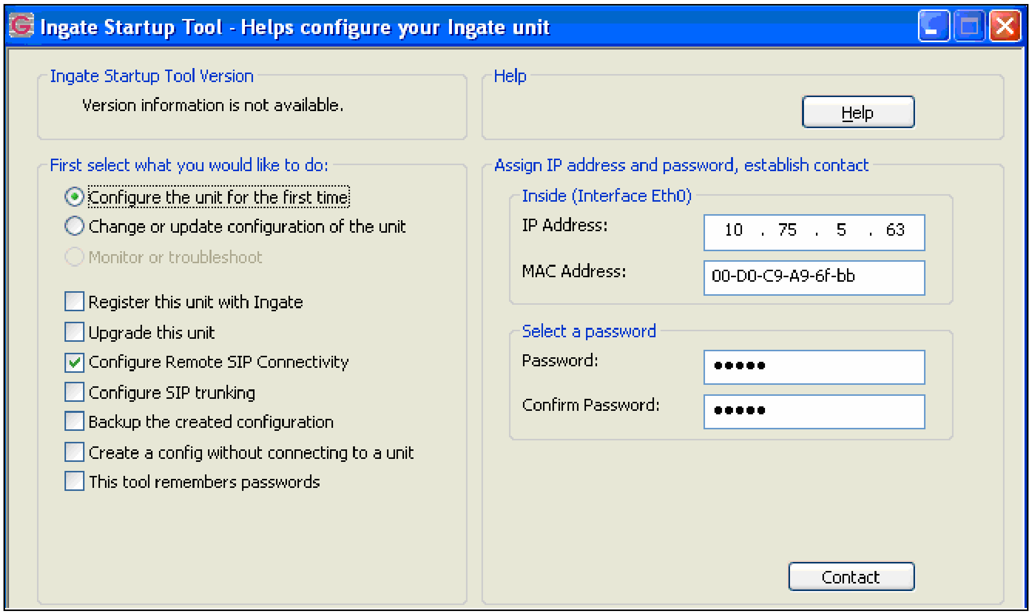
6. Configure the Ingate SIParator

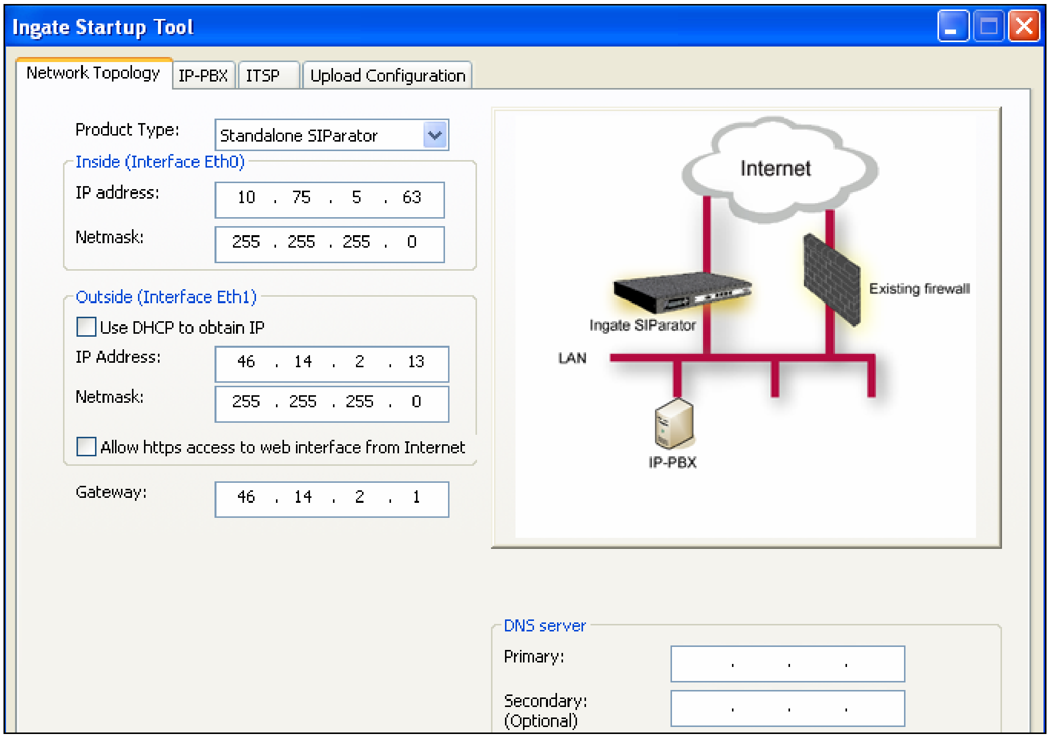
This section describes the configuration of the Ingate SIParator. To support the setting of the Differentiated Services Code Point (DSCP) bits for quality of service, the QoS module must be installed and requires additional licensing.

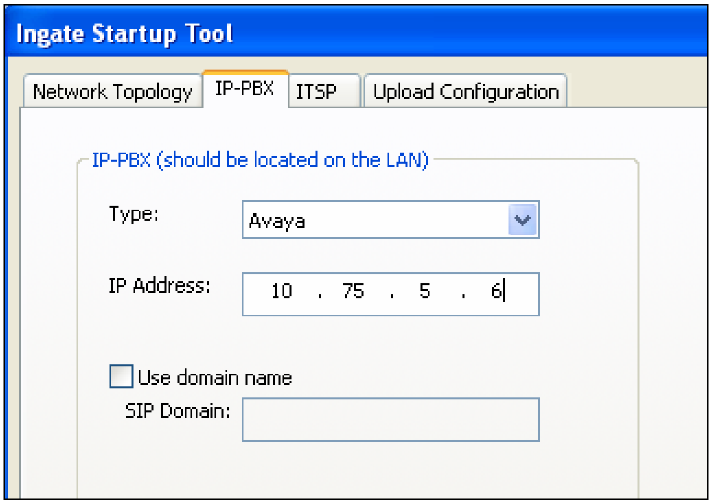
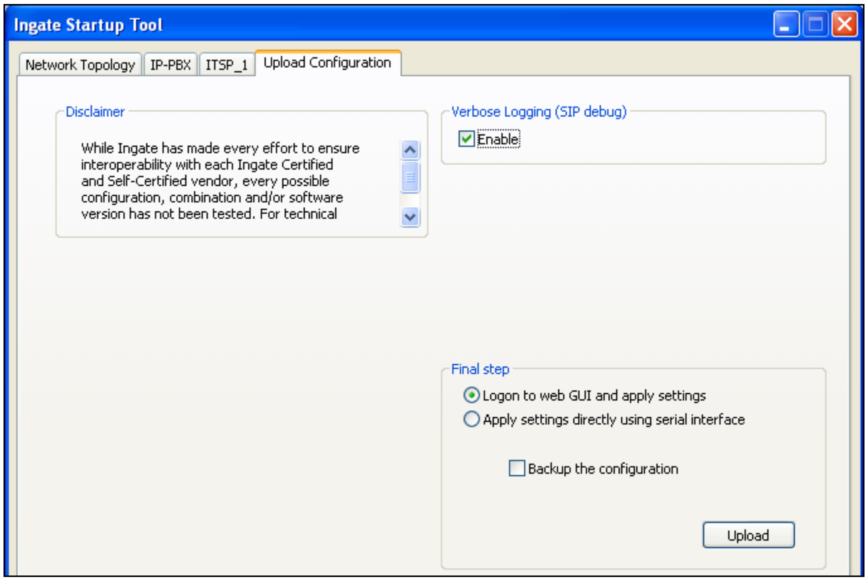
The SIParator is configured initially with the Ingate Startup Tool. Based on the provided input, the Startup Tool will create an initial configuration that can be uploaded to the SIParator. The results of this configuration can then be viewed or expanded using the SIParator web interface. To access the web interface, enter the IP address of the SIParator as the destination address in a web browser. When prompted for login credentials, enter an appropriate user name and password.

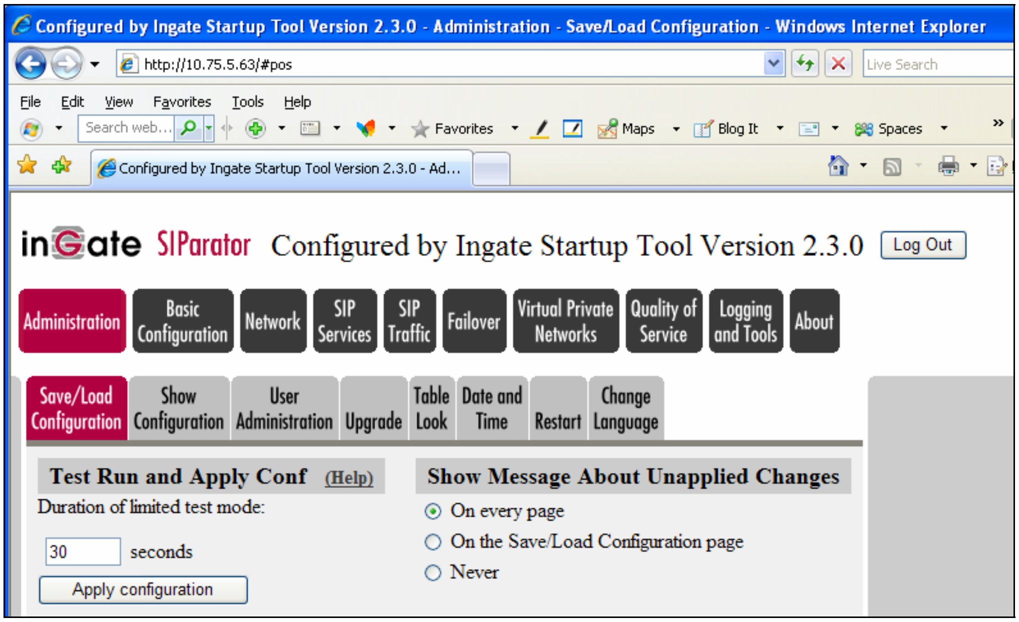
Much of the detailed SIP configuration is not visible from the Startup Tool but is driven by the type of IP-PBX and Service Provider chosen in the Startup Tool. The detailed SIP configuration resulting from the following procedure is captured in **Appendix A** for reference.

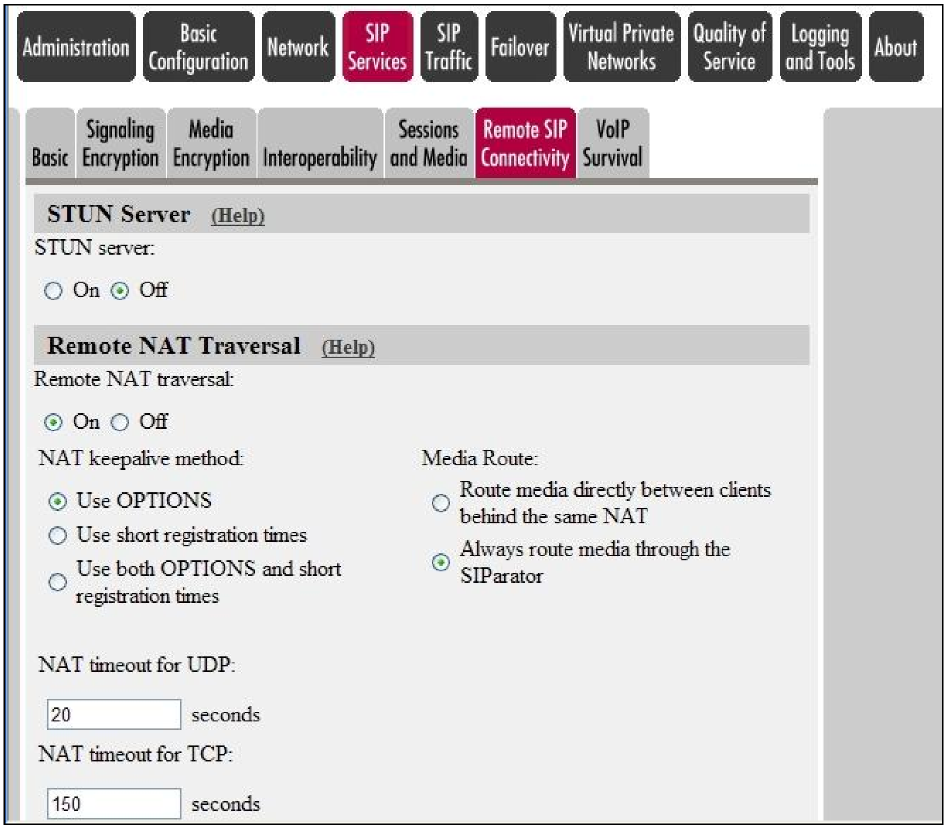
Step	Description
1.	**Launch Startup Tool** The Ingate Startup Tool is a Windows application which is launched from the Windows Start Menu by navigating to **Start→All Programs→Shortcut to StartupTool.exe**.

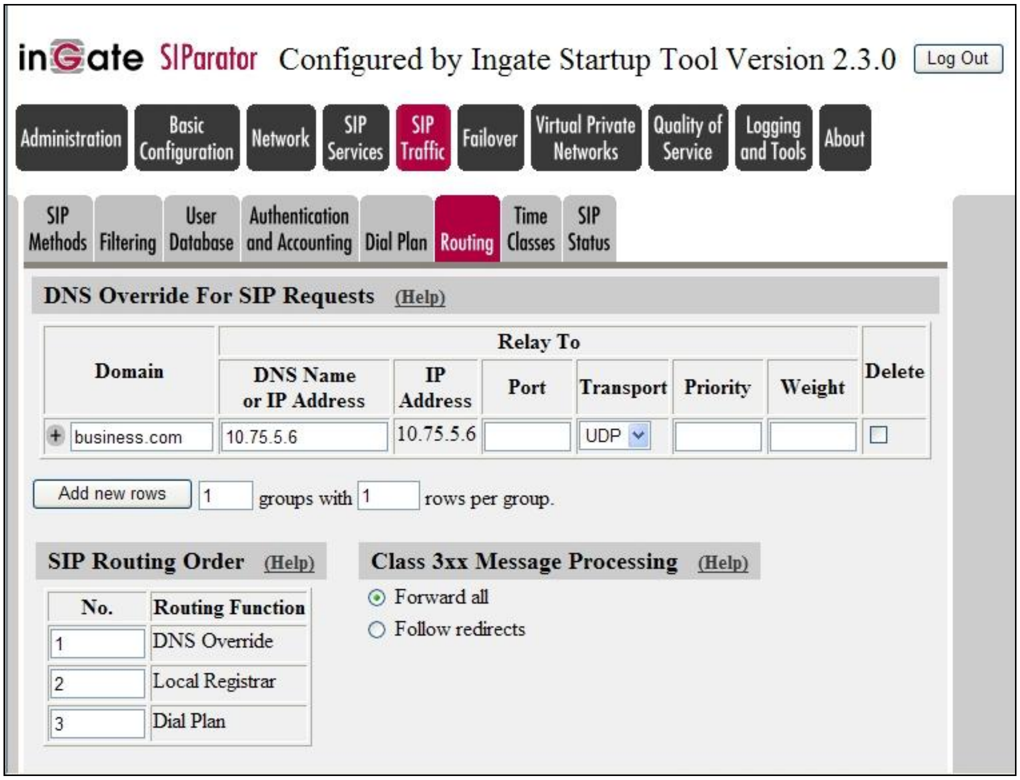
Step	Description
2.	**Select Product Type** The initial Ingate Startup Tool screen is shown below. Verify the PC is running on the same LAN subnet as the SIParator as shown in the diagram. This is necessary in order to assign the initial IP address to the SIParator from the Startup Tool. Select the SIParator model from the **Ingate model** drop-down menu. Click the **Next** button.  Select Product Type Welcome to the Ingate Startup tool - this tool will assist you in setting up your new Ingate unit Setup Connect your computer to your Ingate unit like this. Ingate model - Please Select model Firewall 1190/SIParator 19 ☑ Show this screen again
3.	**Select Configuration Options and Assign Private IP** Select options for **Configure the unit for the first time** and **Configure Remote SIP Connectivity**. Enter the inside IP address, MAC address and a password. Click the **Contact** button to establish a connection to the SIParator. For future updates, click the option - **Change or update configuration of the unit**.  Ingate Startup Tool - Helps configure your Ingate unit Ingate Startup Tool Version Version information is not available. Help First select what you would like to do: ● Configure the unit for the first time ○ Change or update configuration of the unit ○ Monitor or troubleshoot □ Register this unit with Ingate □ Upgrade this unit ☑ Configure Remote SIP Connectivity □ Configure SIP trunking □ Backup the created configuration □ Create a config without connecting to a unit □ This tool remembers passwords Assign IP address and password, establish contact Inside (Interface Eth0) IP Address: 10 . 75 . 5 . 63 MAC Address: 00-D0-C9-A9-6f-bb Select a password Password: ••••• Confirm Password: •••••

Step	Description
4.	**Network Topology** After connecting to the SIParator, the following page appears. Select the **Network Topology** tab. Select ***Standalone SIParator*** from the **Product Type** drop-down menu. Enter an IP address and subnet mask for both the inside and outside interfaces as shown in **Figure 1**. The **Gateway** field is set to the IP address of the default gateway on the public side of the SIParator. A DNS server was not used for the compliance test so the DNS server values were left blank.  Ingate Startup Tool Network Topology IP-PBX ITSP Upload Configuration Internet Existing firewall Ingate SIParator LAN IP-PBX Product Type: Standalone SIParator Inside (Interface Eth0) IP address: 10 . 75 . 5 . 63 Netmask: 255 . 255 . 255 . 0 Outside (Interface Eth1) □ Use DHCP to obtain IP IP Address: 46 . 14 . 2 . 13 Netmask: 255 . 255 . 255 . 0 □ Allow https access to web interface from Internet Gateway: 46 . 14 . 2 . 1 DNS server Primary: . . . Secondary: (Optional) . . .

Step	Description
5.	**IP-PBX Settings** Select the **IP-PBX** tab. Select ***Avaya*** from the **Type** drop-down menu. This will instruct the Startup Tool to configure the SIP parameters on the internal interface to be compatible with the Avaya SES. Enter the Avaya SES IP address in the **IP Address** field.  Ingate Startup Tool Network Topology IP-PBX ITSP Upload Configuration IP-PBX (should be located on the LAN) Type: Avaya IP Address: 10 . 75 . 5 . 6 □ Use domain name SIP Domain:
6.	**Upload Configuration** Select the **Upload Configuration** tab to upload the configuration to the SIParator. Click the **Upload** button to begin the upload.  Ingate Startup Tool Network Topology IP-PBX ITSP_1 Upload Configuration Disclaimer While Ingate has made every effort to ensure interoperability with each Ingate Certified and Self-Certified vendor, every possible configuration, combination and/or software version has not been tested. For technical Verbose Logging (SIP debug) ☑ Enable Final step ● Logon to web GUI and apply settings ○ Apply settings directly using serial interface □ Backup the configuration

Step	Description
7.	**Apply Configuration** After uploading the configuration, the Startup Tool opens a web browser to the **Administration→Save/Load Configuration** page of the SIParator. Click the **Apply configuration** button to apply the configuration. The Startup Tool configuration is complete at this point. However, additional configuration was required to support all the test cases in the compliance test. This configuration is performed using the SIParator web interface and is covered in the remaining steps.  Configured by Ingate Startup Tool Version 2.3.0 - Administration - Save/Load Configuration - Windows Internet Explorer http://10.75.5.63/#pos inGate SIParator Configured by Ingate Startup Tool Version 2.3.0 Log Out Administration Basic Configuration Network SIP Services SIP Traffic Failover Virtual Private Networks Quality of Service Logging and Tools About Save/Load Configuration Show Configuration User Administration Upgrade Table Look Date and Time Restart Change Language **Test Run and Apply Conf** (Help) Duration of limited test mode: 30 seconds **Show Message About Unapplied Changes** ● On every page ○ On the Save/Load Configuration page ○ Never

Step	Description
8.	**Enable NAT Traversal** To support remote endpoints that may reside behind NAT devices, NAT traversal must be enabled on the SIParator. Navigate to **SIP Services → Remote SIP Connectivity**, under **Remote NAT Traversal** click the **On** radio button.  Administration Basic Configuration Network SIP Services SIP Traffic Failover Virtual Private Networks Quality of Service Logging and Tools About Basic Signaling Encryption Media Encryption Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival **STUN Server** (Help) STUN server: ○ On ● Off **Remote NAT Traversal** (Help) Remote NAT traversal: ● On ○ Off NAT keepalive method: ● Use OPTIONS ○ Use short registration times ○ Use both OPTIONS and short registration times Media Route: ○ Route media directly between clients behind the same NAT ● Always route media through the SIParator NAT timeout for UDP: 20 seconds NAT timeout for TCP: 150 seconds

Step	Description
9.	**DNS Override** In the compliance test, no DNS server was used. However, the remote SIP endpoints were configured with the domain ***business.com*** and sent SIP requests using this domain. As a result, the SIParator was configured to map this domain to the IP address of the Avaya SES. The example below illustrates this mapping on the **SIP Traffic → Routing** page. Alternatively, this same result can be achieved using the Startup Tool by clicking the **Use domain name** box and entering the domain name in **Step 5**. By doing this, the same DNS Override entry is created as shown below and this step can be omitted. 

Configured by Ingate Startup Tool Version 2.3.0

DNS Override For SIP Requests

Domain	Relay To						Delete
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
business.com	10.75.5.6	10.75.5.6		UDP			□

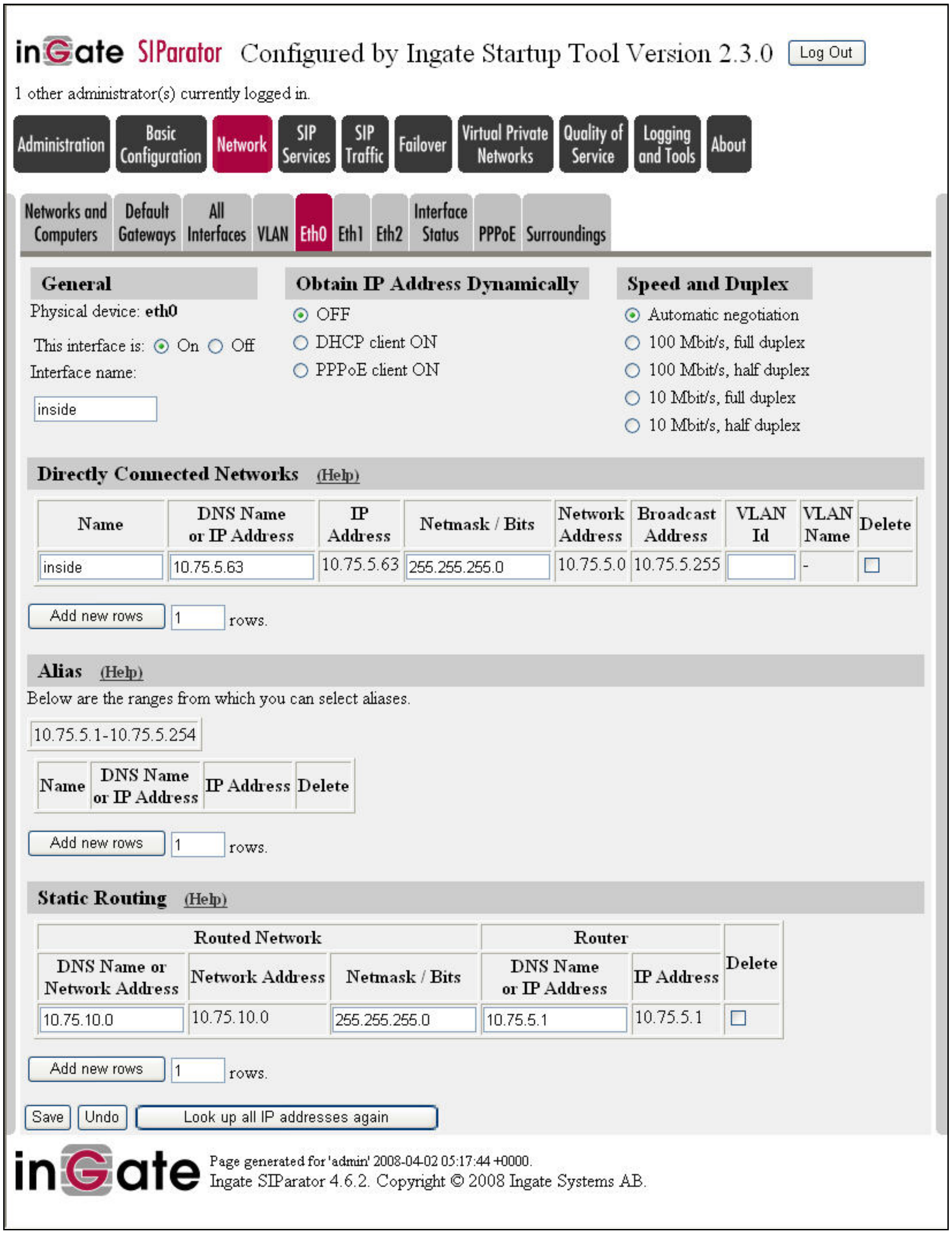
Add new rows 1 groups with 1 rows per group.

SIP Routing Order

No.	Routing Function
1	DNS Override
2	Local Registrar
3	Dial Plan

Class 3xx Message Processing

● Forward all
○ Follow redirects

Step	Description
10.	**Configure Static Routes** In order to support endpoints on networks within the enterprise other than the subnet to which the SIParator is directly connected, a static route must be configured on the internal interface. In the case of the compliance test, one endpoint was located on the 10.75.10.0/24 network. Thus, to view the static route configured for this network, navigate to **Network→Eth0**. Scroll down to the **Static Routing** section. In this case, the routed network with **Network Address** ***10.75.10.0*** and **Netmask** of ***255.255.255.0*** is reached using **Router IP address** ***10.75.5.1***. 

inGate SIParator Configured by Ingate Startup Tool Version 2.3.0 [Log Out]

1 other administrator(s) currently logged in.

General

Physical device: eth0

This interface is: ● On ○ Off

Interface name: inside

Obtain IP Address Dynamically

● OFF
○ DHCP client ON
○ PPPoE client ON

Speed and Duplex

● Automatic negotiation
○ 100 Mbit/s, full duplex
○ 100 Mbit/s, half duplex
○ 10 Mbit/s, full duplex
○ 10 Mbit/s, half duplex

Directly Connected Networks (Help)

Name	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete
inside	10.75.5.63	10.75.5.63	255.255.255.0	10.75.5.0	10.75.5.255		-	□

[Add new rows] 1 rows.

Alias (Help)

Below are the ranges from which you can select aliases.

10.75.5.1-10.75.5.254

Name	DNS Name or IP Address	IP Address	Delete

[Add new rows] 1 rows.

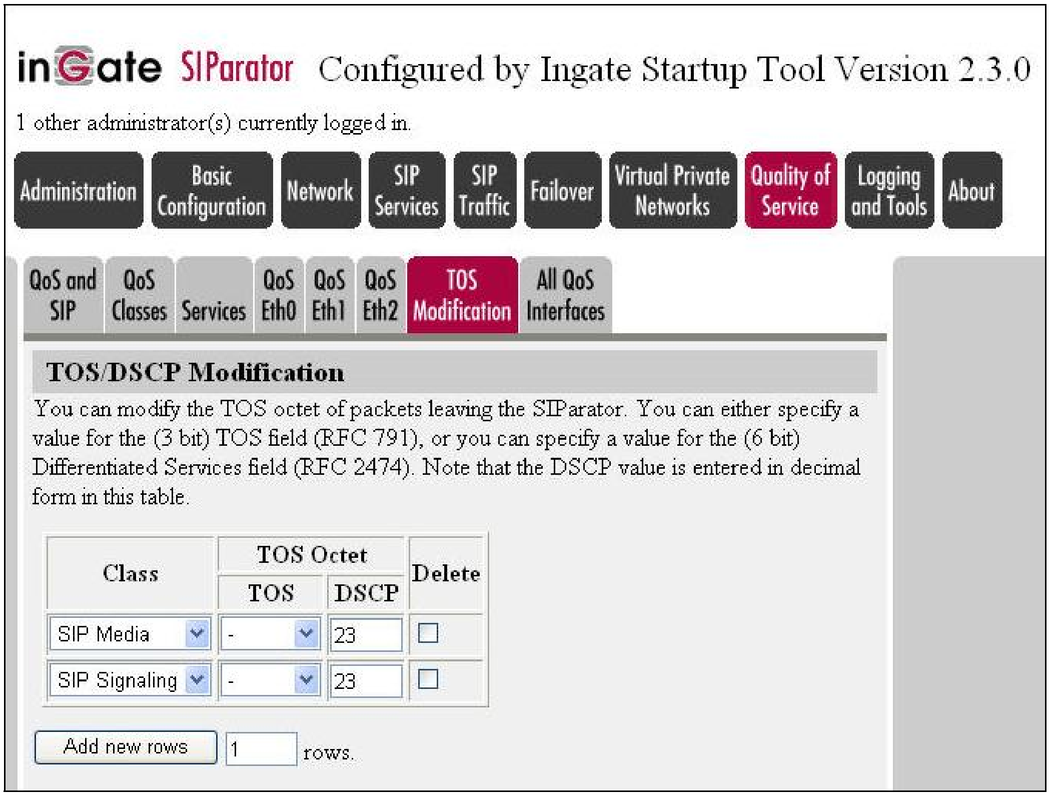
Static Routing (Help)

Routed Network			Router		
DNS Name or Network Address	Network Address	Netmask / Bits	DNS Name or IP Address	IP Address	Delete
10.75.10.0	10.75.10.0	255.255.255.0	10.75.5.1	10.75.5.1	□

[Add new rows] 1 rows.

[Save] [Undo] [Look up all IP addresses again]

inGate Page generated for 'admin' 2008-04-02 05:17:44 +0000.
Ingate SIParator 4.6.2. Copyright © 2008 Ingate Systems AB.

Step	Description
11.	**Quality of Service** In order to set the Type of Service (TOS) or DSCP bits, the optional QoS module must first be installed. To set the values for these bits, navigate to **Quality of Service→ TOS modification**. In the case of the compliance test, both the SIP media and SIP signaling packets were marked with a DSCP value of 23 (decimal). 

inGate SIParator Configured by Ingate Startup Tool Version 2.3.0

1 other administrator(s) currently logged in.

TOS/DSCP Modification

You can modify the TOS octet of packets leaving the SIParator. You can either specify a value for the (3 bit) TOS field (RFC 791), or you can specify a value for the (6 bit) Differentiated Services field (RFC 2474). Note that the DSCP value is entered in decimal form in this table.

Class	TOS Octet		Delete
	TOS	DSCP	
SIP Media	-	23	□
SIP Signaling	-	23	□

Add new rows 1 rows.

7. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of the Ingate SIParator with Avaya SIP Enablement Services and Avaya Communication Manager to support remote SIP endpoints. This section covers the general test approach and the test results.

7.1. General Test Approach

The general test approach was to make calls between the remote SIP endpoints and the main site using various codec settings and exercising common PBX features.

7.2. Test Results

The SIParator passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.

- Successful registrations of remote endpoints to the main site.
- Calls between the remote SIP endpoints and the main site.

- G.711MU and G.729AB codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Call Park, Call Pickup, Automatic Callback and Send All Calls. For more information on FNEs, please refer to [4].
- Proper system recovery after a SIParator restart and loss of IP connection.

The following observations were made during the compliance test.

- IP-IP Direct Audio (media shuffling) must be disabled for calls passing through the SIParator. See **Section 3.2**.
- For interoperability with the 4600 Series IP Telephones as remote SIP endpoints, the SIParator requires the software update ***ig-patch-4-6-2-media_stream_linger_2.fup*** on software version 4.6.2.
- The Conference On Answer and Drop Last Party FNEs are not supported.

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all endpoints are registered with the local Avaya SES. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed between the remote SIP endpoints and the main site.

9. Support

For technical support on the SIParator, contact Ingate via the support link at www.ingate.com.

10. Conclusion

The Ingate SIParator passed compliance testing. These Application Notes describe the procedures required to configure the Ingate SIParator to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support remote SIP endpoints shown in **Figure 1**.

11. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 6.0, January 2008.

[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4, January 2008.

[3] *SIP support in Avaya Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 8, January 2008.

[4] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, version 6.0, Doc # 210-100-500, Issue 9, June 2005

[5] *Installing and Administering SIP Enablement Services*, Doc# 03-600768, Issue 5, January 2008.

[6] *Avaya IA 770 INTUITY AUDIX Messaging Application Release 5.0, Administering Communication Manager Servers to Work with IA 770*, January 2008.

[7] *Ingate SIParator Getting Started Guide*.

[8] *Ingate SIParator Reference Guide.*

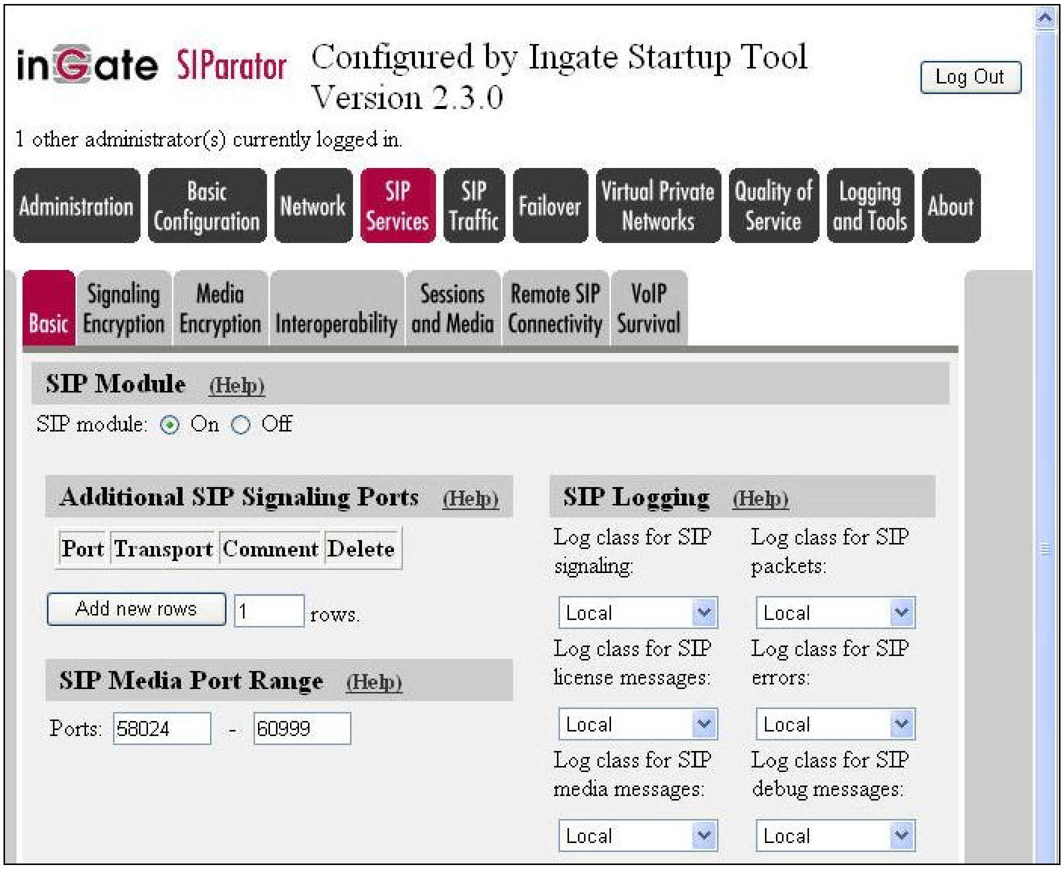
Product documentation for Avaya products may be found at http://support.avaya.com.

Product documentation for the SIParator can be obtained from Ingate. Contact Ingate using the contact link at http://www.ingate.com.

Appendix A: SIParator SIP Configuration

This section contains the key SIP configuration screens resulting from the procedure described in **Section 6** using the Ingate Startup Tool. These screens are included only as a reference with minimal explanation.

SIP Services → Basic Page



Configured by Ingate Startup Tool Version 2.3.0

1 other administrator(s) currently logged in.

SIP Module

SIP module: ● On ○ Off

Additional SIP Signaling Ports

Port	Transport	Comment	Delete

Add new rows 1 rows.

SIP Media Port Range

Ports: 58024 - 60999

SIP Logging

Log class for SIP signaling: Local

Log class for SIP packets: Local

Log class for SIP license messages: Local

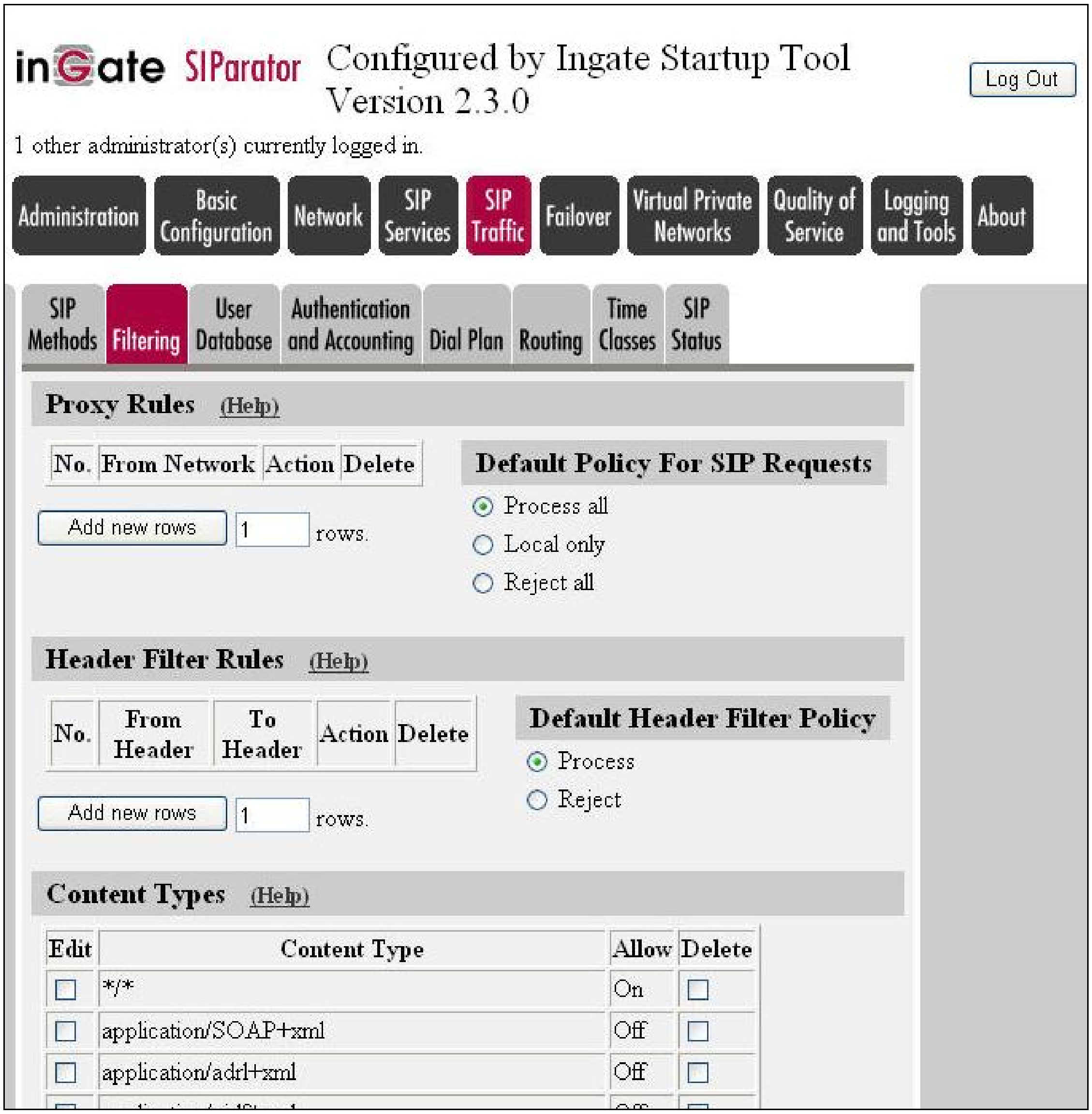
Log class for SIP errors: Local

Log class for SIP media messages: Local

Log class for SIP debug messages: Local

SIP Traffic → Filtering Page

In the **Proxy Rules** section, **Process all** is selected. In the **Content Types** section, the first entry in the table allows all content types (*/*) to be processed.



Configured by Ingate Startup Tool Version 2.3.0

1 other administrator(s) currently logged in.

Proxy Rules

No.	From Network	Action	Delete

Add new rows 1 rows.

Default Policy For SIP Requests

- ● Process all
- ○ Local only
- ○ Reject all

Header Filter Rules

No.	From Header	To Header	Action	Delete

Add new rows 1 rows.

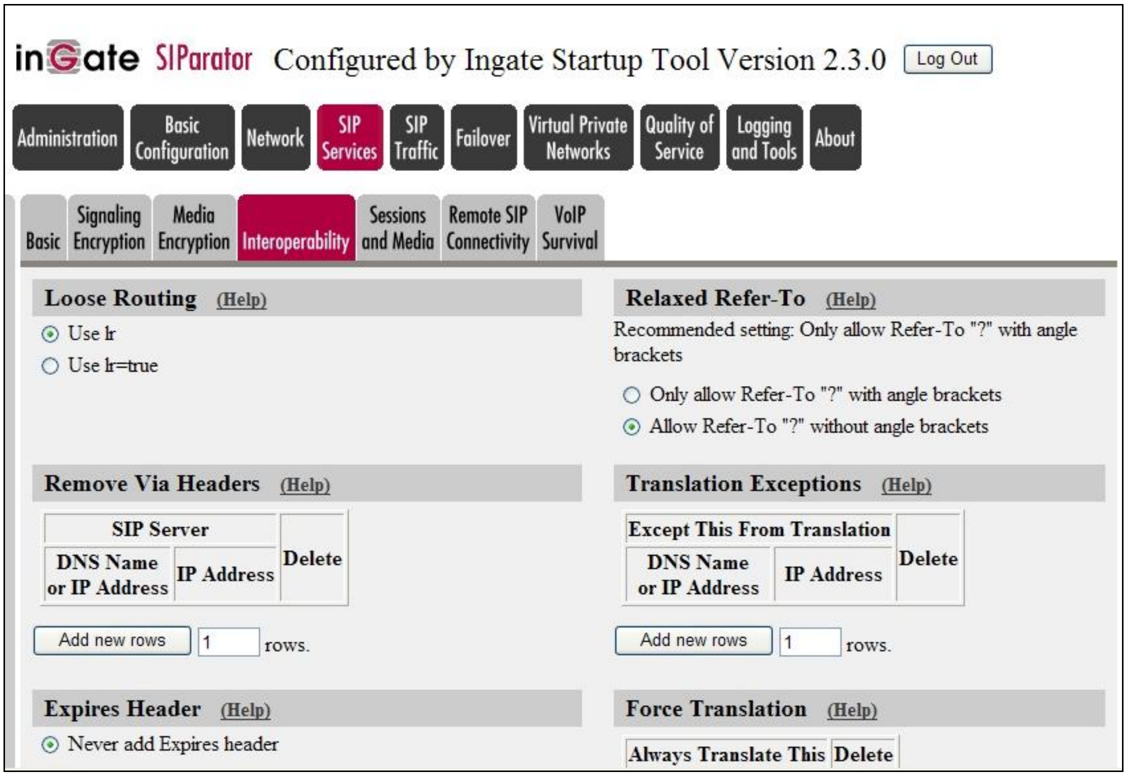
Default Header Filter Policy

- ● Process
- ○ Reject

Content Types

Edit	Content Type	Allow	Delete
□	*/*	On	□
□	application/SOAP+xml	Off	□
□	application/adrl+xml	Off	□

SIP Services → Interoperability Page
For Avaya SES interoperability, the SIParator was configured to allow REFER messages without requiring angle brackets around the question mark in the Refer-To header. See the option setting under **Relaxed Refer-To** in the example below.



Loose Routing (Help)

● Use lr
○ Use lr=true

Relaxed Refer-To (Help)

Recommended setting: Only allow Refer-To "?" with angle brackets

○ Only allow Refer-To "?" with angle brackets
● Allow Refer-To "?" without angle brackets

Remove Via Headers (Help)

SIP Server		Delete
DNS Name or IP Address	IP Address	

Add new rows [1] rows.

Translation Exceptions (Help)

Except This From Translation		Delete
DNS Name or IP Address	IP Address	

Add new rows [1] rows.

Expires Header (Help)

● Never add Expires header

Force Translation (Help)

Always Translate This	Delete

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.