

Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring Ingate SIParator with Avaya Aura™ SIP Enablement Services and Avaya Aura™ Communication Manager to support SIP remote endpoints.

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.

©2009 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Ingate SIParator with Avaya Aura™ SIP Enablement Services and Avaya Aura™ Communication Manager to support SIP remote endpoints.

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. Interoperability Compliance Testing

The compliance testing tested interoperability between Ingate SIParator (4.7.1) and SIP Enablement Services (5.2) / Communication Manager (5.2) by making calls between remote users and users at the main site. Following specific SIP telephony functions were tested in the test environment set up for the compliance test:

- Registration of remote user SIP endpoints on SIP Enablement Services through SIParator
- Calls from remote users with and without network address translation (NAT) to users at the main site via SIParator
- Calls from users at the main site to remote users with and without NAT via SIParator
- PSTN calls to/from remote users with and without NAT via SIParator
- Calls between remote users with and without NAT via SIParator
- Basic call scenarios using G.711 and G.729 codecs
- SIPPING-19 supplementary call features (including Hold, Transfer, Conference, Bridged Calls, etc.)
- Advanced call features provided via Feature Name Extensions (FNE) on Communication Manager (such as Call Forwarding, Call Park, Call Pickup, Automatic Redial, Send All Calls, etc.)
- Voice mail support for remote users
- Different types of remote user SIP endpoints (including Avaya 9600 series IP phones and Avaya one-X Communicator soft phone)

1.2. Support

Technical support for SIParator can be obtained by contacting Ingate at

- Phone: +46-13-21 08 52
- Email: support@ingate.com
- Web: http://www.ingate.com

2. 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

©2009 Avaya Inc. All Rights Reserved.

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 a SIP Enablement Services server and an Avaya S8300B Server running Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300B Server. Endpoints include both SIP and non-SIP endpoints. An ISDN-PRI trunk connects the media gateway to the PSTN.

Remote SIP endpoints include Avaya 9600 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 SIP Enablement Services on behalf of the remote endpoints using its own private IP address. Thus, the SIParator appears to the SIP Enablement Services 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 HTTP server to obtain their configuration files.

For the compliance test, the SIParator configured a pair of "untrusted" IP addresses (public-side and private-side) for remote users as well as a pair of "trusted" IP addresses (public-side and private-side) for direct SIP trunking interface to a second site simulating a service provider (SP) service node[1]. With this co-resident configuration, the remote users and connection to a 2nd site (simulating a SP service node) can function at the same time. The configuration for remote users is documented in this Application Notes document; the configuration for direct SIP trunking interface to a second site is documented in separate Application Notes.

[1] In the compliance test, the pair of inside/outside IP addresses configured on the SIParator for the remote user application were not configured on (or known to) the SIP Enablement Services or Communication Manager, therefore this pair of IP addresses can be viewed as "**untrusted**" from the perspective of Avaya telephony components. For the direct SIP trunking application, a separate pair of inside/outside IP addresses were configured on the SIParator that were configured on (or known to) the connected Avaya telephony components, therefore this pair of IP addresses can be viewed as "**trusted**" from Avaya's perspective. The terms "**trusted**" and "**untrusted**" used in this particular context are not to be confused with the same terms in general networking terminology. The words "**trusted**" and "**untrusted"**, when used in their particular semantics for this DevConnect compliance test, are quoted in their occurrences throughout this document.

©2009 Avaya Inc. All Rights Reserved.

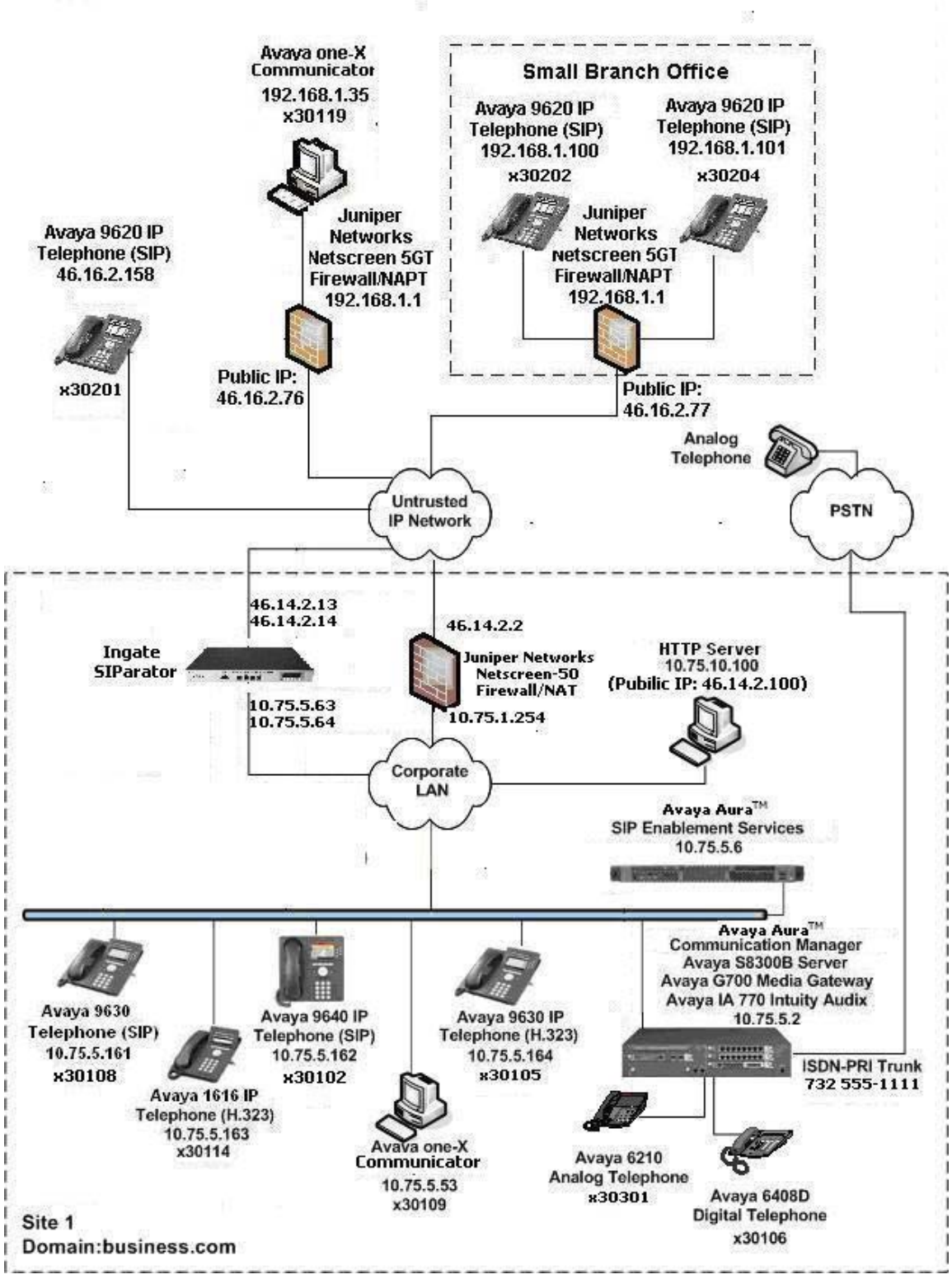


Figure 1: SIP Remote Access Test Configuration

©2009 Avaya Inc. All Rights Reserved.

3. 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 Aura™ Communication Manager 5.2 (R015x.02.0.947.3 with update 17294)
Avaya S8500 Server	Avaya Aura™ SIP Enablement Services 5.2 (SES-5.2.0.0-947.3b with update SES-2.0.947.3-SP1)
Avaya 9600 Series IP Telephones (SIP)	Avaya one-X™ Deskphone Edition SIP 2.2
Avaya 9600 Series IP Telephones (H.323)	Avaya one-X™ Deskphone Edition H.323 Release 3.0
Avaya 1600 Series IP Telephone (H.323)	Avaya one-X™ Deskphone Value Edition Release 1.100
Windows PC (Soft Phone)	Windows XP Professional SP2 Avaya one-X™ Communicator (SIP) R1.030-SP3-16918
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows Server (HTTP Server)	Windows Server 2003 SP 2
Juniper Networks Netscreen-50	5.4.0r9.0
Ingate SIParator with installed modules: • Standard SIP features • SIP Trunking • Remote SIP Connectivity (NAT Traversal) • Failover • VPN (IPsec and PPTP)	4.7.1

©2009 Avaya Inc. All Rights Reserved.

4. Configure Communication Manager

This section describes the 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 SIP Enablement Services have been performed as described in [3]. It also assumes that an off-PBX station (OPS) has been configured on 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 4.2**.

This section is divided into two parts. **Section 4.1** summarizes the user-defined parameters used in the SIP 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 also describes any deviations from the standard procedures, if any.

Section 4.2 describes 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 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.

©2009 Avaya Inc. All Rights Reserved.

4.1. Summary of Initial SIP Installation

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

Step	Description

1.	**IP network region**
	The Avaya S8300B Server, SIP Enablement Services 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 SIP Enablement Services. 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`

©2009 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Codecs** 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.

```
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.729A             n          2        20
 3:
 4:
 5:
 6:
 7:


    Media Encryption
 1: none
 2:
 3:
```


©2009 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Signaling Group** For the compliance test, signaling group 1 was used for the SIP trunk group between Communication Manager and SIP Enablement Services as configured in the next step. 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 S8300B 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 SIP Enablement Services. ▪ **Far-end Network Region**: ***1*** This defines the IP network region which contains SIP Enablement Services. ▪ **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
  IMS Enabled? n




   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
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? n                  Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```


©2009 Avaya Inc. All Rights Reserved.

Step	Description

4.	**Trunk Group**
	For the compliance test, trunk group 1 was used for the SIP trunk group between Communication Manager and SIP Enablement Services. Trunk group 1 was configured using the parameters highlighted below. All other fields were set as described in [3].
	▪ **Signaling Group**: ***1*** This field was set to the signaling group shown in the previous step.
	▪ **Number of Members: *24*** 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.
	▪ **Service Type:** Set this field to ***tie*** to indicate this trunk is used for direct interconnection.
	
	`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? y`
	`Dial Access? n Night Service:`
	`Queue Length: 0`
	`Service Type: tie` `Auth Code? n`
	`Signaling Group: 1`
	`Number of Members: 24`

©2009 Avaya Inc. All Rights Reserved.

Step	Description
5.	**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 Restricted Numbers? n Replace Unavailable Numbers? n Show ANSWERED BY on Display? y
6.	**Public Unknown Numbering** Public unknown numbering defines the calling party number to be sent to the far-end. 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: 14 **5 3** **5** Maximum Entries: 240

4.2. 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 Communication Manager for each remote endpoint supported by the SIParator. For interoperability, IP-IP Direct Audio (media shuffling) is turned on for calls passing through the SIParator.

©2009 Avaya Inc. All Rights Reserved.

Step	Description
1.	**IP Network Region For Remote Users** A separate IP network region was created for the remote endpoints. It was configured the same as the IP network region described in **Section 4.1**, **Step 1**, except a different descriptive name was used for the **Name** field. 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: 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
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 4.1**, **Step 1**). Optionally, a different codec set could have been chosen for inter-region calls. change ip-network-region 3 Page 3 of 19 Source Region: 3 Inter Network Region Connection Management I M G A e **dst codec** direct WAN-BW-limits Video Intervening Dyn A G a **rgn set** WAN Units Total Norm Prio Shr Regions CAC R L s **1 1** y NoLimit n 2 3 1 all

©2009 Avaya Inc. All Rights Reserved.

Step	Description

3.	**Signaling Group**
	A second signaling group was created for the remote endpoints. It has the same properties as the signaling group described in **Section 4.1**, **Step 3**, except the **Far-end Network Region** was set to ***3***.
	
	`change signaling-group 11`
	`SIGNALING GROUP`
	
	`Group Number: 11 Group Type: sip`
	`Transport Method: tls`
	`IMS Enabled? n`
	
	`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? y`**
	`Session Establishment Timer(min): 3 IP Audio Hairpinning? n`
	`Enable Layer 3 Test? n Direct IP-IP Early Media? n`
	`H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6`

4.	**Trunk Group**
	A second trunk group was created for the remote endpoints. It has the same properties as the trunk group described in **Section 4.1, Step 4**, except the **Signaling Group** field was set to ***11***. In **Step 9**, the remote SIP endpoints will be mapped to use this trunk group set up specifically for remote users.
	
	`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`

©2009 Avaya Inc. All Rights Reserved.

Step	Description
5.	**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. change trunk-group 11 Page 3 of 21 TRUNK FEATURES ACA Assignment? n Measured: none Maintenance Tests? y **Numbering Format: public** UUI Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n Show ANSWERED BY on Display? y

©2009 Avaya Inc. All Rights Reserved.

Step	Description

6.	**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 30201. The **Type** field was set to match the type of telephone used - ***9620***. 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.
	
	Note that In the case of the Avaya one-X Communicator soft phone, the **Type** field should be set to ***4620*** and the **IP Soft phone** field must be set to ***y***.
	
	`add station 30201` `Page 1 of 6`
	`STATION`
	
	`Extension: 30201` `Lock Messages? n` `BCC: 0`
	`Type: 9620` `Security Code:` `TN: 1`
	`Port: IP` `Coverage Path 1: 1` `COR: 1`
	`Name: Remote SIP1` `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: 30201`
	`Speakerphone: 2-way` `Mute Button Enabled? y`
	`Display Language: english` `Button Modules: 0`
	`Survivable GK Node Name:`
	`Survivable COR: internal` `Media Complex Ext:`
	`Survivable Trunk Dest? y` `IP SoftPhone? n`

©2009 Avaya Inc. All Rights Reserved.

Step	Description
7.	**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 30201 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 EC500 State: disabled 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: 30202 Always Use? n IP Audio Hairpinning? n
8.	**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 30201 Page 4 of 5 STATION SITE DATA Room: [A 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:

©2009 Avaya Inc. All Rights Reserved.

Step	Description

9.	**Off-PBX station mapping**
	All SIP endpoints, including the remote SIP endpoints, are configured as OPS stations on Communication Manager. Thus, they require a mapping between the station extension and the **Phone Number** and **Trunk** used to reach SIP Enablement Services. In the example below, the station extension 30201 is listed as an OPS station that is mapped to phone number 30201 via trunk 11. (The phone number in this case refers to the user name defined on the SIP Enablement Services – see **Section 5.2**, **Step 1**). Configuration set 1 which contains the default phone settings was specified for **Config Set**. Default values were used for all other fields.
	
	`change off-pbx-telephone station-mapping 30201 Page 1 of 3`
	`STATIONS WITH OFF-PBX TELEPHONE INTEGRATION`
	
	Station Extension **Application** Dial Prefix CC **Phone Number** **Trunk Selection** **Config Set** Dual Mode
	30201 **OPS** **-** **30201** **11** **1**

10.	**Off-PBX station mapping - Continued**
	On **Page 2**, the **Call Limit** was set to ***3*** to match the number of call appearances in **Step 8**. **Mapping Mode** and **Bridged Calls** were set to ***both*** for incoming and outgoing calls. Default values were used for all other fields.
	
	`change off-pbx-telephone station-mapping 30201 Page 2 of 3`
	`STATIONS WITH OFF-PBX TELEPHONE INTEGRATION`
	
	Station Extension / Appl Name / **Call Limit** / **Mapping Mode** / Calls Allowed / **Bridged Calls** / Location
	30201 / OPS / **3** / **both** / all / **both** /

©2009 Avaya Inc. All Rights Reserved.

5. Configure SIP Enablement Services

This section covers the configuration of SIP Enablement Services at the main site. SIP Enablement Services is configured via an Internet browser using the administration web interface. It is assumed that the SIP Enablement Services 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 SIP Enablement Services. For additional information on these installation tasks, refer to [5].

Each SIP endpoint used in the compliance test that registers with SIP Enablement Services requires that a user and Communication Manager extension be created on SIP Enablement Services. The creation of users and Communication Manager extensions for the internal enterprise SIP endpoints are not covered here. These procedures are covered in [5]. The creation of users and Communication Manager extensions for the remote SIP endpoints are covered in **Section 5.2**.

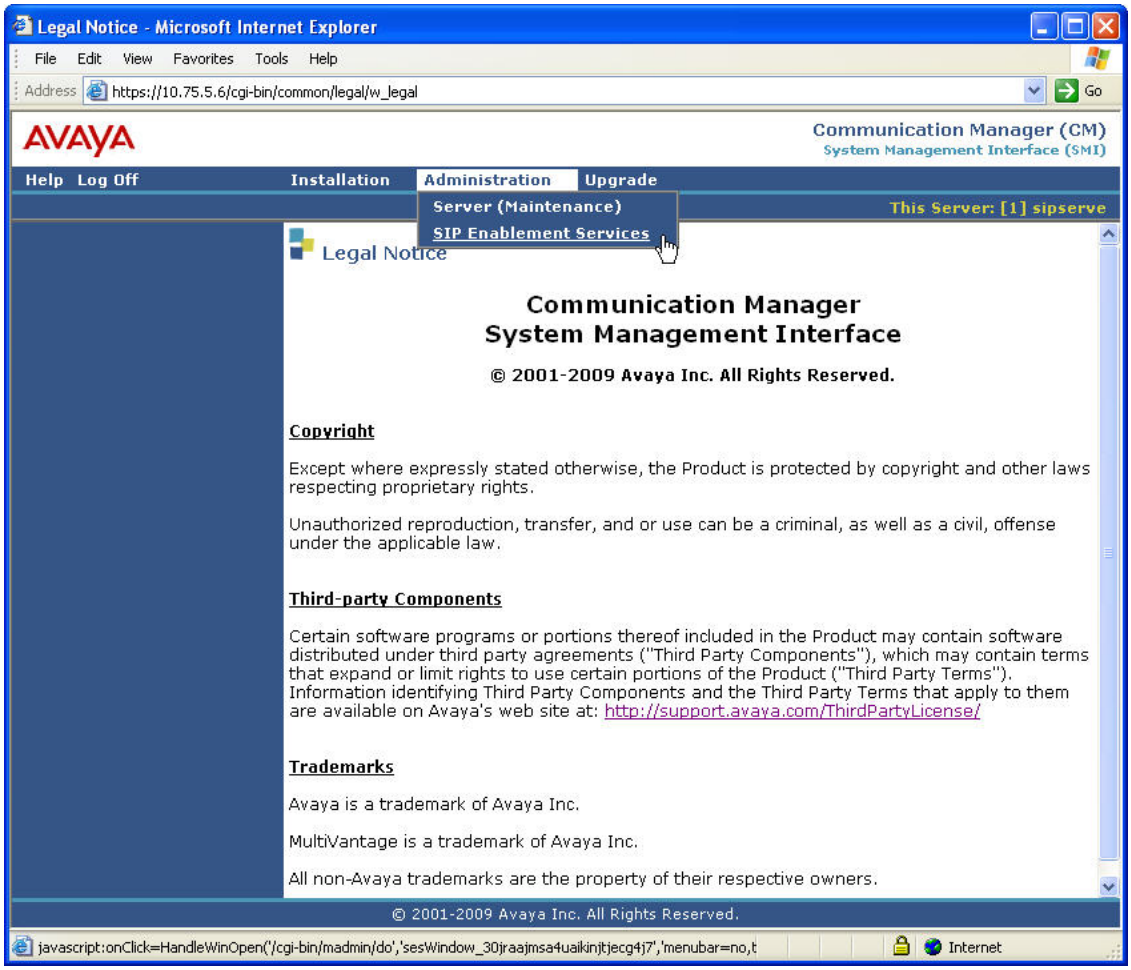
This section is divided into two parts. **Section 5.1** summarizes the user-defined parameters used in the SIP Enablement Services installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It also describes any deviations from the standard procedures, if any.

Section 5.2 describes procedures beyond the initial SIP Enablement Services installation procedures that are necessary for interoperating with the SIParator. This includes configuration of the remote SIP endpoints.

©2009 Avaya Inc. All Rights Reserved.

5.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters specified during the SIP Enablement Services installation procedures.

Step	Description
1.	**Login** Access the SIP Enablement Services 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 SIP Enablement Services server. Log in with the appropriate credentials and then select **SIP Enablement Services** from the **Administration** drop-down menu on the main page as shown below. 

©2009 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Top Page** The SIP Enablement Services **Top** page will be displayed as shown below. 

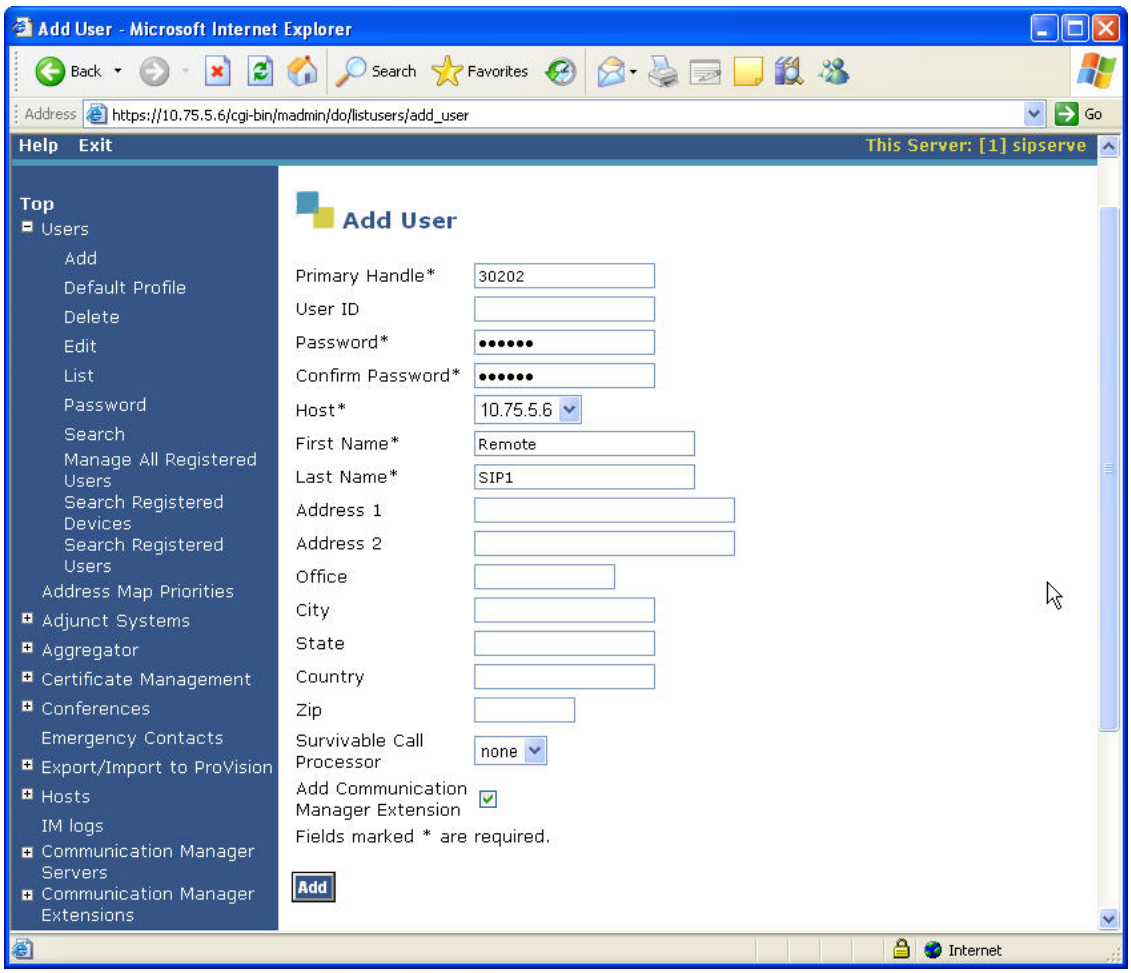
©2009 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Initial Configuration Parameters** As part of the SIP Enablement Services 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 SIP Enablement Services administration top page shown in the previous step. • SIP Domain: ***business.com*** (To view, navigate to **Server Configuration→System Parameters**) • Host IP Address (SIP Enablement Services IP address): ***10.75.5.6*** • Host Type: ***SES combined home-edge*** (To view, navigate to **Hosts→List**; click **Edit**) • Media Server (Communication Manager) Interface Name: ***CMeast*** • SIP Trunk Link Type: ***TLS*** • SIP Trunk IP Address (Avaya S8300B Server IP address): ***10.75.5.2*** (To view, navigate to **Communication Manager Servers→List**; click **Edit**)

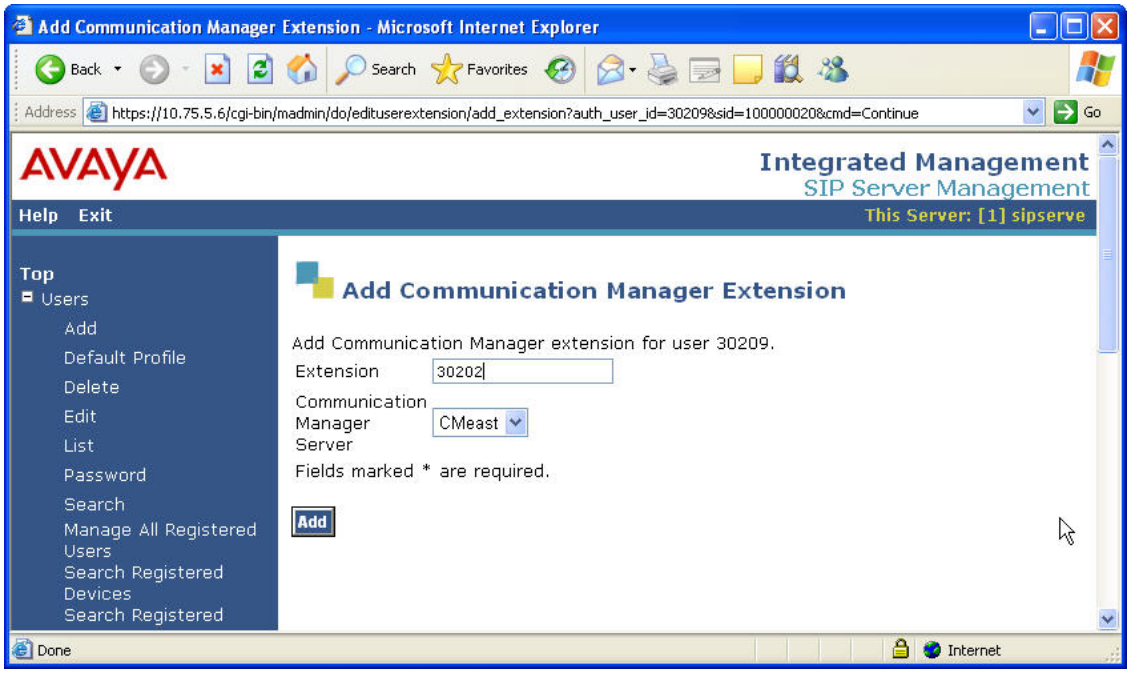
5.2. SIParator Specific Configuration

This section describes additional SIP Enablement Services configuration necessary for interoperating with the SIParator. This involves adding a user and Communication Manager extension for each of the remote SIP endpoints.

©2009 Avaya Inc. All Rights Reserved.

Step	Description
1.	**Users** Each remote SIP endpoint must have a user created for it on the SIP Enablement Services in the same manner as an internal enterprise endpoint. The example below shows the creation of user 30202. The **Primary Handle** is set to the station extension created in **Section 4.2**, **Step 6**. Enter a password to be used for authenticating this user. Enter any descriptive name for the **First Name** and **Last Name** fields. Check the option box **Add Communication Manager Extension**. 

©2009 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Communication Manager Extension** After a confirmation screen (not shown), the following screen appears. In the extension field, enter the Communication Manager extension created in **Section 4.2**, **Step 6**. 
3.	Repeat **Steps 1 – 2** for all remote SIP endpoints.

©2009 Avaya Inc. All Rights Reserved.

6. Configure Avaya SIP Telephones

The SIP telephones at the enterprise site will use the local SIP Enablement Services as the Call Server. The remote SIP endpoints will use the "untrusted" public IP address of the SIParator as the Call Server (refer to the footnote in **Section 2**). 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	30102	30201	30204
IP Address	10.75.5.162	46.16.2.158	192.168.1.101
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	46.14.2.14	46.14.2.14
Transport Type	TCP or TLS	TCP or UDP	TCP or UDP
Avaya Environment	Yes	No	No

Note that for remote endpoints, the SIP configuration on the phone needs to be set as non-Avaya Environment. The non-Avaya Environment setting will prevent Avaya-specific http message exchanges between the phone and SIP Enablement Services during phone registration. Since the Ingate SIParator is a SIP SBC, it does not handle non-SIP protocols like http, therefore failing the remote phone registration if the phone's SIP configuration specifies Avaya Environment.

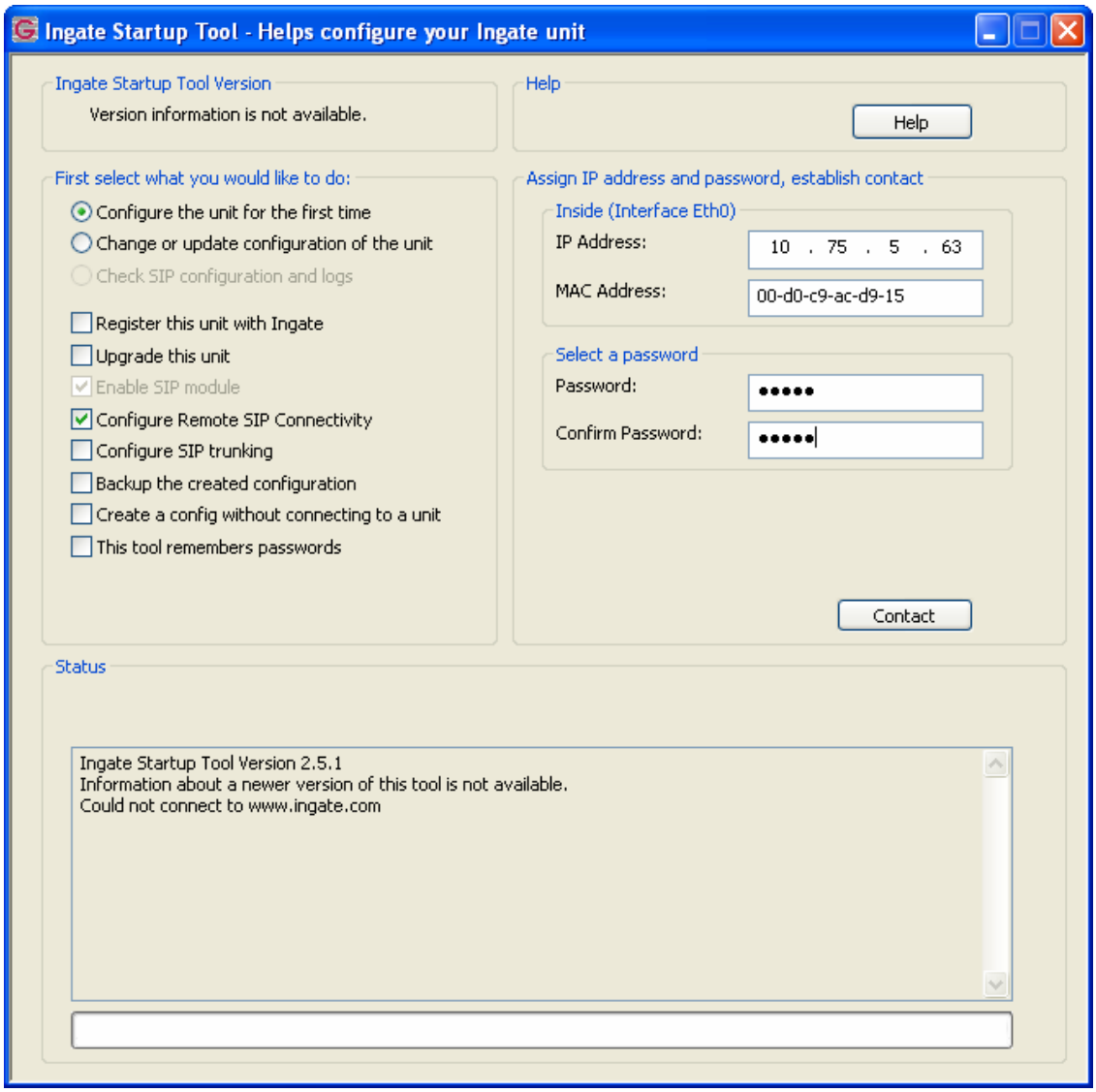
7. Configure Ingate SIParator

The Ingate 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.

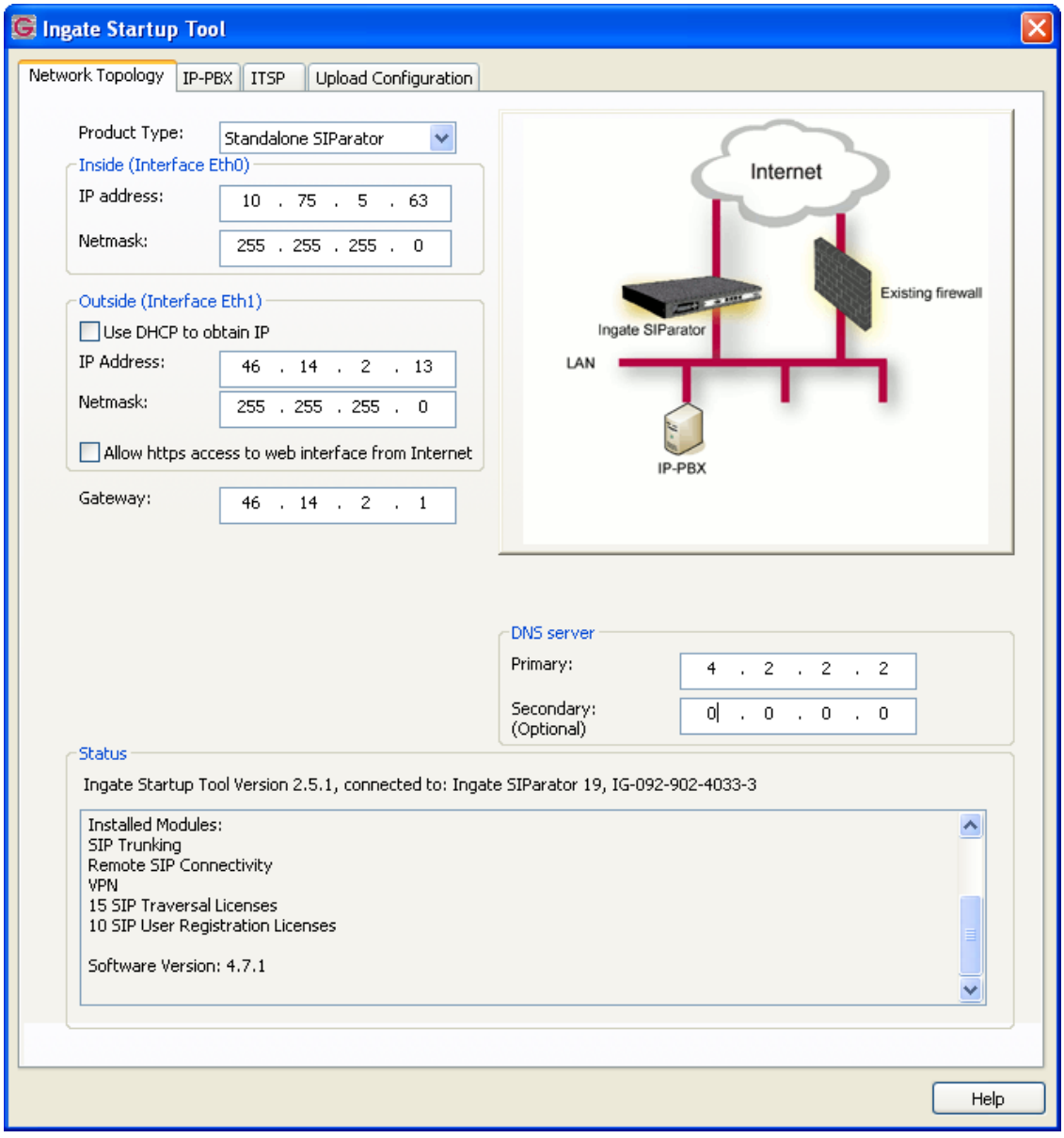
©2009 Avaya Inc. All Rights Reserved.

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**.
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. 

©2009 Avaya Inc. All Rights Reserved.

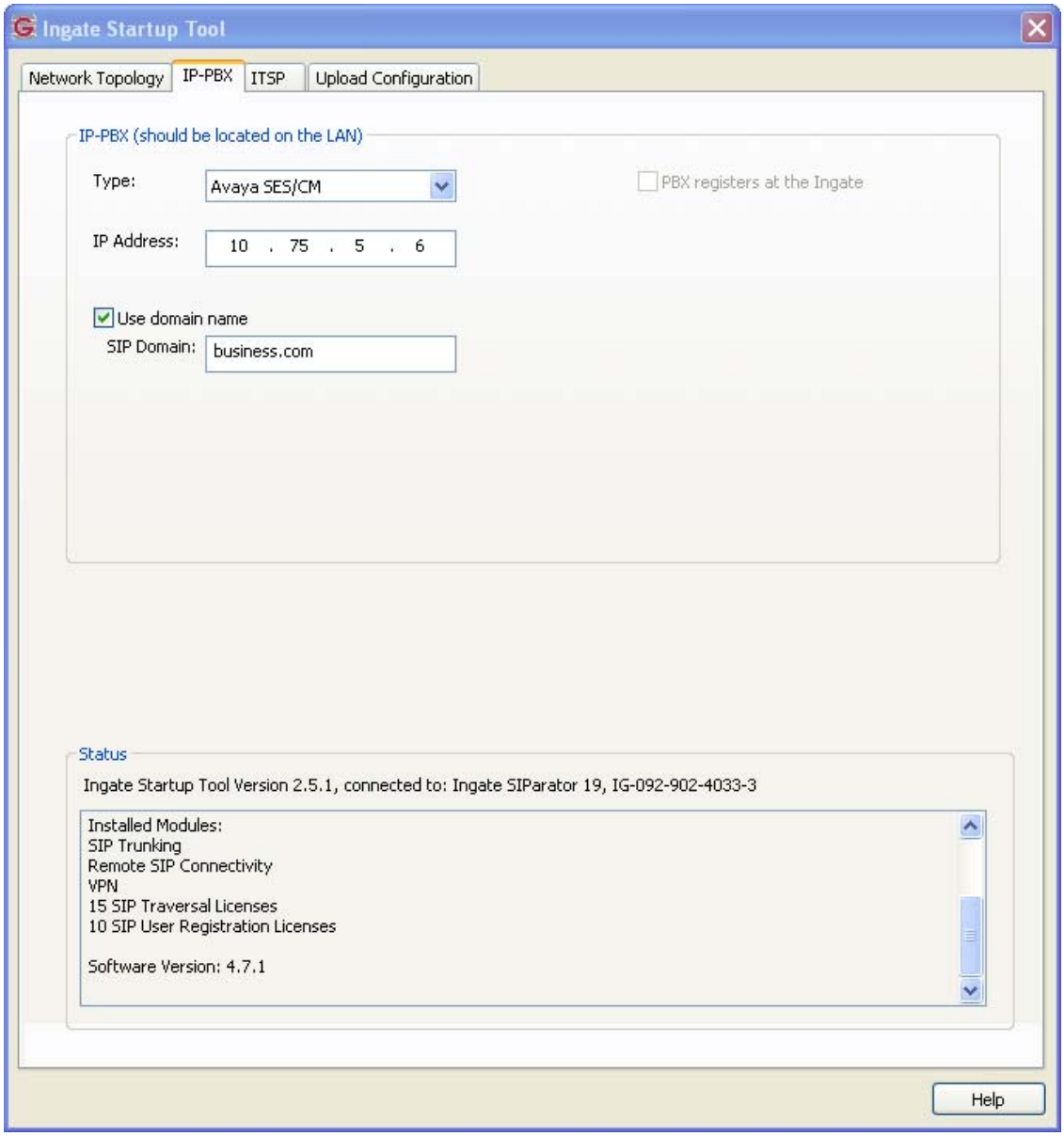
Step	Description
3.	**Select Configuration Options and Assign Private IP** Select options for **Configure the unit for the first time** and **Configure Remote SIP Connectivity**. Enter the inside IP address, MAC address and a password. Click the **Contact** button to establish a connection to the SIParator. For future updates, click the option - **Change or update configuration of the unit**.  Note that the SIParator configuration uses the "untrusted" outside/inside IP addresses 46.14.2.14/10.75.5.64 for the remote user application. This will be achieved through aliasing (configured later in **Steps 8** & **9**) on the "trusted" pair of 46.14.2.13/10.75.5.63 (refer to the footnote in **Section 2**).

©2009 Avaya Inc. All Rights Reserved.

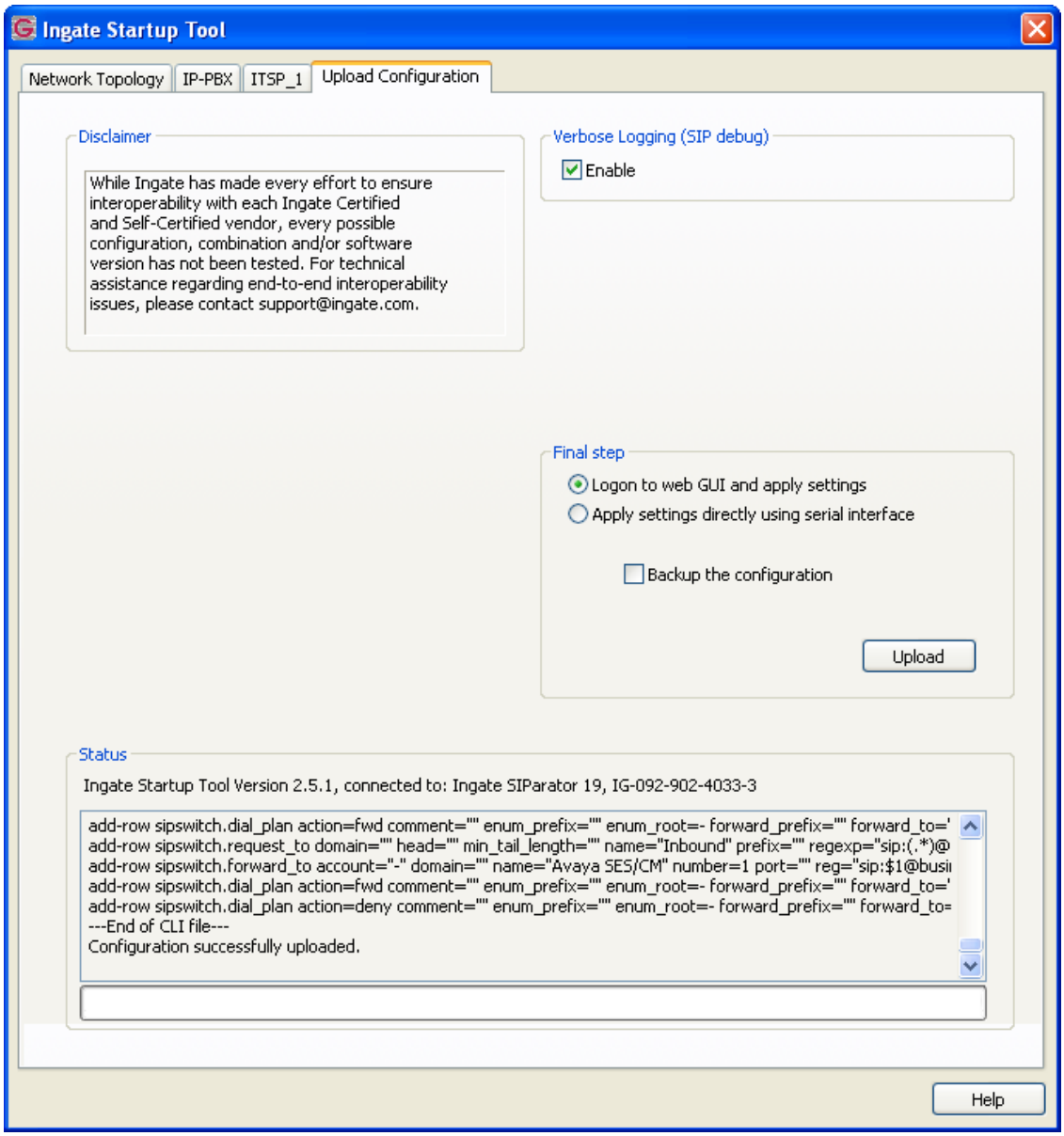
Step	Description
4.	**Network Topology** After connecting to the SIParator, the following page appears. Select the **Network Topology** tab. Select ***Standalone SIParator*** from the **Product Type** drop-down menu. Enter an IP address and subnet mask for both the inside and outside interfaces as shown in **Figure 1** (the "trunsted" pair)[2]. 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. 

[2] As noted in **Step 3**, the untrusted pair of outside/inside IP addresses used for the remote users compliance test will be achieved through aliasing on the trusted pair configured in later steps.

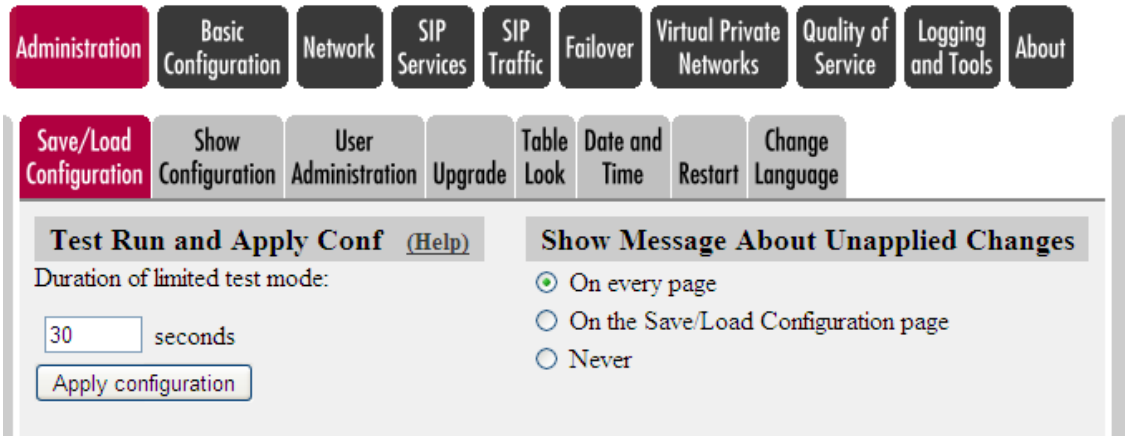
©2009 Avaya Inc. All Rights Reserved.

Step	Description
5.	**IP-PBX Settings** Select the **IP-PBX** tab. Select ***Avaya SES/CM*** 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 SIP Enablement Services. Enter the SIP Enablement Services IP address in the **IP Address** field. Also check the option to **use domain name**, then specify the domain name as set on SIP Enablement Services (see **Section 5.1 Step 3**) 

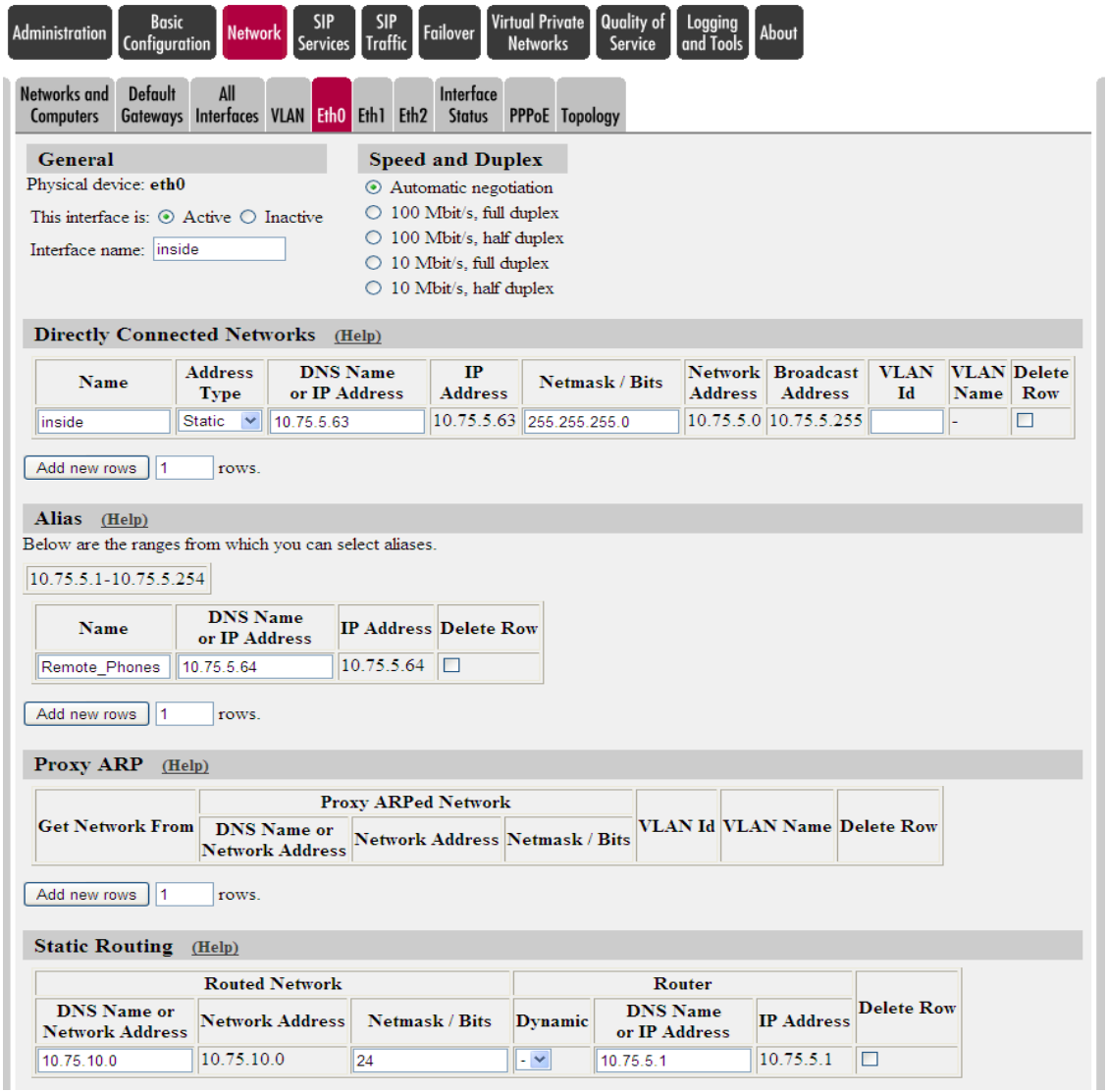
©2009 Avaya Inc. All Rights Reserved.

Step	Description
6.	**Upload Configuration** Select the **Upload Configuration** tab to upload the configuration to the SIParator. Click the **Upload** button to begin the upload. 

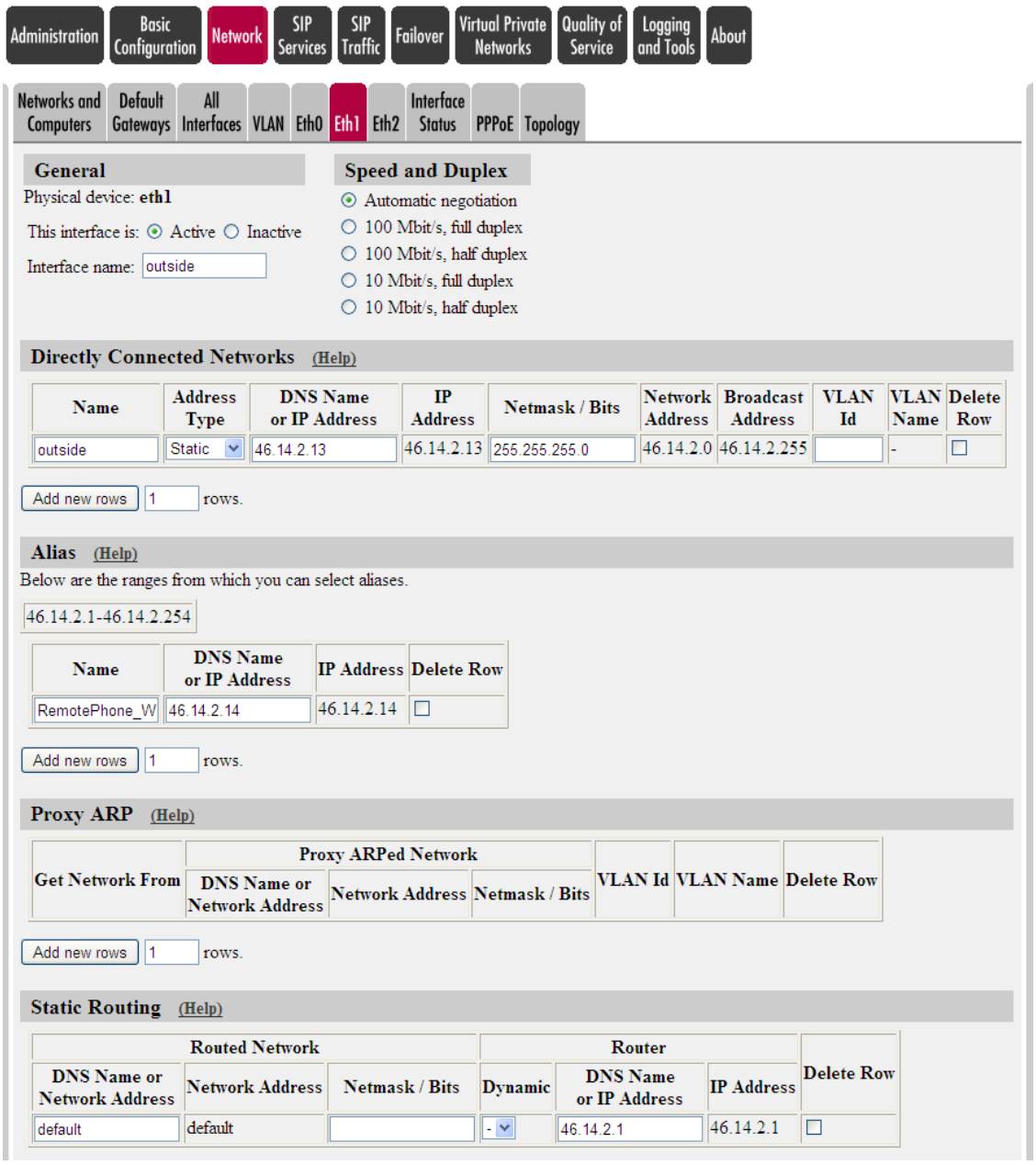
©2009 Avaya Inc. All Rights Reserved.

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. 

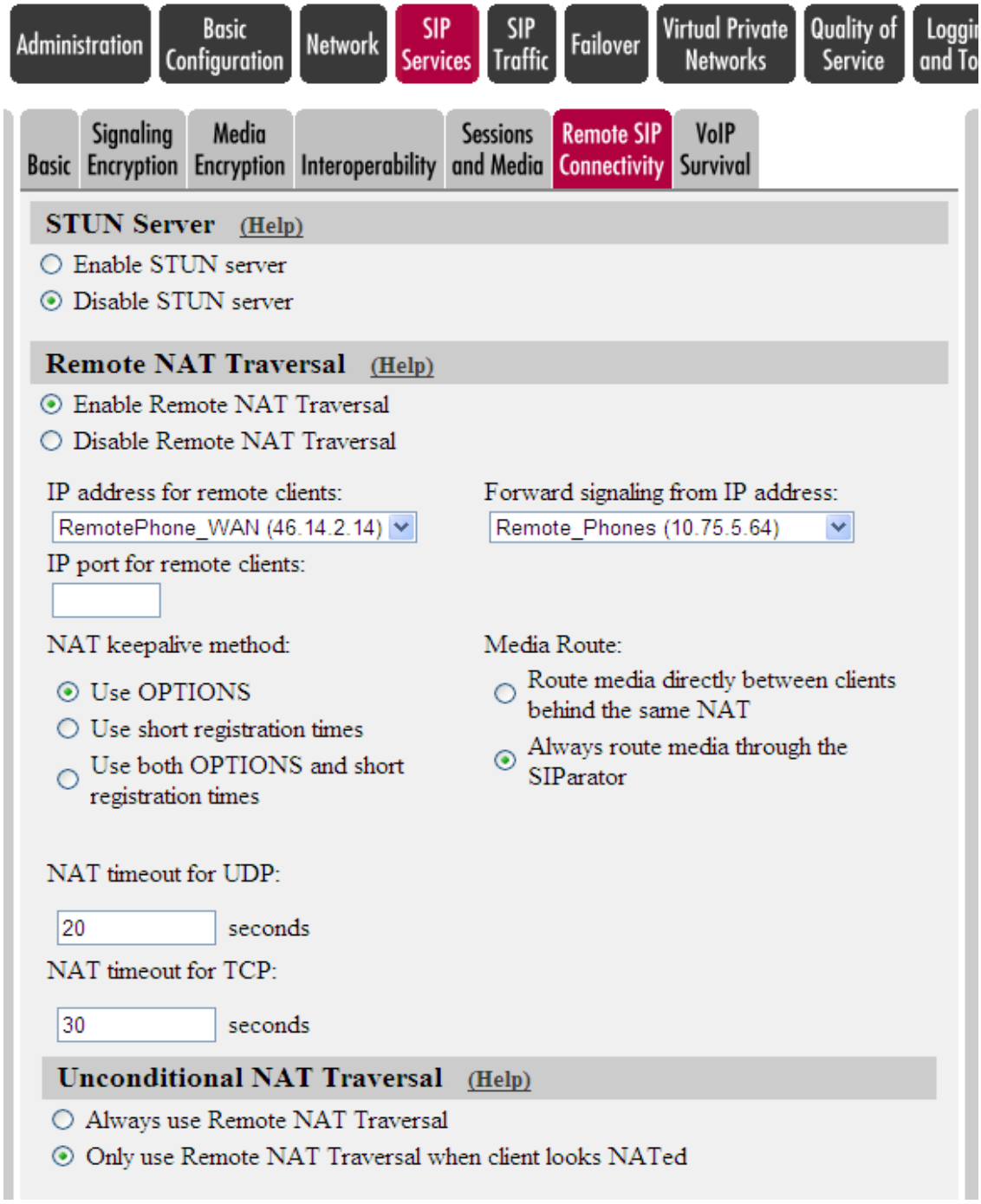
©2009 Avaya Inc. All Rights Reserved.

Step	Description
8.	**Configure Eth0 Inside Interface** In the compliance test, the Ingate SIParator was set up to support both remote users as well as connection to a second site that simulates a service provider service node. A pair of "untrusted" IP addresses (public-side and private-side) were configured for remote users; a pair of "trusted" IP addresses (public-side and private-side) were configured for direct SIP trunking interface to a second site (see footnote in **Section 2**). To achieve this configuration, the "untrusted pair" of IP addresses was aliased from the "trusted" pair. The Eth0 interface was used for the inside network interface (configured in this step); the Eth1 interface was used for the outside network interface (configured in the next step). Navigate to **Network→Eth0** to view the Eth0 configuration. In the **Alias** section, a descriptive name (***Remote_Phones***) was entered for **Name** and the aliased IP ***10.75.5.64*** was specified as the inside "untrusted" IP address. In order to support endpoints on other 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. Scroll down to the **Static Routing** section. The routed network with **Network Address** of ***10.75.10.0*** and **Netmask** of ***255.255.255.0*** is reached using **Router IP address** ***10.75.5.1***. 

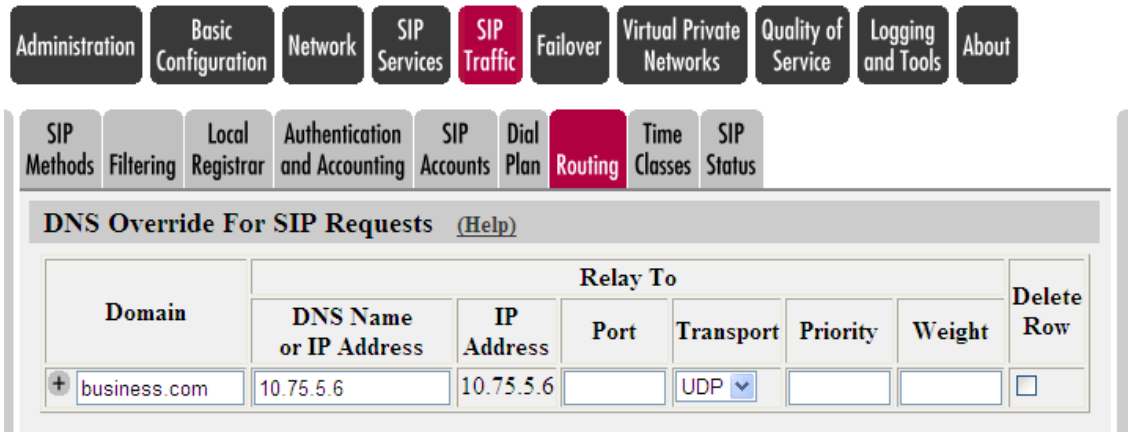
©2009 Avaya Inc. All Rights Reserved.

Step	Description
9.	**Configure Eth1 Outside Interface** Similar to the Eth0 interface configuration for the inside, an outside "untrusted" IP address was configured for remote user application through aliasing on the Eth1 network interface. Navigate to **Network→Eth1** to view the Eth1 configuration. In the **Alias** section, a descriptive name (***RemotePhones_WAN***) was entered for **Name** and the aliased IP ***46.14.2.14*** was specified as the outside "untrusted" IP address. 

©2009 Avaya Inc. All Rights Reserved.

Step	Description
10.	**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 **Enable Remote NAT Traversal** radio button. For **IP address for remote clients**, select the "untrusted" outside address of 46.14.2.14 (as configured in **Step 9**). For **Forward signaling from IP address**, select the "untrusted" inside address of 10.75.5.64 (as configured in **Step 8**). 

©2009 Avaya Inc. All Rights Reserved.

Step	Description
11.	**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 SIP Enablement Services. 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. 

8. General Test Approach and Test Results

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

8.1. 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.

8.2. 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.729A 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.

©2009 Avaya Inc. All Rights Reserved.

- Extended telephony features using Communication Manager Feature Name Extensions (FNE) such as Call Park, Call Pickup, Automatic Callback and Send All Calls.
- Proper system recovery after a SIParator restart and/or loss of IP connection.

The following observation was made during the compliance test.

- As noted in Section 6, the SIP configuration on the remote phones needs to be set as non-Avaya Environment. The SIParator, as a SIP SBC, does not support http messages passed between SIP Enablement Services and endpoints configured as using Avaya Environment during phone registration.

9. Verification Steps

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the SIP Enablement Services web administration interface, verify that all endpoints are registered with the local SIP Enablement Services. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed between a remote user without NAT and endpoints at the main site.
- Verify that calls can be placed between a remote user with NAT and endpoints at the main site.
- Verify that calls can be placed between remote users with and without NAT.
- From the Communication Manager SAT, use the **list trace tac** command to verify that the calls between remote users and endpoints at the main site are routed through the configured SIP trunks.

10. Conclusion

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

©2009 Avaya Inc. All Rights Reserved.

11. Additional References

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Doc # 555-245-205, May 2009.

[2] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, May 2009.

[3] *SIP support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx Servers*, Doc # 555-245-206, May 2009.

[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] *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server*, Doc # 03-602508, May 2009.

[6] *Avaya IA770 INTUITY AUDIX Messaging Application Release 5.1 Administering Communication Manager Servers To Work with IA770*, June 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.

©2009 Avaya Inc. All Rights Reserved.

©2009 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.

©2009 Avaya Inc. All Rights Reserved.