



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunks among Ingate SIParator, Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager - Issue 1.0

Abstract

These Application Notes describe a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Ingate SIParator and Avaya Aura™ Communication Manager using SIP trunks.

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 IP network. The compliance testing focused on telephony scenarios between an enterprise site, where the Ingate SIParator, Session Manager and Communication Manager were located, and a second site simulating a service provider service node.

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 a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Ingate SIParator and Avaya Aura™ Communication Manager using SIP trunks.

The compliance testing focused on telephony scenarios between an enterprise site, where the Ingate SIParator, Session Manager and Communication Manager were located, and a second site simulating a service provider service node.

1.1. Interoperability Compliance Testing

The compliance testing focused on interoperability between Ingate SIParator and Session Manager / Communication Manager by making calls between the enterprise site and a second site simulating a service provide service node that were connected through the SIParator using direct SIP trunks. The following functions and features were tested in the compliance test:

- Calls from both SIP and non-SIP endpoints between sites
- G.711u 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 Multiple Call Appearances, Hold, Transfer, and Conference
- Extended telephony features using Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Conference On Answer, Call Park, Call Pickup, Automatic Redial and Automatic Call Back and Send All Calls.
- Proper system recovery after SIParator restart and/or re-establishment of broken IP connectivity.

1.2. Support

Technical support for Ingate SIParator can be obtained by contacting Ingate at

- EMEA Phone: +46-13-21 08 52
- NA Phone: +1-866-809-0002
- Email: support@ingate.com
- Web: <http://www.ingate.com>

2. Configuration

Figure 1 illustrates the test configuration. The test configuration shows two sites connected via a SIP trunk across an untrusted IP network: the main enterprise site and a second site that simulates a service provider service node. 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 main enterprise site. Also connected to the edge of the main site is a SIParator Session Border Controller (SBC). The public side of the SIParator is connected to the untrusted network and the private side is connected to the trusted corporate LAN.

All SIP traffic between sites 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 TCP 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.

Also connected to the corporate LAN at the main site are:

- A Session Manager and its companion Avaya Aura™ System Manager. The Session Manager serves as a SIP routing hub and System Manager provides management functions for Session Manager.
- 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 to provide Voice Mail functionality.
- An Avaya S8500 Server running Avaya Aura™ SIP Enablement Services that provides SIP registrar and proxy server functions for SIP endpoints in the enterprise IP telephony network.
- An HTTP server for SIP phones at the enterprise site to obtain their configuration information.

The Session Manager connects the SIParator and Communication Manager using SIP trunks. Endpoints include both SIP and non-SIP endpoints. An ISDN-PRI trunk connects the media gateway to the PSTN.

Located at the 2nd site simulating a service provider service node is a SIP Enablement Services server and a Communication Manager with both SIP and non-SIP endpoints.

The SIP endpoints located at both sites are registered to the local SIP Enablement Services. Each site has a separate SIP domain: **business.com** for the main site and **bigtime.com** for the 2nd site. SIP and H.323 telephones at both sites use the local HTTP server to obtain their configuration files.

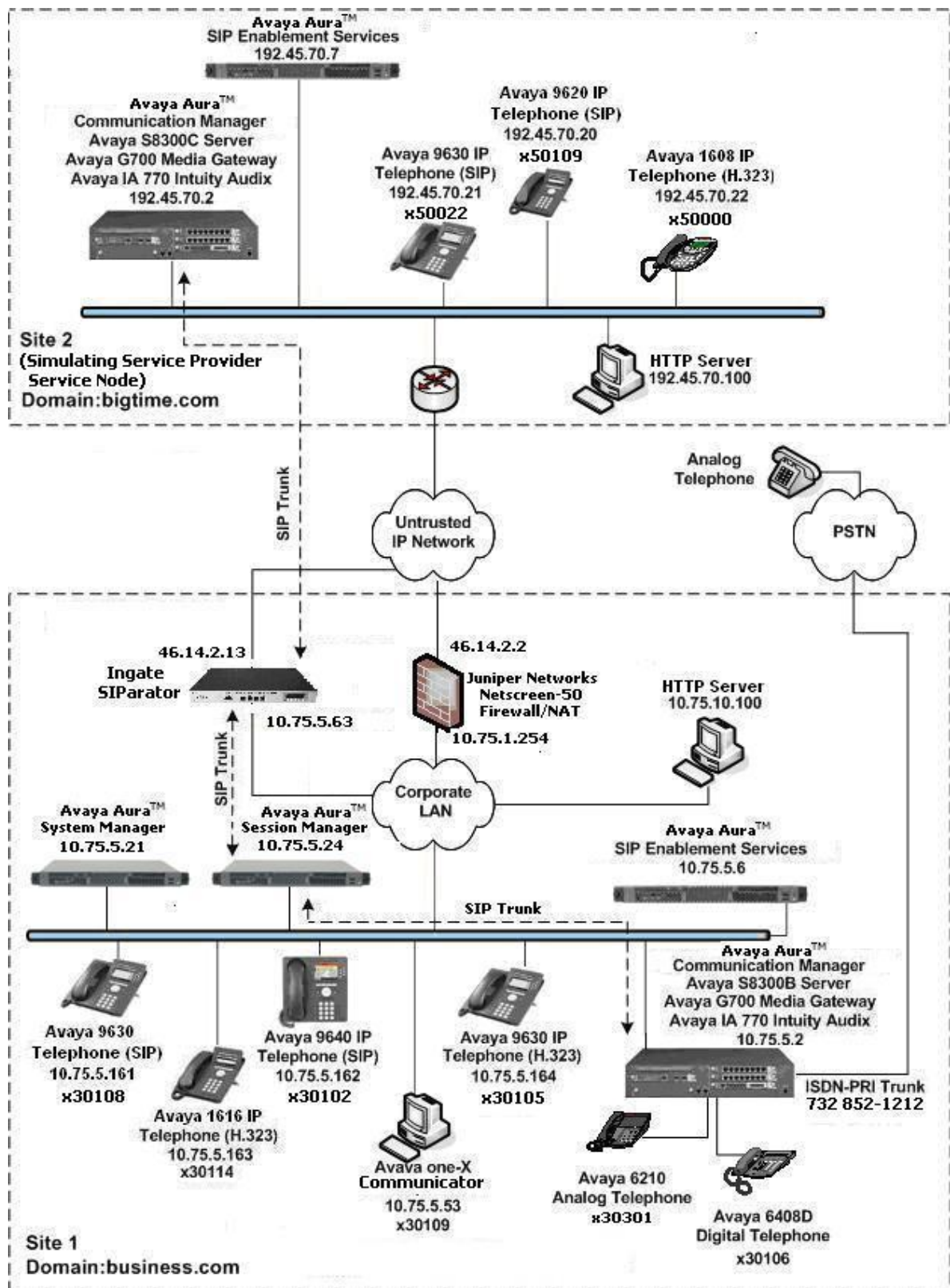


Figure 1: SIParator SIP Trunking Test Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300B/C 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 1616 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 SP2
Juniper Networks Netscreen-50	5.4.0r9.0
Ingate SIParator with installed modules: <ul style="list-style-type: none">• Standard SIP features• SIP Trunking• Remote SIP Connectivity (NAT Traversal)• Failover• VPN (IPsec and PPTP)	4.7.1

4. Configure Communication Manager

This section describes the Communication Manager configuration at the main enterprise 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] and [5]. It also assumes that an off-PBX station (OPS) has been configured on Communication Manager for each SIP endpoint in the configuration as described in [3] and [4].

This section is divided into two parts. **Section 4.1** summarizes 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 also describes any deviations from the standard procedures, if any.

Section 4.2 will describe procedures beyond the initial SIP installation procedures that are necessary for connecting Communication Manager to Avaya Aura™ Session Manager.

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.

Note that in the case of the compliance test, a second site comprised of an Communication Manager and SIP Enablement Services was set up to simulate a service provider service node, therefore the configuration described in this section must be repeated for the Communication Manager at the 2nd site using values appropriate from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions. The specific differences will be called out in the configuration details in this section. A complete set of the key configuration screens on Communication Manager at site 2 is included as an appendix.

4.1. Summary of Initial SIP Installation

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

Step	Description
1.	<p>IP network region</p> <p>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.</p> <ul style="list-style-type: none">▪ Authoritative Domain: <i>business.com</i> 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: <i>Default</i> Any descriptive name may be used.▪ Intra-region IP-IP Direct Audio: <i>yes</i> Inter-region IP-IP Direct Audio: <i>yes</i> 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: <i>1</i> 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. <div><pre>display ip-network-region 1 Page 1 of 19 IP NETWORK REGION Region: 1 Location: Authoritative Domain: business.com Name: Default MEDIA PARAMETERS Codec Set: 1 UDP Port Min: 2048 UDP Port Max: 3329 Intra-region IP-IP Direct Audio: yes Inter-region IP-IP Direct Audio: yes IP Audio Hairpinning? n DIFFSERV/TOS PARAMETERS Call Control PHB Value: 46 Audio PHB Value: 46 Video PHB Value: 26 RTCP Reporting Enabled? y RTCP MONITOR SERVER PARAMETERS Use Default Server Parameters? y 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 H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 RSVP Enabled? n</pre></div>

Step	Description
2.	<p>Codecs</p> <p>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.</p> <div data-bbox="316 474 1416 1024" style="border: 1px solid black; padding: 10px;"> <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.729A n 2 20 3: 4: 5: 6: 7: Media Encryption 1: none 2: 3: </pre> </div>

Step	Description
3.	<p>Signaling Group</p> <p>For the compliance test, signaling group 1 was used for the signaling group associated with the SIP trunk group between Communication Manager and SIP Enablement Services. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as described in [3].</p> <ul style="list-style-type: none"> ▪ Near-end Node Name: <i>procr</i> 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: <i>SES</i> This node name maps to the IP address of SIP Enablement Services. ▪ Far-end Network Region: <i>1</i> This defines the IP network region which contains SIP Enablement Services. ▪ Far-end Domain: <i>business.com</i> This domain is sent in the “To” header of SIP messages of calls using this signaling group. ▪ Direct IP-IP Audio Connections: <i>y</i> This field must be set to <i>y</i> to enable media shuffling on the SIP trunk. <div data-bbox="316 793 1417 1360" style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <pre> 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 </pre> </div>

Step	Description
4.	<p>Trunk Group</p> <p>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].</p> <ul style="list-style-type: none"> ▪ Signaling Group: 1 This field is 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. <pre> 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 </pre>
5.	<p>Trunk Group – continued</p> <p>On Page 3:</p> <ul style="list-style-type: none"> ▪ Verify the Numbering Format field is set to <i>public</i>. 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. <pre> display trunk-group 1 Page 3 of 21 TRUNK FEATURES ACA Assignment? n Measured: none Maintenance Tests? y Numbering Format: public UI Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n Show ANSWERED BY on Display? y </pre>

Step	Description
6.	<p>Public Unknown Numbering</p> <p>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(s) setting is blank) including trunk group1 will be sent as a 5 digit calling number. This calling party number is sent to the far-end in the SIP “From” header.</p> <pre> display public-unknown-numbering 0 NUMBERING - PUBLIC/UNKNOWN FORMAT Page 1 of 2 Ext Ext Trk CPN Total Len Code Grp(s) Prefix CPN 5 3 5 Total Administered: 14 Maximum Entries: 240 </pre>

4.2. Configure SIP Trunks to Session Manager

To connect to Session Manager, 2 SIP trunk groups were configured on Communication Manager, one for sending outgoing calls from Communication Manager to Session Manager, the other for receiving incoming calls from Session Manager.

Step	Description
1.	<p>Node Names</p> <p>Use the change node-names ip command to create a node name for the IP address of Session Manager. Enter a descriptive name in the Name column and the IP address assigned to Session Manager in the IP address column. The example below shows the values used in the compliance test at site 1.</p> <p>At site 2, since a direct SIP trunk needs to be established between the Communication Manager and the SIParater at the main enterprise site, the SIParator and its public side IP address should be configured in the IP Node Names form instead of the entry for Session Manager.</p> <pre> change node-names ip IP NODE NAMES Name IP Address ASMeast 10.75.5.24 SES 10.75.5.6 default 0.0.0.0 myaudix 10.75.5.7 procr 10.75.5.2 </pre>

Step	Description
2.	<p>Signaling Group (for outgoing calls)</p> <p>For the compliance test, signaling group 27 was used for the SIP trunk group defined for sending outgoing calls to Session Manager (see Step 3). Signaling group 27 was configured using the same parameters as signaling group 1 in Section 4.1, Step 3 with the exception of the Far-end Node Name. The Far-end Node Name field was set to the node name for Session Manager.</p> <p>At site 2, this signaling group was used for the trunk group connecting the Communication Manager to the SIParator at the main enterprise site. So the Far-end Node Name field should be set to the node name for the SIParator and the Far-end Domain field should be set to <i>bigtime.com</i>.</p> <div data-bbox="316 621 1401 1171" style="border: 1px solid black; padding: 10px;"> <pre> display signaling-group 27 SIGNALING GROUP Group Number: 27 Group Type: sip Transport Method: tcp IMS Enabled? n Near-end Node Name: procr Far-end Node Name: ASMeast Near-end Listen Port: 5060 Far-end Listen Port: 5060 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 </pre> </div>

Step	Description
3.	<p>Trunk Group (for outgoing calls)</p> <p>For the compliance test, trunk group 27 was used for the SIP trunk group defined for connecting Communication Manager to Session Manager. Trunk group 27 was configured using the same parameters as trunk group 1 in Section 4.1, Step 4 except that the Group Name field was named differently and the Signaling Group field was set to 27. This includes the settings on Page 3 of the trunk group form (not shown). Similar changes should be made for this trunk group form at site 2.</p> <div data-bbox="315 474 1416 812"> <pre> display trunk-group 27 Page 1 of 21 TRUNK GROUP Group Number: 27 Group Type: sip CDR Reports: y Group Name: To ASMeast COR: 1 TN: 1 TAC: 127 Direction: two-way Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Signaling Group: 27 Number of Members: 24 </pre> </div>
4.	<p>Signaling Group (for incoming calls)</p> <p>For the compliance test, signaling group 26 was used for the SIP trunk group defined for receiving incoming calls from Session Manager (see Step 5). Signaling group 26 was configured using the same parameters as signaling group 27 in Step 2 with the exception of the Far-end Domain set to blank.</p> <p>At site 2, this signaling group was used for the trunk group connecting the Communication Manager to the SIParator at the main enterprise site. So the Far-end Node Name field should be set to the node name for the SIParator.</p> <div data-bbox="315 1215 1399 1768"> <pre> display signaling-group 26 SIGNALING GROUP Group Number: 26 Group Type: sip Transport Method: tcp IMS Enabled? n Near-end Node Name: procr Far-end Node Name: ASMeast Near-end Listen Port: 5060 Far-end Listen Port: 5060 Far-end Network Region: 1 Far-end Domain: 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 </pre> </div>

Step	Description
5.	<p>Trunk Group (for incoming calls)</p> <p>For the compliance test, trunk group 26 was used for the SIP trunk group defined for receiving incoming calls from Session Manager. Trunk group 26 was configured using the same parameters as trunk group 27 in Step 3 except that the Group Name field was named differently and the Signaling Group field was set to 26. This includes the settings on Page 3 of the trunk group form (not shown). Similar changes should be made for this trunk group form at site 2.</p> <div> <pre> display trunk-group 26 Page 1 of 21 TRUNK GROUP Group Number: 26 Group Type: sip CDR Reports: y Group Name: From ASMeast COR: 1 TN: 1 TAC: 126 Direction: two-way Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Signaling Group: 26 Number of Members: 24 </pre> </div>
6.	<p>Automatic Alternate Routing</p> <p>Automatic Alternate Routing (AAR) was used to route calls to Session Manager (for onward routing to the 2nd site through the SIParator). In the example shown, numbers that begin with 50 and are 5 digits long use route pattern 27. Route pattern 27 routes calls to the SIP trunk group defined for sending outgoing calls to Session Manager (see Step 7).</p> <div> <pre> display aar analysis 5 Page 1 of 2 AAR DIGIT ANALYSIS TABLE Location: all Percent Full: 3 Dialed Total Route Call Node ANI String Min Max Pattern Type Num Reqd 50 5 5 27 aar n 500 5 5 27 aar n 501 5 5 27 aar n </pre> </div>

Step	Description
7.	<p>Route Pattern</p> <p>For the compliance test, route pattern 27 was used for calls destined for the 2nd site through Session Manager and the SIParator. Route pattern 27 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Pattern Name: Any descriptive name. ▪ Grp No: 27 This field is set to the trunk group number defined in Step 3. ▪ FRL: 0 This field is the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive. <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <pre> display route-pattern 27 Pattern Number: 27 Pattern Name: To ASMeast SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Intw 1: 27 0 2: 3: 4: 5: 6: n user n user n user n user n user n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts Format Subaddress 1: y y y y y n n rest none 2: y y y y y n n rest none 3: y y y y y n n rest none 4: y y y y y n n rest none 5: y y y y y n n rest none 6: y y y y y n n rest none </pre> </div>

5. Configure Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager management server. All SIP call provisioning for Session Manager is performed via the System Manager web interface and are then downloaded into Session Manager.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

The Session Manager server contains an SM-100 security module that provides the network interface for all inbound and outbound SIP signaling and media transport to all provisioned SIP entities. For the Session Manager used for the compliance test, the IP address assigned to the SM-100 interface is 10.75.5.24 as specified in **Figure 1**. The Session Manager server has a separate network interface used for connectivity to System Manager for managing/provisioning Session Manager. For the compliance test, the IP address assigned to the Session Manager management interface is 10.75.5.22. In the configuration for the compliance test, the SM-100 interface and the management interface were both connected to the same IP network. If desired, the SM-100 interface for real-time SIP traffic can be configured to use a different network than the management interface. For more information on Session Manager and System Manager, see [8] and [9].

The procedures described in this section include configurations in the following areas:

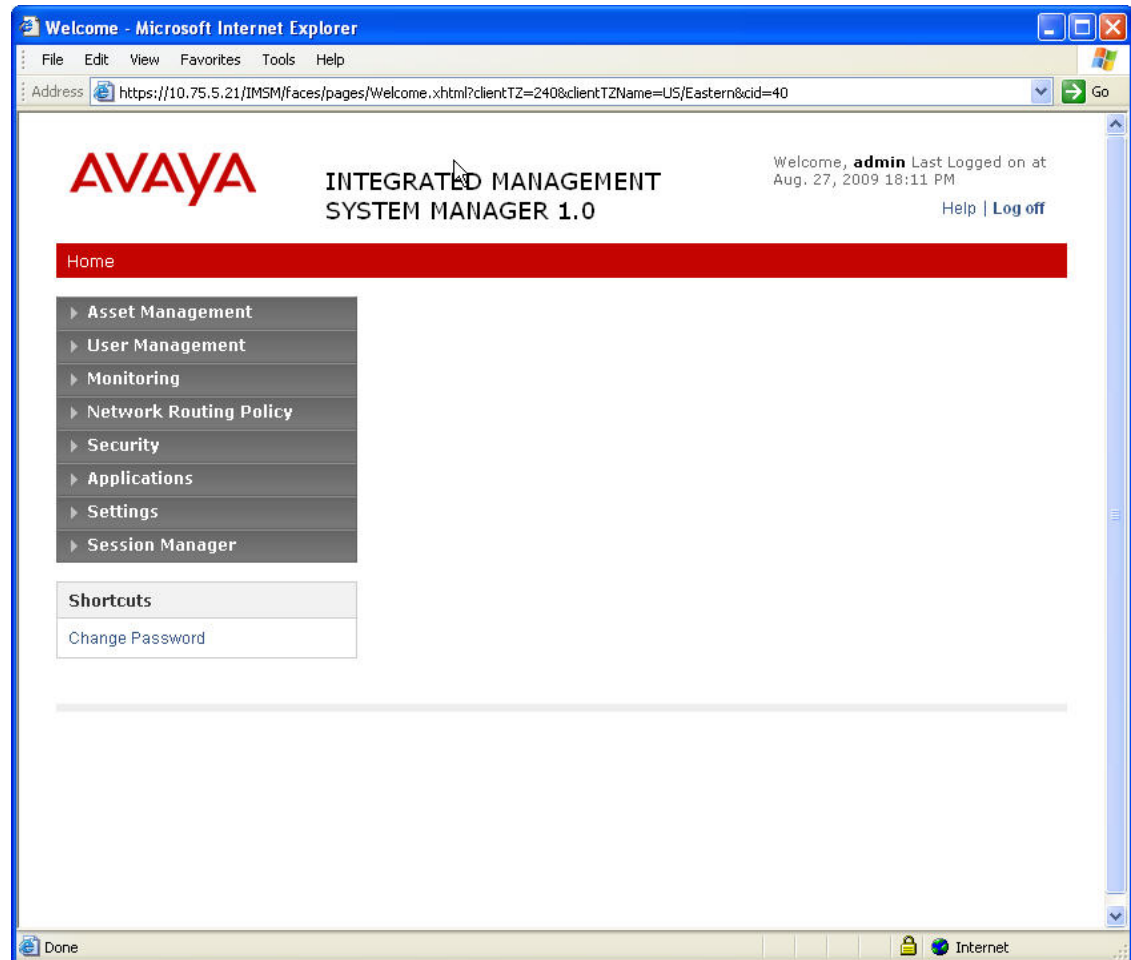
- **SIP domain**
- Logical/physical **Locations** that can be occupied by SIP Entities
- **SIP Entities** corresponding to the SIP telephony systems (including Communication Manager and Session Border Controller) and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Time Ranges** during which routing policies are active
- **Routing Policies** which control call routing between the SIP Entities
- **Adaptations** which specifies any digit conversions or domain modifications needed in SIP Request URI before routing the call to a SIP Entity
- **Dial Patterns** which govern to which SIP Entity a call is routed
- **Session Manager** corresponding to the Session Manager Servers managed by System Manager

1.

Login

Access the Session Manager administration web interface by entering `http://<ip-addr>/IMSM` as the URL in an Internet browser, where `<ip-addr>` is the IP address of the System Manager server.

Log in with the appropriate credentials. The main page for administrative interface is shown below.



2.

Add SIP Domain

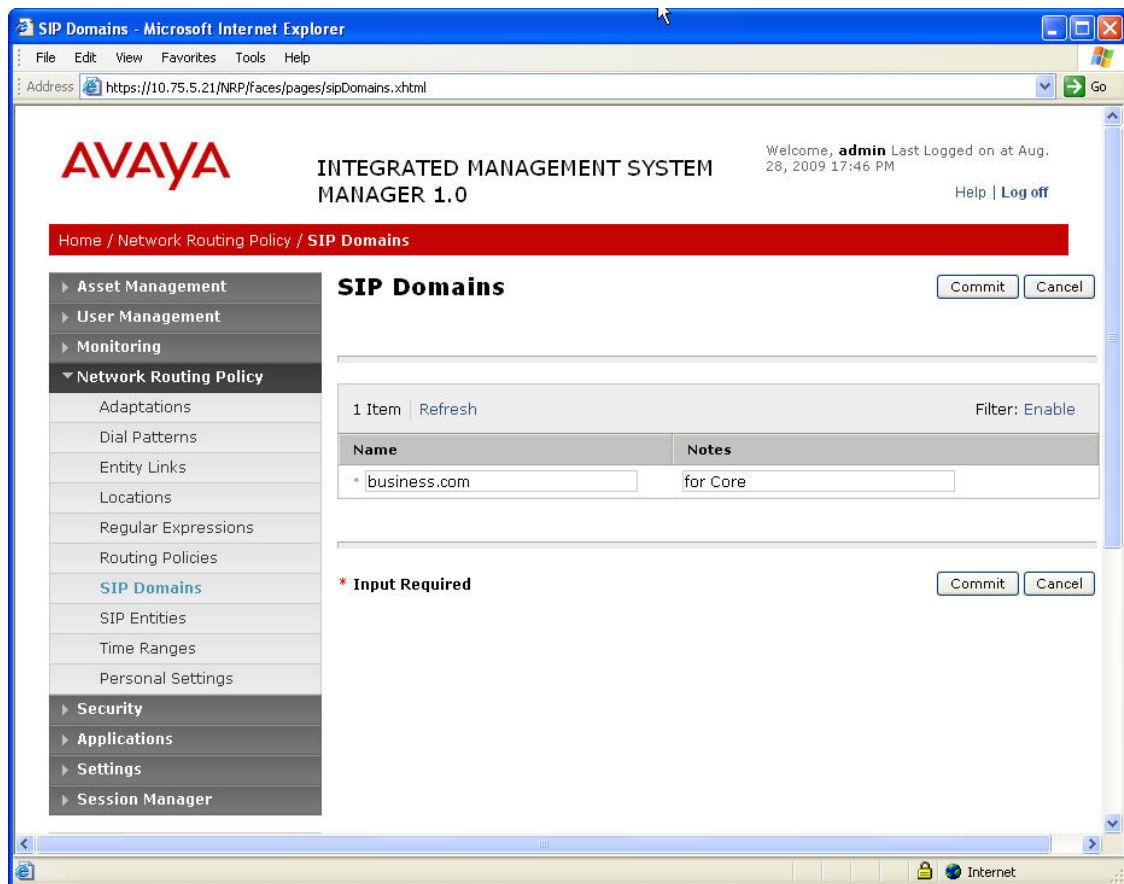
The **Network Routing Policy** sub menus contain all configuration tasks (except the last one) listed at the beginning of this section.

In the compliance test, only one SIP Domain was configured – all Session Manager SIP entities were located in the same authoritative domain.

Navigate to **Network Routing Policy**→**SIP Domains** to add the SIP domain with

- **Name:** *business.com* (as set in **Section 4.2, Step 2**)
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.



3.

Add Location

Locations identify logical and/or physical locations where SIP entities reside. In the compliance test, only one Location was configured – all Session Manager SIP entities were located in the same Location.

Navigate to **Network Routing Policy**→**Locations** to add the Location.

Under **General**:

- **Name:** a descriptive name
- **Notes:** optional descriptive text

Under **Location Pattern**:

- **IP Address Pattern:** *10.75.5.**
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.

Location Details - Microsoft Internet Explorer

Address: https://10.75.5.21/NRP/faces/pages/routingOriginationsDetails.xhtml?cid=23

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, admin Last Logged on at Aug. 28, 2009 17:46 PM

Help | Log off

Home / Network Routing Policy / Locations / Location Details

Location Details [Commit] [Cancel]

General

Name	Notes
* Core	Session Manager and CM/SES

Managed Bandwidth: [] Kbit/sec

* Average Bandwidth per Call: [80] Kbit/sec

* Time to Live (secs): [3600]

Location Pattern

[Add] [Remove]

1 Item | Refresh Filter: Enable

IP Address Pattern	Notes
* 10.75.5.*	Core ASM, CM/SES

Select: All, None (0 of 1 Selected)

* Input Required [Commit] [Cancel]

Shortcuts

Change Password

4.

Add Adaptations

Session Manager provides for specialized code modules, called Adaptations, to process specific call processing requirements. In the compliance test, 2 Adaptations were used to update the domain as contained in the SIP Request-URI based on the SIP Entities to which this adaptation is defined. The screen below shows the configuration details of the Adaptation (when associated with the Communication Manager SIP Entity in **Step 7**) that will replace domain in the SIP Request-URI for all calls to Communication Manager to *business.com*.

Navigate to **Network Routing Policy**→**Adaptations** to add Adaptation.

Under **General**:

- **Name:** a descriptive name
- **Adaptation Module:** enter *DigiConversionAdapter business.com*
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.

Adaptation Details - Microsoft Internet Explorer

Address: <https://10.75.5.21/NRP/faces/pages/adaptationsDetails.xhtml?cid=21>

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Aug. 28, 2009 17:46 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Adaptations / Adaptation Details

Adaptation Details [Commit](#) [Cancel](#)

General

Name	Adaptation Module	Egress URI Parameters	Notes
* business	DigiConversionAdapter business.com		For calls to

Digit Conversion for Incoming Calls

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	-------------------	-------

* Input Required [Commit](#) [Cancel](#)

Adaptation Details field descriptions

5. Add Adaptations (Continued)

Add a second Adaptation that will replace domain in the SIP Request-URI for all calls to the Ingate SIParator SIP Entity (for onward routing to the 2nd site simulating a service provider service node) to **bigtime.com**.

The Adaptations summary screen as shown below list the 2 Adaptations used in the compliance test:

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The top navigation bar includes the Avaya logo, the system name, and a welcome message for the user 'admin'. The left sidebar contains a tree view of the system's configuration options, with 'Network Routing Policy' expanded to show 'Adaptations'. The main content area is titled 'Adaptations' and features a table with two items. The table columns are State, Name, Adaptation Module, Egress URI Parameters, and Notes. The first item is 'bigtime' with a 'Sync' state, using the 'DigitConversionAdapter' module for 'bigtime.com'. The second item is 'business' with a 'Sync' state, using the 'DigitConversionAdapter' module for 'business.com'. The interface also includes buttons for 'Edit', 'New', 'Duplicate', 'Delete', 'More Actions', and 'Commit'.

State	Name	Adaptation Module	Egress URI Parameters	Notes
Sync	bigtime	DigitConversionAdapter bigtime.com		For calls to bigtime.com
Sync	business	DigitConversionAdapter business.com		For calls to business.com

6.	<p>Add SIP Entities – Session Manager</p> <p>A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the compliance test, a SIP Entity was added for the Session Manager itself, the Communications Manager, and the Ingate SIPrator.</p> <p>Navigate to Network Routing Policy→SIP Entities to add SIP Entities. The configuration details for the SIP Entity defined for Session Manager are as follows:</p> <p>Under General:</p> <ul style="list-style-type: none"> • Name: a descriptive name • FQDN or IP Address: 10.75.5.24 as specified in Figure 1. This is the IP address assigned to the SM-100 security module installed in the Session Manager. • Type: select <i>Session Manager</i> • Adaptation: leave blank • Location: select the Location created in Step 3 • Time Zone: select the proper time zone for this installation <p>Under Port, click Add, then edit the fields in the resulting new row as shown below:</p> <ul style="list-style-type: none"> • Port: 5060. This is the port number on which the system listens for SIP requests. • Protocol: TCP. The TCP transport protocol was used in the compliance test to send SIP requests. • Default Domain: select the SIP Domain created in Step 2. <p>Default settings can be used for the remaining fields. Click Commit to save the SIP Entity definition.</p>
----	--

6.

Add SIP Entities – Session Manager (Continued)

The screen below shows the SIP Entity configuration details for the Session Manager.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Aug. 28, 2009 17:46 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details [Commit](#) [Cancel](#)

General

Name	FQDN or IP Address	Type	Notes
* ASMeast	* 10.75.5.24	Session Manager	

Entity Links

Adaptation:

Location:

Outbound Proxy:

Time Zone:

Override Port & Transport with DNS SRV: ☐

SIP Timer B/F (secs): *

Credential name:

Monitoring

Monitoring on/off:

Port

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	business.com	

Select: All, None (0 of 1 Selected)

* Input Required [Commit](#) [Cancel](#)

7.

Add SIP Entities – Communication Manager

The screen below shows the SIP Entity configuration details for the Communication Manager. Note the **CM** selection for **Type** and the **business Adaptation** selection created in **Step 4**.

AVAYA INTEGRATED MANAGEMENT SYSTEM
MANAGER 1.0

Welcome, **admin** Last Logged on at Aug. 28, 2009 17:46 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details [Commit](#) [Cancel](#)

General

Name	FQDN or IP Address	Type	Notes
* Core CM	* 10.75.5.2	CM	

Entity Links

Adaptation: [business](#)

Location: [Core](#)

Time Zone: [America/New_York](#)

Override Port & Transport with DNS SRV: ☐

SIP Timer B/F (secs): *

Credential name:

Call Detail Recording: [egress](#)

Monitoring

Monitoring on/off: [Enable monitoring](#)

Proactive cycle time (secs): *

Reactive cycle time (secs): *

Number of Retries: *

* Input Required [Commit](#) [Cancel](#)

Shortcuts

- [Change Password](#)
- [SIP Entity Details field descriptions](#)
- [Saving Committing Synchronizing](#)

8.

Add SIP Entities – Ingate SIParator

The screen below shows the SIP Entity configuration details for the Ingate SIParator. Note the **SBC** selection for **Type** and the **bigtime** **Adaptation** selection created in **Step 5**.

The screenshot displays the Avaya Integrated Management System Manager 1.0 web interface. The left sidebar contains a navigation menu with categories like Asset Management, User Management, Monitoring, Network Routing Policy, SIP Domains, SIP Entities, Time Ranges, Personal Settings, Security, Applications, Settings, and Session Manager. The main content area is titled 'SIP Entity Details' and shows configuration for the 'SIParator' entity. The 'General' tab is active, displaying a table with columns for Name, FQDN or IP Address, Type, and Notes. Below the table, the 'Entity Links' section shows 'Adaptation' set to 'bigtime', 'Location' set to 'Core', and 'Time Zone' set to 'America/New_York'. The 'Monitoring' section shows 'Monitoring on/off' set to 'Enable monitoring', 'Proactive cycle time (secs)' set to 900, 'Reactive cycle time (secs)' set to 120, and 'Number of Retries' set to 1. The 'Input Required' section is also visible. The interface includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

AVAYA INTEGRATED MANAGEMENT SYSTEM
MANAGER 1.0

Welcome, **admin** Last Logged on at Aug. 28, 2009 17:46 PM
Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details

Commit Cancel

General

Name	FQDN or IP Address	Type	Notes
* SIParator	* 10.75.5.63	SBC	Ingate

Entity Links

Adaptation: bigtime

Location: Core

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

SIP Timer B/F (secs): * 4

Credential name:

Call Detail Recording: egress

Monitoring

Monitoring on/off: Enable monitoring

Proactive cycle time (secs): * 900

Reactive cycle time (secs): * 120

Number of Retries: * 1

* Input Required

Commit Cancel

Shortcuts

Change Password

SIP Entity Details field descriptions

Saving Committing Synchronizing

9.

SIP Entities Summary List

The screen below shows the SIP Entities summary list displayed after the 3 SIP Entities have been added in **Steps 6, 7 and 8**. Note that the SIP Entity named **FaxR CM** was configured for other purposes; it was not used in the compliance test.

The screenshot shows the Avaya Integrated Management System Manager 1.0 web interface. The top navigation bar includes the Avaya logo, the title 'INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0', and a welcome message for 'admin' last logged on at Aug. 28, 2009 17:46 PM. A red breadcrumb trail shows the path: Home / Network Routing Policy / SIP Entities. On the left, a sidebar menu lists various management categories, with 'SIP Entities' highlighted under 'Network Routing Policy'. The main content area is titled 'SIP Entities' and features a table with 4 items. Above the table are buttons for 'Edit', 'New', 'Duplicate', 'Delete', 'More Actions', and 'Commit'. The table columns are: checkbox, State, Name, Entity Links, FQDN or IP Address, Type, and Notes. The data rows are: ASMeast (Session Manager), Core CM (CM), FaxR CM (CM), and SIParator (SBC, Ingate SBC). Below the table, it indicates 'Select: All, None (0 of 4 Selected)'.

	State	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	Sync	ASMeast	▶	10.75.5.24	Session Manager	
<input type="checkbox"/>	Sync	Core CM	▶	10.75.5.2	CM	
<input type="checkbox"/>	Sync	FaxR CM	▶	192.45.70.2	CM	
<input type="checkbox"/>	Sync	SIParator	▶	10.75.5.63	SBC	Ingate SBC

10.

Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the compliance test 2 Entity Links were created: one between Session Manager and Communication Manager; the other between Session Manager and Ingate SIParator.

Navigate to **Network Routing Policy**→**Entity Links** to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager to Communication Manager.

- **Name:** a descriptive name
- **SIP Entity 1:** select the Session Manager SIP Entity created in **Step 6**.
- **Port: 5060.** This is the port number to which the other system sends SIP requests.
- **SIP Entity 2:** select the Communication Manager SIP Entity created in **Step 7**.
- **Port: 5060.** This is the port number on which the other system receives SIP requests.
- **Trusted:** check this box
- **Protocol:** select **TCP** as the transport protocol.
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.

The screenshot shows the Avaya Integrated Management System (IMS) 1.0 web interface. The top header includes the Avaya logo, the text "INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0", and a welcome message for the user "admin" last logged on at Aug. 28, 2009 17:46 PM. The breadcrumb trail indicates the current location: Home / Network Routing Policy / Entity Links. The left sidebar contains a navigation menu with options like Asset Management, User Management, Monitoring, Network Routing Policy (expanded), SIP Domains, SIP Entities, Time Ranges, Personal Settings, Security, Applications, Settings, and Session Manager. The main content area is titled "Entity Links" and shows a table with one item. The table has columns for Name, SIP Entity 1, Port, SIP Entity 2, Port, Trusted, and Protocol. The row shows "ASMeast Core CM" as the Name, "ASMeast" as SIP Entity 1, "5060" as the Port, "Core CM" as SIP Entity 2, "5060" as the Port, a checked "Trusted" box, and "TCP" as the Protocol. Below the table, there is a section labeled "* Input Required" with "Commit" and "Cancel" buttons.

Name	SIP Entity 1	Port	SIP Entity 2	Port	Trusted	Protocol
* ASMeast Core CM	* ASMeast	* 5060	* Core CM	* 5060	<input checked="" type="checkbox"/>	TCP

* Input Required

11. Add Entity Links (Continued)

The Entity Link for connecting Session Manager to Ingate SIParator was similarly defined. The screen below shows the SIP Entity Links summary list displayed after the 2 SIP Entity Links have been configured. Note that the SIP Entity Link named **ASMeast FaxR CM** was configured for other purposes; it was not used in the compliance test.

The screenshot displays the 'Entity Links' page in the Avaya Integrated Management System (IMS) 1.0. The page title is 'Entity Links - Microsoft Internet Explorer'. The address bar shows the URL: <https://10.75.5.21/NRP/faces/pages/entityLinks.xhtml?cid=30>. The page header includes the Avaya logo, 'INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0', and a welcome message for 'admin' last logged on at Aug. 28, 2009 17:46 PM. A navigation menu on the left lists various system components, with 'Network Routing Policy' expanded. The main content area shows a table of 3 items, with a 'Filter: Enable' option. The table columns are: State, Name, SIP Entity 1, Port, SIP Entity 2, Port, Trusted, Protocol, and Notes. The table contains the following data:

State	Name	SIP Entity 1	Port	SIP Entity 2	Port	Trusted	Protocol	Notes
Sync	ASMeast Core CM	ASMeast	5060	Core CM	5060	<input checked="" type="checkbox"/>	TCP	
Sync	ASMeast FaxR CM	ASMeast	5060	FaxR CM	5060	<input checked="" type="checkbox"/>	TCP	
Sync	ASMeast SIParator	ASMeast	5060	SIParator	5060	<input checked="" type="checkbox"/>	TCP	From ASMeast to SIParator

Below the table, there is a selection bar with the text 'Select: All, None (0 of 3 Selected)'.

12.

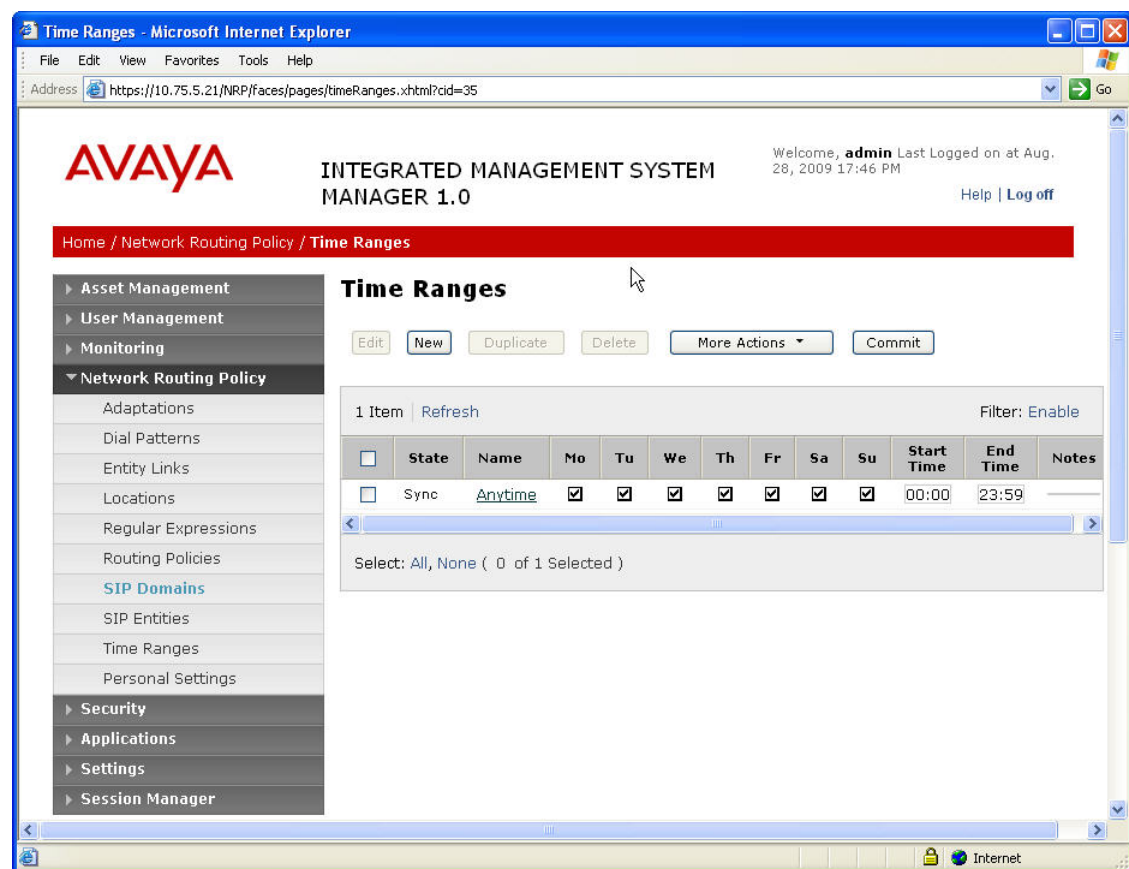
Add Time Ranges

Before adding routing policies (configured in next step), time ranges must be defined during which the policies will be active. For the compliance test, one Time Range was defined that would allow routing to occur at anytime.

Navigate to **Network Routing Policy**→**Time Ranges** to add a new Time Range:

- **Name:** a descriptive name
- **Mo through Su:** check the box under each of these headings
- **Start Time:** enter **00:00**
- **End Time:** enter **23:59**

Click **Commit** to save this time range.



13.	<p>Add Routing Policies</p> <p>Routing policies describe the conditions under which calls will be routed to the SIP Entities connected to the Session Manager. For the compliance test, 2 routing policies were added – one for routing calls to Communication Manager, the other for routing calls to Ingate SIParator.</p> <p>Navigate to Network Routing Policy→Routing Policies to add a new Routing Policy.</p> <p>Under General:</p> <ul style="list-style-type: none"> • Name: a descriptive name • Notes: optional descriptive text <p>Under SIP Entity as Destination</p> <p>Click Select to select the appropriate SIP Entity to which the routing policy applies.</p> <p>Under Time of Day</p> <p>Click Add to select the Time Range configured in Step 12.</p> <p>Default settings can be used for the remaining fields. Click Commit to save the configuration.</p>
-----	---

13. Add Routing Policies (Continued)

The screens below show the configuration details for the 2 Routing Policies defined for the compliance test.

Routing Policy Details - Microsoft Internet Explorer
 Address: https://10.75.5.21/NRP/faces/pages/networkRoutingPolicyDetails.xhtml?cid=37

Welcome, **admin** Last Logged on at Aug. 28, 2009 17:46 PM
 Help | Log off

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details [Commit] [Cancel]

General

Name	Disabled	Notes
* To Core	<input type="checkbox"/>	

SIP Entity as Destination
 [Select]

Name	FQDN or IP Address	Type	Notes
Core CM	10.75.5.2	CM	

Time of Day
 [Add] [Remove] [View Gaps/Overlaps]

1 Item | Refresh Filter: Enable

Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time
0	Anytime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00

Select: All, None (0 of 1 Selected)

Routing Policy Details - Microsoft Internet Explorer
 Address: https://10.75.5.21/NRP/faces/pages/networkRoutingPolicyDetails.xhtml?cid=45

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details [Commit] [Cancel]

General

Name	Disabled	Notes
* to SIPArator	<input type="checkbox"/>	

SIP Entity as Destination
 [Select]

Name	FQDN or IP Address	Type	Notes
SIPArator	10.75.5.63	SBC	Ingate SBC

Time of Day
 [Add] [Remove] [View Gaps/Overlaps]

1 Item | Refresh Filter: Enable

Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time
0	Anytime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00

Select: All, None (0 of 1 Selected)

Dial Patterns

14.	<p>Add Dial Patterns</p> <p>Dial Patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP Entities. In the compliance test, 5-digit extensions beginning with “301” resided on Communication Manager in the main enterprise site; and 5-digit extensions beginning with “50” should be routed to Ingate SIPrator for onward routing to the 2nd site. Therefore 2 Dial Patterns were created accordingly.</p> <p>Navigate to Network Routing Policy→Dial Patterns to add a new Dial Pattern.</p> <p>Under General:</p> <ul style="list-style-type: none"> • Pattern: dialed number or prefix • Min: minimum length of dialed number • Max: maximum length of dialed number • SIP Domain: select the SIP Domain created in Step 2 • Notes: optional descriptive text <p>Under Originating Locations and Routing Policies Click Add to select the appropriate originating Location and Routing Policy from the list.</p> <p>Under Time of Day Click Add to select the time range configured in Step 12.</p> <p>Default settings can be used for the remaining fields. Click Commit to save the configuration.</p>
-----	---

14. Add Dial Patterns (Continued)

The screen below shows the configuration details for the Dialed Pattern defined for matching dialed numbers beginning with “301” destined for the main enterprise site. The Dialed Pattern defined for matching dialed numbers beginning with “50” destined for the Ingate SIParator (for onward routing to the 2nd site simulating a service provider service node) is similarly defined (not shown) with **50** specified for **Pattern** and the **to SIParator** selection for **Routing Policy Name** as defined in **Step 13**.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Aug. 28, 2009 17:46 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / **Dial Pattern Details**

Dial Pattern Details [Commit](#) [Cancel](#)

General

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
* 301	* 5	* 5	<input type="checkbox"/>	business.com	Remote Users to Core

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Core	Session Manager and CM/SES	To Core	<input type="checkbox"/>	Core CM	

Select: All, None (0 of 1 Selected)

Denied Originating Locations

[Add](#) [Remove](#)

0 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required [Commit](#) [Cancel](#)

15.

Add Session Manager

To complete the configuration, adding the Session Manager provided the linkage between System Manager and Session Manager. This configuration procedure should have already been properly executed but is included here for reference and completeness.

Navigate to **Session Manager**→**Session Manager Administration** to add a new Session Manager:

Under **Identity**:

- **SIP EntityName**: select the name of the SIP Entity created for Session Manager
- **Description**: descriptive text
- **Management Access Point Host Name/IP**: enter the IP address of the Session Manager management interface.

Under **Security Module**:

- **Network Mask**: enter the proper network mask for Session Manager.
- **Default Gateway**: enter the default gateway IP address for Session Manager

Accept default settings for the remaining fields. Click **Save** to add this Session Manager..

https://10.75.5.21/ASM/faces/pages/admin/instanceEdit.xhtml?cid=6 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://10.75.5.21/ASM/faces/pages/admin/instanceEdit.xhtml?cid=6

Go

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Aug. 28, 2009 21:46 PM [Help](#) [Log off](#)

Edit Session Manager [Cancel](#) [Save](#)

General | Security Module | Monitoring | CDR

Expand All | Collapse All

General

SIP Entity Name ASMeast

Description Core Session Manager

* Management Access Point Host Name/IP 10.75.5.22

Security Module

SIP Entity IP Address 10.75.5.24

* Network Mask 255.255.255.0

* Default Gateway 10.75.5.1

* Call Control PHB 46

VLAN ID

* QOS Priority 6

Monitoring

Enable Monitoring ☒

Done

Internet

6. Configure Avaya SIP Telephones

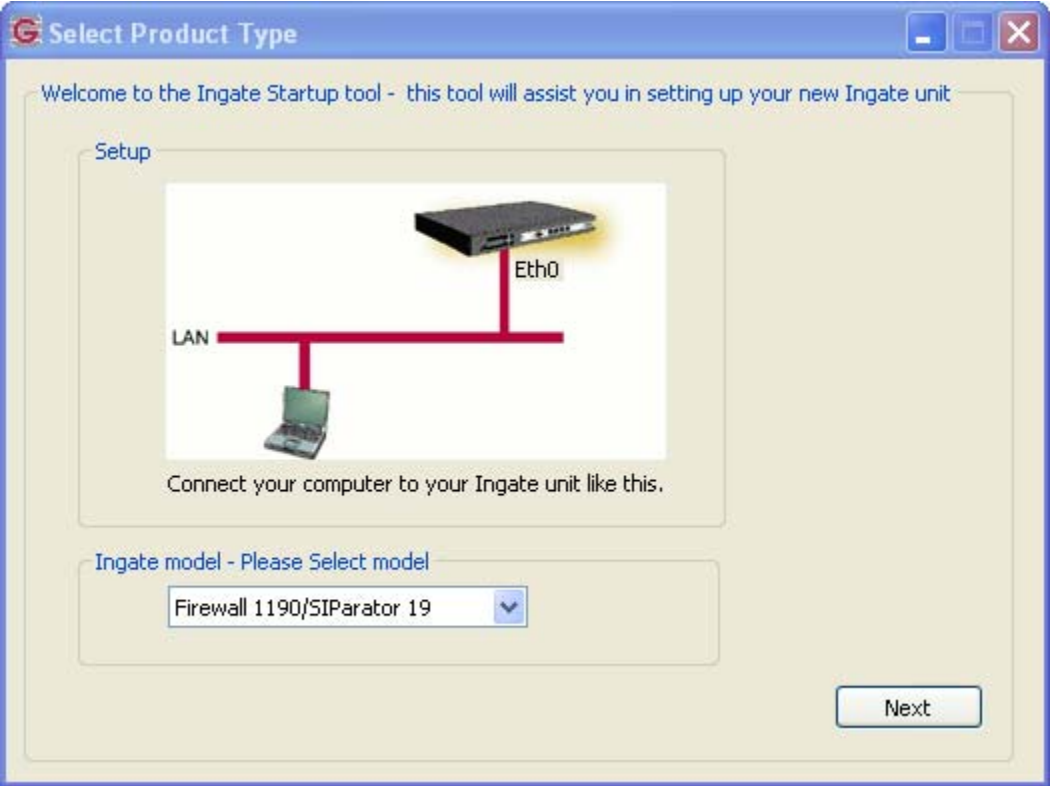
The SIP telephones at each site will use the local SIP Enablement Services as the call server. The table below shows an example of the SIP telephone network settings for each site.

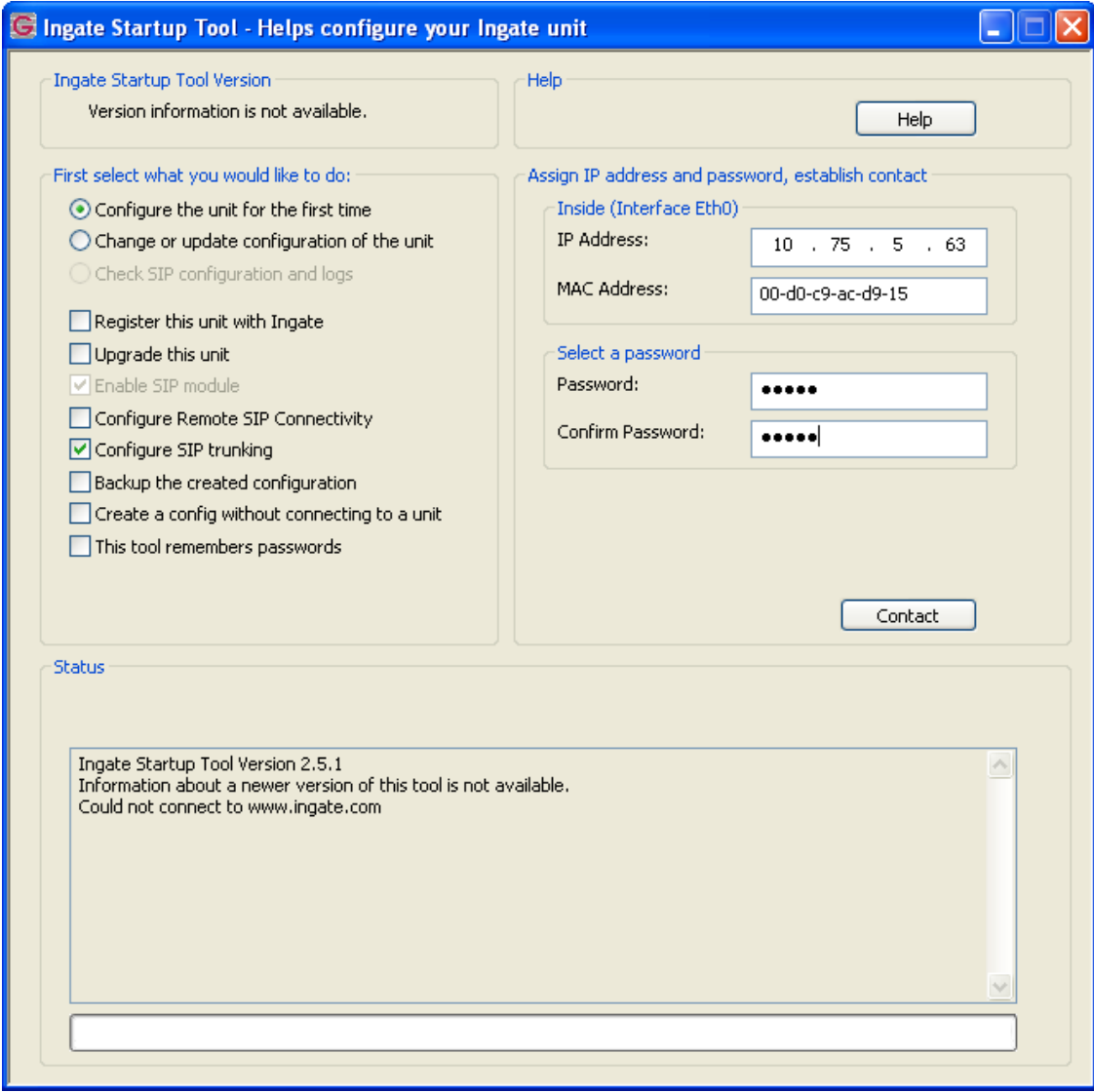
	Main Site	2 nd Site
Extension	30102	50022
IP Address	10.75.5.162	192.45.70.21
Subnet Mask	255.255.255.0	255.255.255.0
Router	10.75.5.1	192.45.70.1
File Server	10.75.10.100	192.45.70.100
DNS Server	0.0.0.0	0.0.0.0
SIP Domain	business.com	bigtime.com
Call Server or SIP Proxy Server	10.75.5.6	192.45.70.7

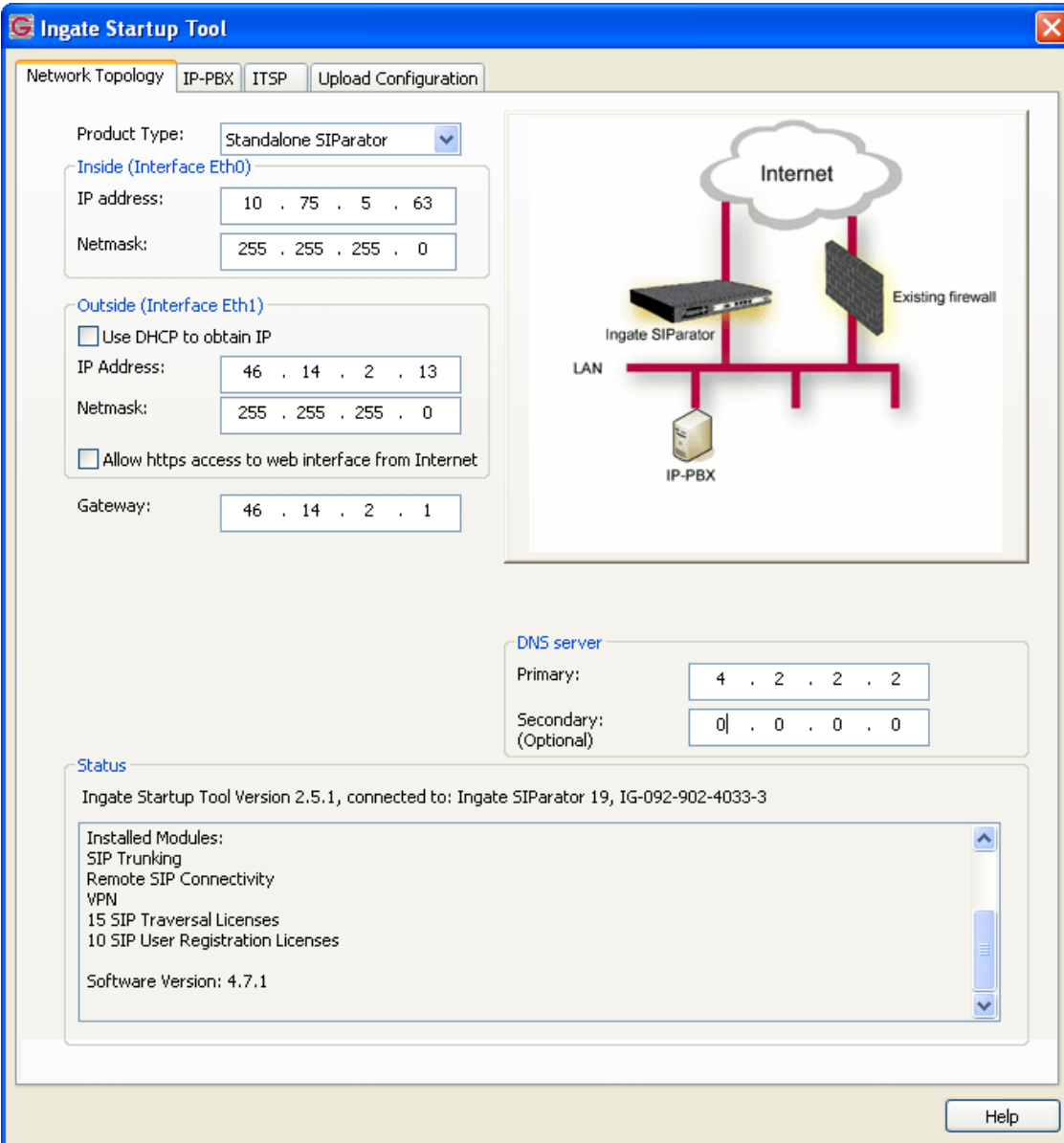
7. Configure the Ingate SIParator

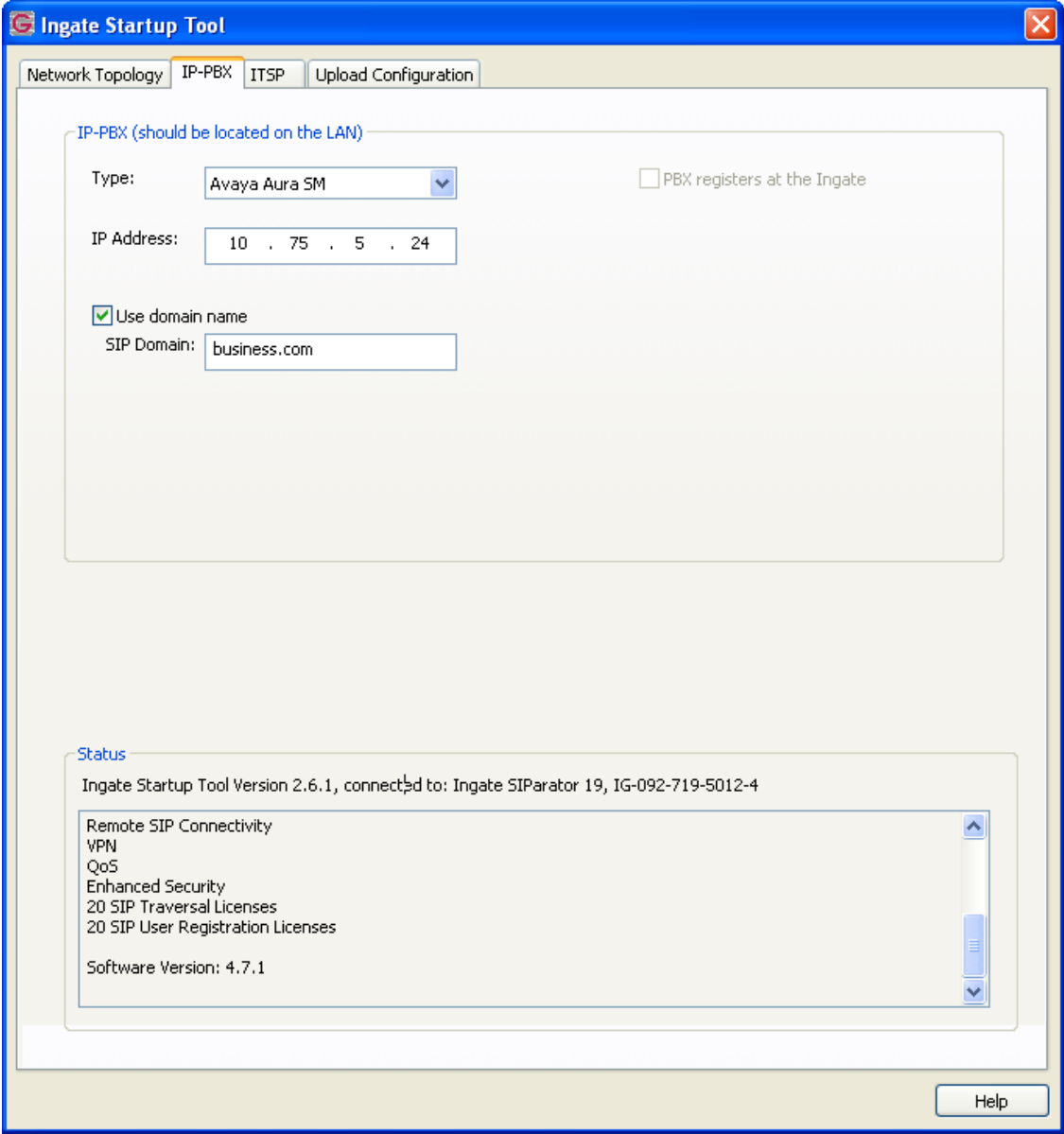
The Ingate SIParator is configured initially with the Ingate Startup Tool. Based on the provided input, the Startup Tool will create an initial configuration that can be uploaded to the SIParator. The results of this configuration can then be viewed or expanded using the SIParator web interface. To access 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.

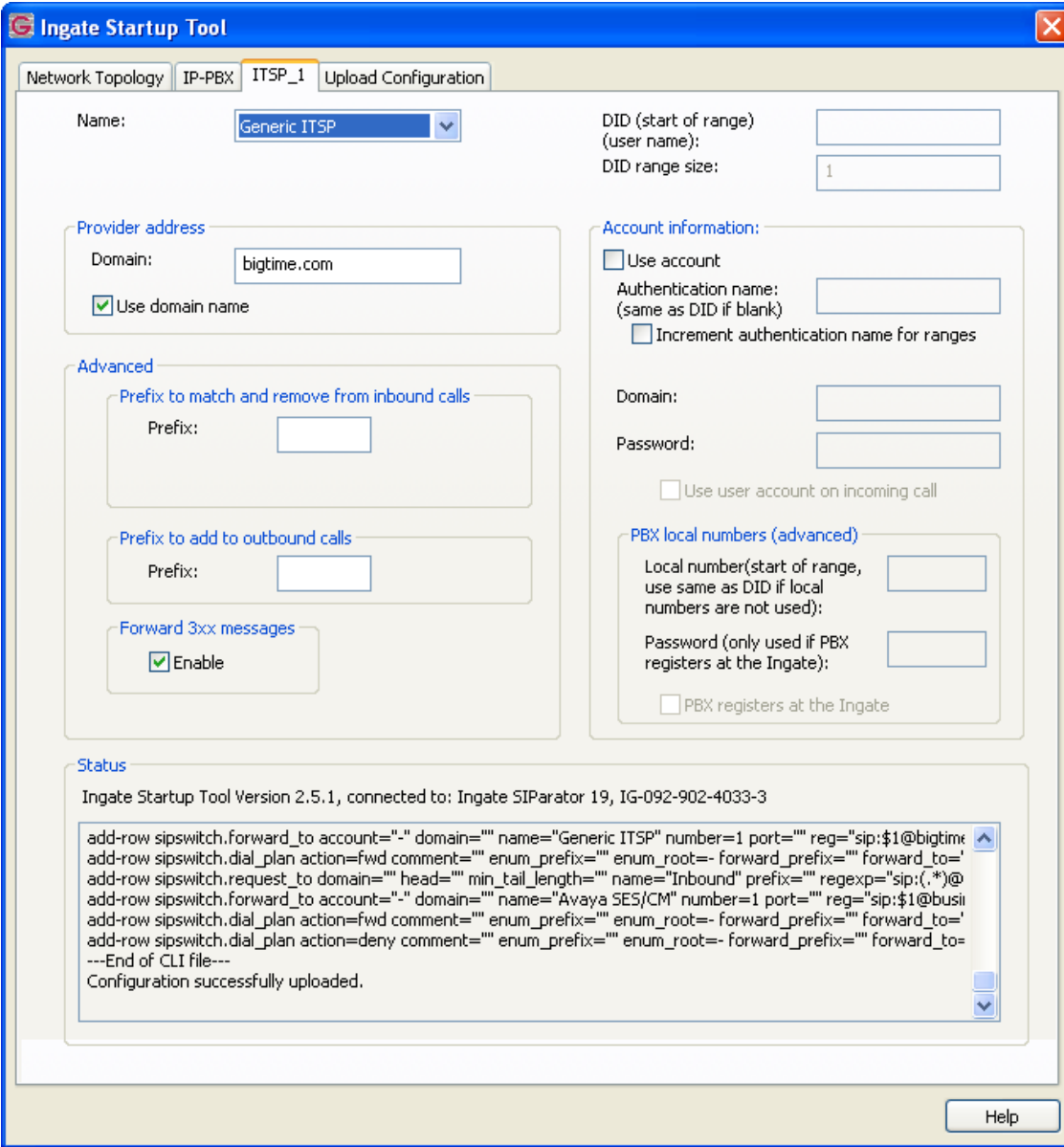
Step	Description
1.	Launch Startup Tool The Ingate Startup Tool is a windows application which is launched from the Windows Start Menu by navigating to Start→All Programs→Shortcut to StartupTool.exe .

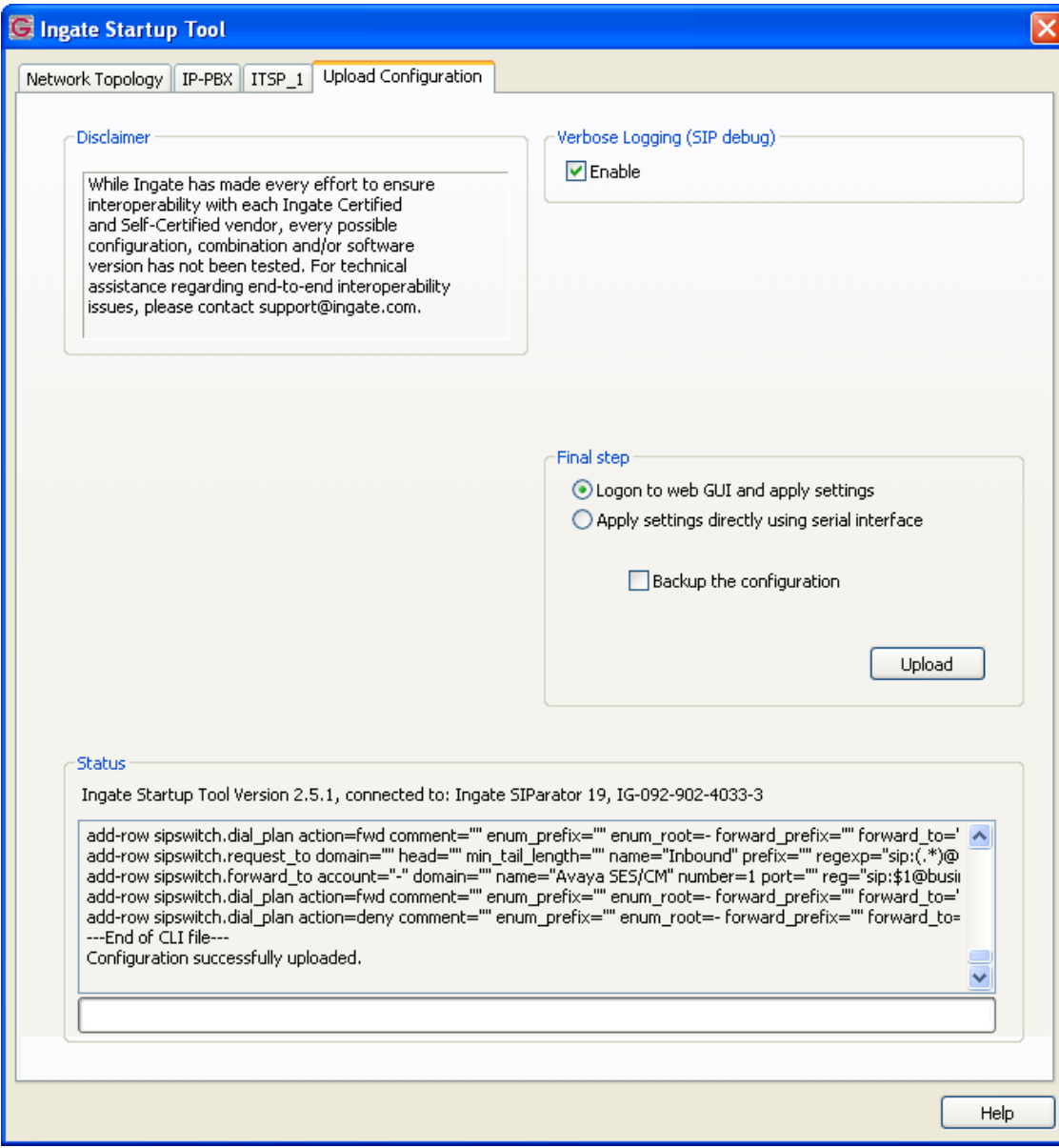
Step	Description
2.	<p>Select Product Type</p> <p>The initial Ingate Startup Tool screen is shown below. Verify the PC is running on the same LAN subnet as the SIParator as shown in the diagram. This is necessary in order to assign the initial IP address to the SIParator from the Startup Tool. Select the SIParator model from the Ingate model drop-down menu. Click the Next button.</p> 

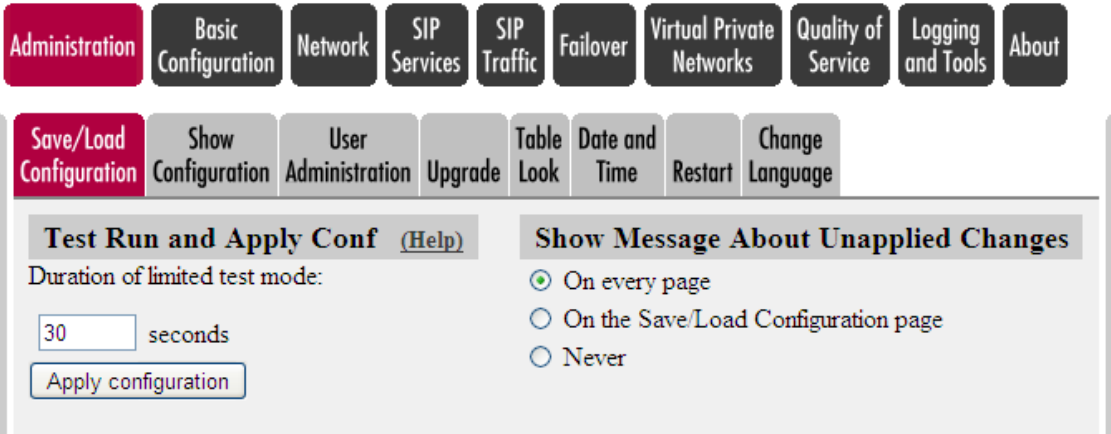
Step	Description
3.	<p>Select Configuration Options and Assign Private IP</p> <p>Select options for Configure the unit for the first time and Configure SIP trunking. Enter the inside IP address, MAC address and a password. Click the Contact button to establish a connection to the SIParator. For future updates, click the option - Change or update configuration of the unit</p>  <p>The screenshot shows the 'Ingate Startup Tool - Helps configure your Ingate unit' window. It has a blue title bar with standard window controls. The main area is divided into several sections:</p> <ul style="list-style-type: none"> Ingate Startup Tool Version: A box stating 'Version information is not available.' with a 'Help' button. First select what you would like to do: A list of radio and checkbox options: <ul style="list-style-type: none"> <input checked="" type="radio"/> Configure the unit for the first time <input type="radio"/> Change or update configuration of the unit <input type="radio"/> Check SIP configuration and logs <input type="checkbox"/> Register this unit with Ingate <input type="checkbox"/> Upgrade this unit <input checked="" type="checkbox"/> Enable SIP module <input type="checkbox"/> Configure Remote SIP Connectivity <input checked="" type="checkbox"/> Configure SIP trunking <input type="checkbox"/> Backup the created configuration <input type="checkbox"/> Create a config without connecting to a unit <input type="checkbox"/> This tool remembers passwords Assign IP address and password, establish contact: <ul style="list-style-type: none"> Inside (Interface Eth0): Fields for 'IP Address:' (10 . 75 . 5 . 63) and 'MAC Address:' (00-d0-c9-ac-d9-15). Select a password: Fields for 'Password:' and 'Confirm Password:', both masked with dots. A 'Contact' button is at the bottom right of this section. Status: A large text area at the bottom showing: <pre>Ingate Startup Tool Version 2.5.1 Information about a newer version of this tool is not available. Could not connect to www.ingate.com</pre>

Step	Description
4.	<p>Network Topology</p> <p>After connecting to the SIParator, the following page appears. Select the Network Topology tab. Select <i>Standalone SIParator</i> 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.</p>  <p>The screenshot displays the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The 'Product Type' is set to 'Standalone SIParator'. The 'Inside (Interface Eth0)' section shows an IP address of 10.75.5.63 and a netmask of 255.255.255.0. The 'Outside (Interface Eth1)' section has the 'Use DHCP to obtain IP' checkbox unchecked, with an IP address of 46.14.2.13 and a netmask of 255.255.255.0. The 'Gateway' is set to 46.14.2.1. The 'DNS server' section shows a primary of 4.2.2.2 and a secondary (optional) of 0.0.0.0. The 'Status' section at the bottom indicates the tool version (2.5.1) and lists installed modules: SIP Trunking, Remote SIP Connectivity, VPN, 15 SIP Traversal Licenses, and 10 SIP User Registration Licenses, with a software version of 4.7.1. A network diagram on the right illustrates the topology: an 'Ingate SIParator' is connected to the 'Internet' cloud, an 'Existing firewall', and an 'IP-PBX' on a 'LAN'.</p>

Step	Description
5.	<p>IP-PBX Settings</p> <p>Select the IP-PBX tab. Select Avaya Aura SM from the Type drop-down menu (this selection was available from Startup Tool version 2.6.0 or greater). This will instruct the Startup Tool to configure the SIP parameters on the internal interface to be compatible with the Avaya component (Session Manager in this case) connected to it through direct SIP trunking interface. Enter the Session Manager IP address in the IP Address field. Also check the option to use domain name, then specify the domain name as set on Session Manager (see Section 5 Step 2)</p> 

Step	Description
6.	<p>Service Provider Settings</p> <p>Select the ITSP_1 tab. Select Generic ITSP from the Name drop-down menu. This will instruct the Startup Tool to configure the SIP parameters on the external interface to be compatible with a generic SIP service provider. In the Domain field in the Provide address section, enter the domain for the 2nd site simulating a service provider service node and check the Use domain name option box.</p>  <p>The screenshot shows the Ingate Startup Tool window with the 'ITSP_1' tab selected. The 'Name' dropdown is set to 'Generic ITSP'. In the 'Provider address' section, the 'Domain' is 'bigtime.com' and the 'Use domain name' checkbox is checked. The 'Account information' section has 'Use account' checked, with 'Authentication name' set to the same as the DID. The 'Advanced' section has 'Prefix to match and remove from inbound calls' and 'Prefix to add to outbound calls' both empty, and 'Forward 3xx messages' checked. The 'Status' section shows the tool version and a successful configuration upload message.</p>

Step	Description
7.	<p>Upload Configuration</p> <p>Select the Upload Configuration tab to upload the configuration to the SIParator. Click the Upload button to begin the upload.</p> 

Step	Description
8.	<p>Apply Configuration</p> <p>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.</p> 

Step	Description
9.	<p>Configure Routing</p> <p>Navigate to SIP Traffic→Routing to add entries for DNS override for SIP requests. Add one entry for the outside interface and one entry for the inside interface as shown below. The configured parameters are:</p> <ul style="list-style-type: none">• Domain: domain names for the main enterprise site (<i>business.com</i>) and the 2nd site simulating a service provider service node (<i>bigtime.com</i>)• DNS Name or IP Address: IP addresses for the Avaya components connected to the SIParator on the outside (2nd site Communication Manager IP address <i>192.45.70.2</i>) and on the inside (Session Manager IP address <i>10.75.5.24</i>)• Transport: select <i>TCP</i>

Administration

Basic Configuration

Network

SIP Services

SIP Traffic

Failover

Virtual Private Networks

Quality of Service

Logging and Tools

About

SIP Methods

Filtering

Local Registrar

Authentication and Accounting

SIP Accounts

Dial Plan

Routing

Time Classes

SIP Status

DNS Override For SIP Requests

(Help)

Domain	Relay To						Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
+ bigtime.com	192.45.70.2	192.45.70.2		TCP			<input type="checkbox"/>
+ business.com	10.75.5.24	10.75.5.24		TCP			<input type="checkbox"/>

Step	Description																																																			
10.	<div><div>Configure Eth0 Inside Interface</div><div>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.</div></div> <div><div><div>Administration</div><div>Basic Configuration</div><div>Network</div><div>SIP Services</div><div>SIP Traffic</div><div>Failover</div><div>Virtual Private Networks</div><div>Quality of Service</div><div>Logging and Tools</div><div>About</div></div><div><div>Networks and Computers</div><div>Default Gateways</div><div>All Interfaces</div><div>VLAN</div><div>Eth0</div><div>Eth1</div><div>Eth2</div><div>Interface Status</div><div>PPPoE</div><div>Topology</div></div><div><div><div>General</div><div>Speed and Duplex</div></div><div><div>Physical device: eth0</div><div>This interface is: <input checked="" type="radio"/> Active <input type="radio"/> Inactive</div><div>Interface name: <input type="text" value="inside"/></div></div><div><div><input checked="" type="radio"/> Automatic negotiation</div><div><input type="radio"/> 100 Mbit/s, full duplex</div><div><input type="radio"/> 100 Mbit/s, half duplex</div><div><input type="radio"/> 10 Mbit/s, full duplex</div><div><input type="radio"/> 10 Mbit/s, half duplex</div></div></div><div><div>Directly Connected Networks (Help)</div><div><table><tr><th>Name</th><th>Address Type</th><th>DNS Name or IP Address</th><th>IP Address</th><th>Netmask / Bits</th><th>Network Address</th><th>Broadcast Address</th><th>VLAN Id</th><th>VLAN Name</th><th>Delete Row</th></tr><tr><td>inside</td><td>Static</td><td>10.75.5.63</td><td>10.75.5.63</td><td>255.255.255.0</td><td>10.75.5.0</td><td>10.75.5.255</td><td></td><td>-</td><td><input type="checkbox"/></td></tr></table><div>Add new rows <input type="text" value="1"/> rows.</div></div><div><div>Alias (Help)</div><div>Below are the ranges from which you can select aliases.</div><div><input type="text" value="10.75.5.1-10.75.5.254"/></div><div><table><tr><th>Name</th><th>DNS Name or IP Address</th><th>IP Address</th><th>Delete Row</th></tr></table><div>Add new rows <input type="text" value="1"/> rows.</div></div><div><div>Proxy ARP (Help)</div><div><table><tr><th rowspan="2">Get Network From</th><th colspan="3">Proxy ARPed Network</th><th rowspan="2">VLAN Id</th><th rowspan="2">VLAN Name</th><th rowspan="2">Delete Row</th></tr><tr><th>DNS Name or Network Address</th><th>Network Address</th><th>Netmask / Bits</th></tr></table><div>Add new rows <input type="text" value="1"/> rows.</div></div><div><div>Static Routing (Help)</div><div><table><tr><th colspan="3">Routed Network</th><th colspan="2">Router</th><th rowspan="2">Delete Row</th></tr><tr><th>DNS Name or Network Address</th><th>Network Address</th><th>Netmask / Bits</th><th>Dynamic</th><th>DNS Name or IP Address</th></tr><tr><td>10.75.10.0</td><td>10.75.10.0</td><td>24</td><td>-</td><td>10.75.5.1</td><td><input type="checkbox"/></td></tr></table></div></div></div></div></div></div>	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row	inside	Static	10.75.5.63	10.75.5.63	255.255.255.0	10.75.5.0	10.75.5.255		-	<input type="checkbox"/>	Name	DNS Name or IP Address	IP Address	Delete Row	Get Network From	Proxy ARPed Network			VLAN Id	VLAN Name	Delete Row	DNS Name or Network Address	Network Address	Netmask / Bits	Routed Network			Router		Delete Row	DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	10.75.10.0	10.75.10.0	24	-	10.75.5.1	<input type="checkbox"/>
Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row																																											
inside	Static	10.75.5.63	10.75.5.63	255.255.255.0	10.75.5.0	10.75.5.255		-	<input type="checkbox"/>																																											
Name	DNS Name or IP Address	IP Address	Delete Row																																																	
Get Network From	Proxy ARPed Network			VLAN Id	VLAN Name	Delete Row																																														
	DNS Name or Network Address	Network Address	Netmask / Bits																																																	
Routed Network			Router		Delete Row																																															
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address																																																
10.75.10.0	10.75.10.0	24	-	10.75.5.1	<input type="checkbox"/>																																															

11.

Configure Eth1 Outside Interface

The Eth1 outside interface is shown below for reference and completeness.

Administration

Basic Configuration

Network

SIP Services

SIP Traffic

Failover

Virtual Private Networks

Quality of Service

Logging and Tools

About

Networks and Computers

Default Gateways

All Interfaces

VLAN

Eth0

Eth1

Eth2

Interface Status

PPPoE

Topology

General

Speed and Duplex

Physical device: eth1

This interface is: ☒ Active ☐ Inactive

Interface name:

☒ 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	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
outside	Static	46.14.2.13	46.14.2.13	255.255.255.0	46.14.2.0	46.14.2.255		-	<input type="checkbox"/>

Add new rows

1

rows.

Alias [\(Help\)](#)

Below are the ranges from which you can select aliases.

Name	DNS Name or IP Address	IP Address	Delete Row
------	------------------------	------------	------------

Add new rows

1

rows.

Proxy ARP [\(Help\)](#)

Get Network From	DNS Name or Network Address	Network Address	Netmask / Bits	VLAN Id	VLAN Name	Delete Row
------------------	-----------------------------	-----------------	----------------	---------	-----------	------------

Add new rows

1

rows.

Static Routing [\(Help\)](#)

Routed Network			Router			Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
default	default		<input checked="" type="radio"/>	46.14.2.1	46.14.2.1	<input type="checkbox"/>

8. General Test Approach and Test Results

This section describes the compliance testing used to verify the interoperability of the Ingate SIParator with Session Manager and Communication Manager using SIP trunking. 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 main enterprise site and the 2nd site simulating a service provider service node using various codec settings and exercising common PBX features.

8.2. Test Results

The Ingate 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.

- Calls from both SIP and non-SIP endpoints between sites.
- 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.
- Extended telephony features using Communication Manager Feature Name Extensions (FNE) such as Conference On Answer, Call Park, Call Pickup, Automatic Redial 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 observation was made during the compliance test.

- When the SIParator was hard-reset to simulate the adverse condition of power outage, the SIP trunk between the SIParator and the Session Manager would not come back to the normal in-service state unless the Session Manager was restarted too.

9. Verification Steps

The following steps may be used to verify the configuration:

- Using System Manager **Monitoring** (from left navigation pane), verify that Entity Links to the SIParator and Communication Manager are up.
- 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.
- Verify that calls can be placed from both SIP and non-SIP endpoints between sites.

10. Conclusion

The Ingate SIParator passed compliance testing. These Application Notes describe the procedures required to configure the Ingate SIParator to interoperate with Session Manager and Communication Manager to support the network shown in **Figure 1** where Session Manager connects the SIParator to Communication Manager using SIP trunking interface.

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] *Avaya Aura™ Session Manager Manage Overview*, Doc # 03-603323
- [8] *Installing and Administering Avaya Aura™ Session Manager*, Doc # 03-603324
- [9] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc # 03-603325
- [10] *Ingate SIParator Getting Started Guide*
- [11] *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: Communication Manager Configuration at 2nd Site

This section contains specific configuration screens that are important to the Communication Manager at the 2nd site simulating a service provider service node.

The **node-names ip** form: note the SIParator and its public side IP address.

```
display node-names ip
```

		IP NODE NAMES
Name	IP Address	
SES	192.45.70.7	
SIParator	46.14.2.13	
procr	192.45.70.2	

The **signaling-group** form (for outgoing calls): note the **Far-end Node Name** and **Far-end Domain** settings.

```
display signaling-group 36
```

		SIGNALING GROUP
Group Number: 36	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
Near-end Node Name: procr	Far-end Node Name: SIParator	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
Far-end Domain: 46.14.2.13	Far-end Network Region: 1	
	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? y	Direct IP-IP Early Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

The **trunk-group** form (for outgoing calls): note the **Group Name** and **Signaling Group** settings.

```
display trunk-group 36                                     Page 1 of 21

                                TRUNK GROUP

Group Number: 36                      Group Type: sip      CDR Reports: y
  Group Name: ToSIParator             COR: 1             TN: 1             TAC: *036
  Direction: two-way                  Outgoing Display? n
  Dial Access? n                      Night Service:
  Queue Length: 0
  Service Type: tie                   Auth Code? n

                                      Signaling Group: 36
                                      Number of Members: 10
```

The **signaling-group** form (for incoming calls): note the **Far-end Node Name** and **Far-end Domain** settings.

```
display signaling-group 37                                SIGNALING GROUP

Group Number: 37                      Group Type: sip
                                Transport Method: tcp
  IMS Enabled? n

Near-end Node Name: procr              Far-end Node Name: SIParator
Near-end Listen Port: 5060             Far-end Listen Port: 5060
                                      Far-end Network Region: 1

Far-end Domain:

                                      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? y                Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n  Alternate Route Timer(sec): 6
```

The **trunk-group** form (for incoming calls): note the **Group Name** and **Signaling Group** settings.

```

display trunk-group 37                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 37          Group Type: sip          CDR Reports: y
  Group Name: FromSIParator    COR: 1          TN: 1          TAC: *037
  Direction: two-way          Outgoing Display? n
  Dial Access? n              Night Service:
  Queue Length: 0
  Service Type: tie           Auth Code? n

                                     Signaling Group: 37
                                     Number of Members: 10

```

The **public-unknown-numbering** form:

```

display public-unknown-numbering 0                         Page 1 of 2
                                     NUMBERING - PUBLIC/UNKNOWN FORMAT

Ext  Ext      Trk      CPN      Total
Len  Code      Grp(s)   Prefix   CPN
5    5                               Len
5                               5
                                     Total Administered: 1
                                     Maximum Entries: 240
                                     Number of Members: 10

```

The **aar analysis** form:

```

display aar analysis 3                                     Page 1 of 2
                                     AAR DIGIT ANALYSIS TABLE
                                     Location: all          Percent Full: 2

      Dialed      Total      Route      Call      Node      ANI
      String      Min  Max    Pattern    Type      Num      Req'd
30                               5    5    36      aar      n

```

The **route-pattern** form: note that trunk group 36 was defined for routing outgoing calls (to the SIParator for onward routing to the main enterprise site).

display route-pattern 36													Page 1 of 3	
Pattern Number: 36 Pattern Name: ToSIPArator														
SCCAN? n Secure SIP? n														
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC
No		Mrk	Lmt	List	Del	Digits						QSIG		
							Dgts						Intw	
1:	36	0										n	user	
2:												n	user	
3:												n	user	
4:												n	user	
5:												n	user	
6:												n	user	
BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature		PARM	No. Numbering		LAR		
0 1 2 M 4 W				Request						Dgts Format				
													Subaddress	
1:	y	y	y	y	y	n	n	rest				none		
2:	y	y	y	y	y	n	n	rest				none		
3:	y	y	y	y	y	n	n	rest				none		
4:	y	y	y	y	y	n	n	rest				none		
5:	y	y	y	y	y	n	n	rest				none		
6:	y	y	y	y	y	n	n	rest				none		

©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.