Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Covergence Eclipse CXC with Avaya SIP Enablement Services and Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Covergence Eclipse CXC to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager using the Session Initiation Protocol (SIP).

The Covergence Eclipse CXC is a network appliance that enables enterprises to secure, control and monitor SIP-based real-time communications and collaboration applications and services. The Eclipse CXC provides a superset of the legacy session border controller and SIP firewall functionality. The Eclipse CXC extends SIP-based applications and services over untrusted networks by ensuring confidentiality, authenticity and integrity of the communications while protecting the corporate infrastructure from SIP-based intrusions and attacks.

The compliance testing focused on SIP telephony scenarios between endpoints across an untrusted network secured by the Eclipse CXC. The testing was done in three separate configurations described as Remote Access, Secure Remote Access and Secure SIP Trunking.

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

©2006 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedure for configuring the Covergence Eclipse CXC to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager using the Session Initiation Protocol (SIP).

The Covergence Eclipse CXC is a network appliance that enables enterprises to secure, control and monitor SIP-based real-time communications and collaboration applications and services. The Eclipse CXC provides a superset of the legacy session border controller and SIP firewall functionality. The Eclipse CXC extends SIP-based applications and services over untrusted networks by ensuring confidentiality, authenticity and integrity of the communications while protecting the corporate infrastructure from SIP-based intrusions and attacks.

The compliance testing focused on SIP telephony scenarios between endpoints across an untrusted network secured by the Eclipse CXC. The testing was done in three separate configurations described as Remote Access, Secure Remote Access and Secure SIP Trunking.

1.1. Remote Access Configuration

Figure 1 illustrates the Remote Access configuration. In the sample configuration, two sites are connected via an untrusted IP network. The main office has an Eclipse CXC at the edge of the network while the branch office does not. In this configuration, the SIP connection is not secured between the two sites. However, the Eclipse CXC at the main office protects the main office infrastructure from any SIP-based attacks. The SIP communication across the network uses SIP over UDP and RTP for the media streams.

The main office has an Avaya SES and an Avaya S8300 Media Server running Avaya Communication Manager with an Avaya G350 Media Gateway. Endpoints include an Avaya 4600 Series IP Telephone (with SIP firmware), an Avaya 4600 Series IP Telephone (with H.323 firmware), an Avaya 6408D Digital Telephone and an Avaya 6210 Analog Telephone. All external calls originating from Avaya Communication Manager at the main office and destined for the branch office will be routed through the on-site Avaya SES, Eclipse CXC and across the untrusted IP network. The branch office has two Avaya 4600 Series IP Telephones with SIP firmware.

All SIP endpoints at both locations are configured to use the Eclipse CXC as the call server. The SIP endpoints at the main office use the Eclipse CXC private side IP address as the call server while the SIP endpoints at the branch office use the Eclipse CXC public side IP address as the call server. When the Eclipse CXC receives SIP signaling traffic from the SIP endpoints, the Eclipse CXC changes the IP address information in the messages to its own IP address before sending the messages to Avaya SES and vice versa. In this manner, all signaling traffic between the SIP endpoints and Avaya SES passes through the Eclipse CXC. The Eclipse CXC will appear as a set of registered endpoints to Avaya SES. The media path also passes through the Eclipse CXC. The media path is controlled by the connection IP addresses in the SIP signaling messages. The Eclipse CXC also modifies these addresses to its own IP address so that the media streams between the endpoints pass through the Eclipse CXC.

©2006 Avaya Inc. All Rights Reserved.

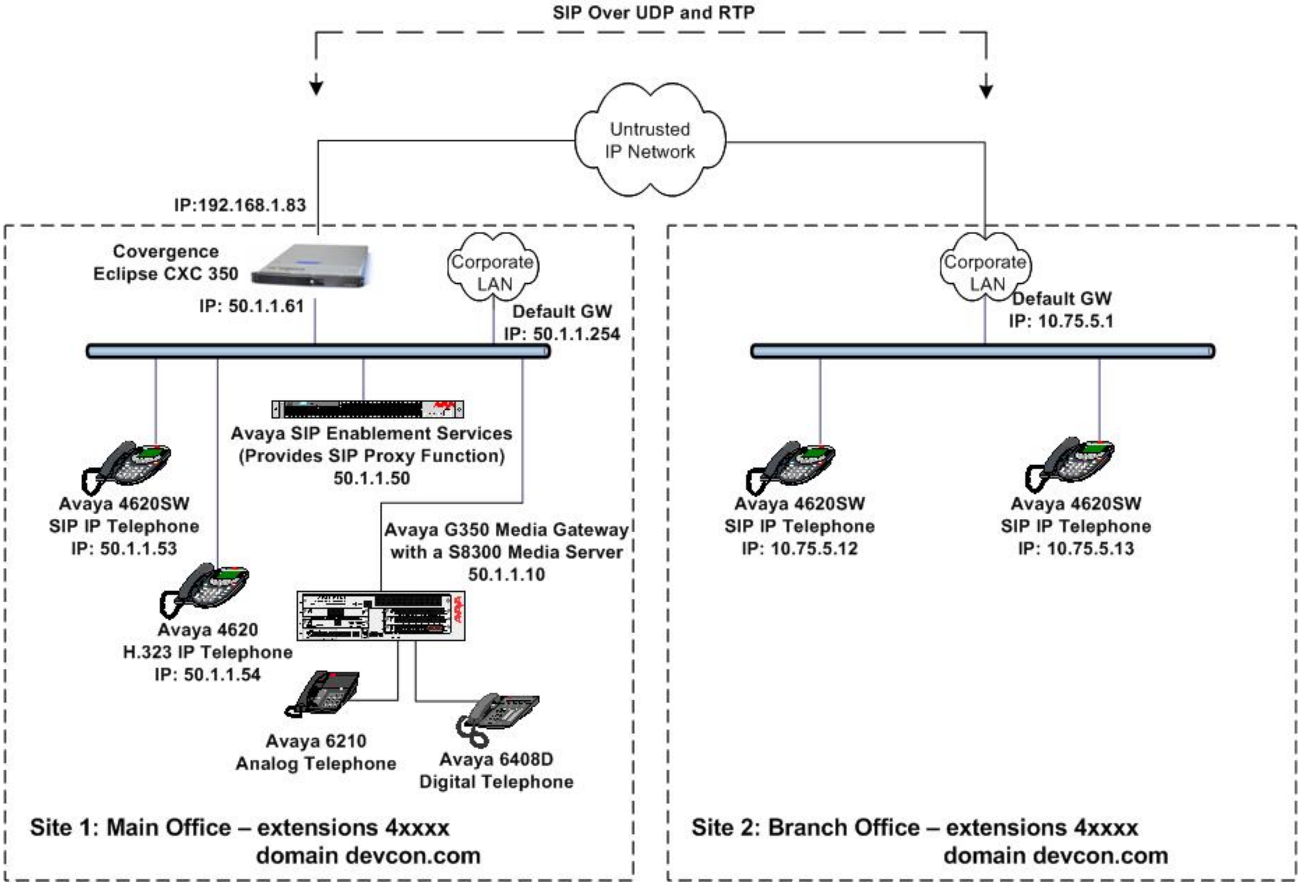


Figure 1: Remote Access Test Configuration

1.2. Secure Remote Access Configuration

Figure 2 illustrates the Secure Remote Access configuration. In the sample configuration, two sites are connected via an untrusted IP network. Each site has an Eclipse CXC at the edge of the network. In this configuration, the SIP connection is secured between the two Eclipse CXCs at each site over the untrusted network. This secured connection uses SIP over TLS and SRTP for the media streams.

The equipment at each site is the same as in **Figure 1** except with the addition of the Eclipse CXC 50 at the branch office.

The SIP endpoints at both locations use the private side IP address of the local Eclipse CXC as the call server. The operation of the Eclipse CXC is the same as the Remote Access configuration with the Eclipse CXCs modifying the IP addresses in the SIP signaling messages such that all SIP signaling and media traffic pass through one or both of the Eclipse CXCs. The main office Eclipse CXC still appears as a set of registered endpoints to Avaya SES.

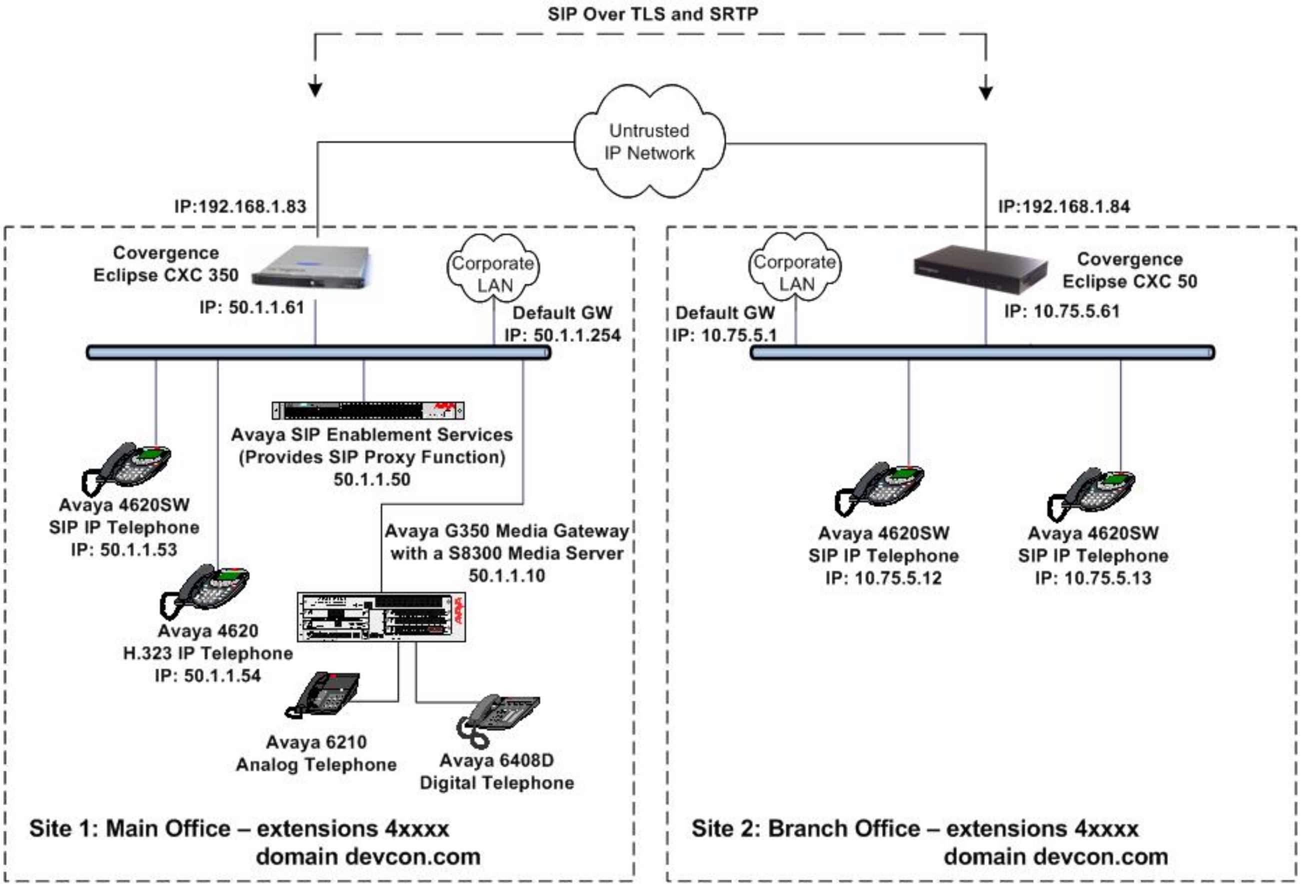

SIP Over TLS and SRTP
Untrusted IP Network
IP:192.168.1.83
IP:192.168.1.84
Covergence Eclipse CXC 350
IP: 50.1.1.61
Corporate LAN
Default GW IP: 50.1.1.254
Avaya SIP Enablement Services (Provides SIP Proxy Function) 50.1.1.50
Avaya 4620SW SIP IP Telephone IP: 50.1.1.53
Avaya G350 Media Gateway with a S8300 Media Server 50.1.1.10
Avaya 4620 H.323 IP Telephone IP: 50.1.1.54
Avaya 6210 Analog Telephone
Avaya 6408D Digital Telephone
Site 1: Main Office – extensions 4xxxx domain devcon.com
Corporate LAN
Covergence Eclipse CXC 50
Default GW IP: 10.75.5.1
IP: 10.75.5.61
Avaya 4620SW SIP IP Telephone IP: 10.75.5.12
Avaya 4620SW SIP IP Telephone IP: 10.75.5.13
Site 2: Branch Office – extensions 4xxxx domain devcon.com

Figure 2: Secure Remote Access Test Configuration

1.3. Secure SIP Trunking

Figure 3 illustrates the Secure SIP Trunking configuration. In the sample configuration, two sites are connected via an untrusted IP network. Each site has an Eclipse CXC at the edge of the network. In this configuration, the SIP connection is secured between the two Eclipse CXCs at each site over the untrusted network. This secured connection uses SIP over TLS and SRTP for the media streams.

The equipment at the main office is the same as in Figure 1. The branch office has an Eclipse CXC 50. In addition, the branch office has an Avaya SES and an Avaya S8300 Media Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Endpoints include two Avaya 4600 Series IP Telephones (with SIP firmware). All external calls originating from Avaya Communication Manager at the main office and destined for the branch office will be routed through the on-site Avaya SES, on-site Eclipse CXC, across the untrusted IP network, through the remote Eclipse and remote Avaya SES to the remote Avaya Communication Manager.

The SIP endpoints at both locations use the local Avaya SES as the call server. Only calls between the two sites pass through the Eclipse CXCs. The Eclipse CXC does not appear as a set of endpoints to Avaya SES but instead is configured as a signaling peer. Address Maps are required on Avaya SES to route calls from Avaya Communication Manager and the Eclipse CXC. For example, an Address Map is configured on Avaya SES at the main office to route extensions starting with a 3 to the Eclipse CXC at the main office for transport to the branch office. Similarly, an Address Map is configured on Avaya SES at the branch office to route extensions starting with a 4 to the Eclipse CXC at the branch office for transport to the main office.

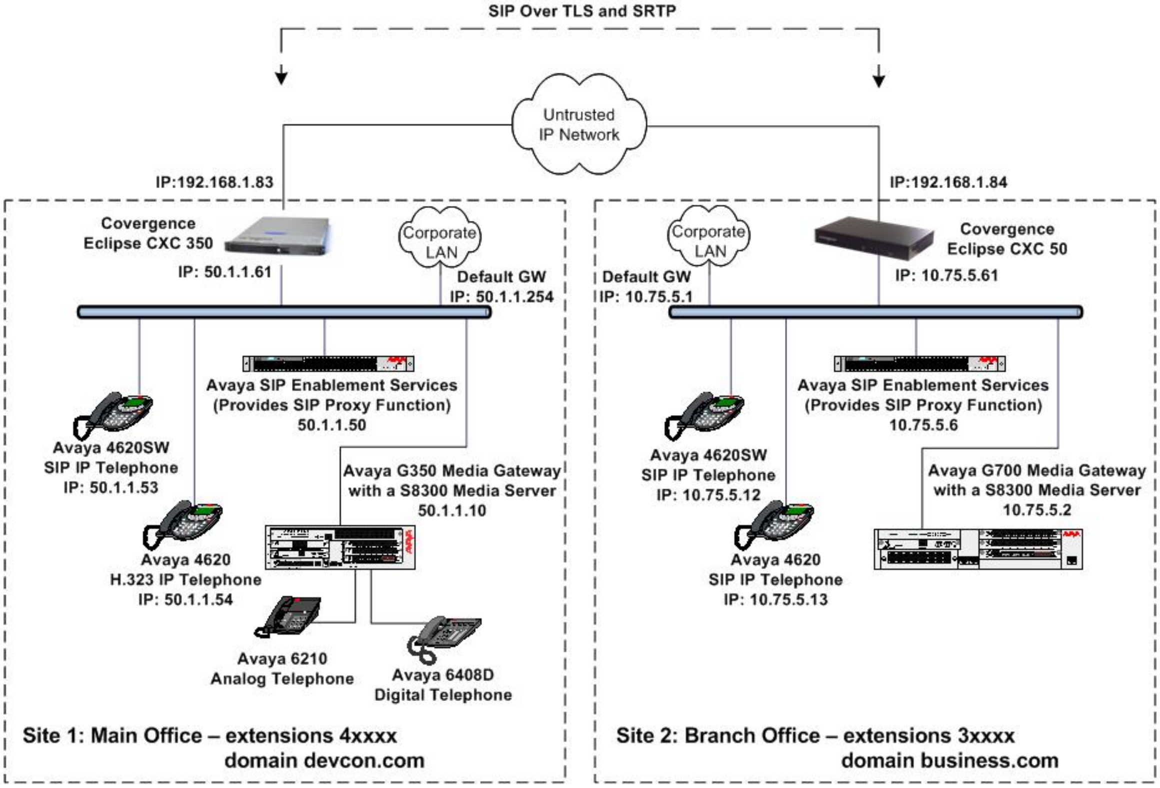

SIP Over TLS and SRTP
Untrusted IP Network
IP:192.168.1.83
IP:192.168.1.84
Covergence Eclipse CXC 350
IP: 50.1.1.61
Corporate LAN
Default GW IP: 50.1.1.254
Avaya SIP Enablement Services (Provides SIP Proxy Function) 50.1.1.50
Avaya 4620SW SIP IP Telephone IP: 50.1.1.53
Avaya G350 Media Gateway with a S8300 Media Server 50.1.1.10
Avaya 4620 H.323 IP Telephone IP: 50.1.1.54
Avaya 6210 Analog Telephone
Avaya 6408D Digital Telephone
Site 1: Main Office – extensions 4xxxx domain devcon.com
Corporate LAN
Default GW IP: 10.75.5.1
Covergence Eclipse CXC 50
IP: 10.75.5.61
Avaya SIP Enablement Services (Provides SIP Proxy Function) 10.75.5.6
Avaya 4620SW SIP IP Telephone IP: 10.75.5.12
Avaya G700 Media Gateway with a S8300 Media Server 10.75.5.2
Avaya 4620 SIP IP Telephone IP: 10.75.5.13
Site 2: Branch Office – extensions 3xxxx domain business.com

Figure 3: Secure SIP Trunking Test Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Media Server with Avaya G350 Media Gateway	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1) with Service Pack (01.2.632.1-11989)
Avaya S8300 Media Server with Avaya G700 Media Gateway	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1) with Service Pack (01.2.632.1-11989)
Avaya SIP Enablement Services (SES)	3.1 (build 18)
Avaya 4620SW IP Telephones	SIP version 2.2.2
Avaya 4620 IP Telephones	H.323 version 2.3
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Covergence Eclipse CXC 350	3.1.1
Covergence Eclipse CXC 50	3.1.1

3. Remote Access Configuration

This section describes the procedures for configuring the devices in the Remote Access network configuration.

3.1. Configure Avaya Communication Manager

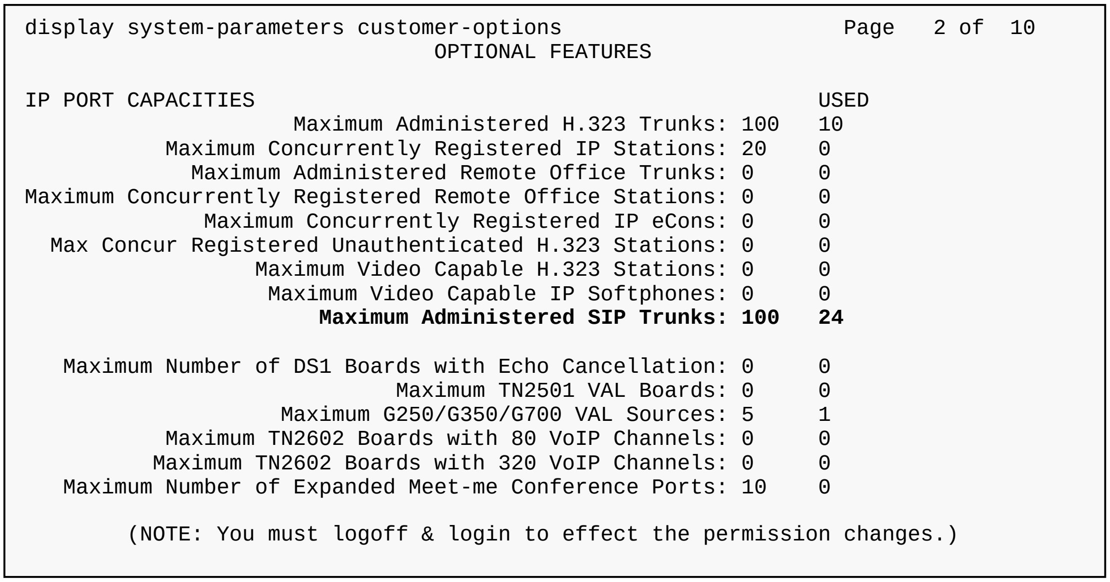
The communication between Avaya Communication Manager and Avaya SES at the main office is via a SIP trunk group. All SIP signaling for calls between Avaya Communication Manager and the Eclipse CXC passes through Avaya SES via this trunk group. This section describes the steps for configuring this trunk group and associated signaling group.

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

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

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 another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.

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.



```
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.)
```

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

Step	Description
2.	On Page 4, verify that the features shown in bold in the example below are enabled.

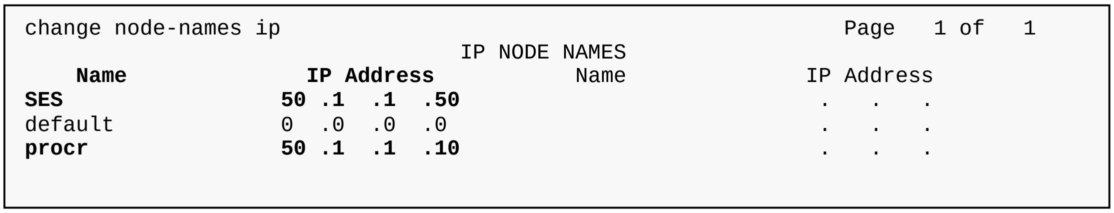
```
display system-parameters customer-options                      Page   4 of  10
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y               Internet Protocol (IP) PNC? n
           Enhanced Conferencing? y                        ISDN Feature Plus? n
                  Enhanced EC500? y            ISDN Network Call Redirection? n
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? n
       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
```

Step	Description
3.	On Page 5, verify that the features shown in bold in the example below are enabled.

```
display system-parameters customer-options                      Page   5 of  10
                                OPTIONAL FEATURES

                Multinational Locations? n             Station and Trunk MSP? n
 Multiple Level Precedence & Preemption? n      Station as Virtual Extension? n
                     Multiple Locations? n
                                             System Management Data Transfer? n
          Personal Station Access (PSA)? n               Tenant Partitioning? n
                        Posted Messages? n       Terminal Trans. Init. (TTI)? n
                        PNC Duplication? n               Time of Day Routing? n
                   Port Network Support? n              Uniform Dialing Plan? n
                                               Usage Allocation Enhancements? y
               Processor and System MSP? n       TN2501 VAL Maximum Capacity? y
                     Private Networking? y
                     Processor Ethernet? y                Wideband Switching? n
                                                                    Wireless? n
                          Remote Office? n
          Restrict Call Forward Off Net? y
                  Secondary Data Module? y
```

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

Use the **change node-name ip** command to assign the node name and IP address for Avaya SES at the main office. In this case, ***SES*** and ***50.1.1.50*** are being used, respectively. The node name ***SES*** will be used throughout the other configuration forms of Avaya Communication Manager. In this example, ***procr*** and ***50.1.1.10*** are the name and IP address assigned to the Avaya S8300 Media Server.



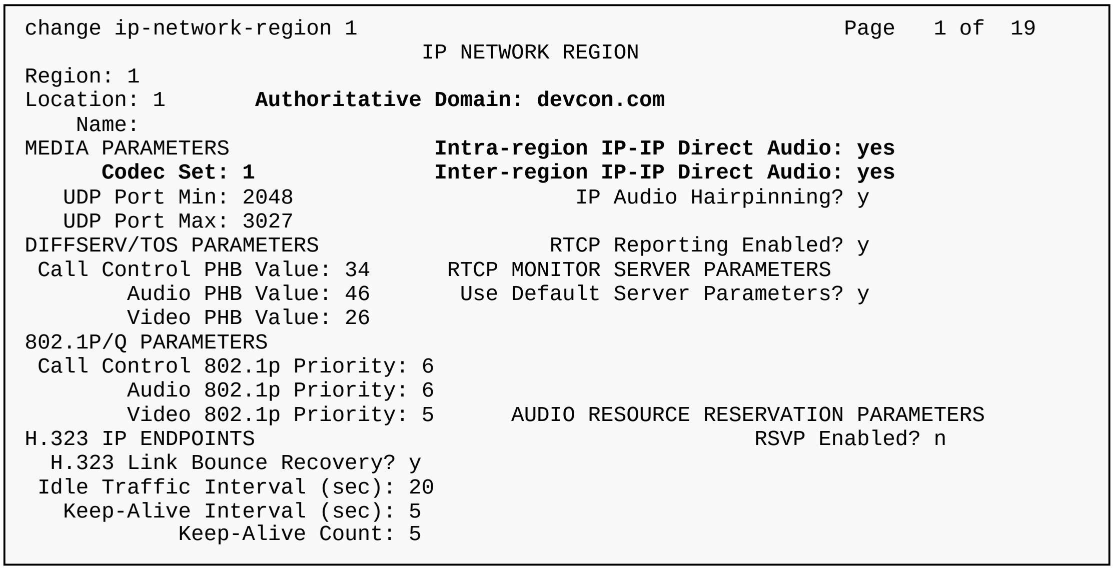
```
change node-names ip                                        Page   1 of   1
                                  IP NODE NAMES
    Name              IP Address           Name              IP Address
SES                 50 .1  .1  .50                            .   .   .
default             0  .0  .0  .0                             .   .   .
procr               50 .1  .1  .10                            .   .   .
```

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

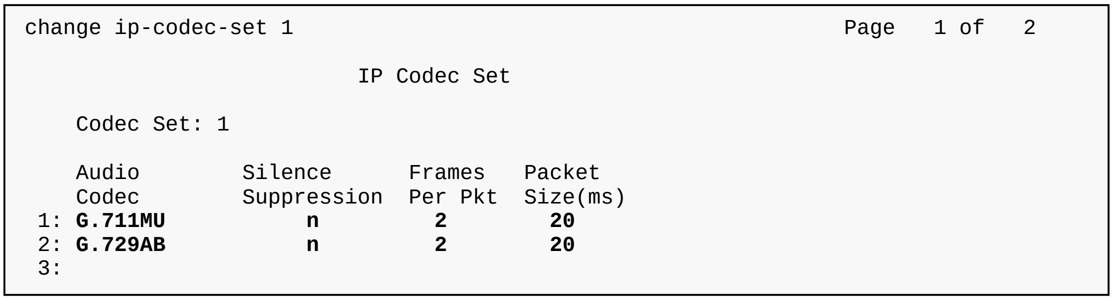
Step	Description
5.	Use the **change ip-network-region *n*** command, where ***n*** is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the region. Select an IP network region that will contain the Avaya SES server. The association between this IP network region and the Avaya SES server will be done on the **Signaling Group** form as shown in Step 7. In the case of the compliance test, the same IP network region that contains the Avaya S8300 Media Server and Avaya IP Telephones was selected to contain the Avaya SES server. By default, the Media Server and IP telephones are in IP Network Region 1.

On the **IP Network Region** form:

- The **Authoritative Domain** field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is ***devcon.com***. 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. 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.



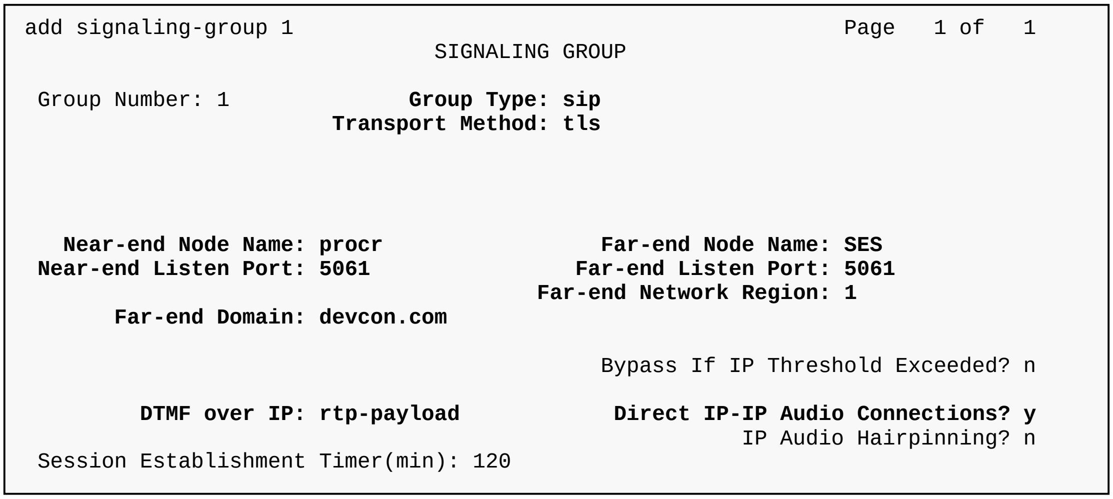
```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
Region: 1
Location: 1       Authoritative Domain: devcon.com
    Name:
MEDIA PARAMETERS              Intra-region IP-IP Direct Audio: yes
      Codec Set: 1            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
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>Use the <b>change ip-codec-set <i>n</i></b> command, where <b><i>n</i></b> is the codec set value specified in Step 5, 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. The example below shows the values used in the compliance test.

<pre>
change ip-codec-set 1   Page   1 of   2

                          IP Codec Set

    Codec Set: 1

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

Step	Description
7.	Use the **add signaling group *n*** command, where ***n*** is the number of an unused signaling group, to create the SIP signaling group as follows: ▪ Set the **Group Type** field to ***sip***. ▪ The **Transport Method** field will default to ***tls*** (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 ***procr***) and the Avaya SES server (node name ***SES***) as the two ends of the signaling group in the **Near-end Node Name** and the **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in Step 4. For alternative configurations that 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 ***5061*** 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 5. 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 ***devcon.com***. 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 ***y***. ▪ The **DTMF over IP** field must be set to the default value of ***rtp-payload*** 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. 

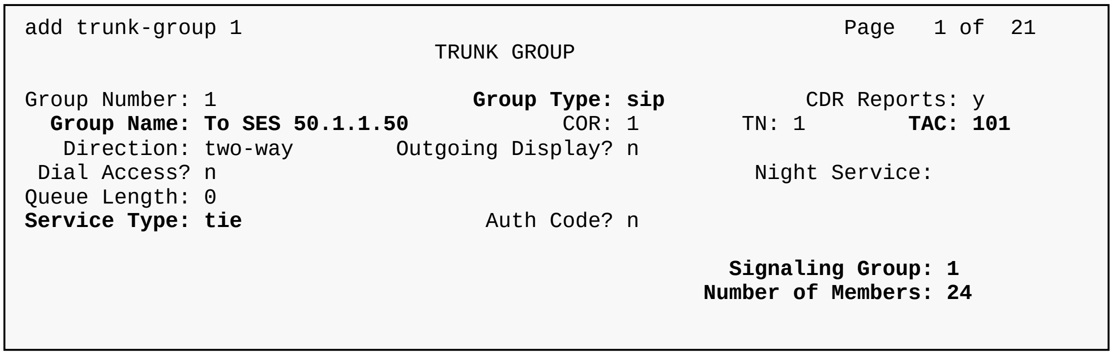
```
add signaling-group 1                                           Page   1 of   1
                                SIGNALING GROUP

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




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

                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
                                                        IP Audio Hairpinning? n
 Session Establishment Timer(min): 120
```

Step | **Description**

8. Add a SIP trunk group by using the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group. For the compliance test, trunk group number 1 was chosen.

   On Page 1, set the fields to the following values:

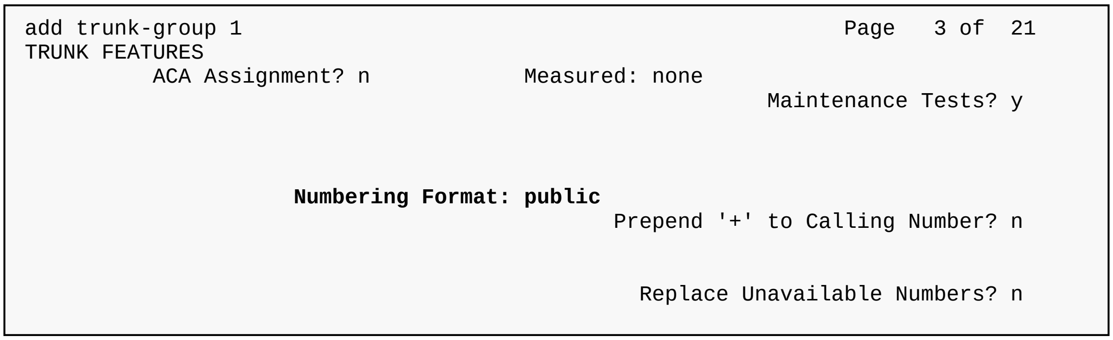
   - Set the **Group Type** field to ***sip***.
   - Choose a descriptive **Group Name**.
   - Specify an available trunk access code (**TAC**) that is consistent with the existing dial plan.
   - Set the **Service Type** field to ***tie***.
   - Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously specified in Step 7.
   - Specify the **Number of Members** supported by this SIP trunk group. As mentioned earlier, 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.
   - The default values may be retained for the other fields.



```
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
```

9. On Page 3:

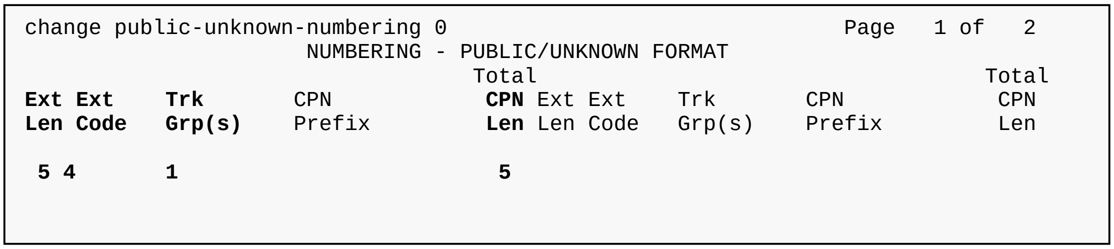
   - Verify the **Numbering Format** field is set to ***public***. This field specifies the format of the calling party number sent to the far-end.
   - The default values may be retained for the other fields.



```
add 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
```

Step **Description**

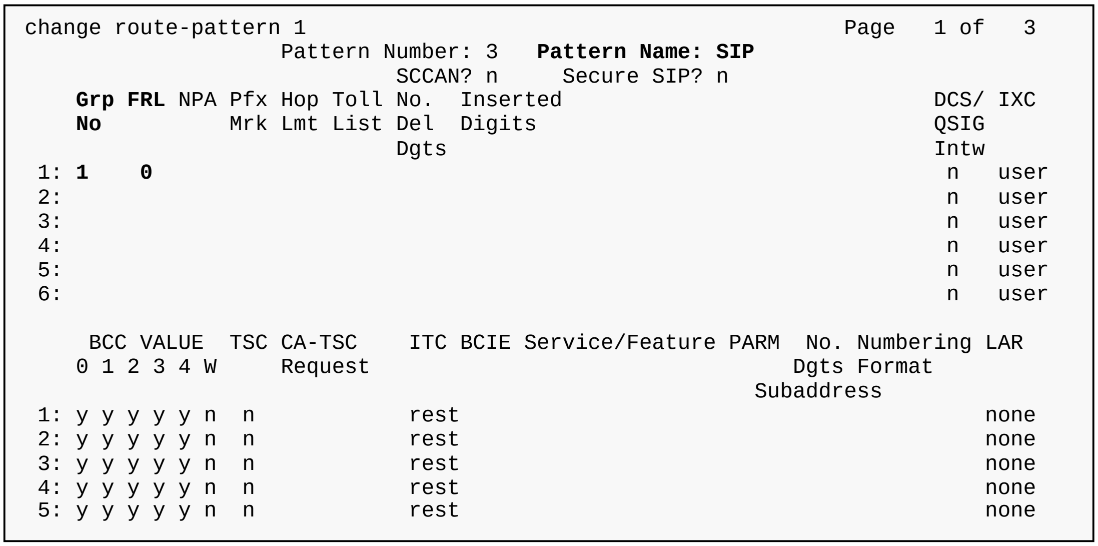
10. Use the **change public-unknown-numbering 0** command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in Step 8. In the example shown below, all calls originating from a 5-digit extension beginning with 4 and routed across trunk group 1 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.



```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                   Total                                 Total
Ext Ext    Trk       CPN            CPN Ext Ext    Trk       CPN            CPN
Len Code   Grp(s)    Prefix         Len Len Code   Grp(s)    Prefix         Len

 5 4       1                         5
```

11. Create a route pattern that will use the SIP trunk that connects to Avaya SES. In general, a route pattern is not required for calling between SIP endpoints registered to Avaya SES. This includes the dialing scenarios performed for this test configuration since the Eclipse CXC appears as registered extensions to Avaya SES. However, some transfer scenarios using alpha-numeric handles (i.e., user names) instead of extensions require a default route pattern. The creation of this default route pattern is included here for completeness.

To create a route pattern, use the **change route-pattern *n*** command, where ***n*** is the number of an unused route pattern. Enter a descriptive name for the **Pattern Name** field. Set the **Grp No** field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. The default values may be retained for all other fields.



```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 3   Pattern Name: SIP
                             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: 1    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 3 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
```

Step | **Description**

12. Use the **change locations** command to assign the default SIP route pattern to the location. In the compliance test, all SIP endpoints at the main office and branch office are part of a single location defined in Avaya Communication Manager. This location uses the default name of ***Main*** and is shown in the example below. Enter the route pattern number from the previous step in the **Proxy Sel. Rte. Pat.** field. The default values may be retained for all other fields.

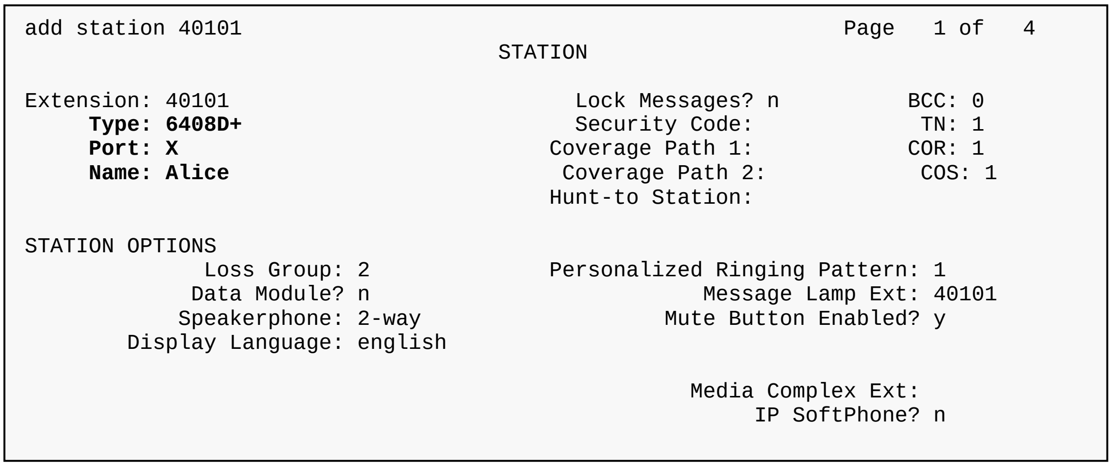
```
change locations                                             Page   1 of   4
                                   LOCATIONS

                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                                   1
 2:
 3:
```

13. All SIP stations are configured as off-PBX station (OPS) stations on Avaya Communication Manager.

Use the **display system-parameters customer-options** command to verify Avaya Communication Manager has sufficient OPS capacity available to add the OPS stations needed for the SIP telephones at the location in **Figure 1**. If there is insufficient capacity, contact an authorized Avaya sales representative or business partner to make the appropriate changes.

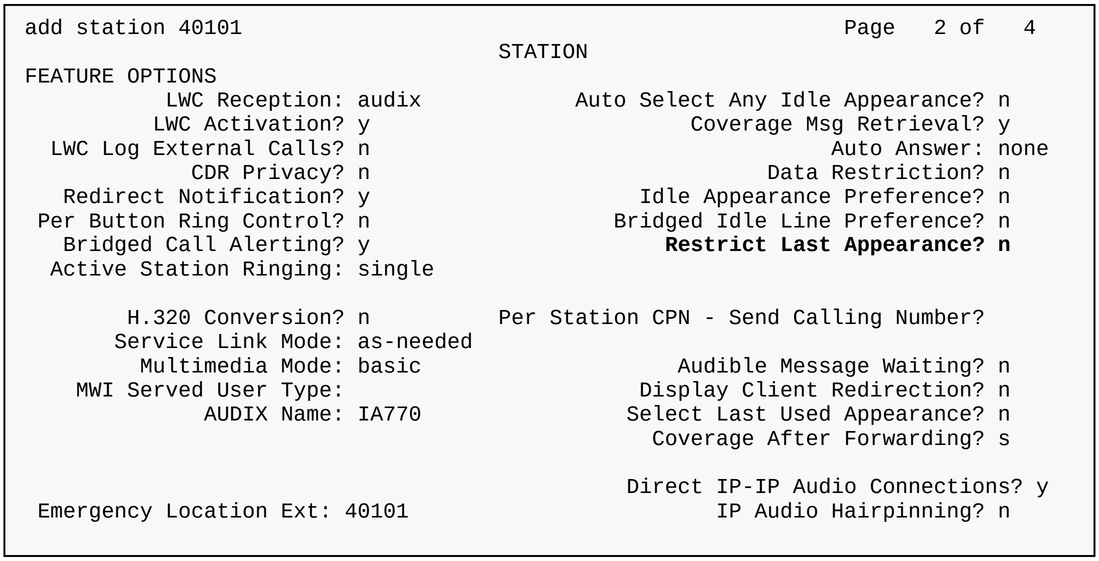
```
display system-parameters customer-options                   Page   1 of  10
                                OPTIONAL FEATURES

     G3 Version: V13
       Location: 1                           RFA System ID (SID): 1
       Platform: 13                          RFA Module ID (MID): 1

                                                            USED
                                Platform Maximum Ports: 900   121
                                      Maximum Stations: 450   41
                              Maximum XMOBILE Stations: 0     0
                    Maximum Off-PBX Telephones - EC500: 50    0
                    Maximum Off-PBX Telephones -   OPS: 50    23
                    Maximum Off-PBX Telephones - SCCAN: 0     0
```

Step	Description
14.	To add a station, use the **add station *n*** command where ***n*** is an unused extension number. Use the default value of ***6408D+*** for the **Type** field. Enter an ***X*** in the **Port** field. This indicates a station is being added without identifying a physical port for the station to use. Enter a descriptive name in the **Name** field. The default values may be retained for all other fields.



```
add station 40101                                               Page   1 of   4
                                     STATION

Extension: 40101                           Lock Messages? n          BCC: 0
     Type: 6408D+                          Security Code:             TN: 1
     Port: X                             Coverage Path 1:            COR: 1
     Name: Alice                          Coverage Path 2:            COS: 1
                                         Hunt-to Station:

STATION OPTIONS
              Loss Group: 2              Personalized Ringing Pattern: 1
             Data Module? n                          Message Lamp Ext: 40101
            Speakerphone: 2-way                   Mute Button Enabled? y
        Display Language: english

                                                    Media Complex Ext:
                                                         IP SoftPhone? n
```

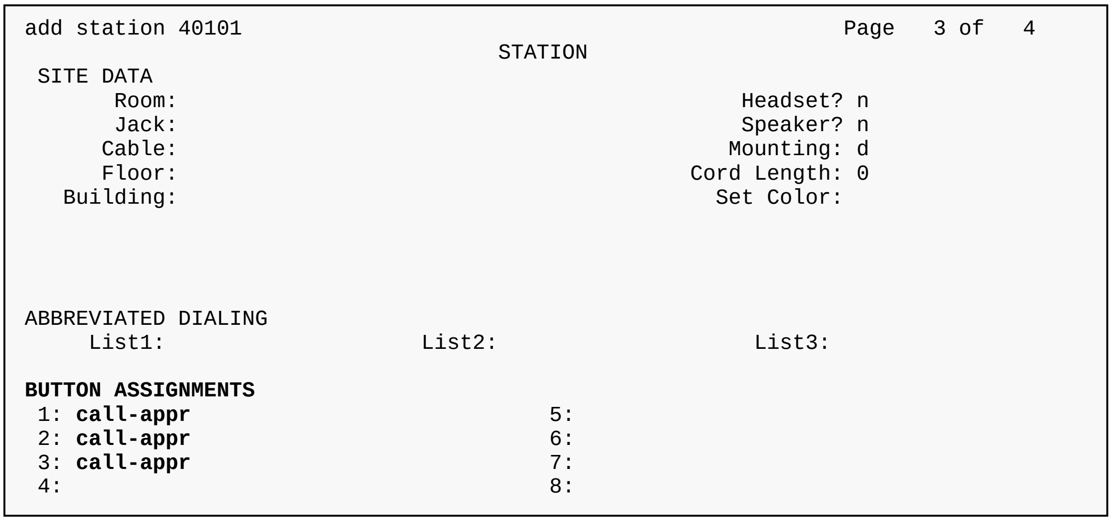
Step	Description
15.	On Page 2, set **Restrict Last Appearance** to ***n***. This will allow the last call appearance to be used for either an incoming or outgoing call.



```
add station 40101                                               Page   2 of   4
                                     STATION
FEATURE OPTIONS
           LWC Reception: audix            Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? y                       Restrict Last Appearance? n
  Active Station Ringing: single

        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                    Audible Message Waiting? n
    MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name: IA770                Select Last Used Appearance? n
                                                 Coverage After Forwarding? s

                                               Direct IP-IP Audio Connections? y
 Emergency Location Ext: 40101                        IP Audio Hairpinning? n
```

Step | **Description**

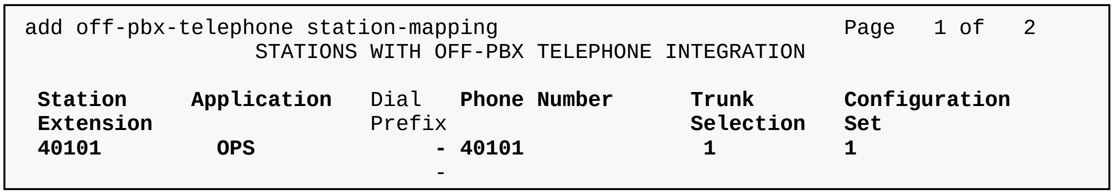
16. On Page 3, under **BUTTON ASSIGNMENTS**, create the appropriate number of call appearances for the SIP endpoint being configured. In general, the appropriate number of call appearances on Avaya Communication Manager is the same as the number of call appearances supported by the endpoint. To create a call appearance, enter ***call-appr*** as the button assignment.



```
add station 40101                                              Page   3 of   4
                                     STATION
 SITE DATA
       Room:                                           Headset? n
       Jack:                                           Speaker? n
      Cable:                                          Mounting: d
      Floor:                                      Cord Length: 0
   Building:                                         Set Color:




ABBREVIATED DIALING
     List1:                   List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                           5:
 2: call-appr                           6:
 3: call-appr                           7:
 4:                                     8:
```

17. Map the Avaya Communication Manager extension to the Avaya SES media server extension defined in Section 3.2, Step 7 with the **add off-pbx-telephone station-mapping** command. Enter the values as shown below:

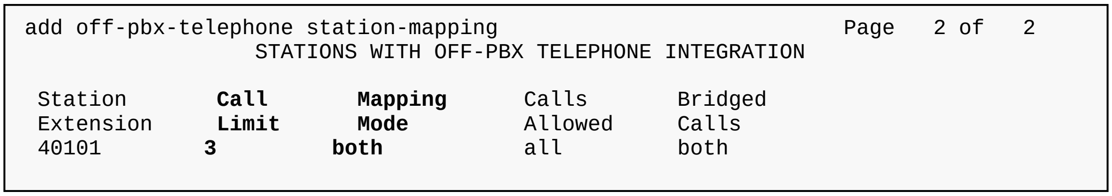
- **Station Extension**: Avaya Communication Manager extension
- **Application**: ***OPS***
- **Phone Number**: Avaya SES media server extension
- **Trunk Selection**: The SIP trunk group number
- **Configuration Set**: Enter a valid configuration set. The compliance test used configuration set 1 which contained the default values.



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

 Station     Application   Dial   Phone Number      Trunk      Configuration
 Extension                 Prefix                   Selection  Set
 40101         OPS            - 40101             1          1
                              -
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>18.</td><td>

On Page 2, set the **Call Limit** to the number of call appearances set on the station form in Step 16. Verify that the **Mapping Mode** is set to ***both***.

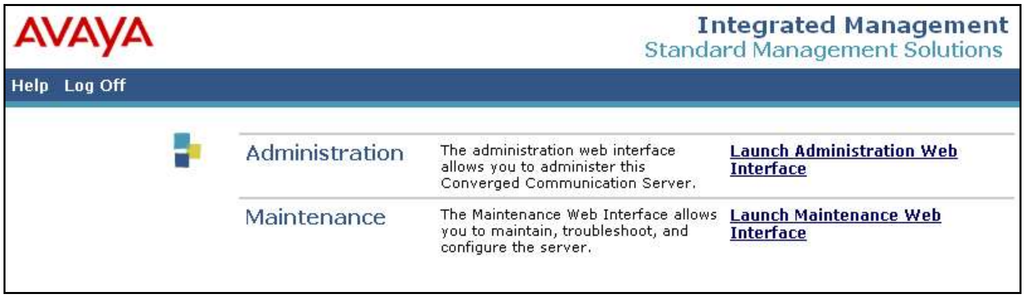


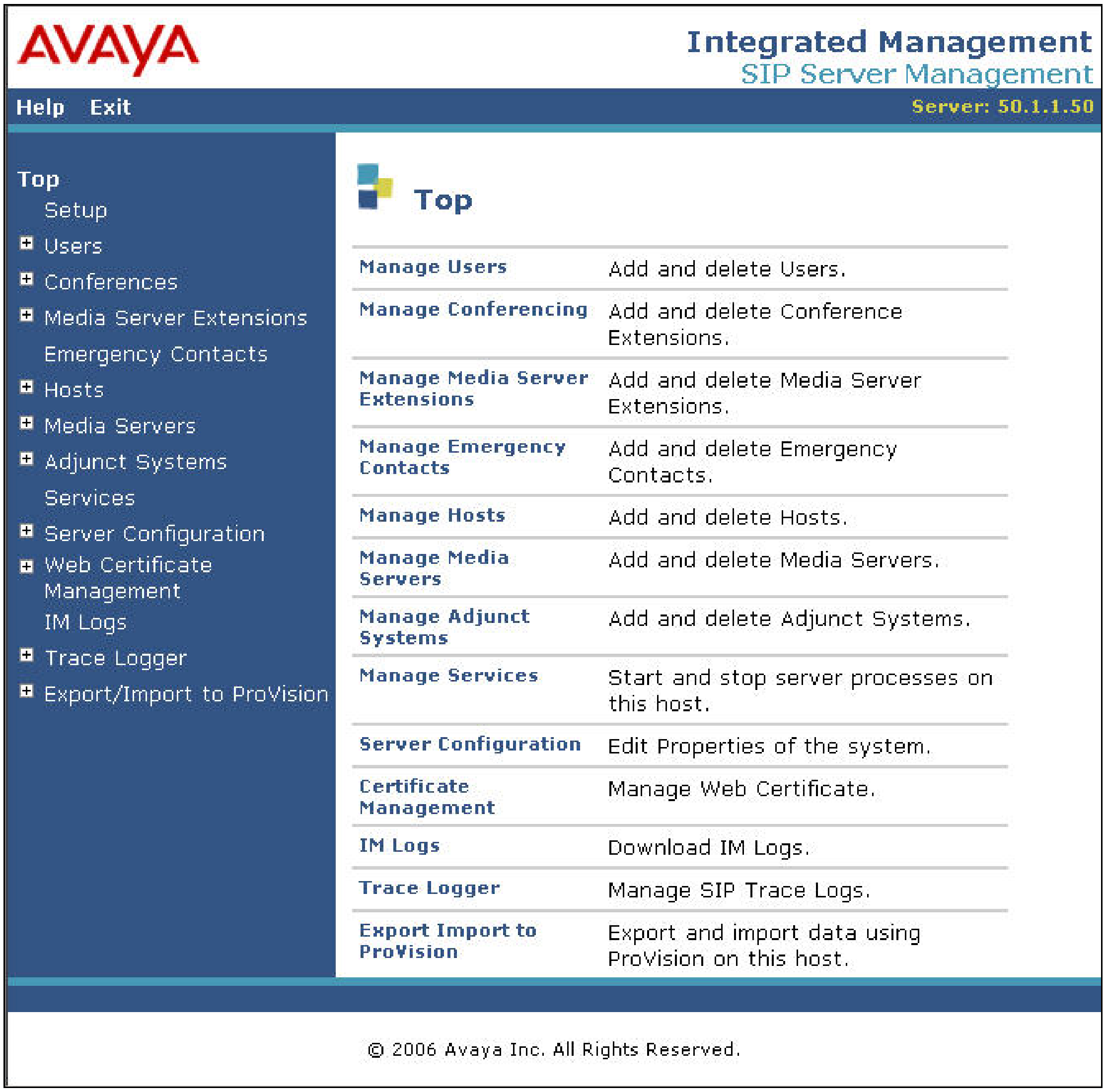
```
add off-pbx-telephone station-mapping                          Page   2 of   2
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Call       Mapping      Calls       Bridged
 Extension     Limit      Mode         Allowed     Calls
 40101        3         both           all         both
```

</td></tr>
<tr><td>19.</td><td>Repeat Steps 14 - 18 for each remaining station located at both sites.</td></tr>
</table>

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

Step	Description
2.	The Avaya SES Administration Home Page will be displayed as shown below. 

AVAYA

Integrated Management
SIP Server Management

Help Exit

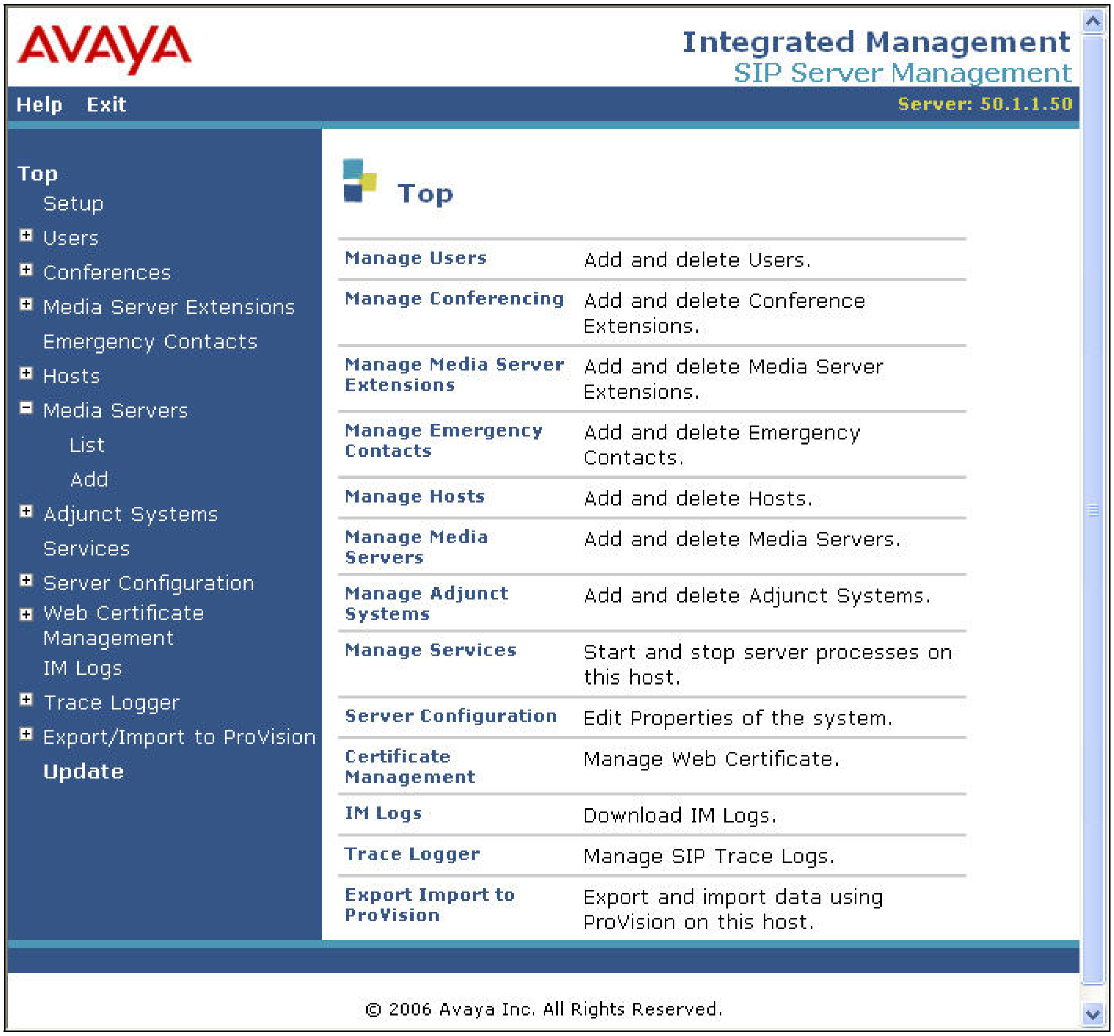
Server: 50.1.1.50

Top
- Setup
- ⊞ Users
- ⊞ Conferences
- ⊞ Media Server Extensions
- Emergency Contacts
- ⊞ Hosts
- ⊞ Media Servers
- ⊞ Adjunct Systems
- Services
- ⊞ Server Configuration
- ⊞ Web Certificate Management
- IM Logs
- ⊞ Trace Logger
- ⊞ Export/Import to ProVision

Top

Manage Users	Add and delete Users.
Manage Conferencing	Add and delete Conference Extensions.
Manage Media Server Extensions	Add and delete Media Server Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Manage Hosts	Add and delete Hosts.
Manage Media Servers	Add and delete Media Servers.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Services	Start and stop server processes on this host.
Server Configuration	Edit Properties of the system.
Certificate Management	Manage Web Certificate.
IM Logs	Download IM Logs.
Trace Logger	Manage SIP Trace Logs.
Export Import to ProVision	Export and import data using ProVision on this host.

© 2006 Avaya Inc. All Rights Reserved.

Step	Description
3.	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 below. It is recommended that this be done after making each set of changes described in the following steps. 

Integrated Management
SIP Server Management

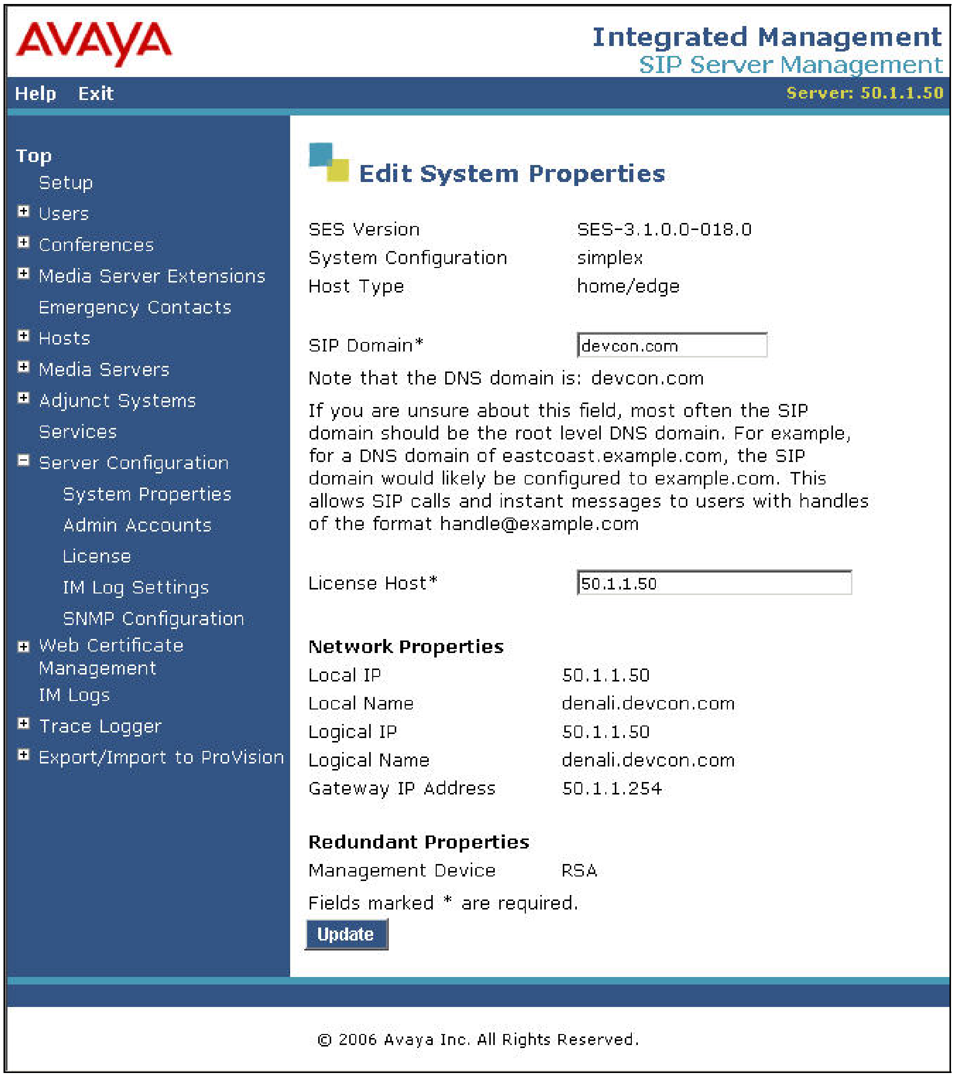
Help Exit

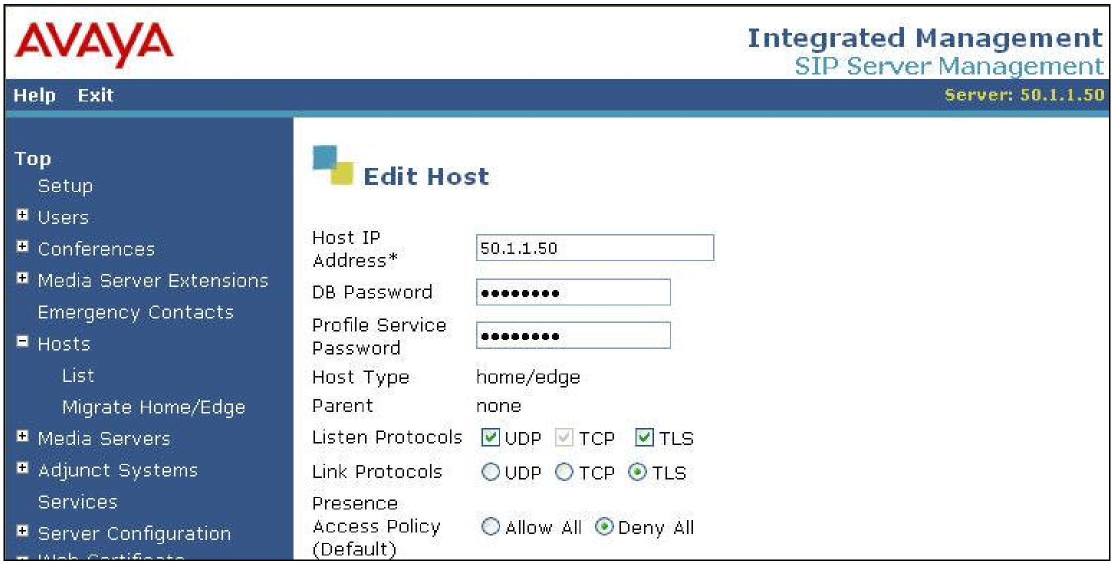
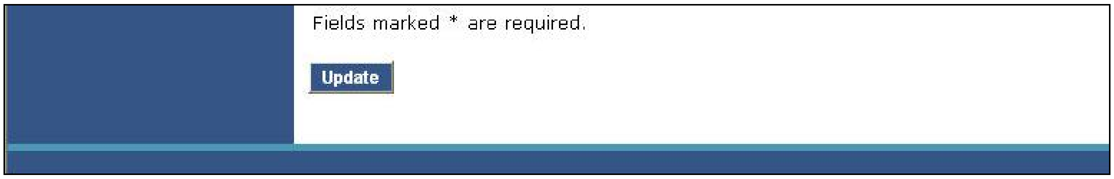
Server: 50.1.1.50

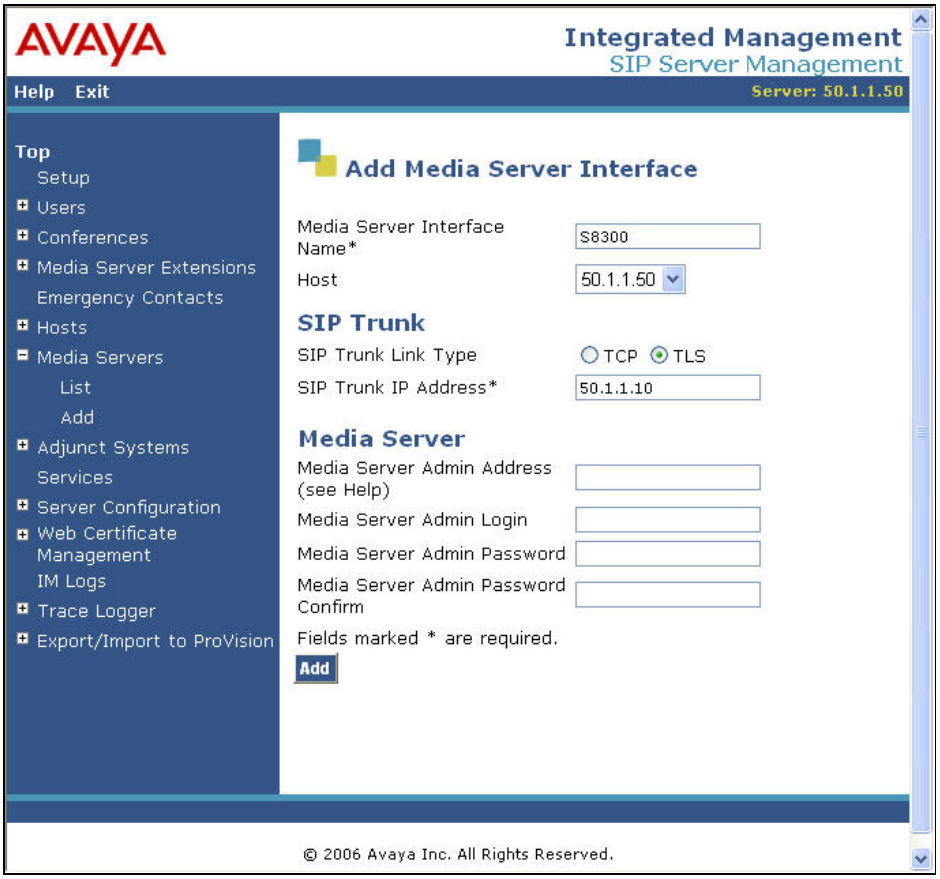
Top

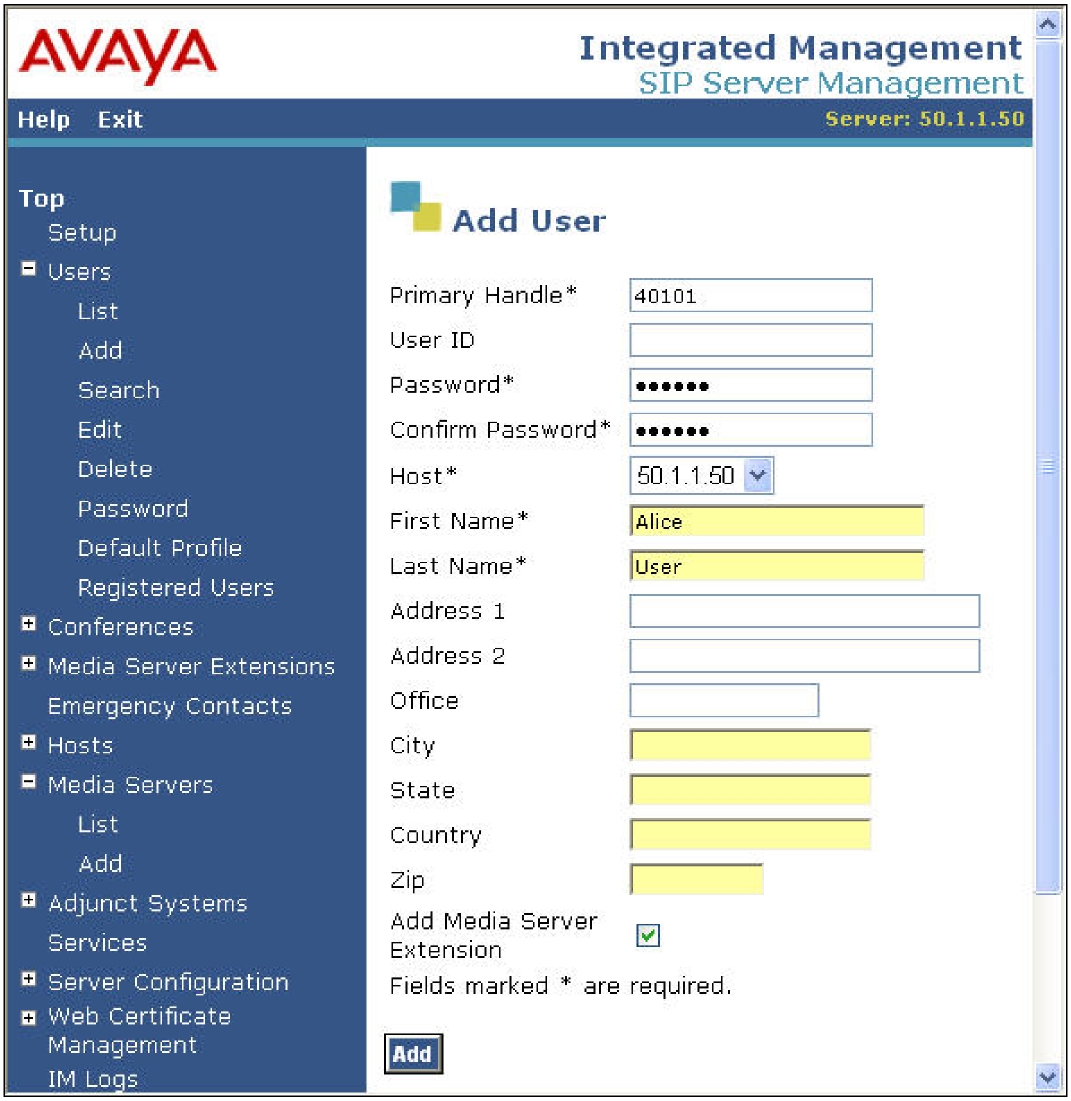
Manage Users	Add and delete Users.
Manage Conferencing	Add and delete Conference Extensions.
Manage Media Server Extensions	Add and delete Media Server Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Manage Hosts	Add and delete Hosts.
Manage Media Servers	Add and delete Media Servers.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Services	Start and stop server processes on this host.
Server Configuration	Edit Properties of the system.
Certificate Management	Manage Web Certificate.
IM Logs	Download IM Logs.
Trace Logger	Manage SIP Trace Logs.
Export Import to ProVision	Export and import data using ProVision on this host.

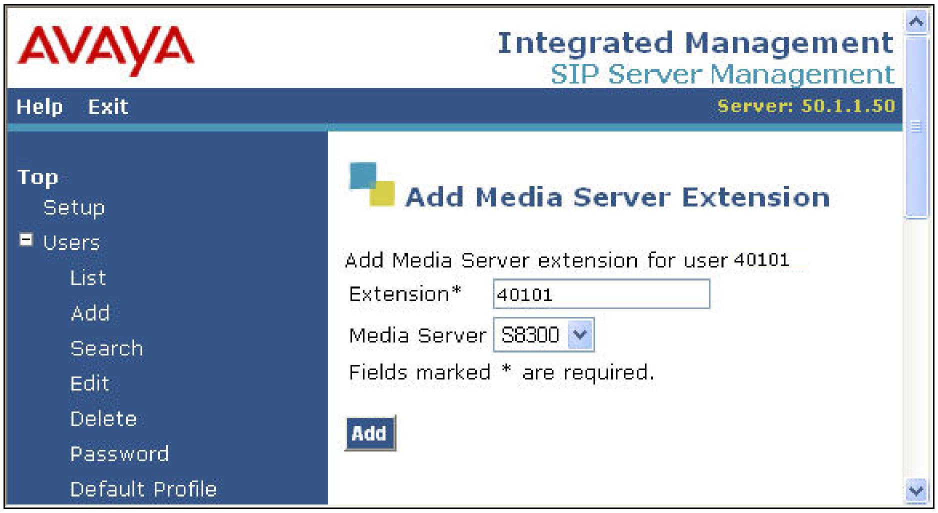
© 2006 Avaya Inc. All Rights Reserved.

Step	Description
4.	From the left pane of the administration web interface, expand the **Server Configuration** option and select **System Properties**. The **Edit System Properties** page displays the software version in the **SES Version** field and the network properties entered during the installation process. On the **Edit System Properties** page: ▪ Enter the **SIP Domain** name assigned to Avaya SES. This must match the **Authoritative Domain** field configured on Avaya Communication Manager shown in Section 3.1, Step 5. ▪ 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.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users Conferences Media Server Extensions Emergency Contacts Hosts Media Servers Adjunct Systems Services Server Configuration System Properties Admin Accounts License IM Log Settings SNMP Configuration Web Certificate Management IM Logs Trace Logger Export/Import to ProVision Update Edit System Properties SES Version SES-3.1.0.0-018.0 System Configuration simplex Host Type home/edge SIP Domain* devcon.com Note that the DNS domain is: devcon.com If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com License Host* 50.1.1.50 Network Properties 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 Management Device RSA Fields marked * are required. © 2006 Avaya Inc. All Rights Reserved.

Step	Description
5.	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. The **Edit Host** page shown below is accessible by clicking on the **Hosts → List** link in the left pane and then clicking on the **Edit** link under the **Commands** section of the subsequent page that is displayed. ▪ In the **Host IP Address** field, enter the IP address of the Avaya SES server. ▪ Enter the **DB Password** that was specified during the system installation. ▪ The default values for the other fields may be used.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users Conferences Media Server Extensions Emergency Contacts Hosts List Migrate Home/Edge Media Servers Adjunct Systems Services Server Configuration Edit Host Host IP Address* 50.1.1.50 DB Password •••••••• Profile Service Password •••••••• Host Type home/edge Parent none Listen Protocols ☑ UDP ☑ TCP ☑ TLS Link Protocols ○ UDP ○ TCP ● TLS Presence Access Policy (Default) ○ Allow All ● Deny All ▪ Scroll down to the bottom of the page and click the **Update** button.  Fields marked * are required.

Step	Description
6.	From the left pane of the administration web interface, expand the **Media Servers** 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. On the **Add Media Server Interface** page, enter the following information: ▪ Enter a descriptive name in the **Media Server Interface Name** field (e.g. S8300). ▪ In the **Host** field, select 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 shown in Step 5. ▪ Select ***TLS*** (Transport Link Security) for the **SIP Trunk 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 alternative configurations that use a C-LAN board, the **SIP Trunk IP Address** would be the IP address of the C-LAN board. ▪ The default values may be retained for all other fields. ▪ After completing the **Add Media Server Interface** page, click the **Add** button.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users Conferences Media Server Extensions Emergency Contacts Hosts Media Servers List Add Adjunct Systems Services Server Configuration Web Certificate Management IM Logs Trace Logger Export/Import to ProVision © 2006 Avaya Inc. All Rights Reserved. Add Media Server Interface Media Server Interface Name* S8300 Host 50.1.1.50 SIP Trunk SIP Trunk Link Type ○ TCP ● TLS SIP Trunk IP Address* 50.1.1.10 Media Server Media Server Admin Address (see Help) Media Server Admin Login Media Server Admin Password Media Server Admin Password Confirm Fields marked * are required. Add

Step	Description
7.	A user must be added on Avaya SES for each of the SIP extensions at the main and branch office created on Avaya Communication Manager in Section 3.1, Steps 14 - 18. From the left pane, navigate to **Users → Add**. Enter the values as shown below. ▪ **Primary Handle**: Enter the extension for this user. ▪ **Password**: Enter a valid password for logging into the SIP endpoint. ▪ **Confirm Password**: Re-enter the password. ▪ **Host**: Select the Avaya SES server from the pull-down menu. ▪ **First Name**: Any descriptive name. ▪ **Last Name**: Any descriptive name. Check the **Add Media Server Extension** checkbox. Click the **Add** button to proceed. A confirmation window will appear. Click **Continue** on this new page to proceed.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users List Add Search Edit Delete Password Default Profile Registered Users Conferences Media Server Extensions Emergency Contacts Hosts Media Servers List Add Adjunct Systems Services Server Configuration Web Certificate Management IM Logs Add User Primary Handle* 40101 User ID Password* •••••• Confirm Password* •••••• Host* 50.1.1.50 First Name* Alice Last Name* User Address 1 Address 2 Office City State Country Zip Add Media Server Extension ☑ Fields marked * are required. Add

Step	Description
8.	The **Add Media Server Extension** page will appear. In the **Extension** field, enter the same extension used in the previous step. In the **Media Server** field, select from the pull-down menu the name of the media server added in Step 6. Click the **Add** button to complete the operation.  Add Media Server extension for user 40101 Extension* 40101 Media Server S8300 Fields marked * are required.
9.	Repeat Steps 7 - 8 for each of the remaining stations at the Main location. Do the same for the branch location using the appropriate IP addresses and extensions for that site.

3.3. Configure Avaya SIP Telephones

The SIP telephones at each location will use the Eclipse CXC 350 at the main office as the call server. The SIP telephones at the main office will use the private side IP address of the Eclipse CXC 350 as the call server. The SIP telephones at the branch site will use the public side IP address of the Eclipse CXC 350 as the call server.

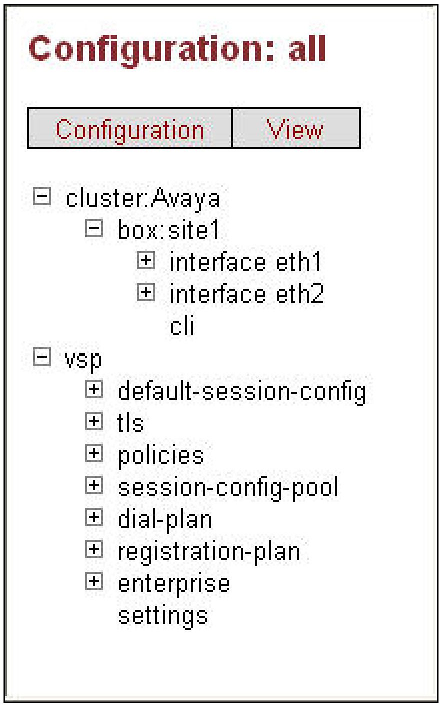
The table below shows an example of the SIP telephone networking settings for both the main and branch offices.

	Main Site	**Branch Site**
IP Address	50.1.1.53	10.75.5.12
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	50.1.1.61	192.168.1.83
Router	50.1.1.254	10.75.5.1
File Server	50.1.1.52	10.75.5.81

3.4. Configure Covergence Eclipse CXC 350

It is recommended that typical users configure the Eclipse CXC via its web interface which creates a configuration file on the device located at */cxc/cxc.cfg*. To access the web interface, launch an Internet browser and enter the IP address of the Eclipse CXC as the desired URL. A login page appears in which to enter a username and password. To view the resulting configuration file, use a text editor to open the file /c*xc/cxc.cfg.*

Whether viewing the data from the web interface or the configuration file, the configuration data is organized in a hierarchical tree structure. On the web interface, the tree structure appears in the left pane of each page. The right pane of the window shows the parameters of the item selected from the tree. The top level of the tree as represented on the web interface is shown below.



Configuration: all

```
⊟ cluster:Avaya
    ⊟ box:site1
        ⊞ interface eth1
        ⊞ interface eth2
          cli
⊟ vsp
    ⊞ default-session-config
    ⊞ tls
    ⊞ policies
    ⊞ session-config-pool
    ⊞ dial-plan
    ⊞ registration-plan
    ⊞ enterprise
      settings
```

Figure 4: Configuration Data Tree Structure

In the configuration file, each level of the tree is represented as a new level of indented text. For the purpose of these Application Notes, the configuration will be documented using excerpts from the configuration file since it is more succinct then the web interface.

Step	Description
1.	Add the private network interface. The interface is defined by the following lines in the configuration file indented under the sections of **cluster** and **box** as shown in **Figure 4**. The lines in bold are specific to the compliance test. The first specifies the IP address and mask of the interface. The second enables NAT translation. The last bold line defines what certificate to use for TLS connections. Strictly speaking, specifying the certificate to use was not required since none of the network configurations tested required use of TLS connections on the private interface. It was included for completeness. All other lines are default values.

```
config interface eth1
 config ip private
  set ip-address static 50.1.1.61/24
  config ssh
  return
  config web
  return
  config sip
   set nat-translation enabled
   set udp-port 5060
   set tcp-port 5060
   set tls-port 5061
   set certificate vsp\tls\certificate wakefield.whatever.com
  return
  config ntp-server
  return
  config icmp
  return
  config media-ports
  return
 return
return
```

Step	Description
2.	Add the public network interface. The interface is defined by the following lines in the configuration file indented under the sections of **cluster** and **box** as shown in **Figure 4**. The lines in bold are specific to the compliance test. The first specifies the IP address and mask of the interface. The second defines what certificate to use for TLS connections. The third defines the default gateway.

In this configuration (Remote Access), the Eclipse CXC does not have any TLS connections on the public interface, so specifying the TLS certificate is not required. However, this same device configuration will be used for later network configurations which will require use of TLS connections on the public interface. At that point, it will be necessary to specify the certificate to use. The details of the certificate are also defined in this file but are not specific to the compliance test and thus are not shown.

All other lines are default values.

```
config interface eth2
 config ip public
  set ip-address static 192.168.1.83/24
  config telnet
  return
  config ssh
  return
  config web
  return
  config sip
   set udp-port 5060
   set tcp-port 5060
   set tls-port 5061
   set certificate vsp\tls\certificate wakefield.whatever.com
  return
  config icmp
  return
  config media-ports
  return
  config routing
   config route default
    set gateway 192.168.1.1
   return
  return
 return
return
```

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

Configure the virtual service partition.

The functionality of the Eclipse CXC can be partitioned into multiple **virtual service partitions**. For the purposes of the compliance test, a single virtual service partition called **vsp** was used. The configuration of the vsp is what defines the behavior of the Eclipse CXC. All remaining configuration steps will configure subsections under vsp.

Locate the section of the configuration file configuring the vsp as shown below. The **domain-name** parameter is set to the SIP domain of Avaya SES as shown in bold below. Other lines show default values.

```
config vsp
 set admin enabled
 set domain-name devcon.com
 set local-normalization disabled
```

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

Step	Description
4.	Define a default session configuration. Locate the section of the configuration file as shown below (vsp→default-session-config). This section defines the default behavior of the Eclipse CXC if there is no policy or subsequent session configuration defined in the registration or dial plans that overrides the parameters set below. The lines in bold are significant to the compliance test. The first defines that the Eclipse will allow the processing of all SIP signaling traffic. The second defines that the Eclipse CXC will also anchor (process) all media streams. The last bold lines enable NAT traversal and sets related parameter **symmetricRTP**.

```
config default-session-config
  config sip-directive
   set directive allow
  return
  config media
   set anchor enabled
   config nat-traversal
    set symmetricRTP true
   return
   config recording-policy
    set record enabled
   return
   set introduction ""
   set music-on-hold ""
   set inactivity-timeout enabled "0 days 01:00:00"
   set mirror enabled
  return
  config media-type
  return
  config log-alert
   set logging enabled
  return
 return
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

Define a policy for the special handling of NOTIFY and SUBSCRIBE messages.

The default handling of NOTIFY and SUBSCRIBE messages does not interoperate with Avaya SES, so a policy was created that overrides the default behavior for these messages. The Eclipse CXC acts as a back to back user agent. The policy below will describe how NOTIFY/SUBSCRIBE messages are changed from the inbound leg of the call to the outbound leg.

Locate the section of the configuration file as shown below (vsp→policies). This section shows a **policy** named ***default*** which contains a **rule** called ***Avaya Interop Rules***. This rule has a condition list which shows when the rule is applied. The rule is applied when the request method is NOTIFY or SUBSCRIBE as shown in the second group of bold lines below. Lastly, the rule contains a description of how the outbound request URI for these messages will be constructed as shown in the third group of bold lines below. Specifically, the **user**, **host**, **port**, **display** and **transport** portions of the outbound request URI will be set to the corresponding value taken from the request URI of the inbound message.

```
config policies
 config session-policies
  set default-policy vsp\policies\session-policies\policy default
  config policy default
   config rule "Avaya Interop Rules"
    set description ""
    config condition-list
     set operation OR
     set sip-message-condition request-method match NOTIFY
     set sip-message-condition request-method match SUBSCRIBE
    return
    config session-config
     config request-uri-specification
      set user request-uri
      set host request-uri
      set port request-uri
      set display request-uri
      set transport request-uri
     return
     config session-control-settings
      set re-evaluate-new-requests enabled
     return
    return
   return
  return
 return
return
```

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

Step	Description

6. Define the session configuration pool.

The set of session configurations that can be made available to the Eclipse CXC are defined in the session configuration pool. If and when these configurations are actually used are defined elsewhere in the configuration file. In the compliance test, four session configurations were defined, named ***decryption***, ***encryption***, ***follow*** and ***Avaya REGISTER modification***.

The start of each session configuration is shown in bold below. Only the session configurations named ***follow*** and ***Avaya REGISTER modification*** are used in this network configuration (Remote Access). The session configurations named ***decryption*** and ***encryption*** will be described in the next section where they are first used.

The ***follow*** session configuration specifies that outbound encryption will follow whatever is received. More specifically, outbound traffic will be encrypted if it was received encrypted and outbound traffic will not be encrypted if it was received unencrypted.

The ***Avaya REGISTER modification*** session configuration specifies modifications required of REGISTER messages sent to Avaya SES for interoperability. Specifically, the **user** portion of the request URI is omitted and the **host**, **port** and **display** portions are set to the next-hop which is the IP address of Avaya SES.

```
config session-config-pool
 config entry decryption
  config in-encryption
   set mode require
  return
 return
 config entry encryption
  config out-encryption
   set mode require
  return
 return
 config entry follow
  config out-encryption
   set mode follow
  return
 return
 config entry "Avaya REGISTER modification"
  config request-uri-specification
   set user omit
   set host next-hop
   set port next-hop
   set display next-hop
  return
 return
return
```

Step	Description
7.	Define the dial plan. The dial plan defines how calls are routed through the Eclipse CXC. Locate the section of the configuration file as shown below (vsp→dial-plan). This section shows a single **route** called ***route SES calls***. The first bold line below defines that the route is taken when the request-uri matches the ***default***. The ***default*** means all calls. The second bold line defines the destination for these calls which is a **peer server** named ***SES***. The characteristics of this server are defined in Step 9.

```
config dial-plan
 config route "route SES calls"
  set request-uri-match default
  set peer server "vsp\enterprise\servers\sip-gateway SES"
  config outbound
   set host-normalizations request-uri+to-header+from-header
  return
  config session-config
   config contact-uri-settings-outLeg
    set add-maddr disabled
   return
  return
 return
return
```

Step	Description
8.	Define the registration plan. The registration plan defines how registrations are routed through the Eclipse CXC. Locate the section of the configuration file as shown below (vsp→registration-plan). This section shows a single **route** called ***SES***. The first bold line below defines that the route is taken when the URI in the To header matches the ***default***. The ***default*** means any value in the To header. The next three lines define the changes in the IP addresses in the request URI, To header and From header that are required when the registrations pass through the Eclipse CXC. Initially, these IP addresses reflect the IP address of the Eclipse CXC and must be changed to the IP address of the next hop. In this case, the next hop is Avaya SES and is defined in the **set peer server** line in the example below. The characteristics of this server are defined in Step 9. The last bold line below specifies that the session configuration named ***Avaya REGISTER modification*** from the session configuration pool defined in Step 6 must also be applied to this route. This configuration defines further modifications to the request URI needed for interoperability.

```
 config registration-plan
  config route SES
   set to-uri-match default
   set alter-request-uri next-hop-ip
   set alter-to-uri next-hop-ip
   set alter-from-uri next-hop-ip
   set peer server "vsp\enterprise\servers\sip-gateway SES"
   set session-config-pool-entry vsp\session-config-pool\entry "Avaya
REGISTER modification"
  return
 return
```

Step	Description
9.	Define the servers.

Servers are entities known to the Eclipse CXC to which it may need to communicate. A server needs to be defined for Avaya SES. Locate the section of the configuration file as shown below (vsp→enterprise→servers). This section shows a single **server** defined as a **sip-gateway** called ***SES***. The lines in bold are relevant to the compliance test. The first two bold lines define the **peer identity** and **domain** of Avaya SES. The third bold line specifies that the session configuration named ***follow*** from the session configuration pool in Step 6 will be applied to all outbound traffic to this server. Specifically, no encryption is applied unless the input media is encrypted. In this configuration, the input is never encrypted so the output isn't either. The last bold lines define the IP address of this server which is the IP address of the Avaya SES server.

```
 config enterprise
  config servers
   config sip-gateway SES
    set peer-identity sip:50.1.1.50
    set domain devcon.com
    set routing-setting ""
    set failover-detection none
    set user ""
    set password-tag ""
    set outbound-session-config-entry vsp\session-config-pool\entry
follow
    config server-pool
     config server ses
      set host 50.1.1.50
     return
    return
   return
  return
 return
config settings
  set max-number-of-sessions 10000
  set out-of-context-message-action refuse 400
  set out-of-context-message-media-cleanup disabled
 return
return
```

4. Secure Remote Access Configuration

This section describes the procedures for configuring the devices in the Secure Remote Access network configuration.

4.1. Configure Avaya Communication Manager

Use the same procedure as described in Section 3.1.

4.2. Configure Avaya SES

Use the same procedure as described in Section 3.2.

4.3. Configure Avaya SIP Telephones

The SIP telephones at the main office will use the private side IP address of the Eclipse CXC 350 as the call server. The SIP telephones at the branch site will use the private side IP address of the Eclipse CXC 50 as the call server.

The table below shows an example of the SIP telephone networking settings for both the main and branch offices.

	Main Site	**Branch Site**
IP Address	50.1.1.53	10.75.5.12
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	50.1.1.61	10.75.5.61
Router	50.1.1.254	10.75.5.1
File Server	50.1.1.52	10.75.5.81

4.4. Configure the Main Office Covergence Eclipse CXC 350

Use the same procedure as described in Section 3.4 with the exception of the following.

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

Define the session configuration pool.

The same session configurations are defined here as were defined in Section 3.4 Step 6. The start of each configuration is shown in bold below. However, this network configuration (Secure Remote Access) will use all four session configurations instead of just the last two like the previous network configuration.

The ***decryption*** session configuration specifies that incoming media will be decrypted and encryption is required on the incoming stream. Any unencrypted media stream will be rejected.

The ***encryption*** session configuration specifies that outgoing media will be encrypted and support for encryption is required by the far-end.

See Section 3.4, Step 6 for descriptions of ***follow*** and ***Avaya REGISTER modification***.

```
config session-config-pool
  config entry decryption
   config in-encryption
    set mode require
   return
  return
  config entry encryption
   config out-encryption
    set mode require
   return
  return
  config entry follow
   config out-encryption
    set mode follow
   return
  return
  config entry "Avaya REGISTER modification"
   config request-uri-specification
    set user omit
    set host next-hop
    set port next-hop
    set display next-hop
   return
  return
 return
```

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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Define the registration plan.

An additional route is added to the configuration in Section 3.4, Step 8 and is shown in bold below. The new route is a **source-route** named ***CXC50-Site2***. If a call matches the criteria of both entries, the source-route takes precedence. Multiple source-routes must be unique. The second bold line below specifies this new route is used when the source of the registration comes from the **server** named ***CXC50-Site2***. The next line specifies the registration is then sent to the **peer server** named ***SES***.

```
config registration-plan
  config route SES
   set to-uri-match default
   set alter-request-uri next-hop-ip
   set alter-to-uri next-hop-ip
   set alter-from-uri next-hop-ip
   set peer server "vsp\enterprise\servers\sip-gateway SES"
   set session-config-pool-entry vsp\session-config-pool\entry "Avaya
REGISTER modification"
  return
  config source-route CXC50-Site2
   set source-match server "vsp\enterprise\servers\sip-connection
CXC50-Site2"
   set peer server "vsp\enterprise\servers\sip-gateway SES"
  return
 return
```

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

Step	Description
3.	Define the servers.

An additional server is added to the configuration in Section 3.4, Step 9 and is shown starting with the line “config sip-connection CXC50-Site2”. The new server is defined as a **sip-connection** named ***CXC50-Site2***. The **host**, **domain** and **peer-identity** parameters are set to values reflecting the IP address and domain of the Eclipse CXC 50 at the branch location. The **transport** and **port** parameters specify that ***TLS*** will be used on port ***5061*** to communicate to this remote server. The **transport** parameter also specifies the certificate to use. The details of the certificate are not specific to the compliance test and thus are not shown. The **inbound-session-config-entry** parameter specifies that the session configuration named ***decryption*** in the session configuration pool defined in Step 1 will be applied to inbound traffic. Lastly, the **outbound-session-config-entry** parameter specifies that the session configuration named ***encryption*** in the session configuration pool defined in Step 1 will be applied to outbound traffic.

```
 config enterprise
  config servers
   config sip-gateway SES
    set peer-identity sip:50.1.1.50
    set domain devcon.com
    set routing-setting ""
    set failover-detection none
    set user ""
    set password-tag ""
    set outbound-session-config-entry vsp\session-config-pool\entry
follow
    config server-pool
     config server ses
      set host 50.1.1.50
     return
    return
   return
   config sip-connection CXC50-Site2
    set peer-identity sip:192.168.1.84
    set domain devcon.com
    set failover-detection none
    set ping-interval 1
    set user ""
    set password-tag ""
    set service-type external
    set inbound-session-config-entry vsp\session-config-pool\entry
decryption
    set outbound-session-config-entry vsp\session-config-pool\entry
encryption
    set host 192.168.1.84
    set transport TLS "vsp\tls\certificate wakefield.whatever.com"
    set port 5061
   return
  return
 return
config settings
  set max-number-of-sessions 10000
  set out-of-context-message-action refuse 400
  set out-of-context-message-media-cleanup disabled
 return
return
```

4.5. Configure the Branch Office Covergence Eclipse CXC 50

This section describes the configuration of the Eclipse CXC 50 located at the branch office.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Add the private network interface. The interface is defined in the same manner as was done in Section 3.4, Step 1. The lines in bold show changes which are specific to the Eclipse CXC 50 at the branch office. The first specifies the IP address and mask of the interface. The next bold line specifies that this interface will only accept SIP connections on UDP port 5060.
<pre>
config interface eth1
 config ip phones
  <b>set ip-address static 10.75.5.61/24</b>
  config telnet
  return
  config ssh
  return
  config web
  return
  config sip
   set nat-translation enabled
   <b>set udp-port 5060</b>
  return
  config icmp
  return
  config media-ports
  return
 return
return
</pre></td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Add the public network interface. The interface is defined in the same manner as was done in Section 3.4, Step 2. The lines in bold show changes which are specific to the Eclipse CXC 50 at the branch office. The first specifies the IP address and mask of the interface. The next two lines define that this interface will only accept SIP connections using TLS on port 5061 and the certificate that is required. The last bold line defines the default gateway.

```
config interface eth0
 config ip To-Site1
  set ip-address static 192.168.1.84/24
  config ssh
  return
  config web
  return
  config sip
   set tls-port 5061
   set certificate vsp\tls\certificate wakefield.whatever.com.pfx
  return
  config icmp
  return
  config media-ports
  return
  config routing
   config route def
    set gateway 192.168.1.1
   return
  return
 return
return
```

</td></tr>
<tr><td>3.</td><td>

Configure the virtual service partition.

The configuration is the same as the Eclipse CXC 350 at the main site (Section 3.4, Step 3) since the branch office is part of the same SIP domain.

```
config vsp
 set admin enabled
 set domain-name devcon.com
 set local-normalization disabled
```

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

Define a default session configuration.

The configuration is the same as the Eclipse CXC 350 at the main site (Section 3.4, Step 4).

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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

Define the session configuration pool.

Two session configurations were defined in the pool, named ***encryption*** and ***decryption***. Although named the same as session configurations on the Eclipse CXC 350 at the main site, they are defined slightly differently. No session configuration is needed for modifications to REGISTER messages since the Eclipse CXC 50 at the branch office in this network configuration (Secure Remote Access) does not interface directly with Avaya SES. The start of each session configuration is shown in bold below.

The ***encryption*** session configuration specifies that use of encryption will be offered to the far-end. If accepted, outgoing media will be encrypted.

The ***decryption*** session configuration specifies that encryption will be allowed on incoming media. If encrypted, decryption will be applied.

```
config session-config-pool
 config entry encryption
  config out-encryption
   set mode offer
  return
 return
 config entry decryption
  config in-encryption
   set mode allow
  return
 return
return
```

</td></tr>
<tr><td>6.</td><td>No special policy is needed for NOTIFY and SUBSCRIBE messages since the Eclipse CXC 50 at the branch site does not interface directly with the SES in this network configuration (Secure Remote Access).</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>

Define the dial plan.

The dial plan shows a single **route** called ***CXC350-Site1***. The first bold line below defines that the route is taken when the request-uri matches the ***default***. The ***default*** means all calls. The second bold line defines the destination for these calls which is a **peer server** named ***CXC350-Site1***. The characteristics of this server are defined in Step 9.

```
 config dial-plan
  config route CXC350-Site1
   set request-uri-match default
   set peer server "vsp\enterprise\servers\sip-gateway CXC350-Site1"
   config outbound
    set host-normalizations request-uri+to-header+from-header
   return
  return
 return
```

</td></tr>
<tr><td>8.</td><td>

Define the registration plan.

The registration plan shows a single **route** named ***CXC350-Site1***. The first bold line below defines that the route is taken when the URI in the To header matches the ***default***. The ***default*** means any value in the To header. The second bold line defines the destination for these calls which is the **peer server** named ***CXC350-Site1***.

```
config registration-plan
  config route CXC350-Site1
   set to-uri-match default
   set peer server "vsp\enterprise\servers\sip-gateway CXC350-Site1"
  return
 return
```

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

Step	Description
9.	Define the servers. A server needs to be defined for the Eclipse CXC at the main office. Locate the section of the configuration file as shown below (vsp→enterprise→servers). This section shows a single **server** defined as a **sip-gateway** called ***CXC350-Site1***. The lines in bold are relevant to the compliance test. The first two bold lines define the peer identity and domain of Eclipse CXC at the main office. The third bold line specifies that the session configuration named ***decryption*** from the session configuration pool in Step 6 will be applied to all inbound traffic to this server. The fourth bold line specifies that the session configuration named ***encryption*** from the session configuration pool in Step 6 will be applied to all outbound traffic to this server. The next bold line defines the IP address of this server which is the public IP address of the Eclipse CXC 350 at the main office. The remaining bold lines define that a ***TLS*** connection using the specified certificate on port ***5061*** will be used to communicate with this server.

```
config enterprise
  config servers
   config sip-gateway CXC350-Site1
    set peer-identity sip:192.168.1.83
    set domain devcon.com
    set routing-setting ""
    set failover-detection none
    set ping-interval 3
    set user ""
    set password-tag ""
    set peer-max-interval 1800
    set peer-min-interval 60
    set client-max-interval 60
    set inbound-session-config-entry vsp\session-config-pool\entry
decryption
    set outbound-session-config-entry vsp\session-config-pool\entry
encryption
    config server-pool
     config server CXC350-Site1
      set host 192.168.1.83
      set transport TLS "vsp\tls\certificate
wakefield.whatever.com.pfx"
      set port 5061
     return
    return
   return
  return
 return
return
```

5. Secure SIP Trunking Configuration

This section describes the procedures for configuring the devices in the Secure SIP Trunking network configuration.

5.1. Configure Avaya Communication Manager

For the main office, use the same procedure as described in Section 3.1. For the branch office, repeat the same procedure to configure Avaya Communication Manager at that site. For the branch office, the following parameters apply:

IP address of Avaya S8300 Media Server – 10.75.5.2
IP address of Avaya SES – 10.75.5.6
SIP domain – business.com
Extensions – 3xxxx

SIP telephones at the branch office need to be added as OPS stations to the branch office Avaya Communication Manager. In this configuration, the branch office SIP telephones will register to the branch office Avaya SES. Lastly, perform the additional steps shown below to add the routing necessary to place calls between the two sites.

Step	Description
1.	Calls are routed to the route pattern via the dial plan and Automatic Alternate Routing (AAR). For the Main site, the dial plan defines dialing patterns of the form 4xxxx are extensions, and patterns of the form 3xxxx are sent to AAR.

```
change dialplan analysis
Page   1 of  12

DIAL PLAN ANALYSIS TABLE

Percent Full:    3

      Dialed  Total  Call
Dialed  Total  Call
Dialed  Total  Call
      String  Length Type
String  Length Type
String  Length Type
        1       3    dac
        2       5    aar
```

For the branch site, the dial plan defines dialing patterns of the form 3xxxx are extensions, and patterns of the form 4xxxx are sent to AAR.

```
change dialplan analysis
Page   1 of  12

DIAL PLAN ANALYSIS TABLE

Percent Full:    3

      Dialed  Total  Call
Dialed  Total  Call
Dialed  Total  Call
      String  Length Type
String  Length Type
String  Length Type
        1       3    dac
        2       5    aar
```

Step	Description
2.	The **AAR Digit Analysis Table** shows the AAR calls are routed to the route pattern which connects to Avaya SES defined in Section 3.1, Step 8. For the Main site, these are calls of the form 3xxxx.

```
change aar analysis 0
Page   1 of   2

AAR DIGIT ANALYSIS TABLE

Percent Full:    3

          Dialed
Total     Route    Call
Node  ANI
          String
Min  Max  Pattern   Type
Num   Reqd
    2
7    7     254      aar
```

At the branch site, calls of the form 4xxxx are routed to the route pattern defined in Section 3.1, Step 8.

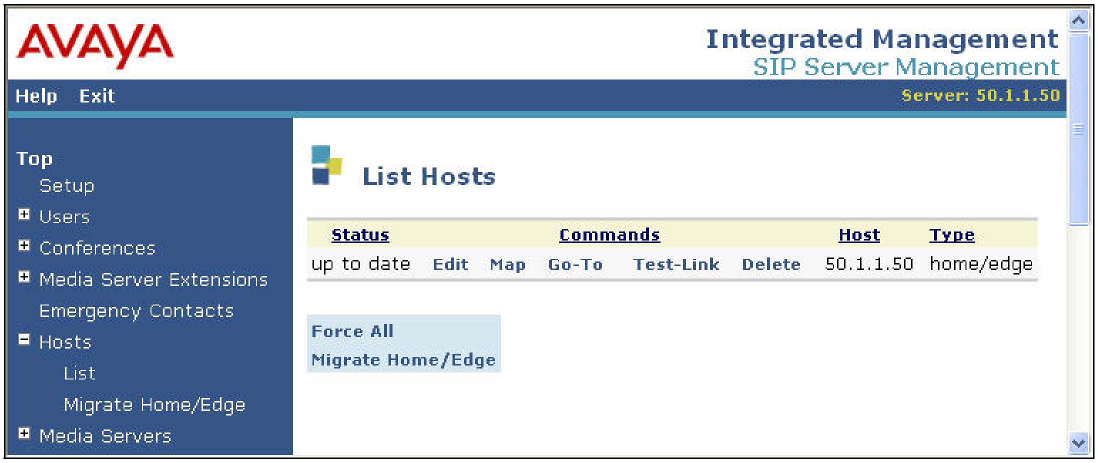
```
change aar analysis 0
Page   1 of   2

AAR DIGIT ANALYSIS TABLE

Percent Full:    3

          Dialed
Total     Route    Call
Node  ANI
          String
Min  Max  Pattern   Type
Num   Reqd
    2
7    7     254      aar
```

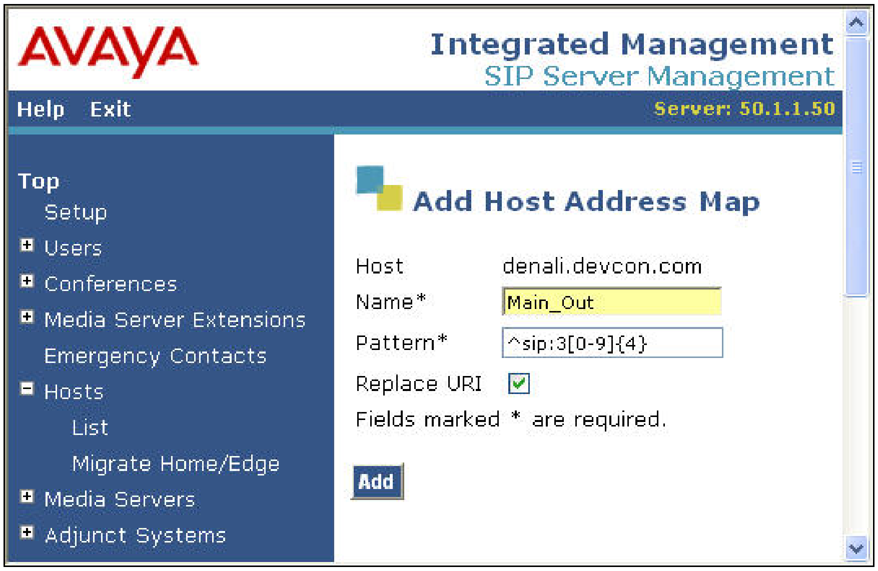
5.2. Configure Avaya SES

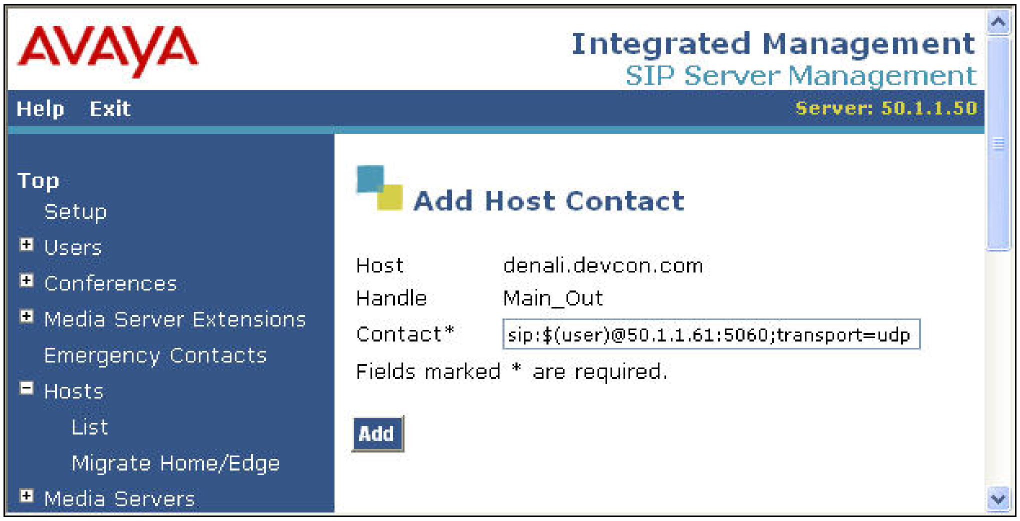
For the main office, use the same procedure as described in Section 3.2. For the branch office, repeat the same procedure to configure Avaya SES at that site. For the branch office, the following parameters apply:

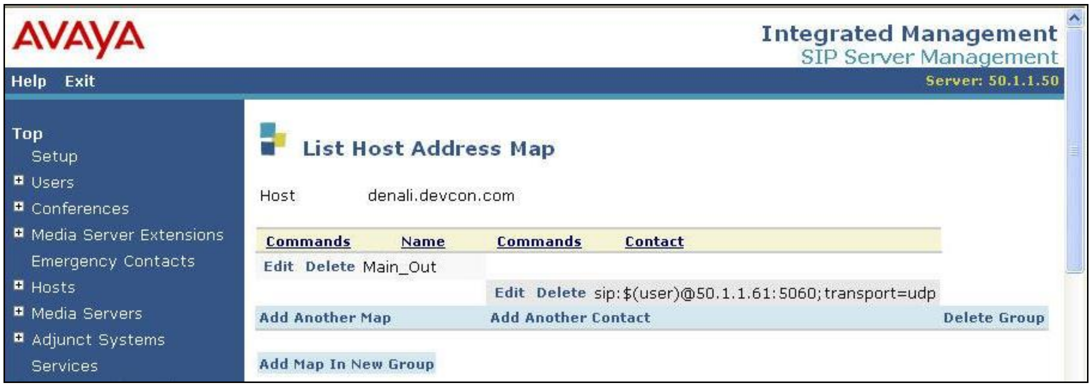
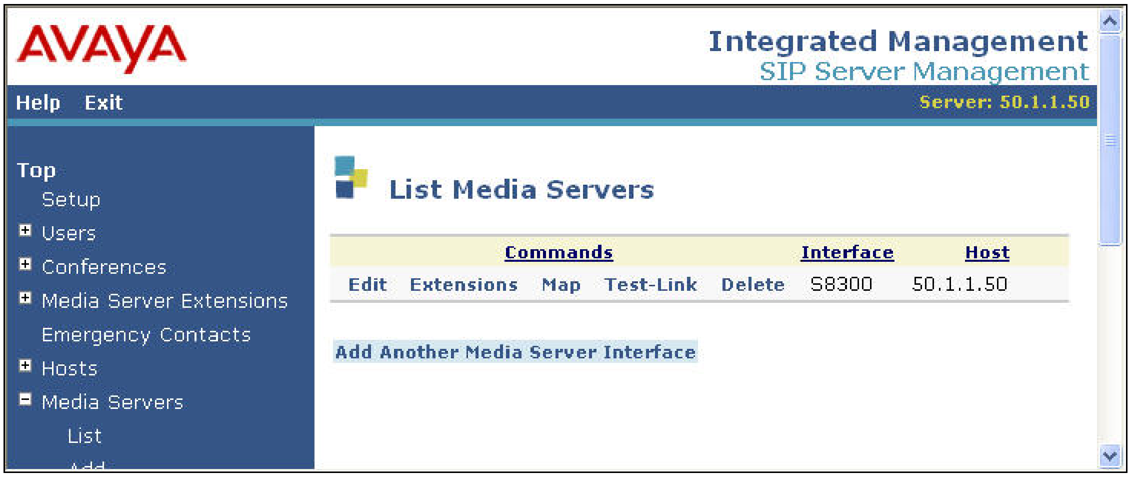
IP address of Avaya S8300 Media Server – 10.75.5.2
IP address of Avaya SES – 10.75.5.6
SIP domain – business.com
Extensions – 3xxxx

SIP users at the branch office are added to Avaya SES at the branch office. Lastly, perform the additional steps shown below to add the routing necessary to place calls between the two sites.

Step	Description
1.	A Host Address Map is required on Avaya SES at the main office to direct calls outbound from Avaya Communication Manager to the Eclipse CXC 350. In this configuration, the Eclipse CXC 350 does not register as a set of endpoints with Avaya SES. Thus, calls are not automatically routed to the Eclipse CXC 350 based on a registered extension. Instead, an Address Map is used to route calls based on the contents of the SIP INVITE URI matching a specified pattern to determine the proper destination of the call. The URI takes the form of *sip:user@domain*, where *domain* can be a domain name or an IP address. The user portion can be an alpha-numeric name, telephone number or extension. In the case of the compliance test, the user portion contained the called party number. All calls bound for the branch office were routed to the Eclipse CXC 350. Thus, the Host Address Map was configured to match all calls dialed with a 5 digit number beginning with a 3. To configure a Host Address Map: ▪ Expand the **Hosts** option in the left pane of the administration web interface and select **List**. This will display the **List Hosts** page below. ▪ Click on the **Map** link associated with the appropriate host to display the **List Host Address Map** page (not shown). On this page, click on the **Add Map In New Group** link.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users Conferences Media Server Extensions Emergency Contacts Hosts List Migrate Home/Edge Media Servers List Hosts Force All Migrate Home/Edge Status — Commands — Host — Type up to date — Edit Map Go-To Test-Link Delete — 50.1.1.50 — home/edge

Step	Description
2.	On the **Add Host Address Map** page that appears: ▪ Enter a descriptive name in the **Name** field. ▪ In the **Pattern** field, enter an expression to define the matching criteria for calls to be routed to the Eclipse CXC 350. The example below shows the expression used in the compliance test. This expression will match an URI that begins with ***sip:3*** followed by any digit between ***0-9*** for the next ***4*** digits. Appendix A contains additional information on the syntax used for Address Map patterns. Click the **Add** button.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users Conferences Media Server Extensions Emergency Contacts Hosts List Migrate Home/Edge Media Servers Adjunct Systems Add Add Host Address Map Host denali.devcon.com Name* Main_Out Pattern* ^sip:3[0-9]{4} Replace URI ☑ Fields marked * are required.

Step	Description
3.	Next, a Host Contact must be entered for the Address Map that was previously defined. The Host Contact defines the destination IP address, port number and transport protocol to use when routing calls that match the Address Map. To add a Host Contact: ▪ Open the **List Host Address Map** page as described (but not shown) in Step 1. ▪ Click on the **Add Another Contact** link associated with the Address Map added previously, to open the **Add Host Contact** page shown below. ▪ In the **Contact** field, enter the destination IP address (ip_addr), port number (port) and transport protocol (protocol) in the following format. `sip:$(user)@`**`ip_addr`**`:`**`port`**`;transport=`**`protocol`** The user part in the original request URI is inserted in place of the "$(user)" string before the message is sent to the destination. For the compliance test, the Eclipse 350 had IP address of 50.1.1.61. Thus, the following Host Contact value was used: `sip:$(user)@50.1.1.61:5060;transport=udp` Click the **Add** button.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup ⊞ Users ⊞ Conferences ⊞ Media Server Extensions Emergency Contacts ⊟ Hosts List Migrate Home/Edge ⊞ Media Servers Add Add Host Contact Host denali.devcon.com Handle Main_Out Contact* sip:$(user)@50.1.1.61:5060;transport=udp Fields marked * are required.

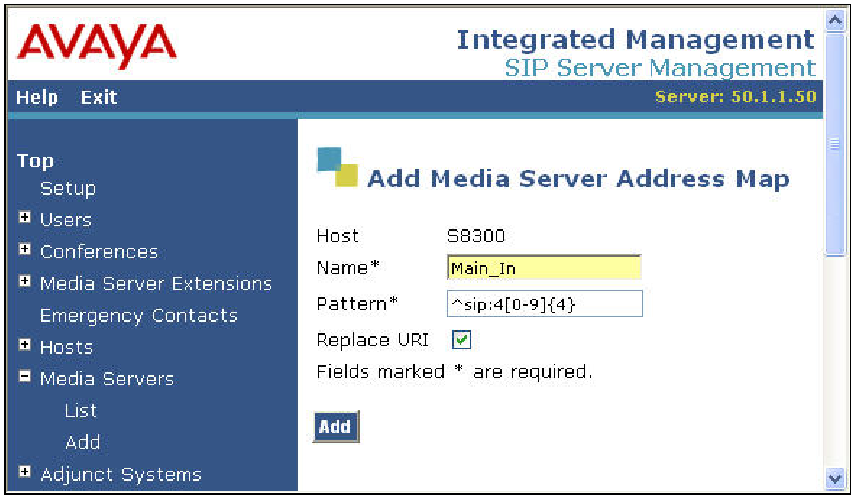
Step	Description
4.	After configuring the Host Address Map and Contact the **List Host Address Map** page will appear as shown below.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users Conferences Media Server Extensions Emergency Contacts Hosts Media Servers Adjunct Systems Services List Host Address Map Host denali.devcon.com Commands / Name / Commands / Contact Edit Delete / Main_Out Edit Delete / sip:$(user)@50.1.1.61:5060;transport=udp Add Another Map / Add Another Contact / Delete Group Add Map In New Group
5.	A Media Server Address Map is required on Avaya SES at the main office to direct calls inbound to Avaya Communication Manager from the Eclipse CXC 350 in the same way that outbound calls from Avaya Communication Manager required a Host Address Map. In the case of the compliance test, calls from the branch office beginning with a 4 were routed from the Eclipse CXC 350 to Avaya Communication Manager at the main office. Thus, the Media Server Address Map was configured to match all calls dialed with a 5 digit number beginning with 4. To configure a Media Server Address Map: ▪ 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 below. ▪ Click on the **Map** link associated with the appropriate host to display the **List Media Server Address Map** page (not shown). On this page, click on the **Add Map In New Group** link.  AVAYA Integrated Management SIP Server Management Help Exit Server: 50.1.1.50 Top Setup Users Conferences Media Server Extensions Emergency Contacts Hosts Media Servers List Add List Media Servers Commands / Interface / Host Edit Extensions Map Test-Link Delete / S8300 / 50.1.1.50 Add Another Media Server Interface

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

On the **Add Media Server Address Map** page that appears:

- Enter a descriptive name in the **Name** field.
- In the **Pattern** field, enter an expression to define the matching criteria for calls to be routed from the Eclipse CXC 350 to Avaya Communication Manager. The example below shows the expression used in the compliance test. This expression will match an URI that begins with ***sip:4*** followed by any digit between ***0-9*** for the next ***4*** digits. Appendix A contains additional information on the syntax used for Address Map patterns.

Click the **Add** button.

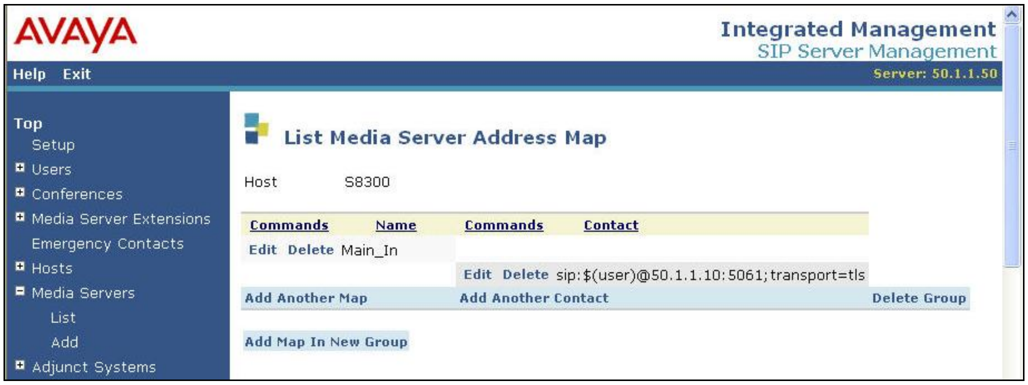


Host S8300
Name* Main_In
Pattern* ^sip:4[0-9]{4}
Replace URI ☑
Fields marked * are required.

</td></tr>
<tr><td>7.</td><td>

After configuring the Media Server Address Map, the **List Media Server Address Map** page appears as shown below. The first Media Server Contact is created automatically and directs the calls to the IP address of the Avaya Media Server (***50.1.1.10***) using port ***5061*** and ***TLS*** as the transport protocol. The user portion in the original request URI is substituted for “$(user)”. For the compliance test, the **Contact** field for the Media Server Address Map is displayed as:

```
sip:$(user)@50.1.1.10:5061;transport=tls
```

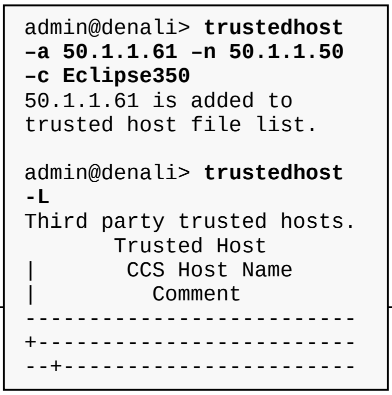


Host S8300

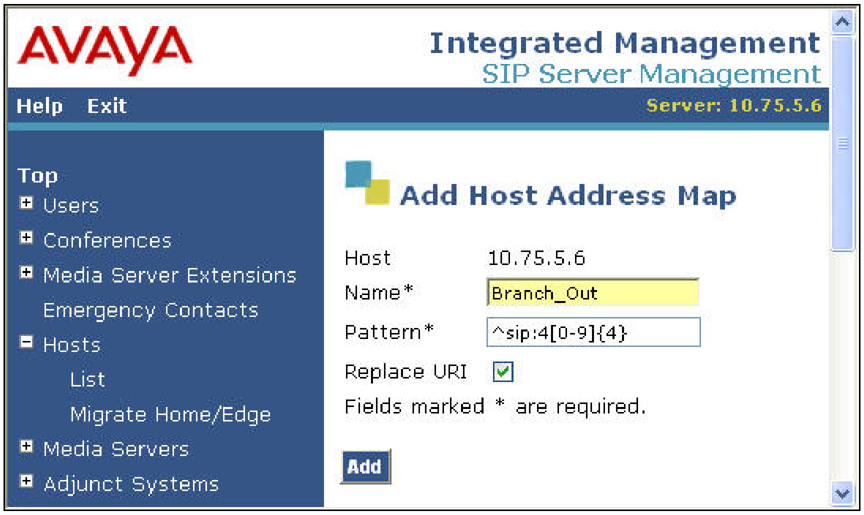
Commands | Name | Commands | Contact
Edit Delete | Main_In | |
| | Edit Delete | sip:$(user)@50.1.1.10:5061;transport=tls

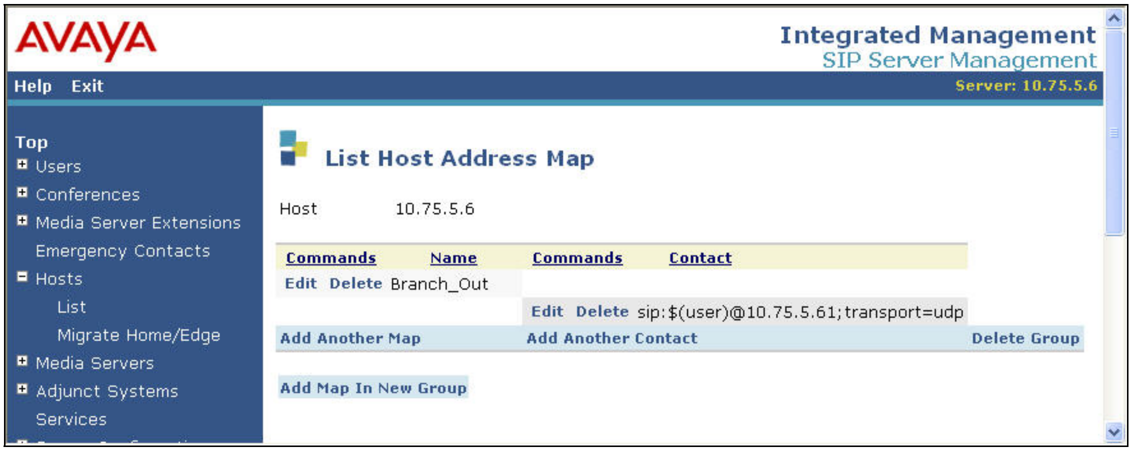
</td></tr>
</table>

Step	Description
8.	Lastly, the IP address of the Eclipse CXC 350 must be configured as a trusted host on Avaya SES. As a trusted host, Avaya SES will not issue SIP authentication challenges for incoming requests from the designated IP address. To configure a trusted host: ▪ Connect to Avaya SES and log in using proper credentials. ▪ Enter the following **trustedhost** command at the Linux shell prompt. **`trustedhost –a 50.1.1.61 –n 50.1.1.50 –c Eclipse350`** ▪ Use the following **trustedhost** command to verify the entry is correct. **`trustedhost –L`** ▪ **Important Note**: Complete the trusted host configuration by returning to the main Avaya SES administration web interface and clicking the **Update** link as shown in Section 3.2, Step 3. If the **Update** link is not visible, refresh the page by selecting the **Top** link from the left menu. This step is required even though the trusted host was configured via the Linux shell. The screen below illustrates the results of the **trustedhost** commands.



```
admin@denali> trustedhost
–a 50.1.1.61 –n 50.1.1.50
–c Eclipse350
50.1.1.61 is added to
trusted host file list.

admin@denali> trustedhost
-L
Third party trusted hosts.
       Trusted Host
|       CCS Host Name
|         Comment
--------------------------
+-------------------------
--+-----------------------
```

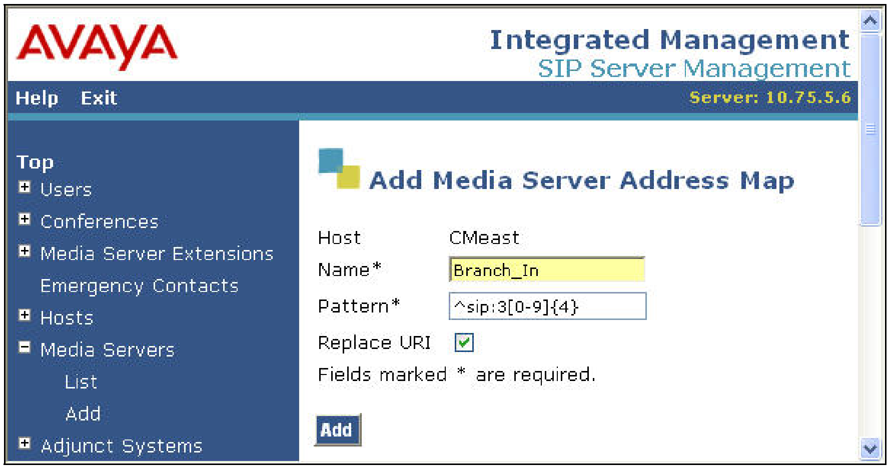
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>9.</td><td>Repeat Steps 1 - 4 to create a Host Address Map at the branch site with the characteristics shown below.


Host 10.75.5.6
Name* Branch_Out
Pattern* ^sip:4[0-9]{4}
Replace URI ☑
Fields marked * are required.


Host 10.75.5.6
Commands | Name | Commands | Contact
Edit Delete | Branch_Out | |
| | Edit Delete | sip:$(user)@10.75.5.61;transport=udp</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>10.</td><td>

Repeat Steps 5 – 7 to create a Media Server Address Map at the branch site with the characteristics shown below.



Add Media Server Address Map

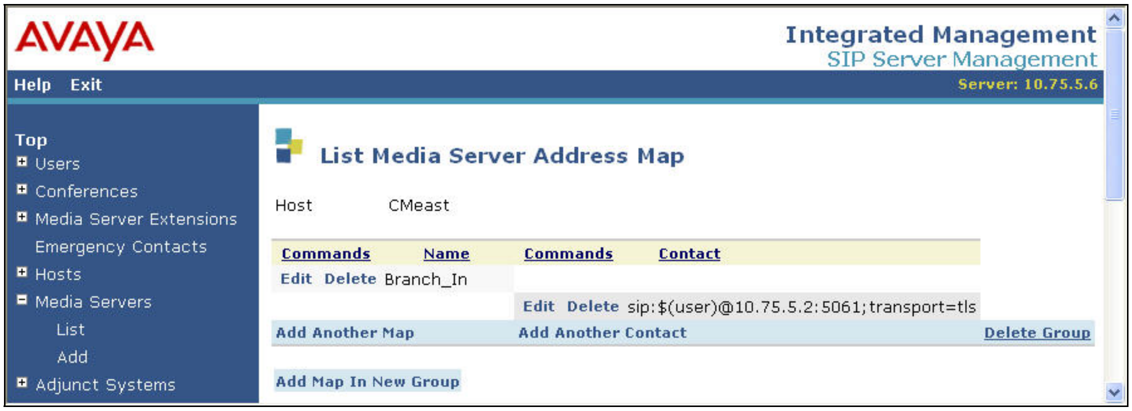
Host CMeast

Name* Branch_In

Pattern* ^sip:3[0-9]{4}

Replace URI ☑

Fields marked * are required.



List Media Server Address Map

Host CMeast

Commands	Name	Commands	Contact
Edit Delete	Branch_In		
		Edit Delete	sip:$(user)@10.75.5.2:5061;transport=tls

</td></tr>
<tr><td>11.</td><td>

Repeat Step 8 to establish the Covergence CXC 50 (10.75.5.61) as a trusted host on Avaya SES (10.75.5.6) at the branch site.

```
admin@sipserve> trustedhost –a 10.75.5.61 –n 10.75.5.6 –c Eclipse50
10.75.5.61 is added to trusted host file list.

admin@sipserve> trustedhost -L
Third party trusted hosts.
       Trusted Host        |       CCS Host Name        |         Comment
--------------------------+----------------------------+--------------------------
10.75.5.61                | 10.75.5.6                  | Eclipse50
```

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

5.3. Configure Avaya SIP Telephones

The SIP telephones at the main office will use the IP address of the Avaya SES server at the main office as the call server. The SIP telephones at the branch site will use the IP address of the Avaya SES server at the branch office as the call server.

The table below shows an example of the SIP telephone networking settings for both the main and branch offices.

	Main Site	**Branch Site**
IP Address	50.1.1.53	10.75.5.12
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	50.1.1.50	10.75.5.6
Router	50.1.1.254	10.75.5.1
File Server	50.1.1.52	10.75.5.81

5.4. Configure the Main Office Covergence Eclipse CXC 350

Use the same procedure as described in Section 4.4 with the exception of the following.

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

Define the dial plan.

In this network configuration, only calls between sites pass through the Eclipse CXC. All inter-sites calls are handled locally by Avaya SES and do not pass through the Eclipse CXC.

The dial plan shows two routes. The start of each route definition is highlighted in bold below. The first route is named ***route calls to remote CXC*** and will match on any request URI and route the call to the **peer server** named ***CXC50-Site2***. The second route is defined as a **source-route** named ***CXC to SES*** and will take precedence over the first route. It will route all calls from the **server** named ***CXC50-Site2*** to the **peer server** named ***SES***. In addition, the request URI, To header and From header will be modified to include the IP address of the next hop which in this case is the IP address of Avaya SES. The characteristics of these servers are defined in Step 9.

```
 config dial-plan
  config route "route calls to remote CXC"
   set request-uri-match default
   set peer server "vsp\enterprise\servers\sip-gateway CXC50-Site2"
   config outbound
    set host-normalizations request-uri+to-header+from-header
   return
   config session-config
    config contact-uri-settings-outLeg
     set add-maddr disabled
    return
   return
  return
  config source-route "CXC to SES"
   set source-match server "vsp\enterprise\servers\sip-gateway CXC50-
Site2"
   set peer server "vsp\enterprise\servers\sip-gateway SES"
   set alter-request-uri next-hop-ip
   set alter-to-uri next-hop-ip
   set alter-from-uri next-hop-ip
  return
 return
```

</td></tr>
<tr><td>2.</td><td>

Define the registration plan.

In this configuration (Secure SIP Trunking), the SIP phones register directly with the local SES on site. No REGISTER messages pass through the Eclipse CXC, so no registration plan is needed.

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

Step	Description
3.	Define the servers. The same servers are defined as was done in Section 4.4, Step 3 except the server ***CXC-Site2*** is defined as a **sip-gateway** instead of a **sip-connection**. Either approach is equivalent for the network configurations used in the compliance test. Shown below is the definition of the ***SES*** server which remains unchanged. The definition of the ***CXC-Site2*** server is shown in the next step.

```
 config enterprise
  config servers
   config sip-gateway SES
    set peer-identity sip:50.1.1.50
    set domain devcon.com
    set routing-setting ""
    set failover-detection none
    set user ""
    set password-tag ""
    set outbound-session-config-entry vsp\session-config-pool\entry
follow
    config server-pool
     config server ses
      set host 50.1.1.50
     return
    return
   return
```

Step	Description
4.	Define servers continued. In the definition of the ***CXC-Site2*** server, the **host**, **domain** and **peer-identity** parameters are set to values reflecting the IP address and domain of the Eclipse CXC 50 at the branch location. The **transport** and **port** parameters specify that ***TLS*** will be used on port ***5061*** to communicate to this remote server. The **inbound-session-config-entry** parameter specifies that the session configuration named ***decryption*** in the session configuration pool will be applied to inbound traffic from this server. Lastly, the **outbound-session-config-entry** parameter specifies that the session configuration named ***encryption*** in the session configuration pool will be applied to outbound traffic to this server.

```
config sip-gateway CXC50-Site2
    set peer-identity sip:192.168.1.84
    set domain devcon.com
    set routing-setting ""
    set failover-detection none
    set ping-interval 3
    set user ""
    set password-tag ""
    set service-type external
    set peer-max-interval 1800
    set peer-min-interval 60
    set client-max-interval 60
    set inbound-session-config-entry vsp\session-config-pool\entry
decryption
    set outbound-session-config-entry vsp\session-config-pool\entry
encryption
    config server-pool
     config server CXC50-Site2
      set host 192.168.1.84
      set transport TLS "vsp\tls\certificate
wakefield.whatever.com.pfx"
      set port 5061
     return
    return
   return
  return
 return
 config settings
  set max-number-of-sessions 10000
  set out-of-context-message-action refuse 400
  set out-of-context-message-media-cleanup disabled
 return
return
```

5.5. Configure the Branch Office Covergence Eclipse CXC 50

Use the same procedure as described in Section 4.5 with the exception of the following.

Step	Description

1.	Configure the virtual service partition.
	Set the domain-name parameter to the SIP domain of the branch office as shown in bold below.
	`config vsp`
	` set admin enabled`
	` set domain-name business.com`
	` set local-normalization disabled`

2.	Define a policy for special handling of NOTIFY and SUBSCRIBE messages. Since the Eclipse CXC at the branch office will interface with the local Avaya SES, create the same policy shown in Section 3.4, Step 5.
3.	Define a session configuration pool. Use the same session configuration pool used on the Eclipse CXC 350 in this network configuration (Secure SIP Trunking) as defined in Section 4.4. Four session configurations are defined named ***decryption***, ***encryption***, ***follow*** and ***Avaya REGISTER modification***.
4.	Define a dial plan. The dial plan will be the same as used on the Eclipse CXC 350 in this network configuration (Secure SIP Trunking) as defined in Section 5.4, Step 1. However, references to the remote server ***CXC50-Site2*** will be changed to ***CXC350-Site1*** which will be defined in Step 7. All references to the ***SES*** server can stay the same because the definition of the ***SES*** server will be changed to reflect the branch office in Step 7.
5.	Define the registration plan. In this configuration (Secure SIP Trunking), the SIP phones register directly with the local SES on site. No REGISTER messages pass through the Eclipse CXC, so no registration plan is needed.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>
Define the servers.

Use the same configuration as defined for the Eclipse 350 at the main office in Section 5.4, Step 4 with the following changes shown in bold below to correspond to the branch office.

<pre>
config enterprise
  config servers
   config sip-gateway SES
    set peer-identity sip:10.75.5.6
    set domain business.com
    set routing-setting ""
    set failover-detection none
    set user ""
    set password-tag ""
    set outbound-session-config-entry vsp\session-config-pool\entry
follow
    config server-pool
     config server ses
      set host 10.75.5.6
     return
    return
   return
   config sip-gateway CXC350-Site1
    set peer-identity sip:192.168.1.83
    set domain business.com
    set routing-setting ""
    set failover-detection none
    set ping-interval 3
    set user ""
    set password-tag ""
    set service-type external
    set peer-max-interval 1800
    set peer-min-interval 60
    set client-max-interval 60
    set inbound-session-config-entry vsp\session-config-pool\entry
decryption
    set outbound-session-config-entry vsp\session-config-pool\entry
encryption
    config server-pool
     config server CXC350-Site1
      set host 192.168.1.83
      set transport TLS "vsp\tls\certificate
wakefield.whatever.com.pfx"
      set port 5061
     return
    return
   return
  return
 return
return
</pre>
</td></tr>
</table>

6. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability between the Eclipse CXC, Avaya SIP Enablement Services (SES) and Avaya Communication Manager. This section covers the general test approach and the test results.

6.1. General Test Approach

The general test approach was to make calls to/from the telephones connected through the Eclipse CXC at the branch site using various codec settings and exercising common PBX features.

6.2. Test Results

The Eclipse CXC successfully passed compliance testing. The following features and functionality were verified during the interoperability compliance test. Direct IP-IP audio connections (also known as media shuffling) was enabled for all calls (see Section 3.1, Step 5).

- Calls between the two sites
- Intra-branch calls
- G.711mu and G.729AB codec support
- Proper recognition of DTMF transmissions
- Support for Hold, Transfer, Conference and Call Waiting
- Proper system recovery after a Eclipse CXC restart
- Proper operation of voicemail with message waiting indicators (MWI).
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Call Park, Call Pickup, Automatic Redial and Send All Calls. For more details on FNEs, please refer to [4].

7. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service at each location.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service at each location.
- From the Avaya SES web administration interface, navigate to **User→Registered Users**. In the window that appears, click the **Search** button using the default search criteria to get a list of all registered users. Verify that all SIP endpoints are registered with their respective Avaya SES.
- Verify that calls can be placed between SIP endpoints at each location through the pair of Eclipse CXCs.

8. Support

For technical support on the Eclipse CXC, contact Covergence via email at support@covergence.com or via the web site www.covergence.com.

9. Conclusion

These Application Notes describe the procedures required to configure the Covergence Eclipse CXC 350 and Eclipse CXC 50 to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager.

10. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 4.0, February 2006

[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2.1, May 2006

[3] *Installing and Administering SIP Enablement Services R3.1*, Doc# 03-600768, Issue 1.5, February 2006

[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] *SIP support in Release3.1 of Avaya Communication Manager*, Doc # 555-245-206, Issue 6, February 2006

[6] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005

[7] *Covergence Eclipse CXC Installation Guide*, Doc #780-0006-00, Revision 03.01.00, July, 2006

[8] *Covergence Eclipse CXC Administration Guide*, Doc #780-0003-00, Revision 03.01.00, July, 2006

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

Product documentation for Covergence Eclipse CXC may be found at http://www.covergence.com

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 the 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.