



Avaya Solution & Interoperability Test Lab

Application Notes for Cantata Technology Converged Services Platform 2090 SIP and ISDN-PRI interfaces with Avaya SIP Enablement Services and Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required for Cantata Technology Converged Services Platform (CSP) 2090 to successfully interoperate with Avaya SIP Enablement Services and Avaya Communication Manager via SIP and ISDN-PRI interfaces.

CSP 2090 is an application development switching platform targeted at service providers. In order to offer a complete solution for the end-user, the service provider must build an application to utilize the capabilities of the CSP 2090. To this end, for the compliance test, Cantata Technology provided a demo application that functioned as a SIP to ISDN-PRI gateway. The goal of the test was to verify the interoperability of the SIP and ISDN-PRI interfaces of the CSP 2090 with Avaya SIP Enablement Services and Avaya Communication Manager. No conclusion is drawn as to the compliance of the demo application itself or any other application that may be built on the CSP 2090.

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

1. Introduction

These Application Notes describe the configuration procedures required for Cantata Technology Converged Services Platform (CSP) 2090 to successfully interoperate with Avaya SIP Enablement Services (SES) and Avaya Communication Manager via SIP and ISDN-PRI interfaces.

CSP 2090 is an application development switching platform targeted at service providers. In order to offer a complete solution for the end-user, the service provider must build an application to utilize the capabilities of the CSP 2090. To this end, for the compliance test, Cantata Technology provided a demo application that functioned as a SIP to ISDN-PRI gateway. The goal of the test was to verify the interoperability of the SIP and ISDN-PRI interfaces of the CSP 2090 with Avaya SIP Enablement Services (SES) and Avaya Communication Manager. No conclusion is drawn as to the compliance of the demo application itself or any other application that may be built on the CSP 2090.

The CSP 2090 platform includes two software components which are necessary for software control and management of the CSP 2090. These applications may reside on the same or separate servers.

1. SwitchKit – This component provides a software API between a software application and the hardware. In the compliance test, the demo application used SwitchKit to communicate to the hardware.
2. Converged Services Administrator (CSA) – This component provides a user-friendly GUI to perform hardware configuration of the CSP 2090. CSA also uses SwitchKit to communicate with the hardware.

The CSP 2090 has two modes of operation: Call Agent Mode enabled or disabled. Call Agent Mode allows two IP endpoints communicating with the CSP 2090 to pass audio (RTP) packets directly between the endpoints without going through the CSP 2090. With Call Agent Mode disabled, the RTP packets pass through the CSP 2090. In either case, the signaling goes through the CSP 2090. This is analogous to the direct IP-to-IP audio feature (also known as media shuffling) on the Avaya Communication Manager. Direct IP-to-IP audio allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

For the compliance test, Call Agent Mode was disabled on the CSP 2090 since the CSP 2090 was used as a SIP to ISDN-PRI gateway. None of the calls switched through the CSP 2090 were connected SIP to SIP. Even with Call Agent Mode disabled, this would not automatically preclude the CSP 2090 from being one end of a media-shuffled call with Avaya Communication Manager. However, the CSP 2090 does not support the specific implementation of media shuffling required of Avaya Communication Manager. Thus, direct IP-to-IP audio is disabled on the Avaya Communication Manager SIP Signaling Group form. By disabling shuffling on the SIP Signaling Group form, shuffling can still take place between non-SIP (H.323) endpoints on the enterprise site.

Figure 1 shows the test configuration used for the compliance test. The test configuration is comprised of two enterprise sites with the CSP 2090 acting as a SIP to ISDN-PRI gateway between the two sites. In this manner, the interoperability of the SIP and ISDN-PRI interfaces with Avaya equipment could be tested in a single configuration. In a more typical configuration, the CSP 2090 would be located in the service provider network and provide SIP to ISDN-PRI gateway functionality to the PSTN for an enterprise site with SIP trunking to the service provider.

In the test configuration, site 1 has no on-site SIP capabilities and contains an Avaya S8300 Media Server running Avaya Communication Manager and an Avaya G700 Media Gateway. An ISDN-PRI trunk connects the Avaya G700 Media Gateway to the CSP 2090 which is also located at site 1. A Windows PC hosts the demo application, SwitchKit and CSA. Endpoints located at site 1 include an Avaya 4600 Series H.323 Telephone, an Avaya 6400D Series Digital Telephone and an Avaya 6200 Series Analog Telephone.

Site 2 is SIP-enabled with Avaya SES, an Avaya S8300 Media Server running Avaya Communication Manager and an Avaya G350 Media Gateway. A SIP trunking connection provides the signaling path across the IP network between Avaya SES and the CSP 2090. Endpoints located at site 2 include an Avaya 4600 Series SIP Telephone, Avaya 4600 Series H.323 Telephone, an Avaya 6400D Series Digital Telephone and an Avaya 6200 Series Analog Telephone.

The CSP 2090 requires three IP addresses. One IP address (192.168.1.74) is used for both management control by SwitchKit and SIP signaling. One IP address (192.168.1.77) is used for the IP Network Interface card that contains the VoIP modules. Lastly, a separate IP address (192.168.1.75) is used by the VoIP module to process the RTP media stream.

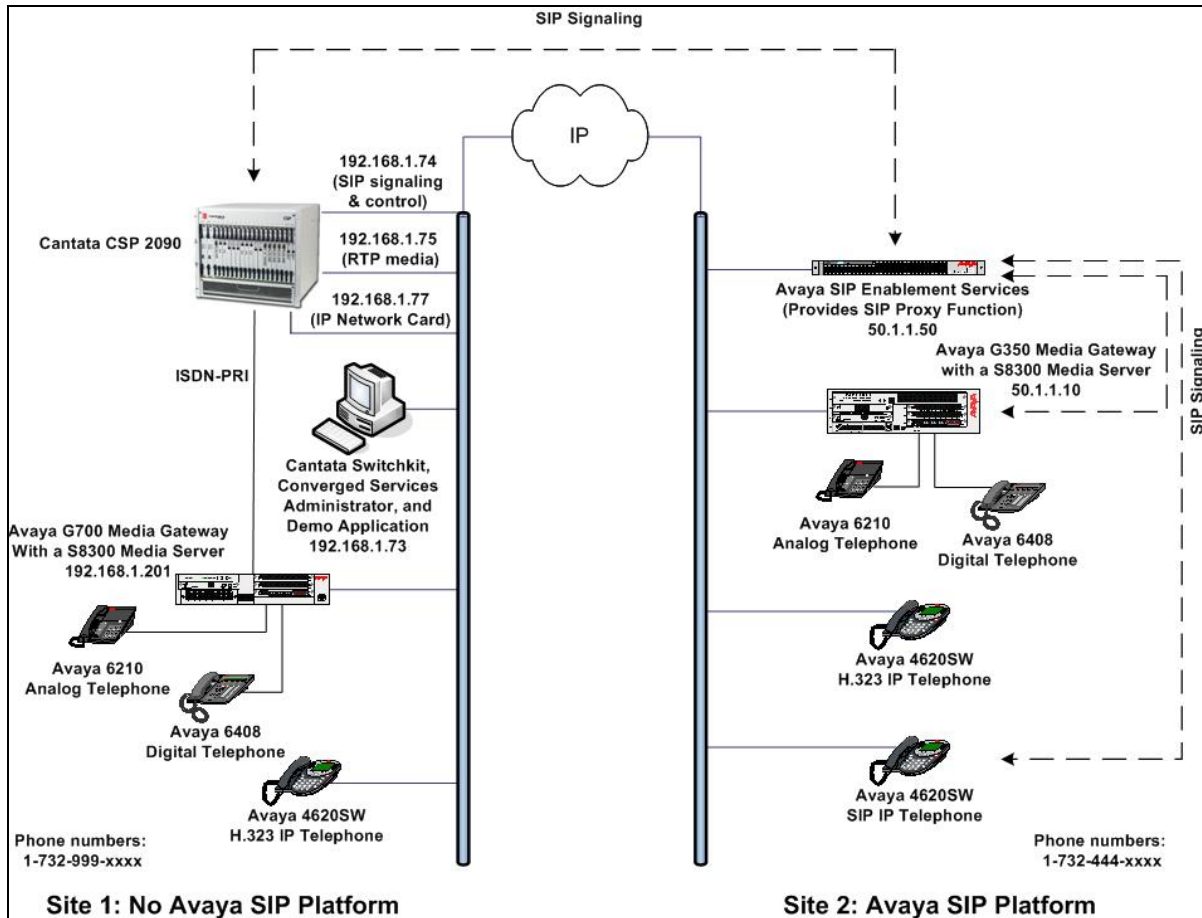


Figure 1: CSP 2090 Test Configuration

2. Equipment and Software Validated

The following equipment and software/firmware were used for the test configuration provided.

Equipment	Software/Firmware
Avaya S8300 Media Server	Avaya Communication Manager 3.1 (R013x.01.0.628.6)
Avaya G700 Media Gateway (Media Gateway Processor)	25.23.0
Avaya S8300 Media Server	Avaya Communication Manager 3.1 (R013x.01.0.628.6)
Avaya G350 Media Gateway (Media Gateway Processor)	25.23.0
Avaya SES	3.1 (3.1.0.0-018.0)
Avaya 4600 Series SIP Telephones	2.2.2 (4620SW)
Avaya 4600 Series IP (H.323) Telephones	2.3 (4620SW)
Avaya 6400D Series Digital Telephones	-

Equipment	Software/Firmware
Avaya 6200 Series Analog Telephones	-
Cantata Technology CSP 2090	8.3.1.127
Cantata Technology Switchkit	8.3.1.50
Cantata Technology Converged Services Administrator (CSA)	8.3.1.50

3. Configure Avaya Communication Manager

This section describes the necessary configuration on Avaya Communication Manager to interoperate with the ISDN-PRI and SIP interfaces of the CSP 2090. The following configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After completion of the configuration in this section, perform a **save translations** command to make the changes permanent.

3.1. Configure an ISDN-PRI Trunk Group

This section describes the configuration of an ISDN-PRI trunk group on Avaya Communication Manager. These steps were performed at site 1 in the test configuration shown in **Figure 1**.

Step	Description
1.	<p>Use the display system-parameters customer-options command to verify that the ISDN-PRI feature is enabled by the presence of a y next to the ISDN-PRI field. If the feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.</p> <pre> display system-parameters customer-options Page 4 of 10 OPTIONAL FEATURES Emergency Access to Attendant? y IP Stations? y Enable 'dadmin' Login? y Internet Protocol (IP) PNC? n Enhanced Conferencing? y ISDN Feature Plus? y Enhanced EC500? y ISDN Network Call Redirection? n Enterprise Survivable Server? n ISDN-BRI Trunks? y Enterprise Wide Licensing? n ISDN-PRI? y ESS Administration? n Local Survivable Processor? n Extended Cvg/Fwd Admin? n Malicious Call Trace? n External Device Alarm Admin? n Media Encryption Over IP? n Five Port Networks Max Per MCC? n Mode Code for Centralized Voice Mail? n Flexible Billing? n Forced Entry of Account Codes? n Multifrequency Signaling? y Global Call Classification? n Multimedia Appl. Server Interface (MASI)? n Hospitality (Basic)? y Multimedia Call Handling (Basic)? n Hospitality (G3V3 Enhancements)? n Multimedia Call Handling (Enhanced)? n IP Trunks? y IP Attendant Consoles? n (NOTE: You must logoff & login to effect the permission changes.) </pre>

Step	Description
2.	<p>Use the add ds1 <i>n</i> command where <i>n</i> is the location in the chassis of the DS1 board to be added. In the example below, the location is slot 1v3. Set the fields in bold to the values shown below. The Name field can be any descriptive name. The combination of Country Protocol (<i>l</i>) and Protocol Version (<i>b</i>) determine which version of ISDN-PRI will be used, specifically NI-2. Default values can be used for all other fields.</p> <pre> add ds1 1v3 Page 1 of 2 DS1 CIRCUIT PACK Location: 001V3 Name: PSTN Bit Rate: 1.544 Line Coding: b8zs Line Compensation: 1 Framing Mode: esf Signaling Mode: isdn-pri Connect: pbx Interface: user TN-C7 Long Timers? n Country Protocol: 1 Interworking Message: PROGress Protocol Version: b Interface Companding: mulaw CRC? n Idle Code: 11111111 DCP/Analog Bearer Capability: 3.1kHz T303 Timer(sec): 4 Slip Detection? n Near-end CSU Type: other Echo Cancellation? n Block Progress Indicator? n </pre>
3.	<p>Use the add signaling-group <i>n</i> command, where <i>n</i> is the number of an unused signaling group to be added. Set the fields in bold to the values shown below. The Primary D-Channel field is set to the 24th channel of the DS1 board in slot 1v3. This board was added to the configuration in the previous step. The Trunk Group for Channel Selection field will be populated at a later step after the trunk group has been created.</p> <pre> add signaling-group 3 Page 1 of 5 SIGNALING GROUP Group Number: 3 Group Type: isdn-pri Associated Signaling? y Max number of NCA TSC: 0 Primary D-Channel: 001V324 Max number of CA TSC: 0 Trunk Group for Channel Selection: Trunk Group for NCA TSC: Supplementary Service Protocol: a </pre>

Step	Description
4.	<p>Use the add trunk-group <i>n</i> command, where <i>n</i> is the number of an unused trunk group, to be added. Set the fields in bold to the values shown below. The Group Name can be any descriptive name. The TAC must be chosen to be consistent with the existing dial plan.</p> <pre> add trunk-group 3 Page 1 of 21 TRUNK GROUP Group Number: 3 Group Type: isdn CDR Reports: y Group Name: PSTN COR: 1 TN: 1 TAC: 103 Direction: two-way Outgoing Display? n Carrier Medium: PRI/BRI Dial Access? y Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: tie Auth Code? n TestCall ITC: rest Far End Test Line No: TestCall BCC: 4 </pre>
5.	<p>On Page 5, enter the group members. For each DS1 port to be added as a member of the trunk group, enter the port number in the Port field and the corresponding signaling group for that port in the Sig Grp field. The Code field is filled in automatically. In the compliance test, each of the 23 bearer channels of the DS1 board added in Step 2 were added to this group. The signaling channel for each of these ports is the signaling channel added in Step 3.</p> <pre> add trunk-group 3 Page 5 of 21 TRUNK GROUP Administered Members (min/max): 1/23 GROUP MEMBER ASSIGNMENTS Total Administered Members: 23 Port Code Sfx Name Night Sig Grp 1: 001V301 MM710 2: 001V302 MM710 3: 001V303 MM710 4: 001V304 MM710 5: 001V305 MM710 6: 001V306 MM710 7: 001V307 MM710 8: 001V308 MM710 9: 001V309 MM710 10: 001V310 MM710 11: 001V311 MM710 12: 001V312 MM710 13: 001V313 MM710 14: 001V314 MM710 15: 001V315 MM710 </pre>

Step	Description
6.	<p>Use the change signaling-group 3 command to return to the Signaling Group form shown in Step 3. Set the Trunk Group for Channel Selection field to the number of the trunk group created in Step 4.</p> <div> <pre> change signaling-group 3 SIGNALING GROUP Page 1 of 5 Group Number: 3 Group Type: isdn-pri Associated Signaling? y Max number of NCA TSC: 0 Primary D-Channel: 001V324 Max number of CA TSC: 0 Trunk Group for NCA TSC: Trunk Group for Channel Selection: 3 Supplementary Service Protocol: a </pre> </div>
7.	<p>The compliance testing used Automatic Route Selection (ARS) to define route pattern 1 as the route for all outbound calls. For more information on ARS see [1] and [2].</p> <p>The example below shows the route pattern used in the compliance test for all outbound traffic. The Pattern Name can be any descriptive name. The Grp No. is set to the trunk-group number for the trunk to be used. The FRL field defines the facility restriction level for this route pattern. The value of 0 is the least restrictive. The Prefix Mark field (Pfx Mrk) is set to 1. The Prefix Mark sets the requirement for sending a prefix digit 1. Setting the Pfx Mrk field to 1, results in a 1 being prefixed to any 10-digit number. An 11-digit number, presumably already preceded with a 1, is left unchanged. Default values for all other fields can be used.</p> <div> <pre> change route-pattern 1 Pattern Number: 1 Pattern Name: PSTN SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted No Mrk Lmt List Del Digits Dgts 1: 3 0 1 2: 3: 4: 5: 6: DCS/ IXC QSIG Intw 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 3 4 W Request 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>

3.2. Configure SIP Trunking

This section describes the steps for configuring a SIP trunk group between Avaya Communication Manager and Avaya SES. Avaya SES acts as a SIP proxy for site 2 in **Figure 1**. Thus, the CSP 2090 will direct all SIP traffic bound for site 2 to the Avaya SES located there. Avaya SES will then forward the inbound SIP traffic to Avaya Communication Manager. The path is the same in the reverse direction with SIP signaling flowing from Avaya Communication Manager to Avaya SES to the CSP 2090. As a result, the SIP trunk group configured in this section carries all the SIP signaling and associated media streams bound to site 2 from the CSP 2090 and vice versa.

These steps were performed at site 2 in the configuration shown in **Figure 1**.

Step	Description
1.	<p>Use the display system-parameters customer-options command to verify that sufficient SIP trunk capacity exists. On Page 2, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. 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 a SIP service provider will use two SIP trunks, as will a call between two local SIP extensions. A call between a non-SIP telephone and a SIP service provider will only use one trunk.</p> <p>The license file installed on the system controls the maximum permitted. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.</p> <div><pre>display system-parameters customer-options Page 2 of 10 OPTIONAL FEATURES IP PORT CAPACITIES USED Maximum Administered H.323 Trunks: 100 10 Maximum Concurrently Registered IP Stations: 20 0 Maximum Administered Remote Office Trunks: 0 0 Maximum Concurrently Registered Remote Office Stations: 0 0 Maximum Concurrently Registered IP eCons: 0 0 Max Concur Registered Unauthenticated H.323 Stations: 0 0 Maximum Video Capable H.323 Stations: 0 0 Maximum Video Capable IP Softphones: 0 0 Maximum Administered SIP Trunks: 100 24 Maximum Number of DS1 Boards with Echo Cancellation: 0 0 Maximum TN2501 VAL Boards: 0 0 Maximum G250/G350/G700 VAL Sources: 5 1 Maximum TN2602 Boards with 80 VoIP Channels: 0 0 Maximum TN2602 Boards with 320 VoIP Channels: 0 0 Maximum Number of Expanded Meet-me Conference Ports: 10 0 (NOTE: You must logoff & login to effect the permission changes.)</pre></div>

Step	Description																																													
2.	<p>Use the change node-name ip command to assign the node name and IP address for Avaya SES at site 2. In this case, <i>SES</i> and <i>50.1.1.50</i> are being used, respectively. The node name <i>SES</i> will be used throughout the other configuration forms of Avaya Communication Manager. In this example, <i>procr</i> and <i>50.1.1.10</i> are the name and IP address assigned to the Avaya S8300 Media Server.</p> <div><div>change node-names ip</div><div><div></div><div>Page 1 of 1</div></div><table><tr><th colspan="2"></th><th colspan="4">IP NODE NAMES</th><th colspan="3"></th></tr><tr><th>Name</th><th colspan="4">IP Address</th><th>Name</th><th colspan="3">IP Address</th></tr><tr><td>SES</td><td>50</td><td>.1</td><td>.1</td><td>.50</td><td></td><td>.</td><td>.</td><td>.</td></tr><tr><td>default</td><td>0</td><td>.0</td><td>.0</td><td>.0</td><td></td><td>.</td><td>.</td><td>.</td></tr><tr><td>procr</td><td>50</td><td>.1</td><td>.1</td><td>.10</td><td></td><td>.</td><td>.</td><td>.</td></tr></table></div>			IP NODE NAMES							Name	IP Address				Name	IP Address			SES	50	.1	.1	.50		.	.	.	default	0	.0	.0	.0		.	.	.	procr	50	.1	.1	.10		.	.	.
		IP NODE NAMES																																												
Name	IP Address				Name	IP Address																																								
SES	50	.1	.1	.50		.	.	.																																						
default	0	.0	.0	.0		.	.	.																																						
procr	50	.1	.1	.10		.	.	.																																						

Step	Description
3.	<p>Use the change ip-network-region <i>n</i> command, where <i>n</i> is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the IP region. Select an IP network region that will contain the Avaya SES server. The association between this IP Network Region and the Avaya SES server will be done on the Signaling Group form as shown in Step 5. In the case of the compliance test, the same IP network region that contains the Avaya S8300 Media Server was selected to contain the Avaya SES server. By default, the Media Server is in IP Network Region 1.</p> <p>On the IP Network Region form:</p> <ul style="list-style-type: none"> ▪ The Authoritative Domain field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is <i>devcon.com</i>. This name will appear in the “From” header of SIP messages originating from this IP region. ▪ By default, IP-IP Direct Audio (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G350 Media Gateway. This is true for both intra-region and inter-region IP-IP Direct Audio. Shuffling can be further restricted at the trunk level on the Signaling Group form. ▪ The Codec Set is set to the number of the IP codec set to be used for calls within this IP network region. In this configuration, this codec set will apply to all calls to and from the CSP 2090 as well as any IP phone (H.323 or SIP) within the enterprise. If different IP network regions are used for the Avaya S8300 Media Server and the Avaya SES server, then Page 3 of each IP Network Region form must be used to specify the codec set for inter-region communications. ▪ The default values can be used for all other fields. <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <pre> change ip-network-region 1 Page 1 of 19 IP NETWORK REGION Region: 1 Location: 1 Authoritative Domain: devcon.com Name: 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? y UDP Port Max: 3027 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 34 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 </pre> </div>

Step	Description																
4.	<p>Use the change ip-codec-set <i>n</i> command, where <i>n</i> is the codec set value specified in Step 3, to enter the supported audio codecs for calls routed to Avaya SES. Multiple codecs can be listed in priority order to allow the codec to be negotiated during call establishment. The list should include the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. It must also include the preferred codec configured on the CSP 2090. The example below shows the values used in the compliance test.</p> <div><div>change ip-codec-set 1</div><div>Page 1 of 2</div><div>IP Codec Set</div><div>Codec Set: 1</div><table><thead><tr><th>Audio Codec</th><th>Silence Suppression</th><th>Frames Per Pkt</th><th>Packet Size(ms)</th></tr></thead><tbody><tr><td>1: G.711MU</td><td>n</td><td>2</td><td>20</td></tr><tr><td>2: G.729B</td><td>n</td><td>2</td><td>20</td></tr><tr><td>3:</td><td></td><td></td><td></td></tr></tbody></table></div>	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	1: G.711MU	n	2	20	2: G.729B	n	2	20	3:			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)														
1: G.711MU	n	2	20														
2: G.729B	n	2	20														
3:																	

Step	Description
5.	<p>Use the add signaling group <i>n</i> command, where <i>n</i> is the number of an unused signaling group, to create the SIP signaling group as follows:</p> <ul style="list-style-type: none"> ▪ Set the Group Type field to <i>sip</i>. ▪ The Transport Method field will default to <i>tls</i> (Transport Layer Security). TLS is the only link protocol that is supported for communication between Avaya SES and Avaya Communication Manager. ▪ Specify the Avaya S8300 Media Server (node name <i>procr</i>) and the Avaya SES Server (node name <i>SES</i>) as the two ends of the signaling group in the Near-end Node Name field and the Far-end Node Name fields, respectively. These field values are taken from the IP Node Names form shown in Step 2. For other Media Server platforms which use a C-LAN board, the near (local) end of the SIP signaling group will be the C-LAN board instead of the Media Server. ▪ Ensure that the recommended TLS port value of <i>5061</i> is configured in the Near-end Listen Port and the Far-end Listen Port fields. ▪ In the Far-end Network Region field, enter the IP Network Region value assigned in the IP Network Region form in Step 3. This defines which IP network region contains the Avaya SES server. If the Far-end Network Region field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the inter-region connectivity for the pair of network regions. ▪ Enter the domain name of Avaya SES in the Far-end Domain field. In this configuration, the domain name is <i>devcon.com</i> as configured in Step 3. This domain is specified in the Uniform Resource Identifier (URI) of the SIP “To” header in the INVITE message. ▪ The Direct IP-IP Audio Connections field is set to <i>n</i>, since this solution does not support this functionality. ▪ The DTMF over IP field must be set to the default value of <i>rtp-payload</i> for a SIP trunk. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833. ▪ The default values for the other fields may be used. <div data-bbox="315 1360 1414 1850" style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <pre> change signaling-group 1 SIGNALING GROUP Page 1 of 1 Group Number: 1 Group Type: sip Transport Method: tls Near-end Node Name: procr Far-end Node Name: SES Near-end Listen Port: 5061 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Domain: devcon.com Bypass If IP Threshold Exceeded? y DTMF over IP: rtp-payload Direct IP-IP Audio Connections? n IP Audio Hairpinning? y Session Establishment Timer(min): 120 </pre> </div>


Step	Description
6.	<p>Add a SIP trunk group by using the add trunk-group <i>n</i> command, where <i>n</i> is the number of an unused trunk group. For the compliance test, trunk group number 1 was chosen.</p> <p>On Page 1, set the fields to the following values:</p> <ul style="list-style-type: none"> ▪ Set the Group Type field to <i>sip</i>. ▪ Choose a descriptive Group Name. ▪ Specify an available trunk access code (TAC) that is consistent with the existing dial plan. ▪ Set the Service Type field to <i>tie</i>. ▪ Specify the signaling group associated with this trunk group in the Signaling Group field as previously specified in Step 5. ▪ Specify the Number of Members supported by this SIP trunk group. As mentioned earlier, each SIP call between two SIP destinations (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to a SIP service provider will use two SIP trunks, as will a call between two local SIP extensions. A call between a non-SIP telephone and a SIP service provider will only use one trunk. ▪ Use the default values for the other fields. <div data-bbox="315 961 1414 1304"> <pre> add trunk-group 1 Page 1 of 21 TRUNK GROUP Group Number: 1 Group Type: sip CDR Reports: y Group Name: To SES 50.1.1.50 COR: 1 TN: 1 TAC: 101 Direction: two-way Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Signaling Group: 1 Number of Members: 24 </pre> </div>

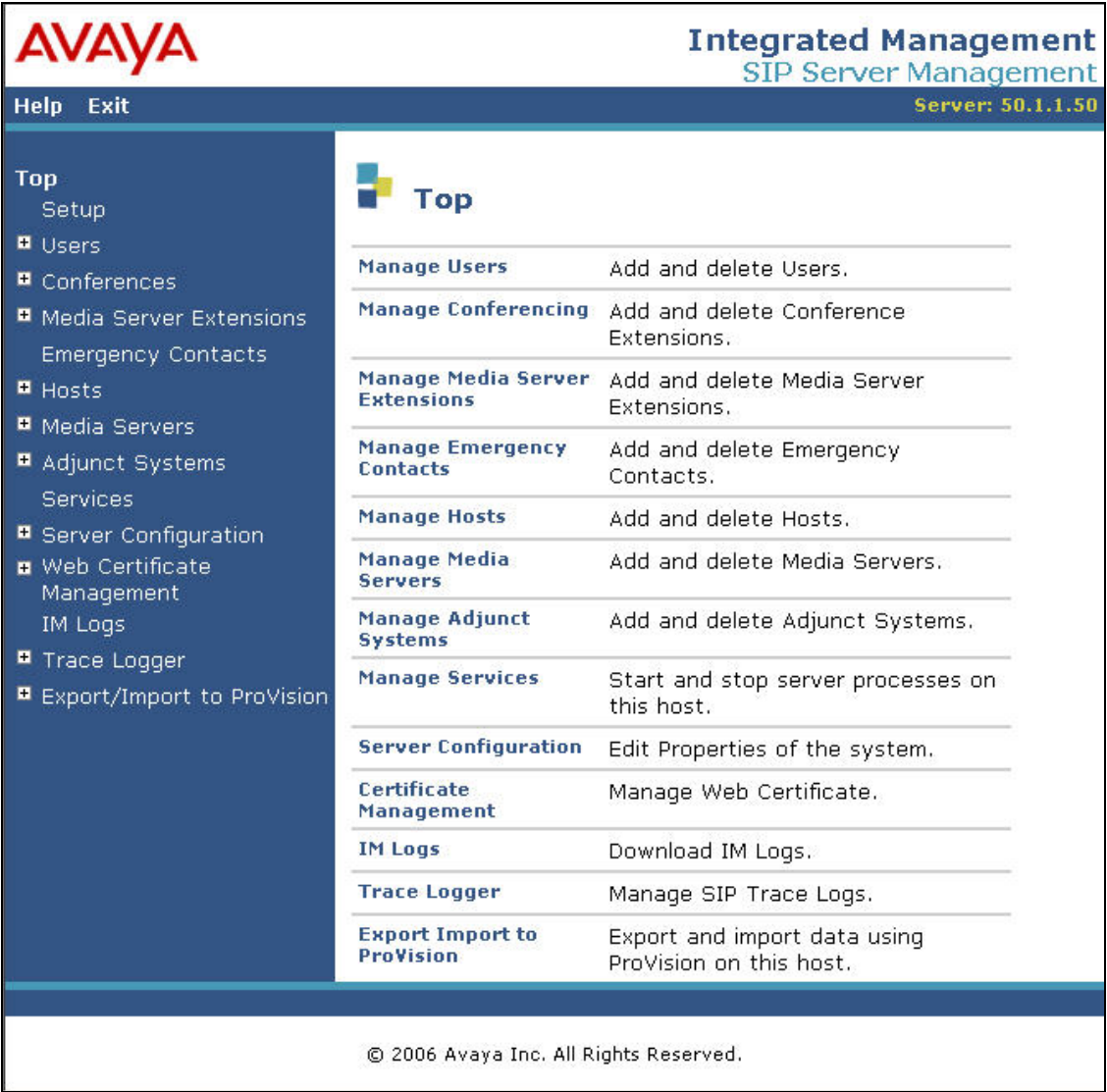
Step	Description
7.	<p>On Page 2:</p> <ul style="list-style-type: none"> Set the Numbering Format field to <i>public</i>. This field specifies the format of the calling party number sent to the far-end. Use the default values for the other fields. <pre> change trunk-group 1 Page 3 of 21 TRUNK FEATURES ACA Assignment? n Measured: none Maintenance Tests? y Numbering Format: public Prepend '+' to Calling Number? n Replace Unavailable Numbers? n </pre>
8.	<p>Use the change public-unknown numbering 0 command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in Step 6. In the example shown below, all calls originating from a 5 digit extension beginning with 4 and routed across trunk group 1 will be sent as a 5-digit calling number. This calling party number will be sent to the far-end in the SIP “From” header.</p> <pre> change public-unknown-numbering 0 Page 1 of 2 NUMBERING - PUBLIC/UNKNOWN FORMAT Total Ext Ext Trk CPN CPN Ext Ext Trk CPN Total Len Code Grp(s) Prefix Len Len Code Grp(s) Prefix Len 5 4 1 5 </pre>
9.	<p>Use the change inc-call-handling-trmt trunk-group <i>n</i> command, where <i>n</i> is the SIP trunk group number, to map incoming DID calls to the proper extension(s). For the compliance test, DID numbers of the form 1-732-999-xxxx were assigned to site 1 and numbers of the form 1-732-444-xxxx were assigned to site 2. The example below shows the configuration at site 2. The entry defines that all incoming calls on trunk group 1 with 11 digits starting with 173244 will have the first 6 digits deleted. The remaining 5 digits map directly to a local 5 digit extension on Avaya Communication Manager. For example, DID number 1-732-444-0001 maps to extension 40001.</p> <pre> change inc-call-handling-trmt trunk-group 1 Page 1 of 3 INCOMING CALL HANDLING TREATMENT Service/ Called Called Del Insert Feature Len Number tie 11 173244 6 </pre>

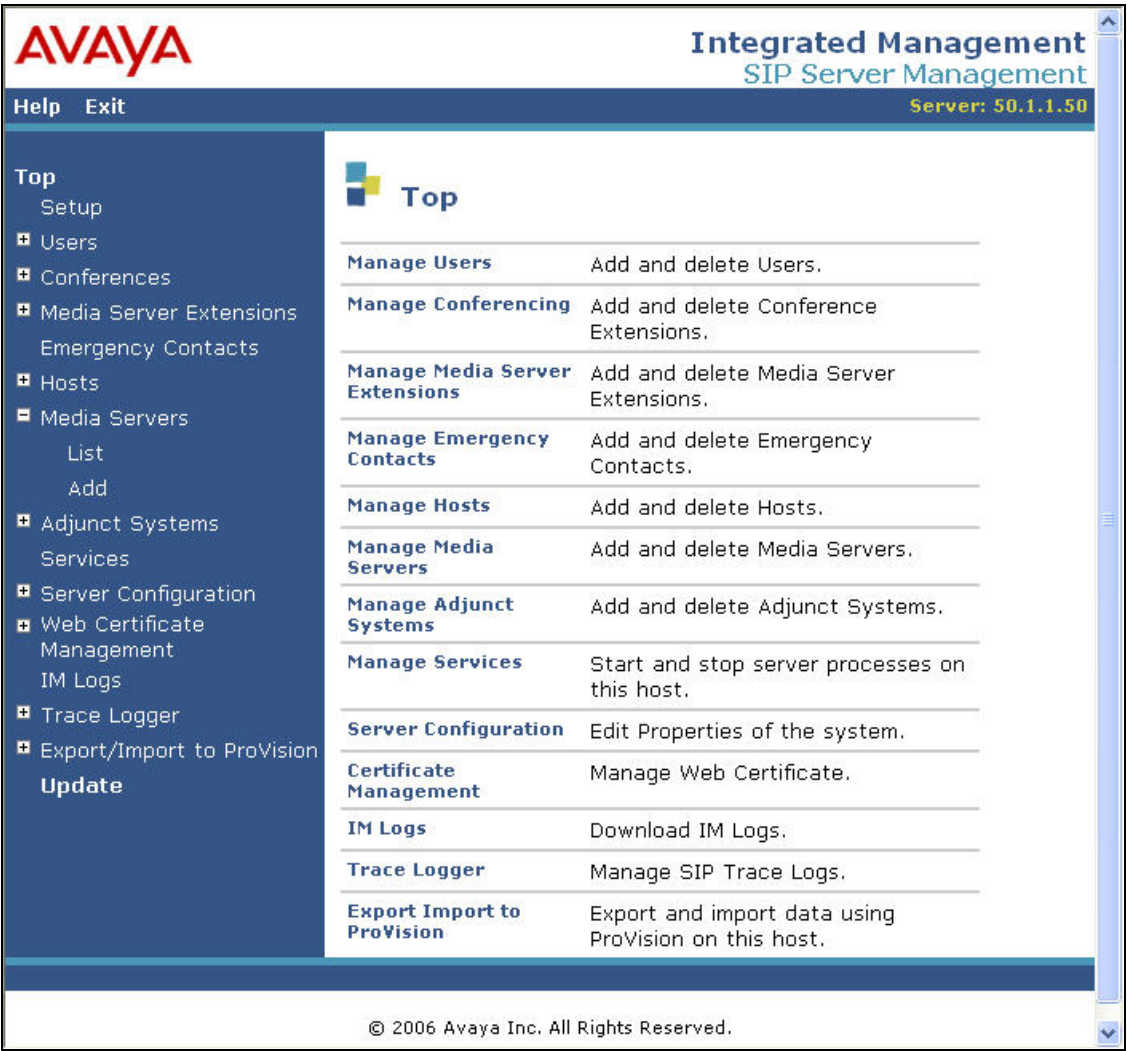
Step	Description
10.	<p>The compliance testing used Automatic Route Selection (ARS) to define route pattern 1 as the route for all outbound calls. For more information on ARS see [1] and [2].</p> <p>The example below shows the route pattern used in the compliance test for all outbound traffic. The Pattern Name can be any descriptive name. The Grp No. is set to the trunk-group number for the trunk to be used. The FRL field defines the facility restriction level for this route pattern. The value of 0 is the least restrictive. The Pfx Mrk field is set to 1. The Prefix Mark sets the requirement for sending a prefix digit 1. Setting the Pfx Mrk field to 1, results in a 1 being prefixed to any 10-digit number. An 11-digit number, presumably already preceded with a 1, is left unchanged. Default values for all other fields can be used.</p> <pre> change route-pattern 2 Pattern Number: 1 Pattern Name: SIP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted No Lmt List Del Digits Dgts 1: 1 0 1 2: 3: 4: 5: 6: DCS/ IXC QSIG Intw 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 3 4 W Request Dgts Format Subaddress 1: y y y y y n n rest 2: y y y y y n n rest 3: y y y y y n n rest 4: y y y y y n n rest 5: y y y y y n n rest 6: y y y y y n n rest none none none none none none </pre>
11.	<p>Use the change locations command to assign the route pattern to the location. Only one location created by default, known as Main, exists for site 2. Enter the route pattern number from the previous step in the Proxy Sel. Rte Pat. field. Use the default values for all other fields.</p> <pre> change locations LOCATIONS ARS Prefix 1 Required For 10-Digit NANP Calls? y Loc. Name Timezone Rule NPA ARS Attd Pre- Proxy Sel. No. Offset FAC FAC fix Rte. Pat. 1: Main + 00:00 0 2: 3: </pre>

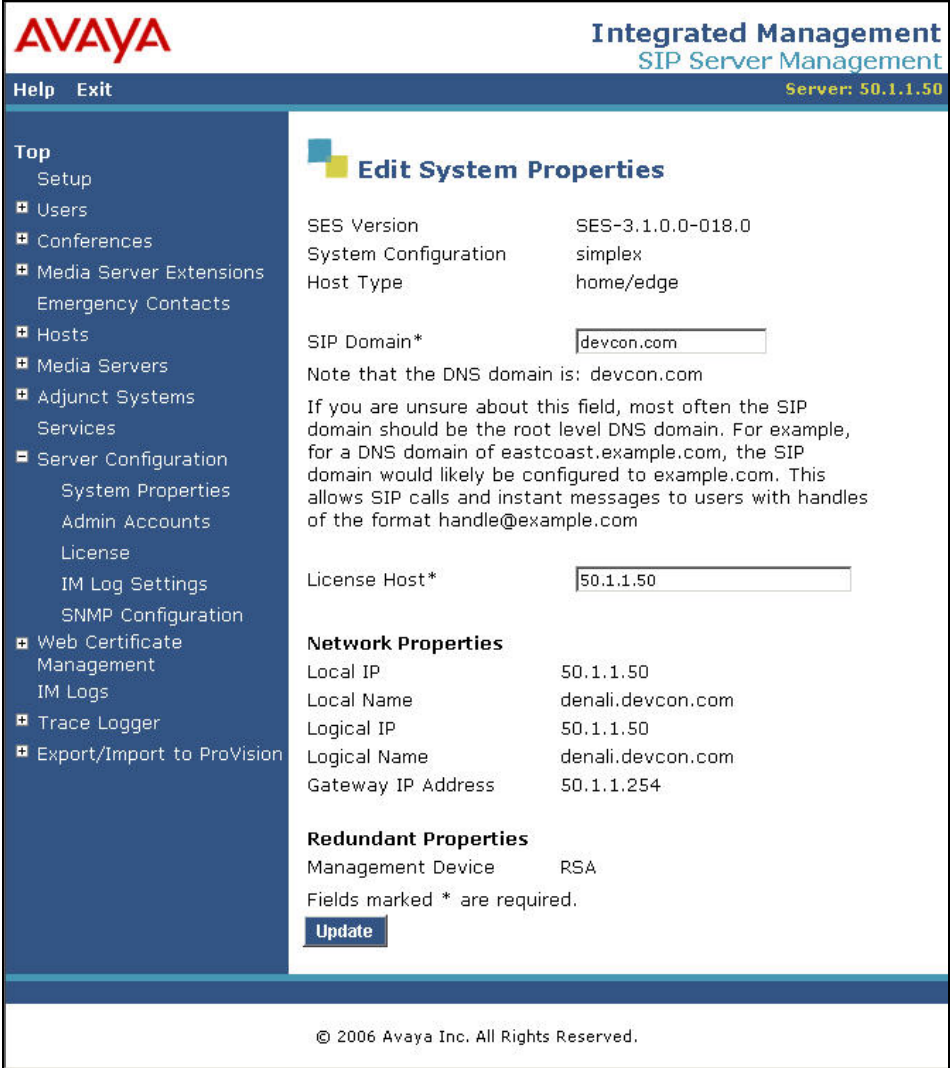
4. Configure Avaya SES

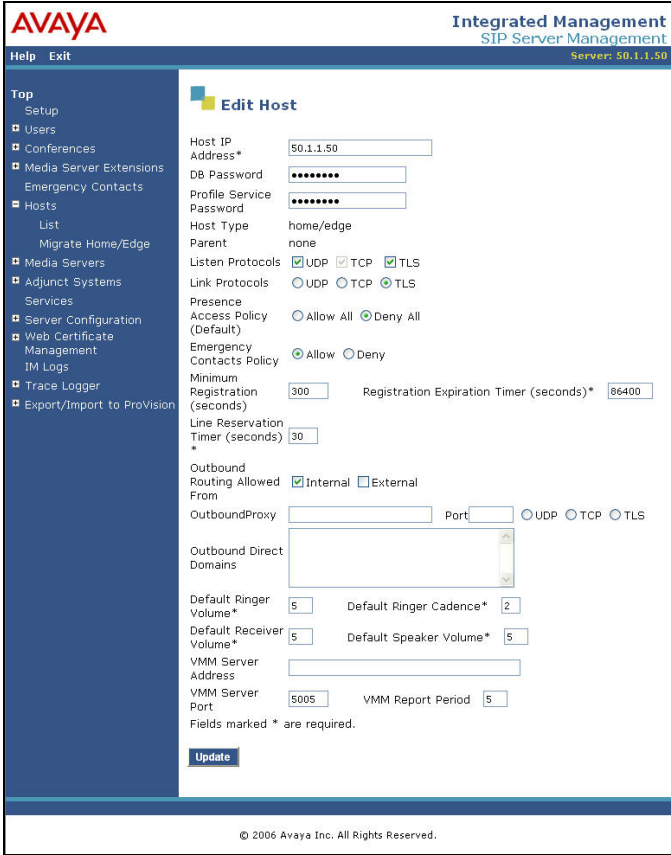
This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that Avaya SES software and the license file have already been installed on the server. During the software installation, the installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. For additional information on these installation tasks, refer to [3].

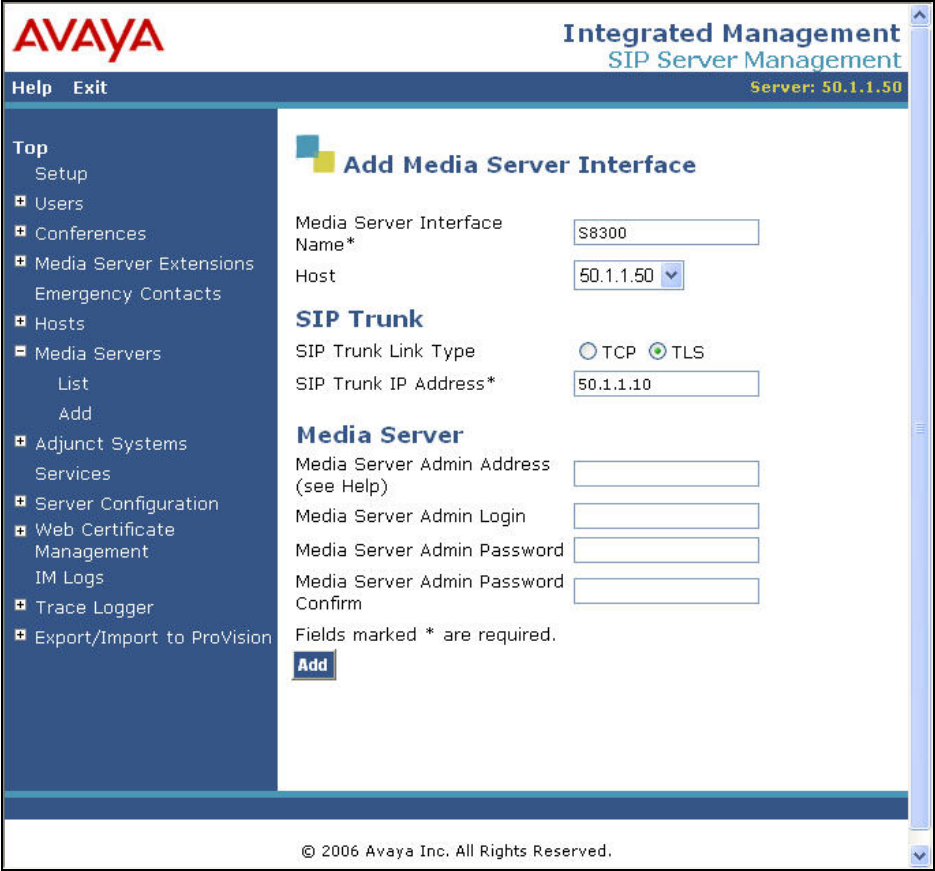
Step	Description
1.	<p>Access the Avaya SES administration web interface, by entering <a href="http://<ip-addr>/admin">http://<ip-addr>/admin as the URL in an Internet browser, where <ip-addr> is the IP address of Avaya SES.</p> <p>Log in with the appropriate credentials and then select the Launch Administration Web Interface link from the main page as shown below.</p> 

Step	Description
2.	<p>The Avaya SES Administration Home Page shown below will be displayed.</p> 

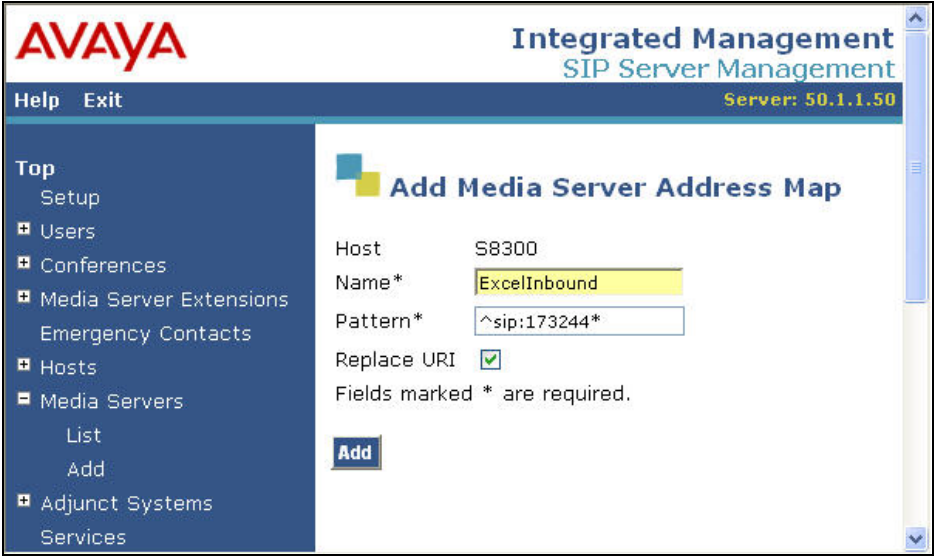
Step	Description
3.	<p>After making changes within Avaya SES, it is necessary to commit the database changes using the Update link that appears when changes are pending. Perform this step by clicking on the Update link found in the bottom of the blue navigation bar on the left side of any of the Avaya SES administration pages as shown in below. It is recommended that this be done after making each set of changes described in the following steps.</p> 

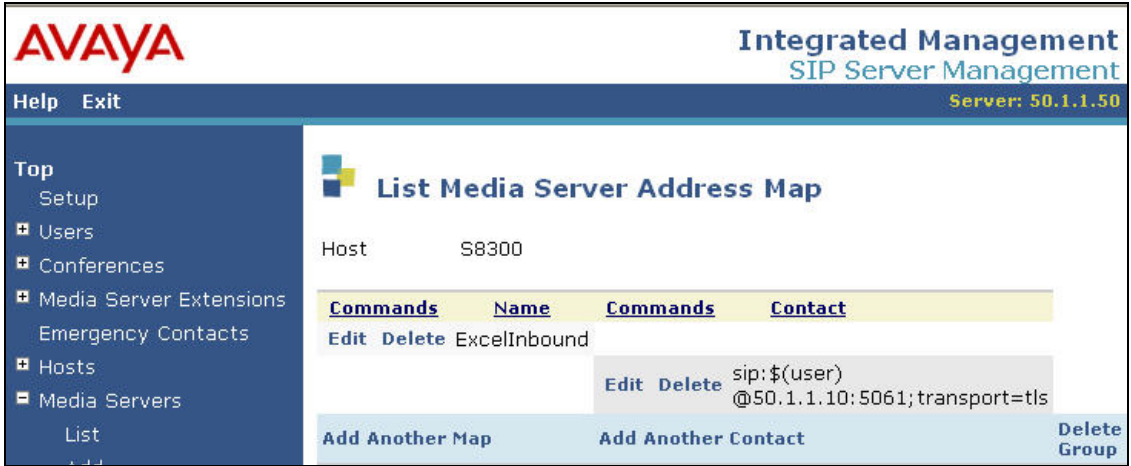
Step	Description
4.	<p>From the left pane of the administration web interface, expand the Server Configuration option and select System Properties. This page displays the software version in the SES version field and the network properties entered via the installation script during the installation process.</p> <p>On the Edit System Properties page:</p> <ul style="list-style-type: none"> Enter the SIP Domain name assigned to Avaya SES. This must match the Authoritative Domain field configured on Avaya Communication Manager shown in Section 3.2, Step 3. Enter the License Host field. This is the host name, the fully qualified domain name, or the IP address of the SIP proxy server that is running the WebLM application and has the associated license file installed. After configuring the Edit System Properties page, click the Update button.  <p>The screenshot shows the 'Edit System Properties' page in the Avaya Integrated Management SIP Server Management interface. The left sidebar contains a navigation tree with 'Server Configuration' expanded, showing 'System Properties' selected. The main content area displays the following information:</p> <ul style="list-style-type: none"> SES Version: SES-3.1.0.0-018.0 System Configuration: simplex Host Type: home/edge SIP Domain*: devcon.com (with a note: 'Note that the DNS domain is: devcon.com' and a detailed explanation of the domain format) License Host*: 50.1.1.50 Network Properties: <ul style="list-style-type: none"> Local IP: 50.1.1.50 Local Name: denali.devcon.com Logical IP: 50.1.1.50 Logical Name: denali.devcon.com Gateway IP Address: 50.1.1.254 Redundant Properties: <ul style="list-style-type: none"> Management Device: RSA <p>At the bottom, there is a note 'Fields marked * are required.' and an 'Update' button. The footer of the page reads '© 2006 Avaya Inc. All Rights Reserved.'</p>

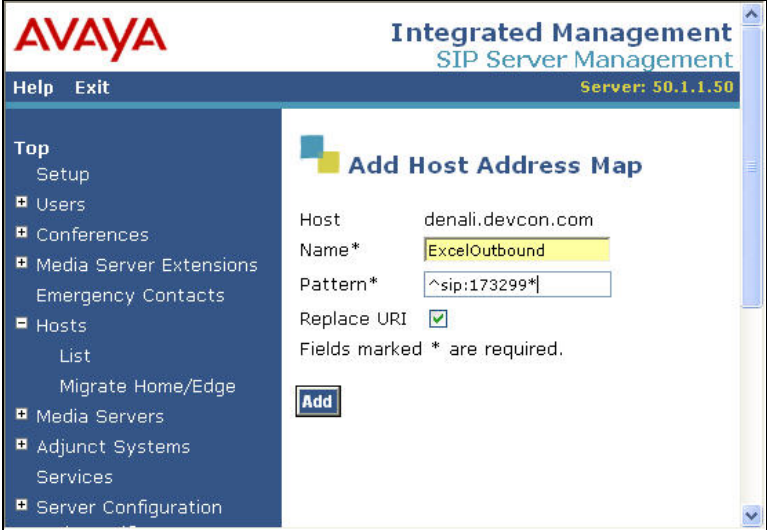
Step	Description
5.	<p>After setting up the domain on the Edit System Properties page, create a host computer entry for Avaya SES. The following example shows the Edit Host page since the host had already been added to the system.</p> <p>The Edit Host page shown below is accessible by clicking on the Hosts link in the left pane and then clicking on the edit option under the Commands section of the subsequent page that is displayed.</p> <ul style="list-style-type: none"> Enter the Logical IP or Logical Name of this server in the Host IP Address field shown in Step 4. Enter the DB Password that was specified while running the installation script during the system installation. Configure the Host Type field. Since only one Avaya SES server exists in the enterprise network of the test configuration, the Avaya SES server provides the functionality of both a <i>home</i> and <i>edge</i> server. Thus, the Host Type is configured as <i>home/edge</i>. The default values for the other fields may be used. Click the Update button. 

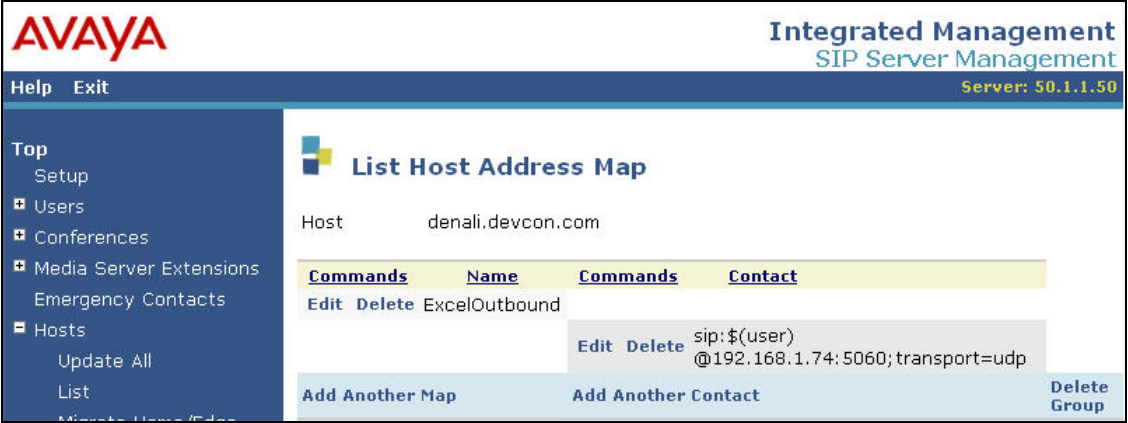
Step	Description
6.	<p>From the left pane of the administration web interface, expand the Media Server option and select Add to add the Avaya Media Server to the list of media servers known to Avaya SES. Adding the media server will create the Avaya SES side of the SIP trunk previously created in Avaya Communication Manager.</p> <p>On the Add Media Server page, enter the following information:</p> <ul style="list-style-type: none"> ▪ A descriptive name in the Media Server Interface Name field (e.g. S8300). ▪ In the Host field, select the name of the Avaya SES server from the pull-down menu that will serve as the SIP proxy for this media server. Since there is only one Avaya SES server in this configuration, the Host field is set to the host name shown in Step 4. ▪ Select TLS (Transport Link Security) for the Link Type. TLS provides encryption at the transport layer. TLS is the only link protocol that is supported for communication between Avaya SES and Avaya Communication Manager. ▪ Enter the IP address of the Avaya S8300 Media Server in the SIP Trunk IP Address field. In other media server platforms, which use a C-LAN board, the SIP Trunk IP Address would be the IP address of the C-LAN board. ▪ Use the default values for all other fields. ▪ After completing the Add Media Server page, click the Add button. 

Step	Description
7.	<p data-bbox="315 233 1435 338">Inbound SIP calls arriving at Avaya SES are routed to the appropriate Avaya Communication Manager for termination services. This routing is specified in a Media Server Address Map configured on Avaya SES.</p> <p data-bbox="315 380 1435 632">This routing compares the Uniform Resource Identifier (URI) of an incoming INVITE message to the pattern configured in the Media Server Address Map, and if there is a match, the call is routed to the designated Avaya Communication Manager. The URI usually takes the form of <i>sip:user@domain</i>, where <i>domain</i> can be a domain name or an IP address. Patterns must be specific enough to uniquely route incoming calls to the proper destination if there are multiple Avaya Media Servers supported by the Avaya SES server.</p> <p data-bbox="315 674 1435 814">In this test configuration, only incoming calls from site 1 require a Media Server Address Map entry. Calls originated by Avaya SIP telephones configured as OPS stations are automatically routed to Avaya Communication Manager by the assignment of a media server extension to that phone.</p> <p data-bbox="315 856 1435 926">From site 1, the <i>user</i> portion of the SIP URI will contain the incoming direct inward dialed telephone number.</p> <p data-bbox="315 968 1435 1003">An example of a SIP URI in an INVITE message received from site 1 would be:</p> <p data-bbox="412 1045 802 1081">sip: 17324440001@50.1.1.50.</p> <p data-bbox="315 1123 1435 1159">In this example, the user portion is the called party number 17324440001.</p> <p data-bbox="315 1201 1435 1291">For the compliance test, phone numbers beginning with the prefix of 1732999 were assigned to site 1. Phone numbers beginning with the prefix of 1732444 were assigned to site 2.</p> <p data-bbox="315 1333 1435 1438">Thus, the media server address map strategy was to define pattern matches for the first 6 digits in the URI and have Avaya SES forward the messages that match to the appropriate media server.</p> <p data-bbox="315 1480 1435 1516">To configure a Media Server Address Map:</p> <ul data-bbox="363 1516 1435 1837" style="list-style-type: none"> <li data-bbox="363 1516 1435 1585">▪ Expand the Media Servers option in the left pane of the administration web interface and select List. This will display the List Media Servers page. <li data-bbox="363 1585 1435 1654">▪ Click on the Map link associated with the appropriate media server to display the List Media Server Address Map page. <li data-bbox="363 1654 1435 1766">▪ Click on the Add Map In New Group link. The page shown below is displayed. The Host field displays the name of the media server to which this map applies. <li data-bbox="363 1766 1435 1801">▪ Enter a descriptive name in the Name field. <li data-bbox="363 1801 1435 1837">▪ Enter the regular expression to be used for the pattern matching in the Pattern

Step	Description
	<p>field. The example below shows the pattern specification for DID numbers assigned to site 2: <code>^sip:173244*</code>. This expression will match any SIP URI that begins with the text string <code>sip:173244</code>. Based on the value of the Host field, these SIP calls will then be routed to host S8300. Appendix A provides a detailed description of the syntax for address map patterns.</p> <ul style="list-style-type: none"> Click the Add button once the form is completed. 

Step	Description
8.	<p>After configuring the media server address map, the List Media Server Address Map page appears as shown below.</p>  <p>After the first Media Server Address Map is added, the Media Server Contact is created automatically. For the Media Server Address Map that was added, the following contact was created and displayed in the Contact field:</p> <pre> sip:\$(user)@50.1.1.10:5061;transport=tls </pre> <p>The contact specifies the IP address of the Avaya S8300 Media Server and the transport protocol used to send SIP signaling messages. The user in the original request URI is substituted for <code>\$(user)</code>.</p>

Step	Description
9.	<p>Outbound SIP calls are first directed by Avaya Communication Manager routing decisions to the SIP trunk group. These calls are then subject to further routing decisions determined by the Host Address Maps in Avaya SES. Similar to the inbound Media Server Address Maps, these Host Address Maps use pattern matching to direct outbound SIP messages to the proper destination. Furthermore, to ensure correct routing of calls by Avaya SES, the Host Address Maps and Media Server Address Maps must be mutually exclusive. Stated differently, any sequence of dialed digits or received digits in an external SIP call should match only one address map.</p> <p>The example below shows the Host Address Map that routes numbers beginning with 173299 to the Avaya Communication Manager at site 1 via the CSP 2090. It should be noted that a user dialed access code such as a 9 to place an outbound call is deleted by Avaya Communication Manager prior to routing the call to Avaya SES. Thus, the access code does not appear in the matching pattern.</p> <p>The configuration of the Host Address Map for all calls starting with digits 173299 is shown below.</p> <ul style="list-style-type: none"> Expand the Hosts link in the left pane of the administration web interface and select List. On the List Host page that appears, select the Map link associated with the appropriate host (e.g., denali.devcon.com as shown in Step 4. This name is configured as part of the initial installation). The List Host Address Map page is displayed. From this page, click the Add Map In New Group link to display the Add Host Address Map page shown below. Enter a descriptive name for the map. Specify an appropriate pattern for the call type. In this example, the pattern is <code>^sip:173299*</code> Leave the Replace URI checkbox selected. Click the Add button. 

Step	Description
10.	<p>The IP address for the CSP 2090 must be administered in Avaya SES. In the example shown below, the IP address 192.168.1.74 is used.</p> <p>To enter the SIP proxy information for the CSP 2090:</p> <ul style="list-style-type: none"> As described in Step 9, display the List Host Address Map page. Click on the Add Another Contact link associated with the address map added previously to open the Add Host Contact page. On this page, the Contact field specifies the destination for the call and it is entered as: <pre>sip:\$(user)@192.168.1.74:5060;transport=udp</pre> <p>The user part in the original request URI is inserted in place of the “\$(user)” string before the message is sent to the CSP 2090.</p> <ul style="list-style-type: none"> Click the Add button when completed. <p>After configuring the host contact information, the List Host Address Map page will appear as shown below.</p> 

Step	Description						
11.	<p>Complete the administration of Avaya SES by designating the IP address of the CSP 2090 as a trusted host. As a trusted host, Avaya SES will not issue SIP authentication challenges for incoming requests from the designated IP address.¹</p> <p>If multiple SIP proxies are used, the IP address of each SIP proxy must be added as a trusted host.</p> <p>To configure a trusted host:</p> <ul style="list-style-type: none">Connect to the Avaya SES IP address (50.1.1.50) and log in using the administrative login and password.Enter the following trustedhost command at the Linux shell prompt. <pre>trustedhost -a 192.168.1.74 -n 50.1.1.50 -c CSP2090</pre> <p>The -a argument specifies the address to be trusted; -n specifies the Avaya SES host name or IP address; -c adds a comment.</p> <ul style="list-style-type: none">Use the following trustedhost command to verify the entry is correct. <pre>trustedhost -L</pre> <p>The screen below illustrates the results of the trustedhost commands.²</p> <ul style="list-style-type: none">Important Note: Complete the trusted host configuration by returning to the main Avaya SES administration web interface and clicking on the Update link as shown in Step 3. If the Update link is not visible, refresh the page by selecting Top from the left hand menu. This step is required even though the trusted host was configured via the Linux shell. <div><pre>admin@k2> trustedhost -a 192.168.1.74 -n 50.1.1.50 -c CSP2090 20.1.1.54 is added to trusted host list.</pre><pre>admin@k2> trustedhost -L Third party trusted hosts.</pre><table><thead><tr><th>Trusted Host</th><th>CCS Host Name</th><th>Comment</th></tr></thead><tbody><tr><td>192.168.1.74</td><td>50.1.1.50</td><td>CSP2090</td></tr></tbody></table></div>	Trusted Host	CCS Host Name	Comment	192.168.1.74	50.1.1.50	CSP2090
Trusted Host	CCS Host Name	Comment					
192.168.1.74	50.1.1.50	CSP2090					

¹ Note, if the trusted host step is not done, authentication challenges to incoming SIP messages (such as INVITEs and BYEs) will be issued but not responded to. This may cause call setup to fail, active calls to be disconnected after timeout periods, and/or SIP protocol errors.

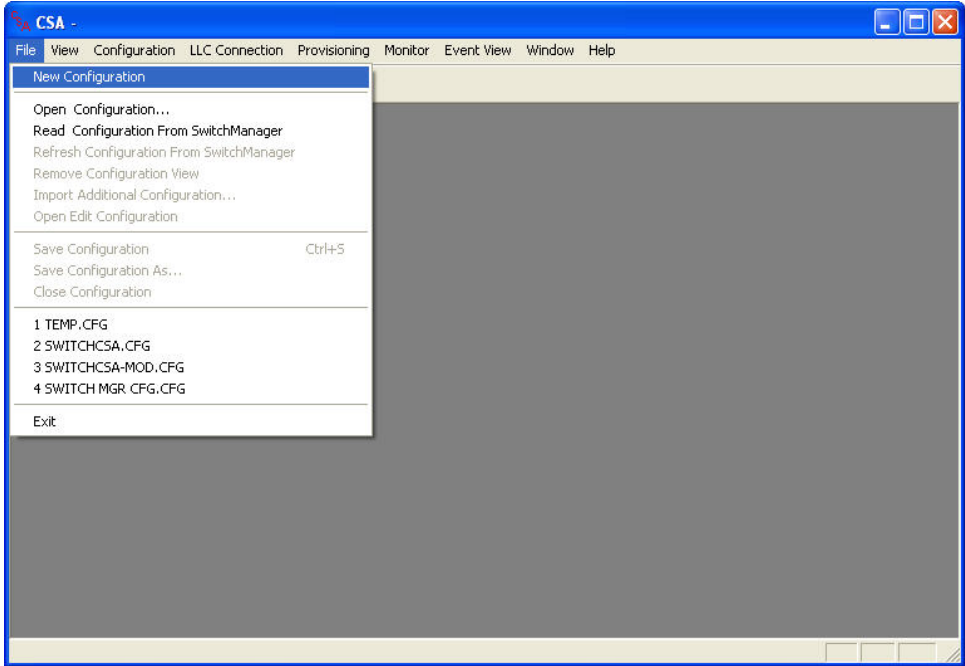
² For completeness, the **-d** argument allows the trust relationship to be deleted. For, example,

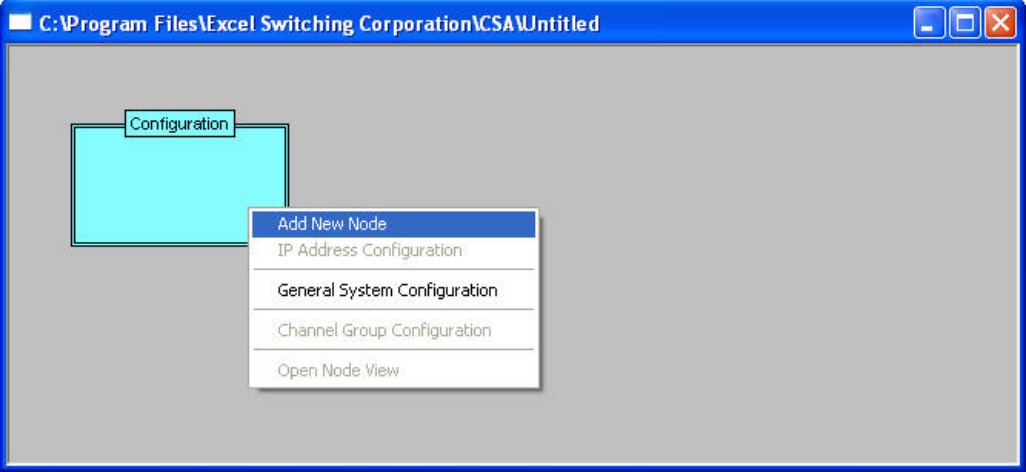
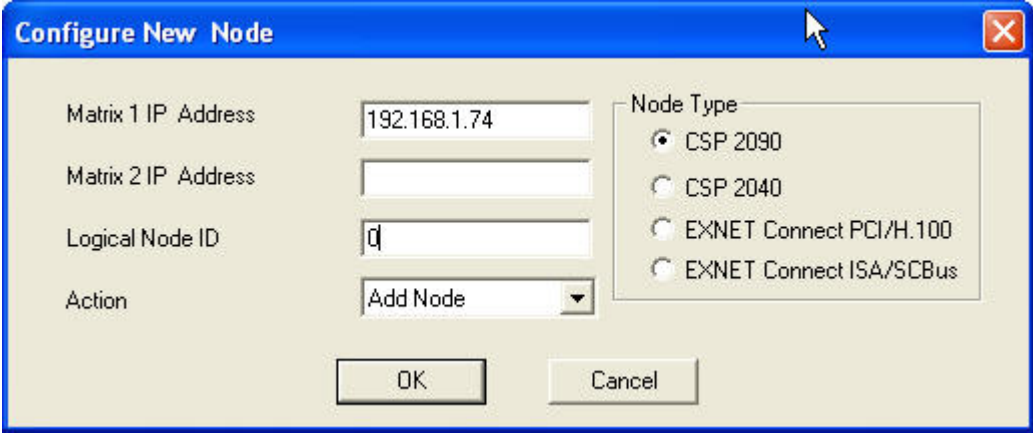
```
trustedhost -d 192.168.1.74 -n 50.1.1.50
```

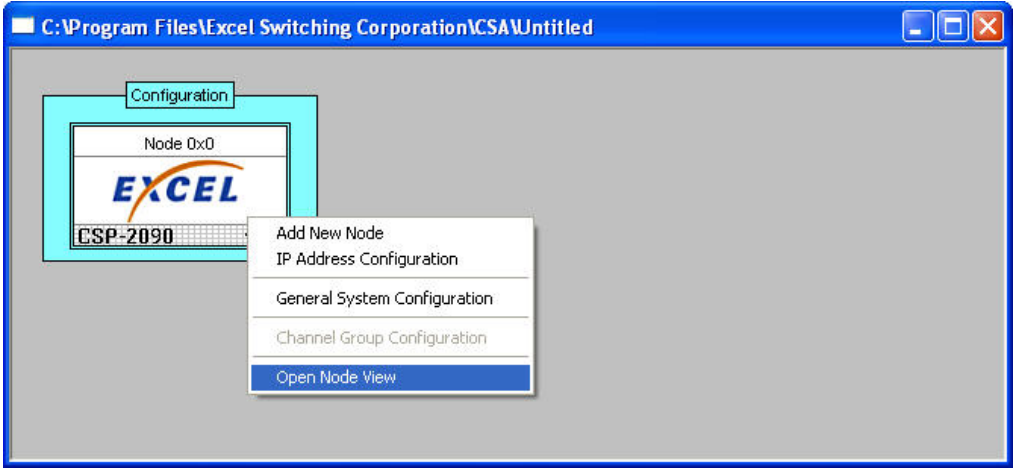
removes the trust relationship added above.

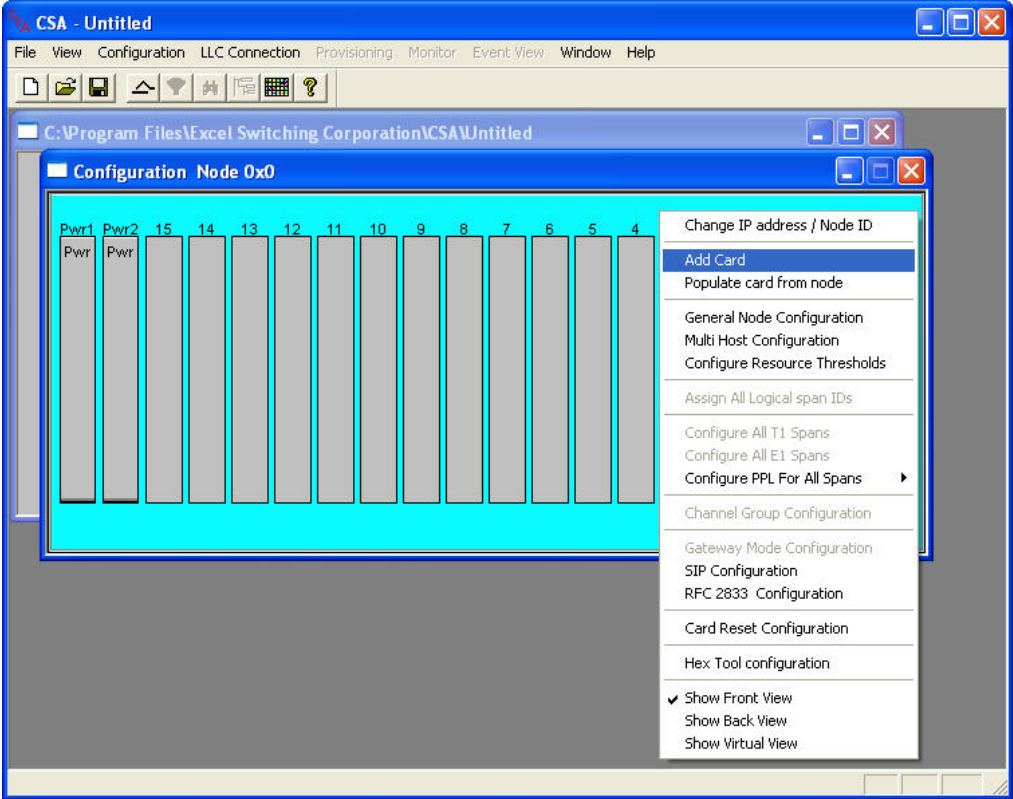
5. Configure Cantata Technology CSP 2090

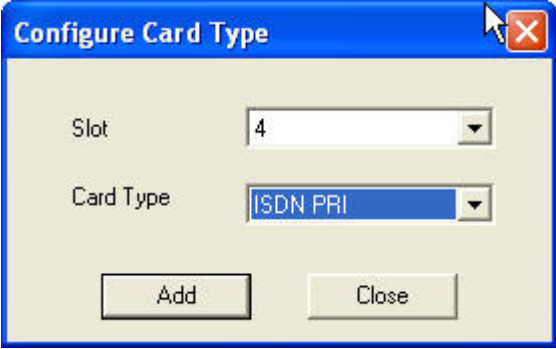

The configuration of the CSP 2090 is performed using the Converged Services Administration (CSA) application. The following steps describe the configuration of both the ISDN-PRI and SIP interfaces. For installation information for the CSP 2090, SwitchKit or CSA see references [6] and [7].

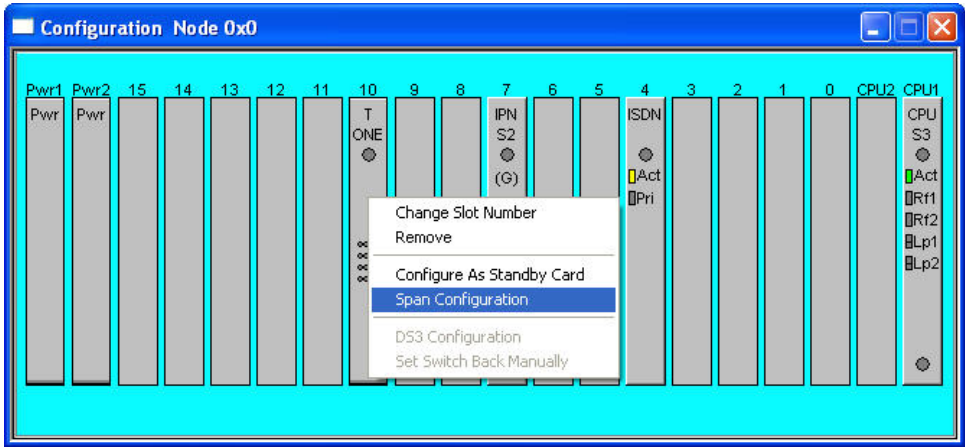
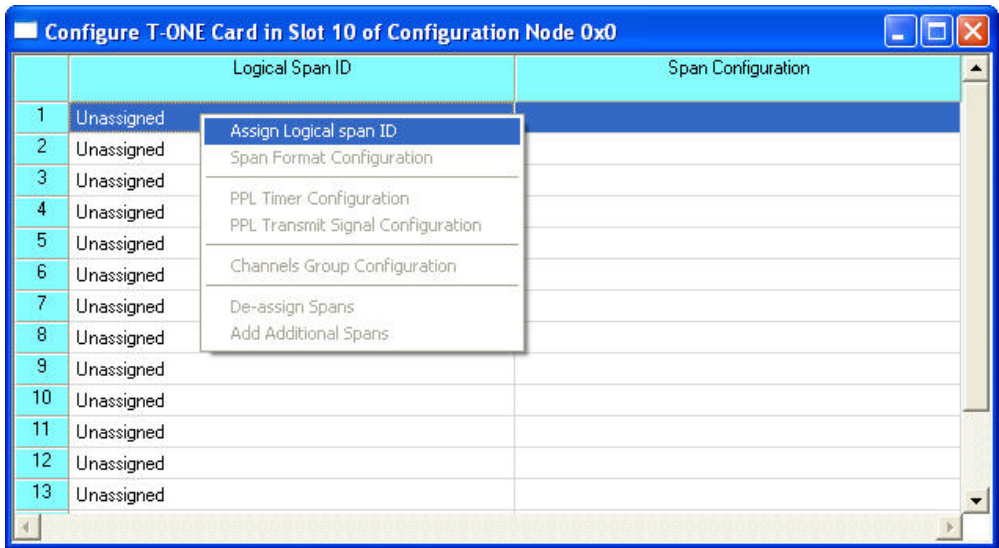
Step	Description
1.	<p>Launch CSA by navigating from the Windows Start menu to Programs → Excel Switching Corporation → CSA. Excel Switching Corporation was the former name of Cantata Technology. From the pull-down menu, select File → New Configuration.</p>  <p>The screenshot shows the CSA application window. The 'File' menu is open, displaying options such as 'Open Configuration...', 'Read Configuration From SwitchManager', 'Refresh Configuration From SwitchManager', 'Remove Configuration View', 'Import Additional Configuration...', 'Open Edit Configuration', 'Save Configuration' (with a Ctrl+S shortcut), 'Save Configuration As...', 'Close Configuration', a list of configuration files (1 TEMP.CFG, 2 SWITCHCSA.CFG, 3 SWITCHCSA-MOD.CFG, 4 SWITCH MGR CFG.CFG), and 'Exit'. The 'New Configuration' option is highlighted at the top of the menu.</p>


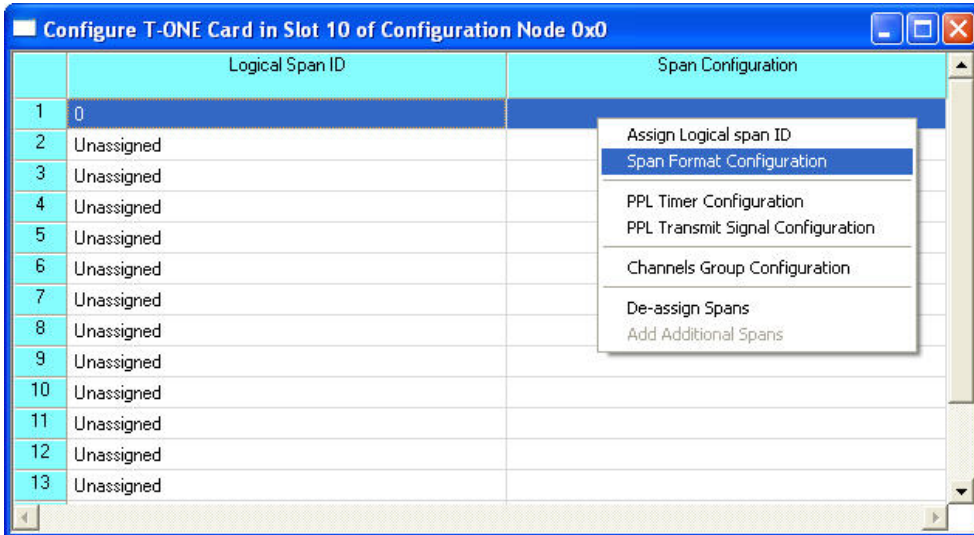
Step	Description
2.	<p>The following window appears with an aqua sub-window labeled Configuration. Right-click the aqua sub-window to get a menu of possible actions.</p> <p>Select Add New Node.</p> 
3.	<p>The Configure New Node window will appear in response to the Add New Node operation in the previous step. In the Matrix 1 IP Address field, enter the IP address of the CSP 2090 that will be used for SIP signaling and communication with SwitchKit. Set the Node Type to CSP 2090. Enter a Logical Node ID. Since this was the only node in the test configuration, the value of <i>0</i> was chosen. Select Add Node for the Action field.</p> <p>Select OK to continue.</p> 

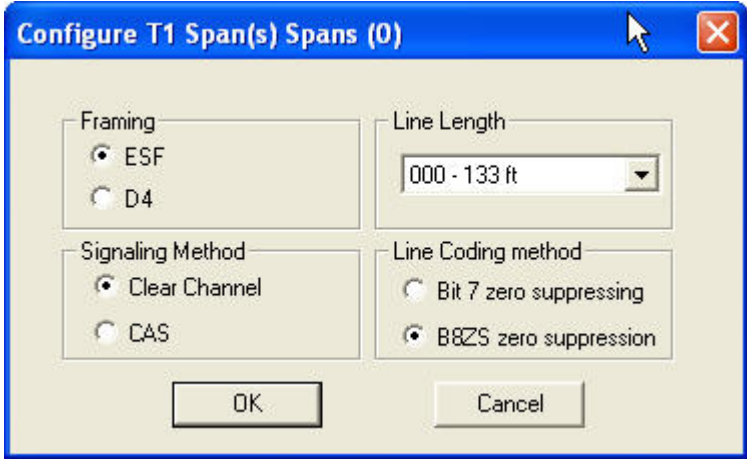
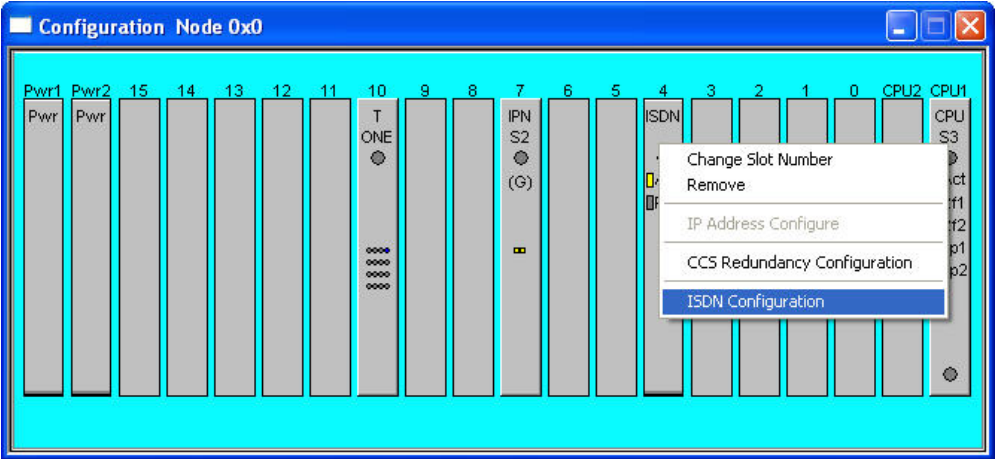
Step	Description
4.	<p>An image of a node is added to the Configuration sub-window. Right-click the node image and select Open Node View from the menu.</p>  <p>The screenshot shows a software window titled "C:\Program Files\Excel Switching Corporation\VCSA\Untitled". Inside, there is a "Configuration" sub-window. Within this sub-window, there is a node image labeled "Node 0x0" with the "EXCEL" logo and "CSP-2090" below it. A right-click context menu is open over the node image, listing the following options: "Add New Node", "IP Address Configuration", "General System Configuration", "Channel Group Configuration", and "Open Node View". The "Open Node View" option is highlighted in blue.</p>

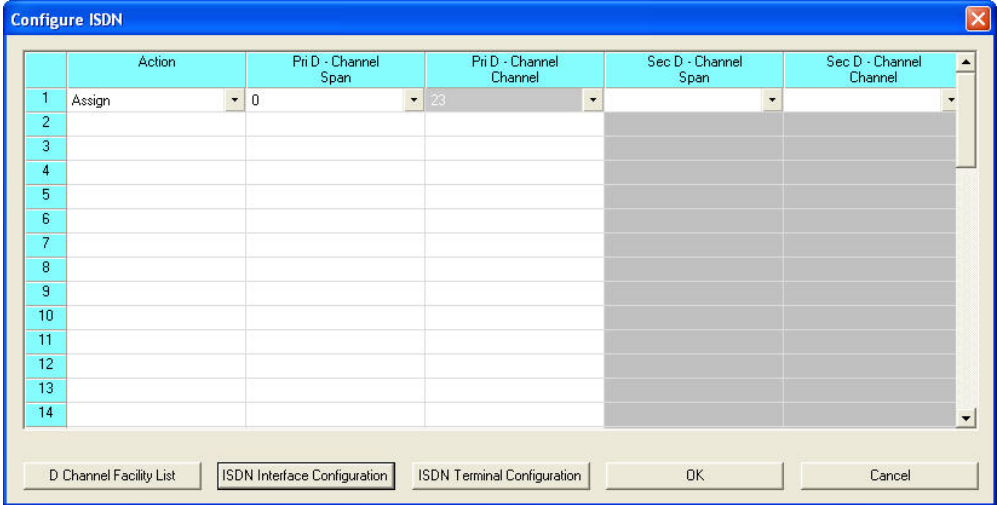
Step	Description
5.	<p>For each physical card that resides in the CSP 2090, the card must be added to the node configuration using the Node View window that appears. To add a card to the configuration, right-click the aqua-colored background and select Add Card from the menu.</p> <p>For the compliance test, the CSP 2090 contained the following: Slot 4 – ISDN-PRI Slot 7 – IPN Series 2 (IP Network Interface) Slot 10 – T One 16-span (T1 Interface)</p> 

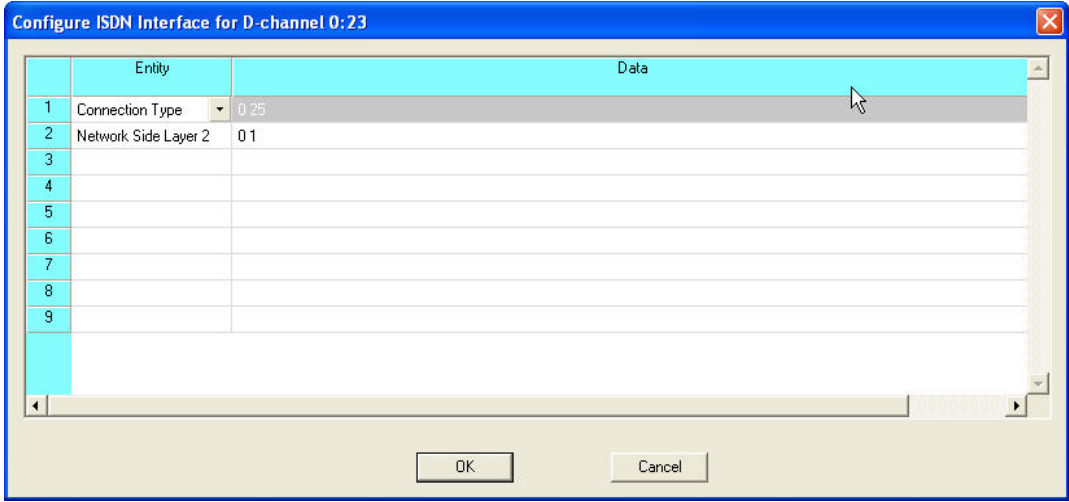
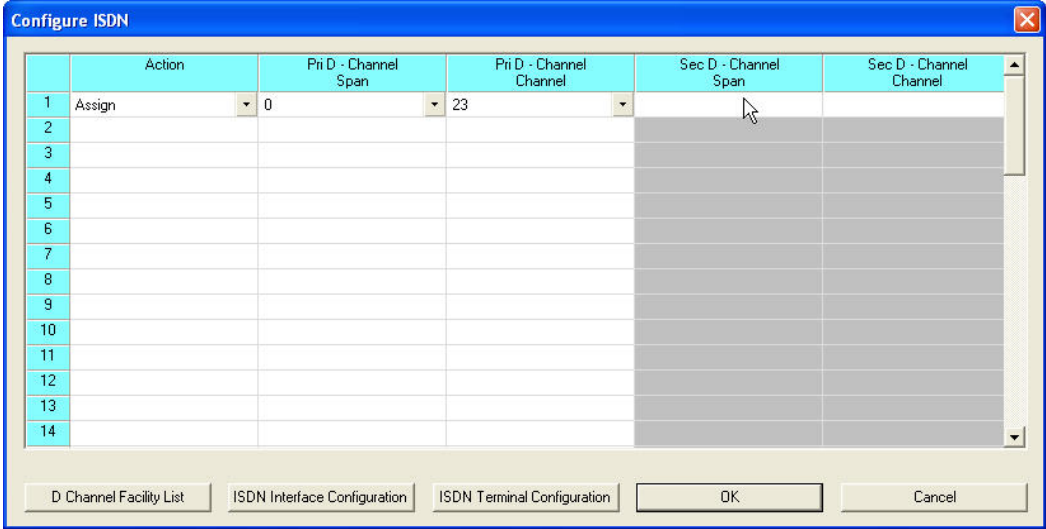
Step	Description
6.	<p>The Configure Card Type window appears. Select the physical slot number from the pull-down menu for the Slot field. From the pull-down menu for the Card Type, select the type of card in the slot. The example below shows the values for the ISDN-PRI card.</p> <p>Select Add to continue.</p> 
7.	<p>Repeat the two previous steps for each card in the configuration. The CPU and Pwr cards are added automatically. The example below shows the Node View window after all the cards have been added.</p> 

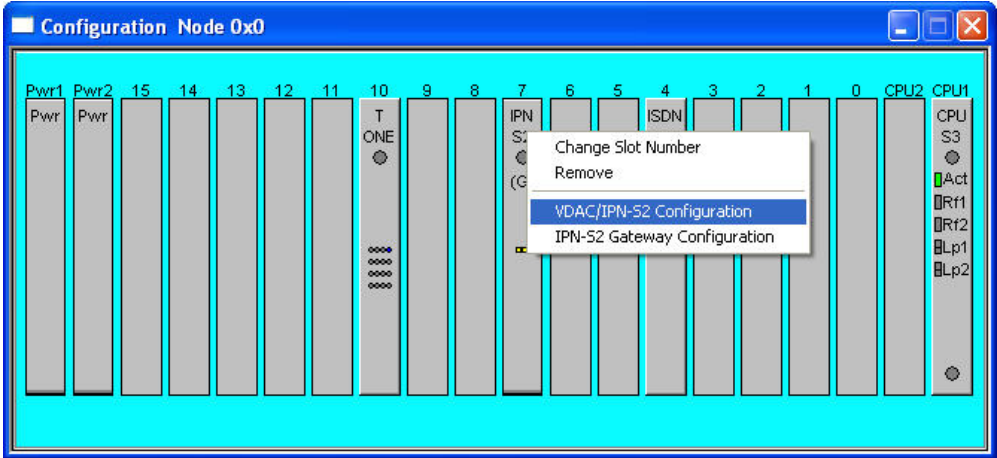
Step	Description
8.	<p>Configure the T1 card by right-clicking on the T ONE card in the Node View window below and select Span Configuration from the menu.</p> 
9.	<p>Highlight the span to be configured. Sixteen spans are available on the T1 card but only the first one was used for the compliance test. Right-click the Logical Span ID field for span 1 and select Assign Logical span ID.</p> 

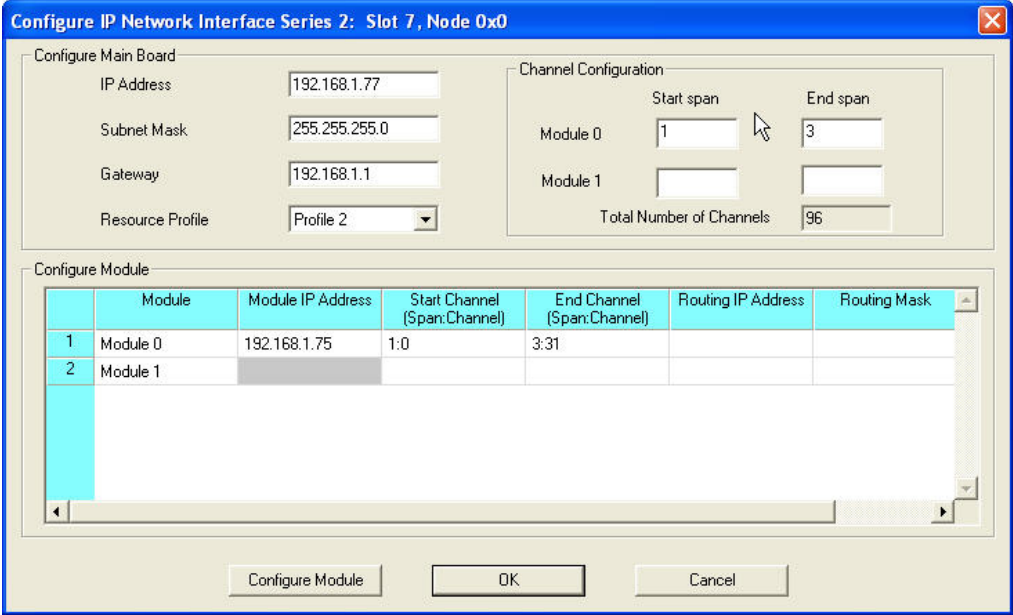
Step	Description
10.	<p>Enter a value for the Logical Span ID. For the compliance test, 0 was chosen since only one span was used.</p> <p>Select OK to continue.</p> 
11.	<p>Returning to the Span Configuration window, right-click the Span Configuration field for span 1 and select Span Format Configuration.</p> 

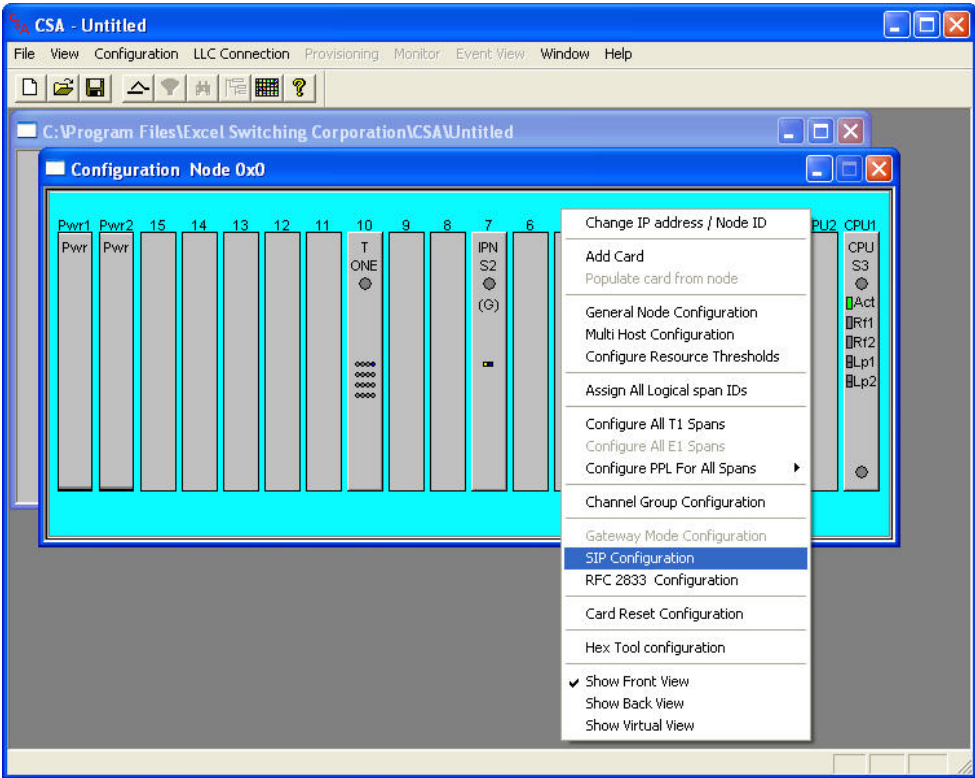
Step	Description
12.	<p>Set the Span format values to the values shown below. These values must match the corresponding values configured on Avaya Communication Manager.</p> <p>Select OK to continue.</p> 
13.	<p>Configure the ISDN card by right-clicking on the ISDN card in the Node View window below and select ISDN Configuration from the menu.</p> 


Step	Description
14.	<p>For the Logical Span 0 created in step 10, assign the ISDN-PRI D-channel to channel 23. Channels are numbered from 0 to 23, so channel 23 is the 24th channel of the ISDN-PRI trunk.</p> <p>Select the ISDN Interface Configuration button to continue.</p> 

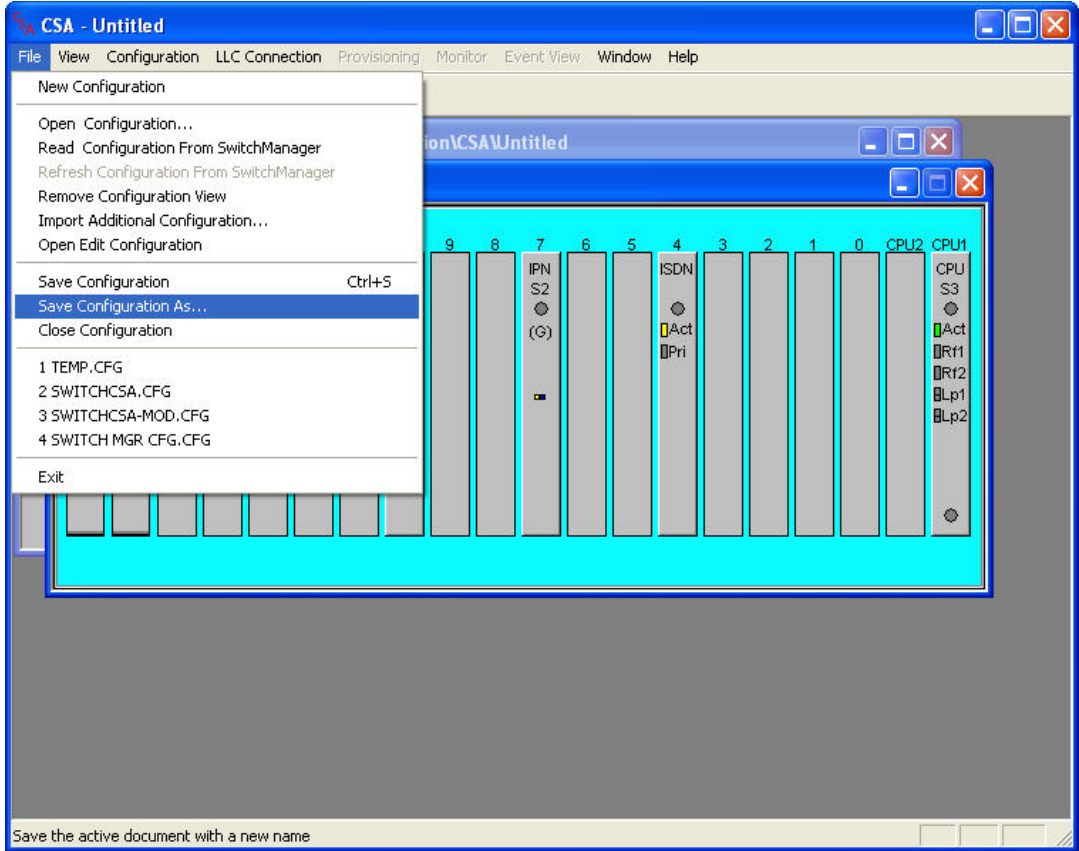
Step	Description
15.	<p>Next configure the D-channel by entering the data shown below. First, select <i>Connection Type</i> in the Entity column and enter <i>0 25</i> in the Data column. This specifies the D-Channel as using NI-2 ISDN-PRI. Next, select <i>Network Side Layer 2</i> in the Entity column followed by <i>0 1</i> in the Data column. This specifies the D-Channel as the network side. The other end of this trunk on Avaya Communication Manager must be set to use NI-2 ISDN-PRI and set to the user side.</p> <p>The available values and corresponding meanings of data used to populate the Data column are defined in [9]. Please refer to this document for complete details.</p> <p>Select OK to continue.</p> 
16.	<p>Return to the Configure ISDN window and select OK.</p> 

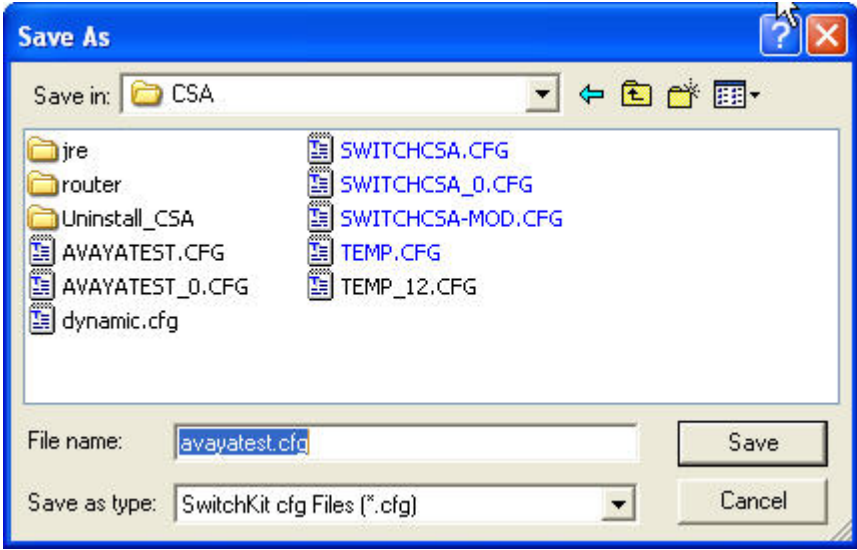
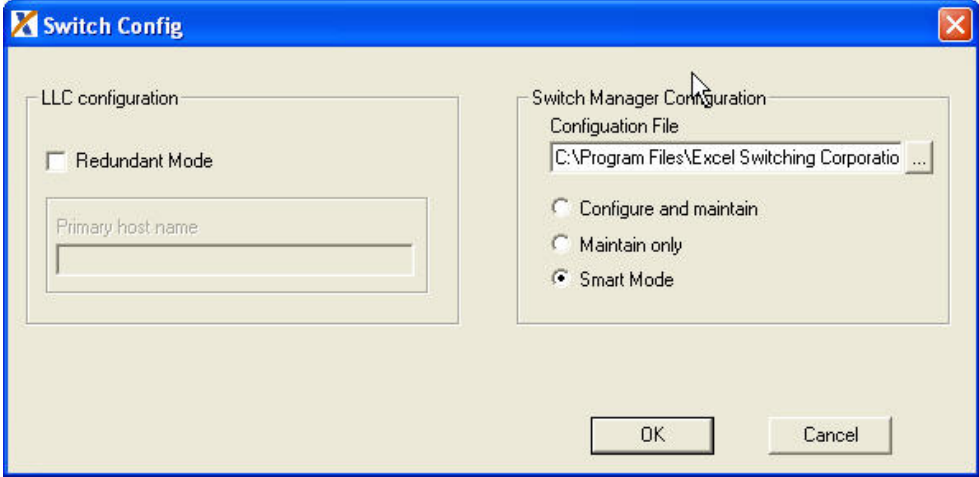
Step	Description
17.	<p>Configure the IP Network Interface card by right-clicking on the IPN S2 card in the Node View window below and select VDAC/IPN-S2 Configuration from the menu.</p> 

Step	Description
18.	<p>The IP Network Interface card contains the VoIP modules for processing the RTP media stream. The main card and each VoIP module require separate IP addresses. The window below shows the configuration used for the compliance test. Only one VoIP module was used. The IP Address, Subnet Mask and Gateway of the main board are entered in the top half of the form. Select a Resource Profile from the pull-down menu. The resource profile defines which codecs are available for use by the IP Network Interface card. Profile 1 allows only G.711 ulaw/alaw with a maximum of 512 channels per module. Profile 2 allows G.711 ulaw/alaw, G.729A/B, G.723.1, and G.726 with a maximum of 256 channels per module. Profile 2 was used for the compliance test. The default preferred codec is G.711.</p> <p>The card was configured with 3 spans on module 0 based on the licensing available on the CSP 2090 tested. Each span supports 32 channels. Under Channel Configuration, the Start span for Module 0 was set to 1 and the End span was set to 3.</p> <p>In the lower half of the form, VoIP module 0 was configured. The Module IP Address was set to the IP address that will be used for RTP traffic. The Start Channel was set to be span 1, channel 0 and the End Channel was set to be span 3, channel 31.</p> <p>Select OK to continue.</p> 

Step	Description
19.	<p>All the cards have been configured. Next, perform the SIP configuration. From the Node View window, right-click the aqua background to get the menu shown below. Select SIP Configuration.</p> 

Step	Description
20.	<p>Enter a descriptive name for the Site ID field. Verify that the Enable Call Agent check box is unchecked.</p> <p>The IP address of the SIP proxy where outbound calls will be directed can be configured on this screen or be supplied by the host application running on the CSP 2090. For the compliance test, this IP address was the IP address of Avaya SES and it was supplied by the demo application running on the CSP 2090. Thus, the Local Outbound Proxy Server was not enabled and the Avaya SES IP address was not configured on the CSP 2090. Default values can be used for all other fields.</p> <p>Select OK to continue.</p> 

Step	Description
21.	<p>Save the configuration just created by navigating to File→ Save Configuration As from the CSA task bar.</p>  <p>The screenshot shows the 'CSA - Untitled' application window. The 'File' menu is open, and 'Save Configuration As...' is highlighted. The menu also includes options like 'New Configuration', 'Open Configuration...', 'Read Configuration From SwitchManager', 'Refresh Configuration From SwitchManager', 'Remove Configuration View', 'Import Additional Configuration...', 'Open Edit Configuration', 'Save Configuration' (with a 'Ctrl+S' shortcut), 'Close Configuration', a list of recent files (1 TEMP.CFG, 2 SWITCHCSA.CFG, 3 SWITCHCSA-MOD.CFG, 4 SWITCH MGR.CFG.CFG), and 'Exit'. The background interface shows a configuration view with a grid of components labeled 9 through 0, CPU2, and CPU1. The status bar at the bottom indicates 'Save the active document with a new name'.</p>

Step	Description
22.	<p>The pop-up window defaults to the directory where CSA is installed. Enter a file name in the File Name field and select Save. The new configuration is then saved in the location indicated.</p> 
23.	<p>In order for the newly saved configuration to be used the next time that the CSP 2090 is booted, SwitchKit must be configured to use this file. To do this, navigate to Programs→SwitchKit→SwitchConfig from the Windows Start Menu. The window shown below will appear. Select the browse icon (...) next to the Configuration File text box. Navigate to the file saved in the previous step and select it. The full pathname of the file will appear in the Configuration File text box. Use the default values for the other fields.</p> <p>Select OK to save the configuration.</p> 

6. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify the interoperability between the SIP and ISDN-PRI interfaces of the CSP 2090 and Avaya Communication Manager and Avaya SES. This section covers the general test approach and the test results.

6.1. General Test Approach

A software application built for the CSP 2090 is required to provide feature functionality to the end user. As part of the compliance test, a demo application was used to allow the CSP 2090 to operate as a SIP to ISDN-PRI gateway. This provided the means to exercise the SIP and ISDN-PRI interfaces and the interoperability of these interfaces with Avaya Communication Manager and Avaya SES.

The test configuration was comprised of two enterprise sites. One site connected to the CSP 2090 via ISDN-PRI and the other site connected to the CSP 2090 via SIP. In this manner, the interoperability of the SIP and ISDN-PRI interfaces with Avaya equipment could be tested in a single configuration.

6.2. Test Results

The following features and functionality were successfully verified during interoperability compliance test:

- Calls connected through the CSP 2090 from ISDN-PRI to SIP.
- Calls connected through the CSP 2090 from SIP to ISDN-PRI.
- Calls to/from SIP, H.323, digital and analog endpoints in the Avaya enterprise network.
- Calls using G.711 and G.729B codecs.
- Calls were left up for more than 35 seconds to verify certain SIP protocol timers.
- DTMF transmission using RFC 2833.
- Proper feature operation with hold, call forward, transfer and conference.
- Proper feature name extension (FNE) operation. Avaya Communication Manager uses FNEs to provide extended telephony features to SIP phones (e.g. Call Pickup, Automatic Callback, Send All Calls, and Whisper Page).
- Reestablishment of the connection to the CSP 2090 from Avaya Communication Manager and Avaya SES after network outages and system reboots.

The following observations were made during the CSP 2090 compliance testing.

- As previously mentioned, the CSP 2090 does not support the specific implementation of media shuffling required of Avaya Communication Manager. As a result, direct IP-to-IP audio must be disabled on the SIP Signaling Group form as shown in Section 3.2, Step 5.
- The CSP 2090 supports multiple codecs for use by the SIP interface and is configured with a preferred codec which by default is G.711. When sending SIP INVITE messages to Avaya SES, the CSP 2090 only advertises the preferred codec. Thus, the CSP 2090 preferred codec must be in the codec list of Avaya Communication Manager or the call will not be established. For calls originating in the opposite direction, when SIP INVITE messages are sent to the CSP 2090, the CSP 2090 will accept calls requesting use of other

codecs but only if the preferred codec of the CSP 2090 is not in the SIP INVITE message.

7. Verification Steps

This section provides verification steps that may be performed to verify that the solution described in these Application Notes is configured properly.

- Verify that the both the ISDN-PRI and SIP trunk groups are in-service. To do this, use the **status trunk *n*** command, where *n* is the number of the trunk group to be verified.
- Verify that the both the ISDN-PRI and SIP signaling groups are in-service. To do this, use the **status signaling-group *n*** command, where *n* is the number of the signaling group to be verified.
- Verify that a call can be placed from an endpoint on the ISDN-PRI side of the CSP 2090 to an endpoint on the SIP side.
- Verify that a call can be placed from an endpoint on the SIP side of the CSP 2090 to an endpoint on the ISDN-PRI side.

8. Support

Technical support for the CSP 2090 can be obtained from Cantata Technology. See the Support link at www.cantata.com for contact information.

9. Conclusion

The SIP and ISDN-PRI interfaces of the CSP 2090 have successfully passed interoperability compliance testing with Avaya Communication Manager and Avaya SIP Enablement Services (SES). No conclusion is drawn as to the compliance of the demo application used during the testing or any other application that may be built on the CSP 2090.

10. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>.

- [1] *Feature Description and Implementation For Avaya Communication Manager*, Issue 4.0, February 2006, Document Number 555-245-205.
- [2] *Administrator Guide for Avaya Communication Manager*, Issue 2.1, May 2006, Document Number 03-300509.
- [3] *Converged Communications Server R3.0 Installation and Administration Guide (SIP Enablement Services R3.0)*, July 2005, Issue 5.1, Document Number 555-245-705.
- [4] *SIP Support in Release 3.1 of Avaya Communication Manager Running on the Avaya S8300, S8500, S8500B, S8700, and S8710 Media Server*, February 2006, Issue 6, Document Number 555-245-206.
- [5] *4600 Series IP Telephone Release 2.4 LAN Administrator Guide*, April 2006, Issue 2.3, Document Number 555-233-507.

The following CSP 2090 product documentation is available from Cantata Technology. Visit <http://www.cantata.com> for company and product information.

- [6] *Converged Services Platform Developer's Overview*, Release 8.4.0, November 2005.

- [7] *Converged Services Platform – SwitchKit Installation & Maintenance Guide*, Release 8.4.0, November 2005.
- [8] *SwitchKit Converged Services Administrator's User Guide*, Release 8.4.0, November 2005.
- [9] *Converged Services Platform API Reference*, Release 8.4.0, November 2005.

APPENDIX A: Specifying Pattern Strings in Address Maps

The syntax for the pattern matching used within Avaya SES is a Linux regular expression used to match against the URI string found in the SIP INVITE message.

Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special *metacharacters*, which may represent items like quantity, location or types of character(s).

In the pattern matching string used in Avaya SES:

- Normal text characters and numbers match themselves.
- Common metacharacters used are:
 - A period `.` matches any character once (and only once).
 - A asterisk `*` matches zero or more of the preceding characters.
 - Square brackets enclose a list of any character to be matched. Ranges are designated by using a hyphen. Thus, the expression `[12345]` or `[1-5]` both describe a pattern that will match any single digit between 1 and 5.
 - Curley brackets containing an integer 'n' indicate that the preceding character must be matched exactly 'n' time. Thus, `5{3}` matches '555' and `[0-9]{10}` indicates any 10 digit number.
 - The circumflex character `^` as the first character in the pattern indicates that the string must begin with the character following the circumflex.

Putting these constructs together as used in this document, the pattern to match the SIP INVITE string for any valid 1+ 10 digit number in the North American dial plan would be:

`^sip:1[0-9]{10}`

This reads as: "Strings that begin with exactly **sip:1** and having any 10 digits following will match.

A typical INVITE request below uses the shaded portion to illustrate the matching pattern.

```
INVITE sip:17325551638@20.1.1.54:5060;transport=udp SIP/2.0
```

©2006 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 Developer*Connection* Program at devconnect@avaya.com.