Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager to Support SIP Trunking - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager.

Sipera IPCS 310 is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

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

1. Introduction

These Application Notes describe the procedures for configuring Sipera IPCS 310 with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

Sipera IPCS 310 is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows two enterprise sites connected via a SIP trunk across an untrusted IP network. Site 1 has a Juniper Networks Netscreen-50 firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise. Also connected to the edge of site 1 is an IPCS 310. The public side of IPCS is connected to the untrusted network and the private side is connected to the trusted corporate LAN. IPCS could also reside in the demilitarized zone (DMZ) of the enterprise but this configuration was not tested.

All SIP traffic between the sites flows through IPCS. In this manner, IPCS can protect the infrastructure at site 1 from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams. All non-SIP traffic bypasses IPCS and flows directly between the untrusted network to the private LAN of the enterprise if permitted by the firewall.

Located at site 1 on the private LAN side of the firewall is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include Avaya 4600 Series IP Telephones (with SIP and H.323 firmware), Avaya 9600 Series IP Telephones (with SIP and H.323 firmware), an Avaya one-X Desktop Edition, an Avaya 6408D Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. The PSTN numbers assigned to the ISDN-PRI trunk at site 1 is mapped to telephone extensions at site 1. There are two Windows PCs on site; one is used as a TFTP/HTTP server and the other is used to manage IPCS.

Located at site 2 on the private LAN side of the firewall is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G350 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include Avaya 4600 Series IP Telephones (with SIP and H.323 firmware), an Avaya 9600 Series IP Telephone (with SIP firmware), and an Avaya one-X Desktop Edition. It also has a TFTP/HTTP server.

The Avaya 4600 and 9600 Series IP Telephones (with SIP firmware) located at both sites are registered to the local Avaya SES. Each enterprise has a separate SIP domain: business.com for site 1 and dev4.com for site 2. SIP telephones at both sites use the local TFTP/HTTP server to obtain their configuration files.

All calls originating from Avaya Communication Manager at site 1 and destined for site 2 will be routed through the on-site Avaya SES to the on-site IPCS and from IPCS to the untrusted IP network. Once across the untrusted network, the call is routed to site 2's Avaya SES and finally to Avaya Communication Manager. Calls from the site 2 to site 1 follow this same path in the reverse order.

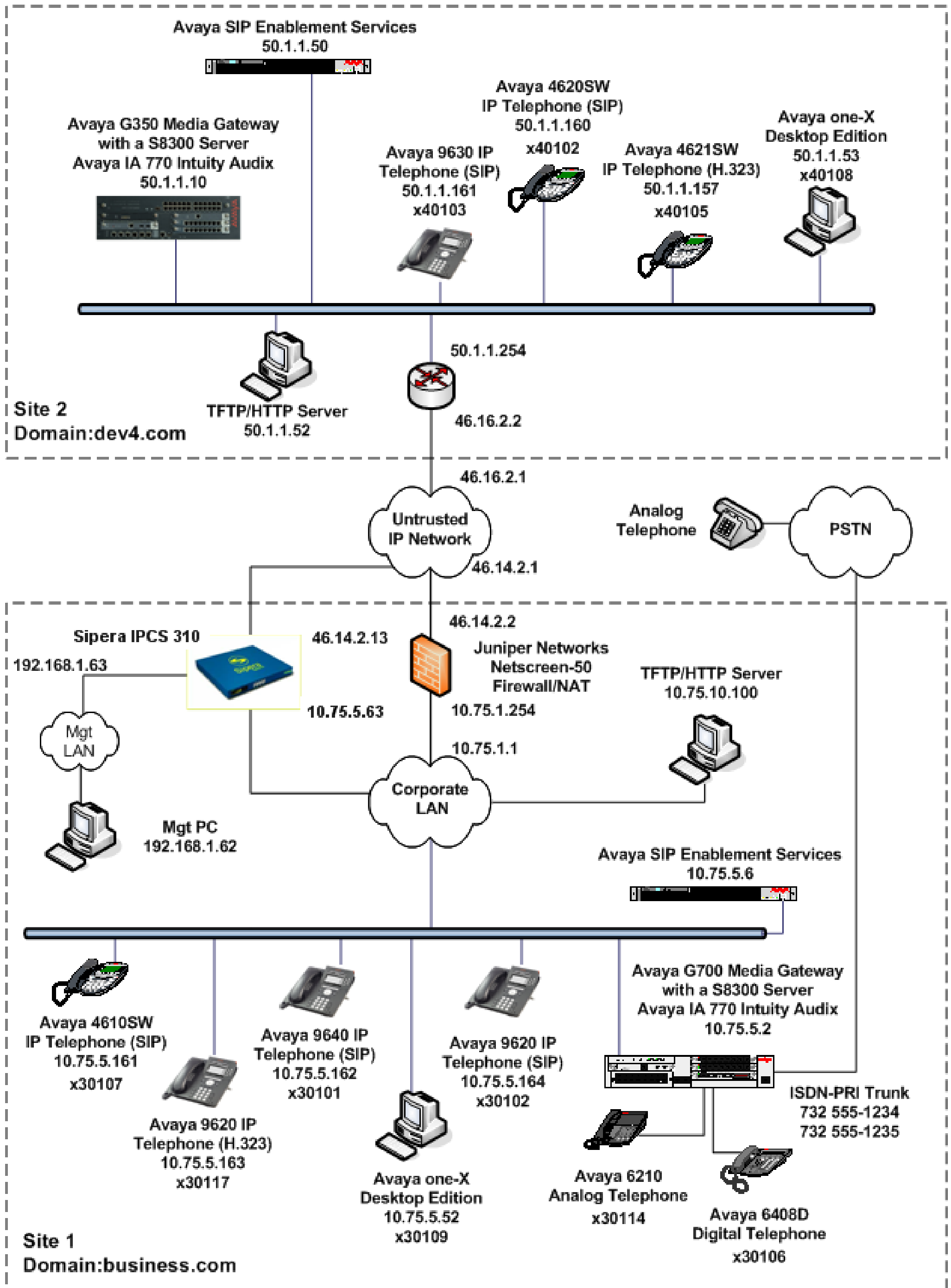


Figure 1: IPCS 310 Test Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server (site 1)	Avaya Communication Manager 5.0 Service Pack (00.0.825.4-15175) with Avaya IA 770 Intuity Audix
Avaya G700 Media Gateway (site 1)	27.26.0
Avaya SIP Enablement Services (site 1)	5.0 SP2d
Avaya S8300 Server (site 2)	Avaya Communication Manager 4.0.1 Service Pack (00.01.731.2-14300) with Avaya IA 770 Intuity Audix
Avaya G350 Media Gateway (site 2)	26.33.0
Avaya SIP Enablement Services (site 2)	4.0
Avaya 4621SW IP Telephone (H.323) Avaya 4625SW IP Telephone (H.323)	2.8.3
Avaya 4610SW IP Telephone (SIP) Avaya 4620SW IP Telephone (SIP)	2.2.2
Avaya 9620 IP Telephone (H.323)	Avaya one-X Deskphone Edition 1.5
Avaya 9630 IP Telephones (SIP) Avaya 9640 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.0.3
Avaya one-X Desktop Edition (SIP)	2.1 Service Pack 2
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (Management PC and TFTP/HTTP Server)	Windows XP Professional SP2
Juniper Networks Netscreen 50	5.4.0r9.0
Sipera IPCS 310	3.6 (Build Q.41)

3. Configure Avaya Communication Manager

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

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

Section 3.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with IPCS. It will describe the SIP connection used by Avaya Communication Manager to route calls to Avaya SES bound for site 2.

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

This configuration must be repeated for Avaya Communication Manager at site 2 using values appropriate for site 2 from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

3.1. Summary of Initial SIP Installation

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

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

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

The Authoritative Domain field was configured to match the domain name configured on Avaya SES. In this configuration, the domain name is business.com. This name appears in the “From” header of SIP messages originating from this IP region.
A descriptive name was entered for the Name field.
IP-IP Direct Audio (shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both intra-region and inter-region IP-IP Direct Audio. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
The Codec Set field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. If different IP network regions are used for the Avaya S8300 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 were used for all other fields.

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

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

```
display ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729A            n         2        20
 3:
```

Step	Description
3.	**Signaling Group** For the compliance test, signaling group 1 was used for the signaling group associated with the SIP trunk group between Avaya Communication Manager and Avaya SES. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. ▪ The **Group Type** was set to ***sip***. ▪ The **Transport Method** was set to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.*** ▪ The **Near-end Node Name** was set to ***procr***. This node name maps to the IP address of the Avaya Server. Node names are defined using the **change node-names ip** command. ▪ The **Far-end Node Name** was set to ***SES***. This node name maps to the IP address of Avaya SES as defined using the **change node-names ip** command. ▪ The **Far-end Network Region** was set to ***1***. This is the IP network region which contains Avaya SES. ▪ The **Far-end Domain** was set to ***business.com***. This is the domain configured on Avaya SES. This domain is sent in the "To" header of SIP INVITE messages for calls using this signaling group. ▪ **Direct IP-IP Audio Connections** was set to ***y***. This field must be set to ***y*** to enable media shuffling on the SIP trunk. ▪ The **DTMF over IP** field was set to the default value of ***rtp-payload***. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833. ▪ The default values were used for all other fields.

```
display signaling-group 1
                                SIGNALING GROUP

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



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

                                             Bypass If IP Threshold Exceeded? n

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

Step	Description
4.	**Trunk Group** For the compliance test, trunk group 1 was used for the SIP trunk group between Avaya Communication Manager and Avaya SES. Trunk group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. On **Page 1**: ▪ The **Group Type** field was set to ***sip***. ▪ A descriptive name was entered for the **Group Name**. ▪ An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the **TAC** field. ▪ The **Service Type** field was set to ***tie***. ▪ The **Signaling Group** was set to the signaling group shown in the previous step. ▪ The **Number of Members** field contained the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk. ▪ The default values were used for all other fields.

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

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

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

Step	Description
5.	**Trunk Group – continued** On **Page 3**: ▪ The **Numbering Format** field was set to ***public***. This field specifies the format of the calling party number sent to the far-end. ▪ The default values were used for all other fields.

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


                     Numbering Format: public
                                                 UUI Treatment: service-provider

                                                  Replace Restricted Numbers? n
                                                 Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

Step	Description
6.	**Public Unknown Numbering** Public unknown numbering defines the calling party number to be sent to the far-end. An entry was created that will be used by the trunk group defined in **Step 4**. In the example shown below, all calls originating from a 5-digit extension beginning with 6 and routed across any trunk group (**Trk Grp** column is blank) will be sent as a 5-digit calling number. This calling party number is sent to the far-end in the SIP "From" header.

```
display public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext              Trk       CPN          CPN
Len Code            Grp(s)    Prefix        Len
                                                     Total Administered: 1
 5  6                                      5            Maximum Entries: 9999
```

3.2. Configure SIP Trunk and Routing to Site 2

To communicate to site 2, a second SIP trunk with the appropriate call routing must be configured on Avaya Communication Manager. This SIP trunk will be used to route SIP calls to Avaya SES that are destined the SIP domain at site 2.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Signaling Group
Create a new SIP signaling group using the add signaling-group n command where n is the number of an unused signaling group. Use the same parameters as shown in Section 3.1, Step 3 with the following exception. Set the Far-end Domain field to the SIP domain of site 2. The compliance test used signaling group 12 as shown below.
<pre>
add signaling-group 12   Page   1 of   1
                                SIGNALING GROUP

 Group Number: 12   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: dev4.com

                                            Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload   Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? n
         Enable Layer 3 Test? n
 Session Establishment Timer(min): 3
</pre></td></tr>
<tr><td>2.</td><td>Trunk Group
Create a new trunk group using the add trunk-group n command where n is the number of an unused trunk group. Use the same parameters as shown in Section 3.1, Steps 4 - 5 with the following exceptions. Use unique values for the Group Name and TAC fields. Set the Signaling Group field to the signaling group number created in the previous step. The compliance test used trunk group 12 with the following values.

Group Name: Sipera
TAC: 112
Signaling Group: 12
</td></tr>
</table>

Step	Description
3.	**Public Unknown Numbering** Public unknown numbering defines the calling party number to be sent to the far-end. The entry created in **Section 3.1**, **Step 6** applies to all trunks since the **Trk Grp** column was left blank. Thus, a separate entry does not need to be created for this new SIP trunk. Based on the previous entry, all calls originating from a 5-digit extension beginning with 6 will be sent as a 5-digit calling number. This calling party number is sent to the far-end in the SIP "From" header.
4.	**Route Pattern** Create a route pattern for use by Automatic Alternate Routing (AAR) when routing calls to site 2. 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 in **Step 2**. 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 6                                            Page   1 of   3
                    Pattern Number: 6   Pattern Name: Site2SES
                             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: 12   0                                                              n   user
  2:                                                                     n   user
  3:                                                                     n   user
  4:                                                                     n   user
  5:                                                                     n   user
  6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
                                                        Subaddress
  1: y y y y y n  n            rest                                         none
  2: y y y y y n  n            rest                                         none
  3: y y y y y n  n            rest                                         none
  4: y y y y y n  n            rest                                         none
  5: y y y y y n  n            rest                                         none
  6: y y y y y n  n            rest                                         none
```

Step	Description
5.	Use the **change aar analysis 4** command to add an entry in the AAR Digit Analysis Table for the dialed string beginning with 4 since all extensions at site 2 begin with a 4. In the example shown, numbers that begin with ***4*** and are ***5*** digits long use route pattern ***6***. Route pattern 6 routes calls from site 1 to site 2 via the second SIP trunk with the far-end domain set to the SIP domain of site 2 (dev4.com).

```
change aar analysis 4                                        Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                                         Percent Full:    3

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    4                     5    5     6        aar          n
    5                     7    7     254      aar          n
    6                     7    7     254      aar          n
    7                     7    7     254      aar          n
    8                     7    7     254      aar          n
    9                     7    7     254      aar          n
```

4. Configure Avaya SIP Enablement Services

This section covers the configuration of Avaya SES at site 1. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure Avaya SES. For additional information on these installation tasks, refer to [5].

Each SIP endpoint used in the compliance test that registers with Avaya SES requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of IPCS so it is not included here. These procedures are covered in [5].

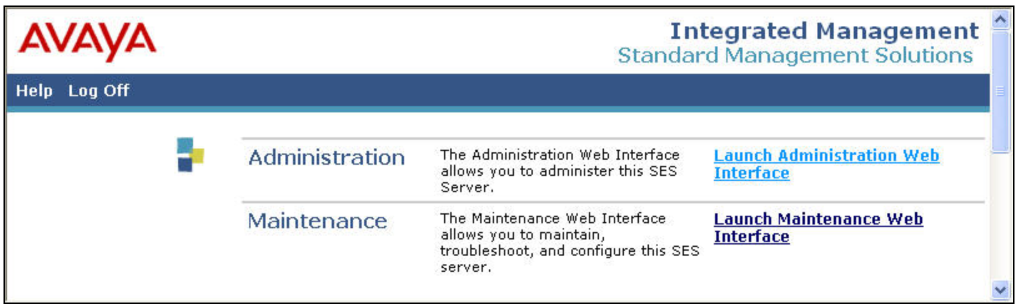
This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations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

Section 4.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with IPCS.

This configuration must be repeated for Avaya SES at site 2 using values appropriate for site 2 from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

4.1. Summarize Initial Configuration Parameters

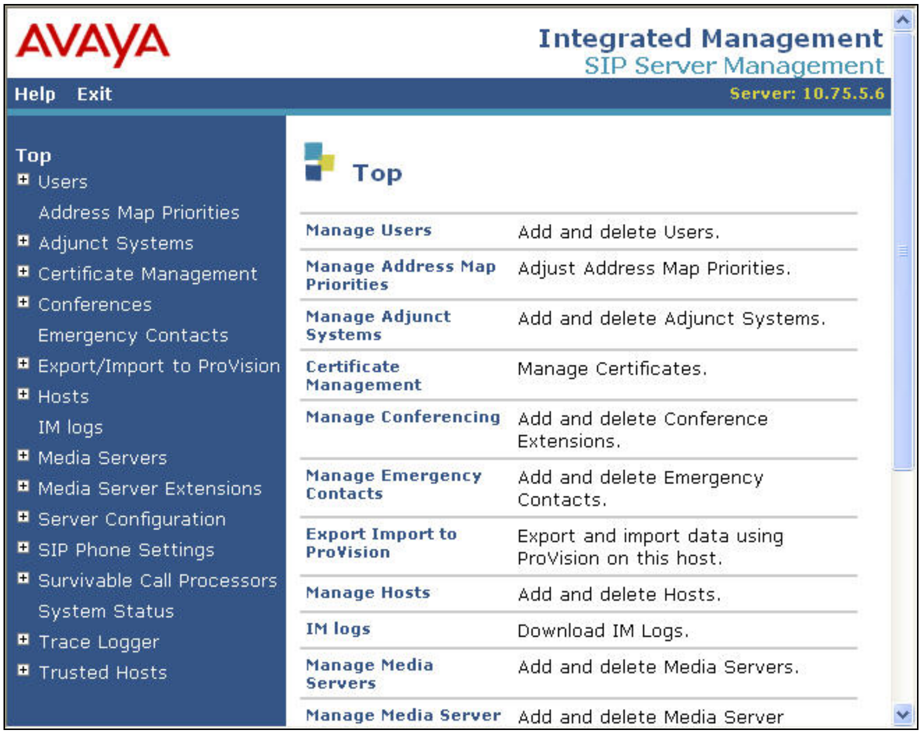
This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

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

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

Top Page

The Avaya SES **Top** page will be displayed as shown below.



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

Initial Configuration Parameters

As part of the Avaya SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the Avaya SES administration home page shown in the previous step.

- SIP Domain: ***business.com***
  (To view, navigate to **Server Configuration→System Parameters**)

- Host IP Address (SES IP address): ***10.75.5.6***
- Host Type: ***SES combined home-edge***
  (To view, navigate to **Host→List**; click **Edit**)

- Media Server (Avaya Communication Manager) Interface Name: ***CMeast***
- SIP Trunk Link Type: ***TLS***
- SIP Trunk IP Address (Avaya S8300 Server IP address): ***10.75.5.2***
  (To view, navigate to **Media Server→List**; click **Edit**)

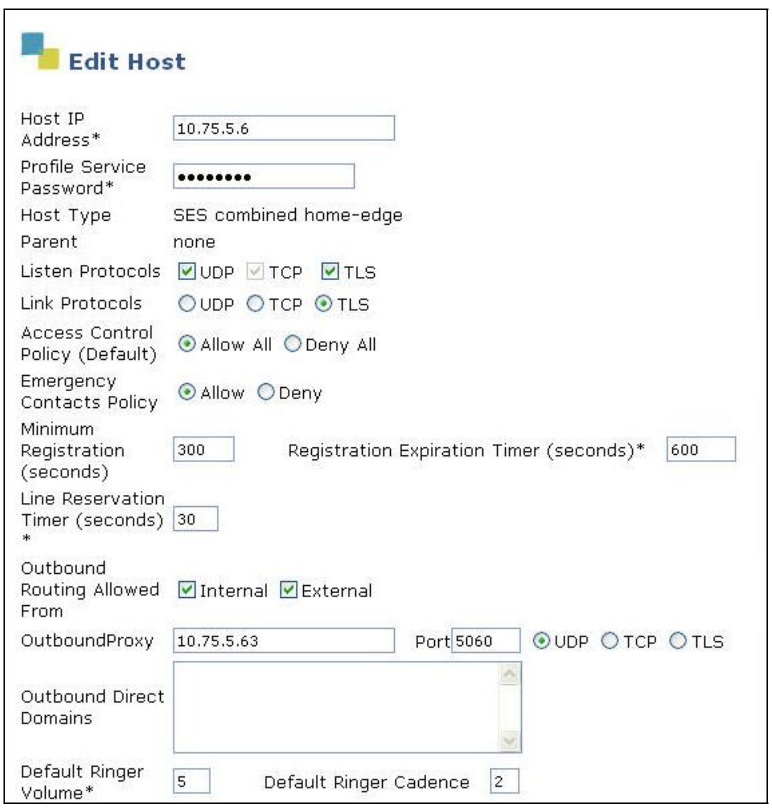
</td></tr>
</table>

4.2. IPCS Specific Configuration

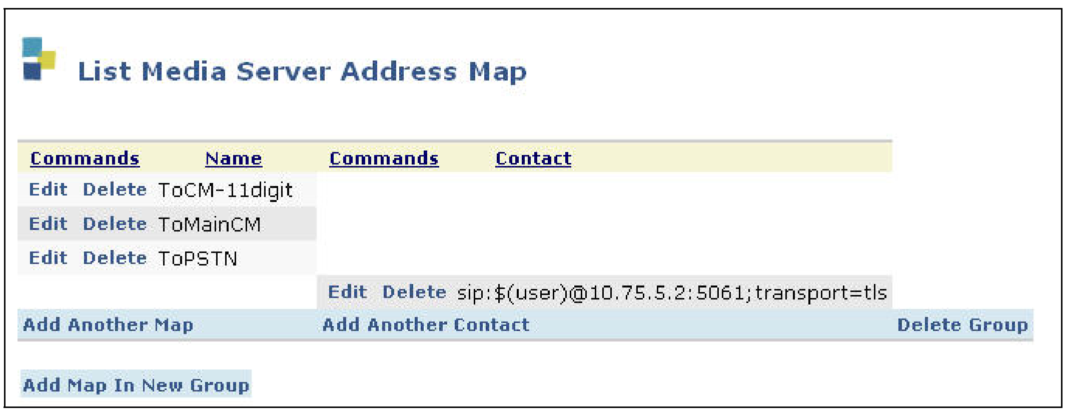
This section describes additional Avaya SES configuration necessary for interoperating with IPCS.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>
Outbound Proxy
Set the outbound proxy of Avaya SES to be the IPCS. When Avaya SES receives a call request (INVITE message) with a destination containing a foreign domain (dev4.com), Avaya SES will perform a DNS look-up on this domain. Since no DNS server was used in the compliance test, the DNS look-up will fail and Avaya SES will route the call to the outbound proxy (IPCS). The IPCS will then be responsible for routing the call to site 2. In addition, Avaya SES will automatically assume that the outbound proxy is a trusted host.

In the case of site 2 which does not have a local IPCS, set the Avaya SES outbound proxy to be the public IP address of the IPCS at site 1. The IPCS at site 1 will then be responsible for routing these calls to the Avaya SES at site 1.

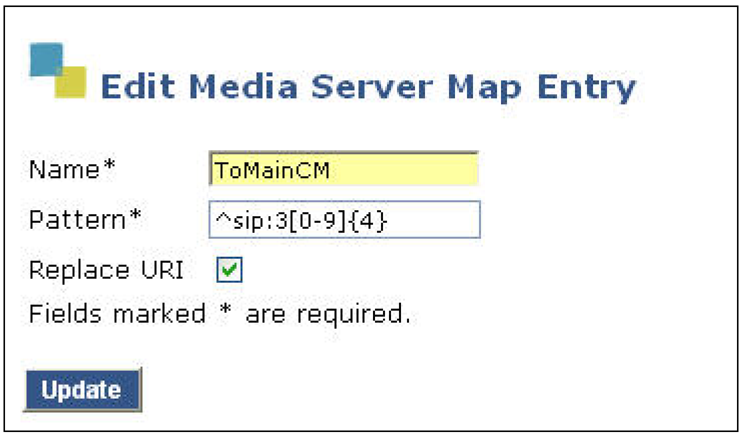
To configure the proxy settings, navigate to Hosts→Lists in the left pane. In the window that appears (not shown), select the Edit link next to the host name of Avaya SES. In the Edit Host window that appears, configure the following:
• Outbound Routing Allowed From: Check both Internal and External.
• Outbound Proxy: IP address of IPCS. Port field is set to 5060. Select the UDP radio button.


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

Step	Description
2.	**Media Server Address Map** A media server address map is needed to route calls from the remote site to a non-SIP phone at the local site. This is because neither the caller nor the called party is a registered user on the local Avaya SES with a media server extension assigned to it. Thus, Avaya SES does not know to route this call to Avaya Communication Manager. Thus to accomplish this task, a media server address map is needed. To view the configured media server address maps, navigate to **Media Server→List** in the left pane. In the window that appears (not shown), click the **Map** link next to the Avaya S8300 Server name. The list of media server address maps will appear. Each map defines criteria for matching calls to Avaya SES based on the contents of the SIP Request-URI of the call. If a call matches the map, then the call is directed to the **Contact**. In the example below, three maps are shown. Only the map named ***ToMainCM*** was used for the compliance test. This map were associated to a **Contact** that directs the calls to the IP address of the Avaya S8300 Server (***10.75.5.2***) using port ***5061*** and ***TLS*** as the transport protocol. The user portion in the original request URI is substituted for ***$(user)*** in the **Contact** expression shown below. `sip:$(user)@10.75.5.2:5061;transport=tls` To view or edit the call matching criteria of the map, click the **Edit** link next to the map name. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>Media Server Address Map – continued
The content of the media server address map is described below.

Name: Contains any descriptive name
Pattern: Contains an expression to define the matching criteria for calls to be routed from the remote site to the local Avaya Communication Manager. For the address map named ToMainCM, the expression will match any URI that begins with sip:3 followed by any digit between 0-9 for the next 4 digits. Additional information on the syntax used for address map patterns can be found in [5].
Replace URI: Check the box.

If any changes are made, click Update.


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

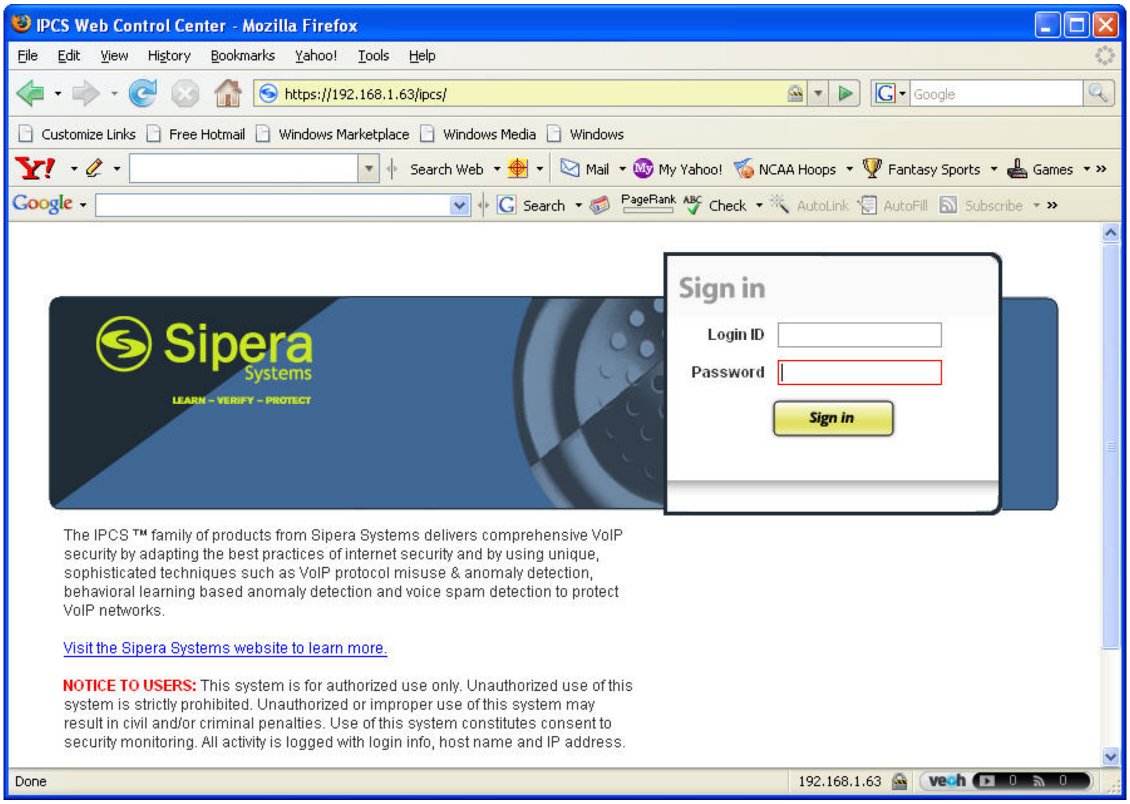
5. Configure the Avaya SIP Telephones

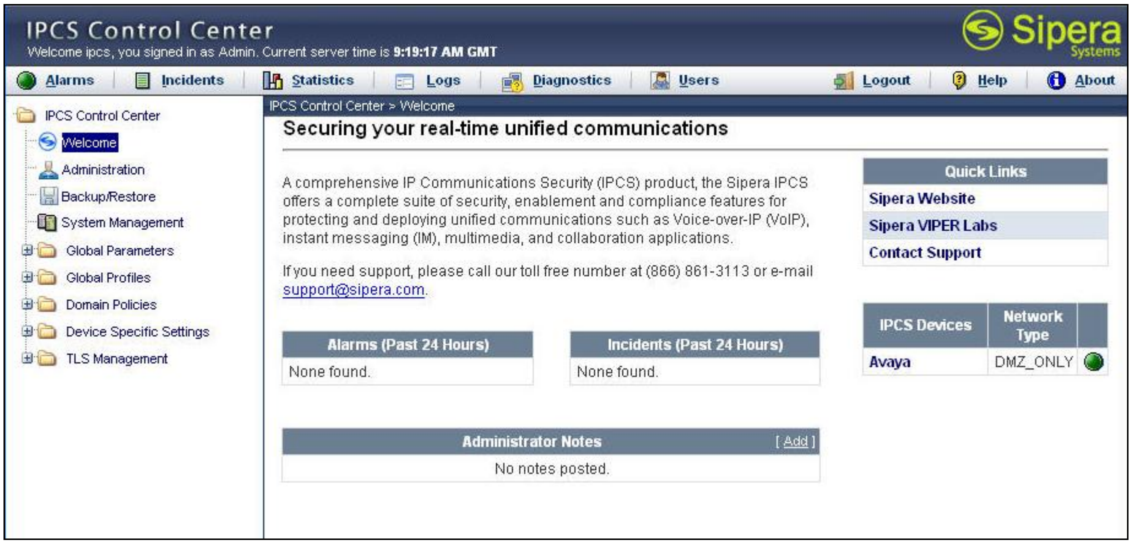
The SIP telephones at each site will use the local Avaya SES as the call server. The table below shows an example of the SIP telephone network settings for each site.

	Site 1	**Site 2**
Extension	30107	40102
IP Address	10.75.5.161	50.1.1.160
Subnet Mask	255.255.255.0	255.255.255.0
Router	10.75.5.1	50.1.1.254
File Server	10.75.10.100	50.1.1.52
DNS Server	0.0.0.0	0.0.0.0
SIP Domain	business.com	dev4.com
Call Server or SIP Proxy Server	10.75.5.6	50.1.1.50

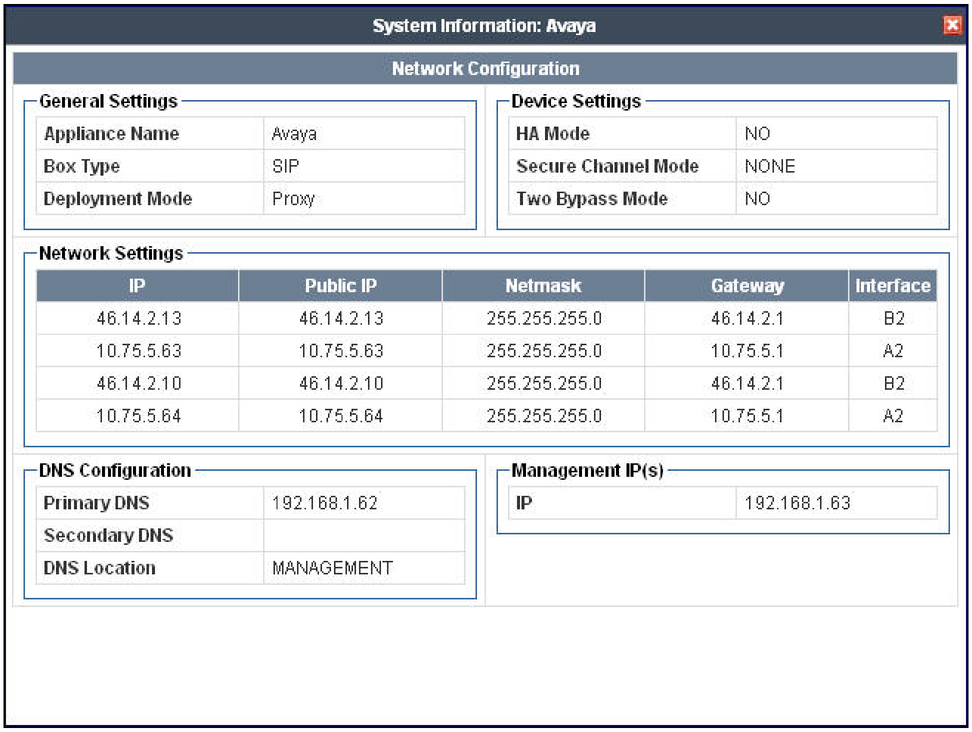
6. Configure Sipera IPCS

This section covers the configuration of IPCS. It is assumed that the IPCS software has already been installed. For additional information on these installation tasks, refer to [7].

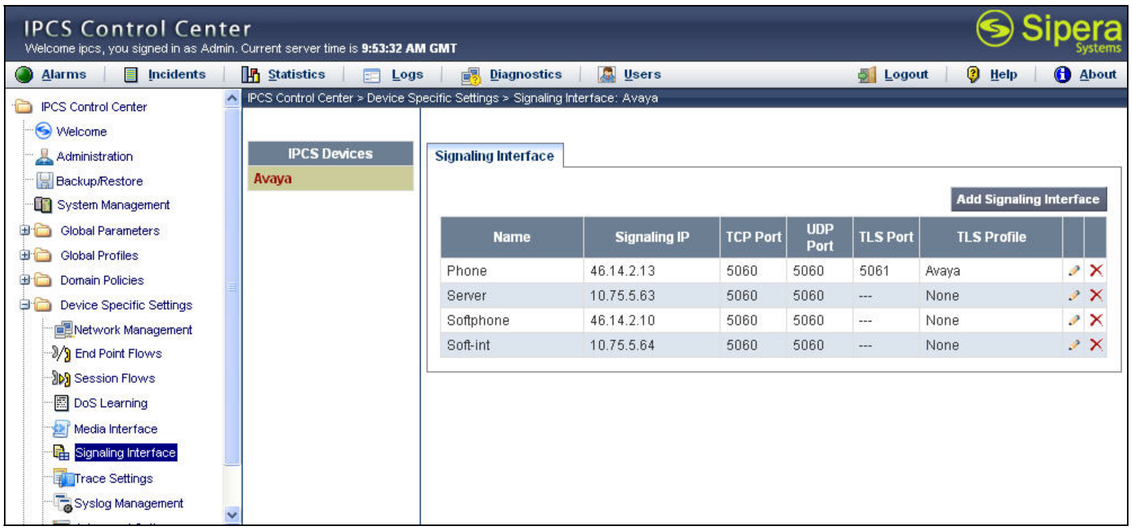
Step	Description
1.	IPCS is configured via the Mozilla Firefox web browser. IPCS does not support Internet Explorer. To access the web interface, enter https://<*ip-addr*>/ipcs in the address field of the web browser, where <*ip-addr*> is the IP address of IPCS. Log in with the appropriate credentials. Click **Sign In**. 

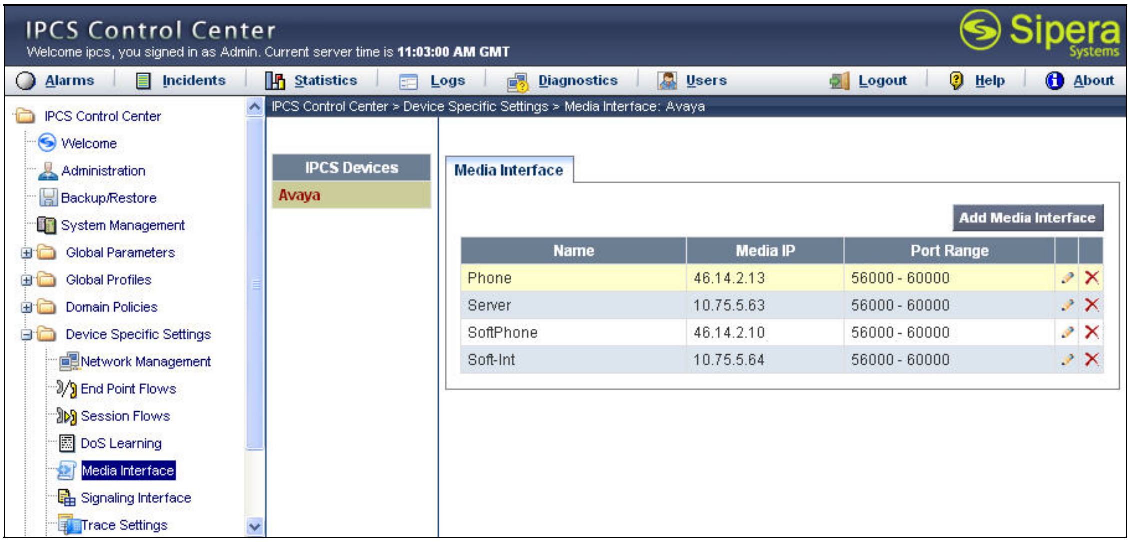
Step	Description
2.	The main page of the IPCS Control Center will appear. 
3.	To view system information that was configured during installation, navigate to **IPCS Control Center→System Management**. A list of installed devices is shown in the right pane. In the case of the compliance test, a single device named ***Avaya*** is shown. To view the configuration of this device, click the monitor icon highlighted below. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>The System Information screen shows the Network Settings, DNS Configuration and Management IP information provided during installation and corresponds to Figure 1. Only the first two entries in the Network Settings list below were used for the compliance test. The compliance test did not use a DNS server, but an entry was required by IPCS. An arbitrary IP address was used for the Primary DNS field. The Box Type was set to SIP and the Deployment Mode was set to Proxy. Default values were used for all other fields.



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

Step	Description
5.	**Signaling Interface** A signaling interface is created that maps a signaling interface name to an IP address and a set of ports and transport protocols that can be used on that interface. To define a new signaling interface, navigate to **IPCS Control Center→Device Specific Settings→Signaling Interface**. Select the IPCS device name in the middle pane. Select the **Add Signaling Interface** button in the right pane. A new page is opened (not shown) where the new information can be entered and submitted. The example below shows four interfaces. Only the interfaces named ***Phone*** and ***Server*** were used for the compliance test. The ***Phone*** interface maps to the public interface of IPCS and the ***Server*** interface maps to the private interface. 

Step	Description
6.	**Media Interface** A media interface maps a media interface name to an IP address and a range of ports that can be used on that interface. A media interface is created similar to a signaling interface by navigate to **IPCS Control Center→Device Specific Settings→Media Interface**. The example below shows four interfaces. Only the interfaces named ***Phone*** and ***Server*** were used for the compliance test. The ***Phone*** interface maps to the public interface of IPCS and the ***Server*** interface maps to the private interface. 

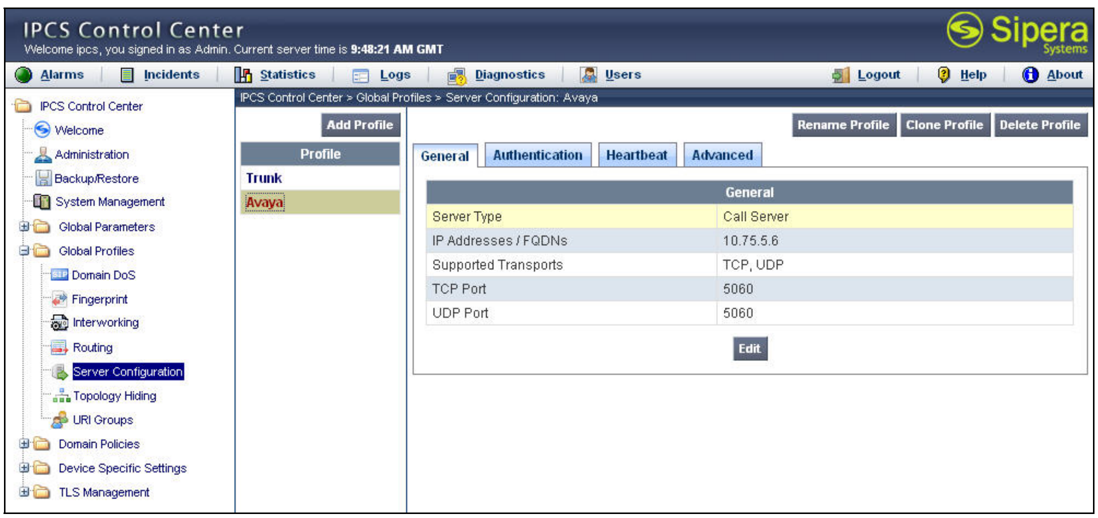
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>

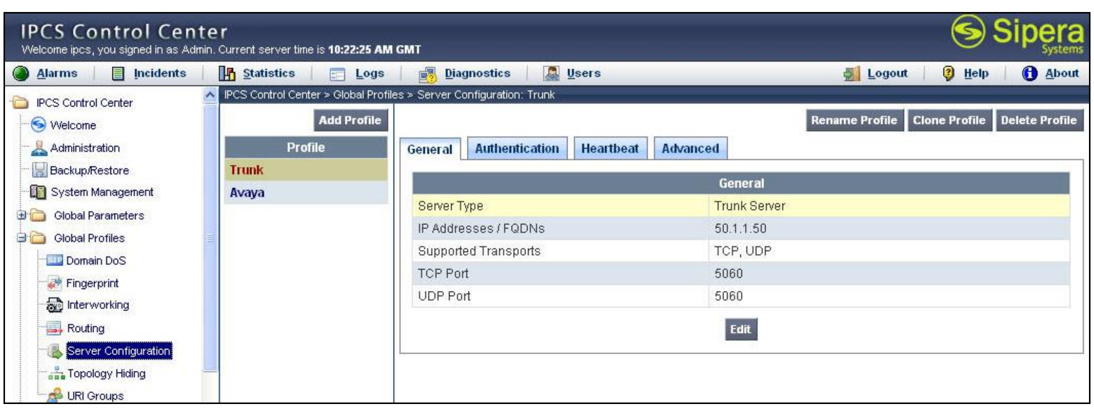
Server Definition - General
A server configuration profile is created to define the characteristics of a server to which the IPCS will communicate.

To define a new server configuration profile, navigate to **IPCS Control Center→Global Profiles→Server Configuration**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

The first screen below shows the server configuration profile named ***Avaya*** used to represent the local Avaya SES. The **General** tab shows the **Server Type** as ***Call Server*** and the IP address of the local Avaya SES (***10.75.5.6***) in the **IP Addresses/FQDNs** field. The remaining fields show the transport protocols and ports supported for traffic between IPCS and Avaya SES.

The second screen shows the server configuration profile named ***Trunk*** used to represent the remote Avaya SES. The **General** tab shows the **Server Type** as ***Trunk Server*** and the IP address of the remote Avaya SES (***50.1.1.50***) in the **IP Addresses/FQDNs** field.





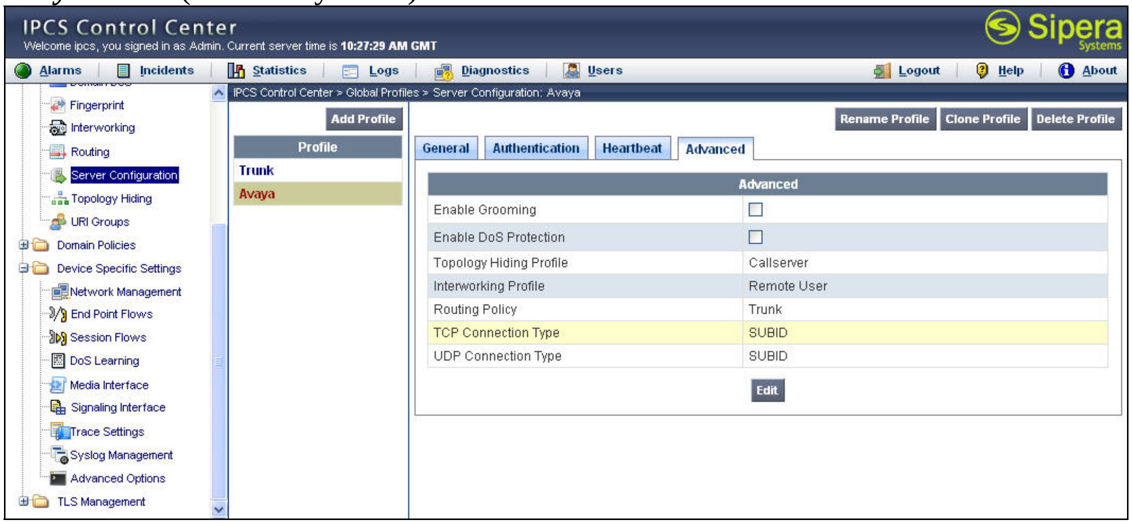
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>8.</td><td>

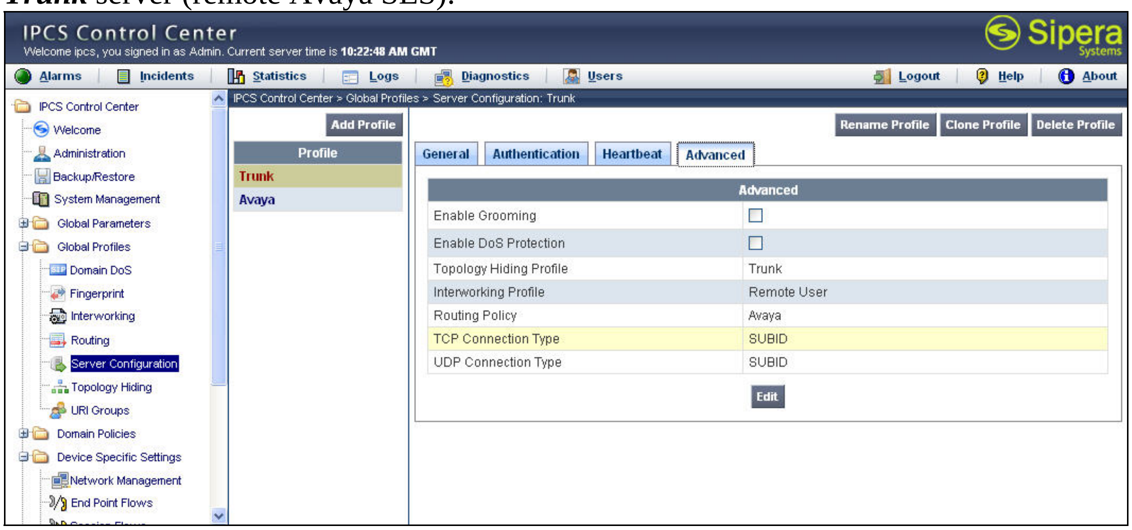
Server Definition – Advanced

On the **Advanced** tab, profiles are specified that will be applied to traffic between the IPCS and the server. These profiles: **Topology Hiding**, **Interworking** and **Routing** are described in **Steps 9 – 13**. Default values were used for all other fields.

Avaya server (local Avaya SES):

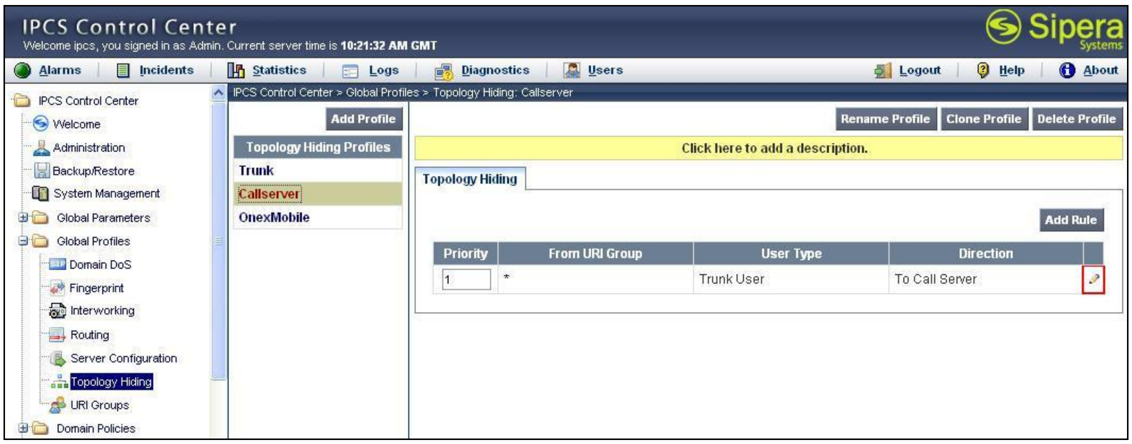


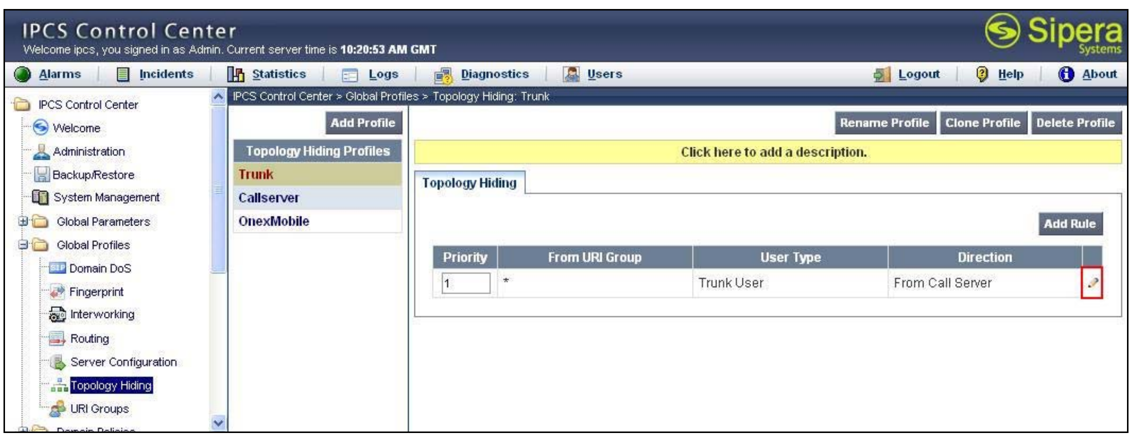
Trunk server (remote Avaya SES):

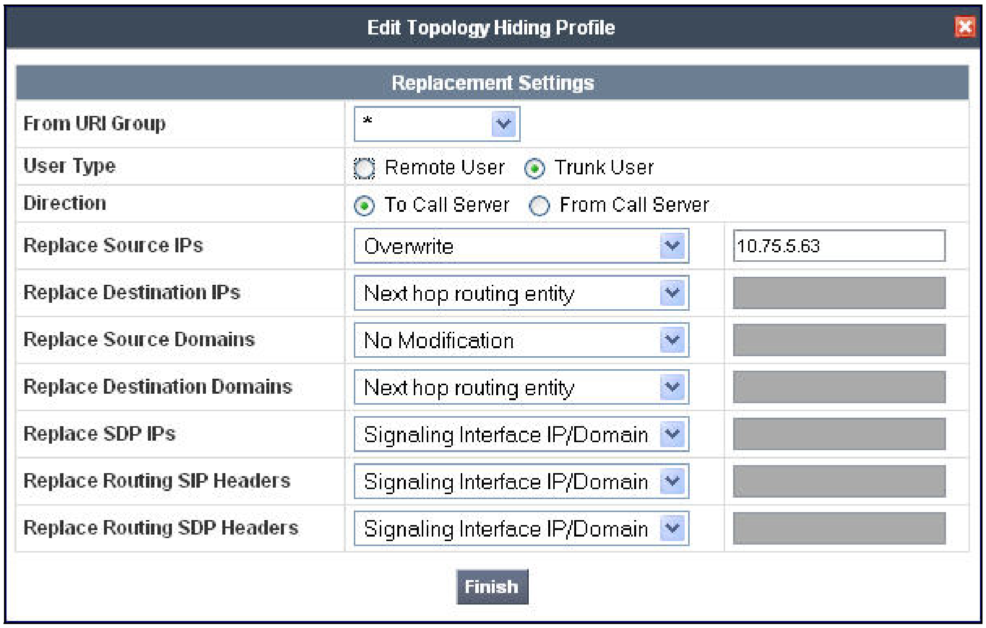


</td></tr>
</table>

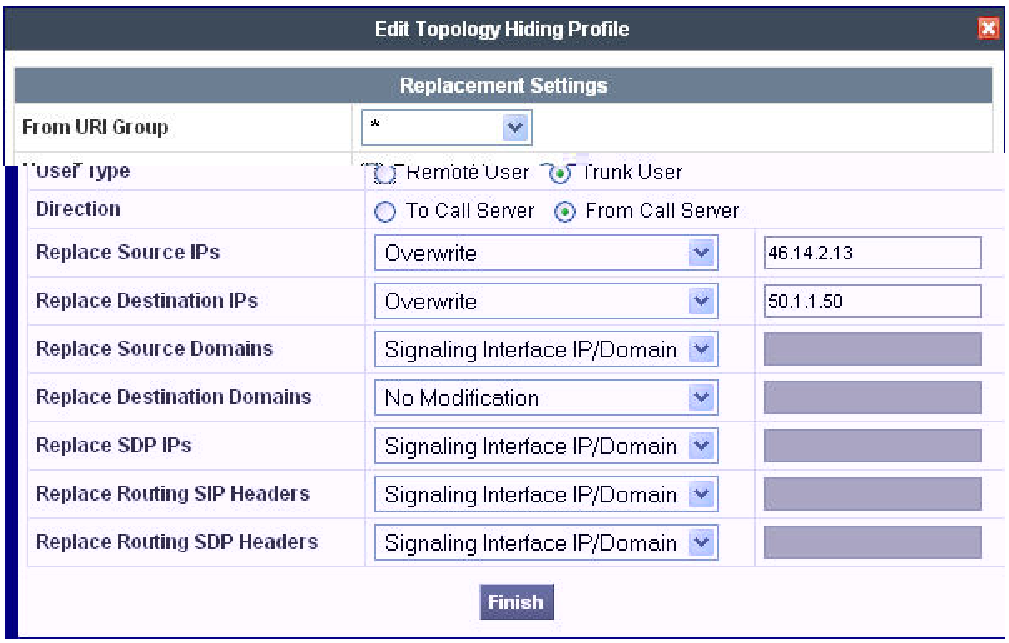
Step	Description
9.	**Server - Topology Hiding Profile** A topology hiding profile defines how the manipulation of IP addresses and domains is to be applied to SIP messages for traffic between IPCS and the server. To define a new topology hiding profile, navigate to **IPCS Control Center→Global Profiles→Topology Hiding**. Select the **Add Profile** button in the middle pane to enter and submit the new information. In the example below, three profiles are shown in the middle pane. Only the profiles named ***Callserver*** and ***Trunk*** were used for the compliance test. The ***Callserver*** profile was used by the ***Avaya*** server and the ***Trunk*** profile was used by the ***Trunk*** server. By highlighting a profile in the middle pane, its details are shown in the right pane. To see the details of a rule, click the pencil icon associated with the rule of interest in the right pane.

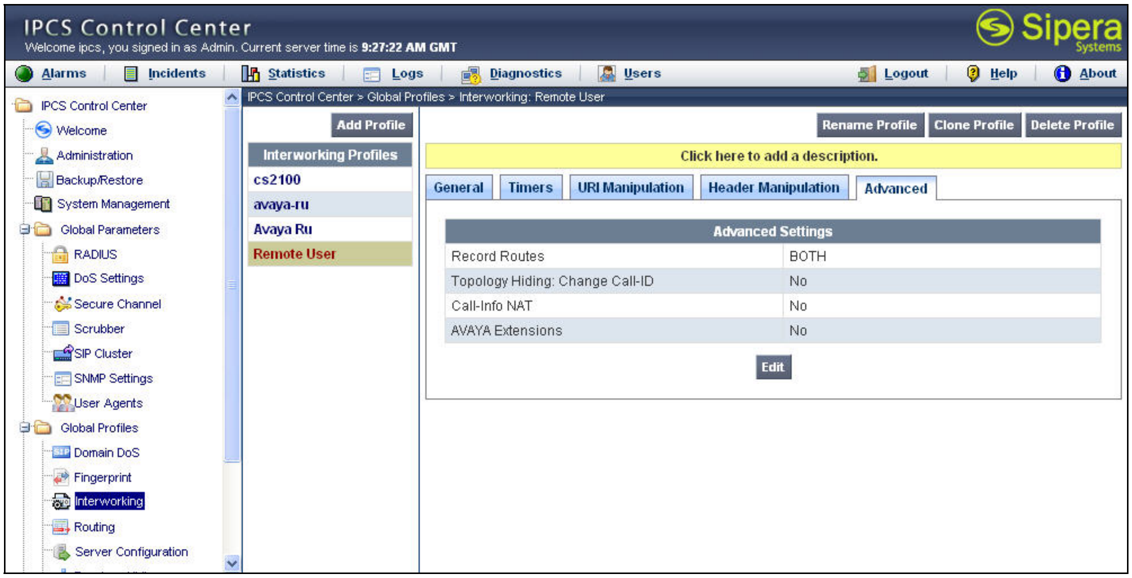




<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>10.</td><td>Server - Topology Hiding Profile - Continued
The topology hiding profile named CallServer was created to modify IP addresses in the SIP messages from the remote Avaya SES to the local Avaya SES. Thus, the URI is set to match on anything (From URI Group = *), the User Type is set to Trunk User and the Direction field is set to To Call Server. Before sending messages to the local Avaya SES, all external source IP addresses from the remote Avaya SES will be overwritten with the private IP address of IPCS and the source domains will be left unchanged.


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

Step	Description
11.	**Server - Topology Hiding Profile - Continued** The topology hiding profile named ***Trunk*** was created to modify IP addresses in the SIP messages from the local Avaya SES to the remote Avaya SES. Thus, the URI is set to match on anything (**From URI Group** = *****), the **User Type** is set to ***Trunk User*** and the **Direction** field is set to ***From Call Server***. Before sending messages to the remote Avaya SES, all source IP addresses from the local Avaya SES will be overwritten with the public IP address of IPCS, the destination IP addresses will be overwritten with the IP address of the remote Avaya SES, the source domains will be set to the signaling interface IP which results in the domain being overwritten with the public IP address of IPCS (see **Step 5**) and the destination domain is left unchanged. 

Step	Description
12.	**Server – Interworking Profile** An interworking profile defines how SIP message headers and content (other than the IP addresses) may be manipulated for interoperability with different call servers. To define a new interworking profile, navigate to **IPCS Control Center→Global Profiles→Interworking**. Select the **Add Profile** button in the middle pane to enter and submit the new information. In the example below, four profiles are shown in the middle pane. Only the profile named ***Remote User*** was used for the compliance test. By highlighting this profile in the middle pane, its details are shown in the right pane. On the **Advanced** tab, the **Topology Hiding: Change Call-ID** field was set to ***No*** to disable the changing of the Call-ID in the SIP messages passed through the IPCS to the Avaya SES. Default values were used for all other fields. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>13.</td><td>

Server – Routing Profile

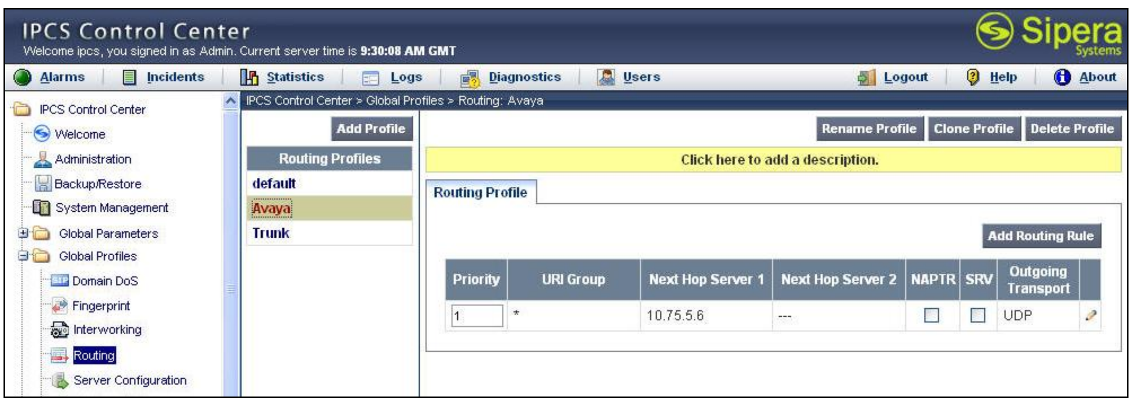
A routing profile defines how a call is to be routed. In this case, the routing profile is applied to calls from the server to IPCS.

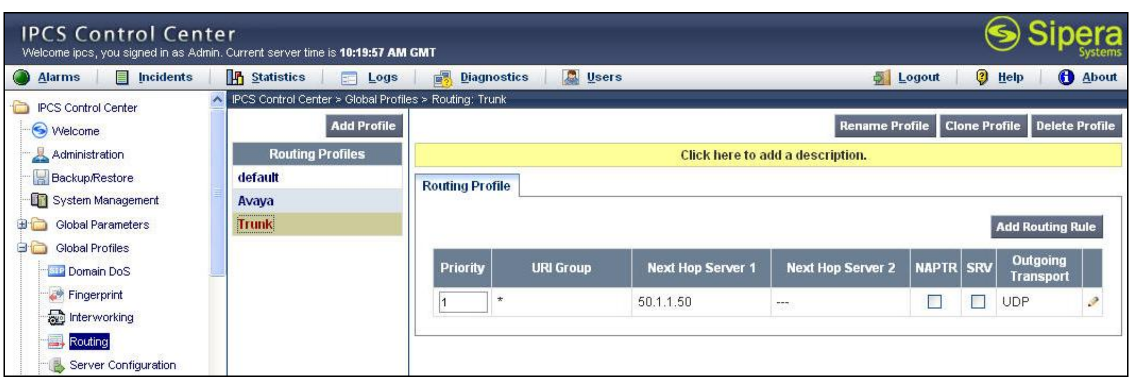
To define a new routing profile, navigate to **IPCS Control Center→Global Profiles→Routing**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

In the example below, three profiles are shown in the middle pane. Only the profiles named ***Avaya*** and ***Trunk*** were used for the compliance test. By highlighting a profile in the middle pane, its details are shown in the right pane.

The first screen below shows the routing profile named ***Avaya***. It shows that all traffic (**URI Group** = *****) using this profile will be routed to IP address 10.75.5.6 (local Avaya SES) as the next hop as defined in the **Next Hop Server 1** field.

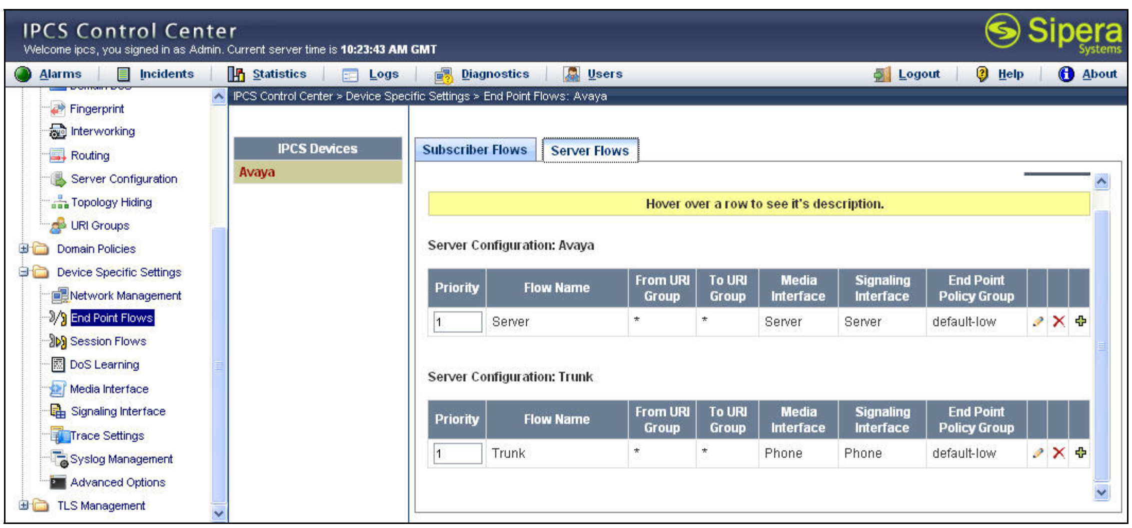
The second screen shows the routing profile named ***Trunk***. It shows that all traffic (**URI Group** = *****) using this profile will be routed to IP address 50.1.1.50 (remote Avaya SES) as the next hop as defined in the **Next Hop Server 1** field.





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

Step	Description
14.	**End Point Policy Groups** An end point policy group defines a set of rules that may be applied to different aspects of the data traffic. For the compliance test, the end point policy group was used to specify if (and how) the media stream should be encrypted. To define a new policy group, navigate to **IPCS Control Center→Domain Policies→End Point Policy Groups**. Select the **Add Group** button in the middle pane to enter and submit the information. For the compliance test, one policy group was used. Policy group ***default-low*** defines the use of unencrypted media (RTP). This policy group will be used in the server flows defined in the next step.

Step	Description
15.	**Server Flow** Many of the previous steps have defined policies that will be applied to traffic if it is present. The server flow defines what traffic is actually allowed between the IPCS and the specified server, as well as which interfaces and media encryption will be used. To define a new server flow, navigate to **IPCS Control Center→Device Specific Settings→End Point Flows**. Select the **Server Flows** tab. Select the **Add Flow** button in the right pane to enter and submit the new information. The example below shows the two server flows used for the compliance test. The flow named ***Server*** specifies that all traffic to or from any URI Group will be allowed to the server named ***Avaya*** (local Avaya SES). Media traffic will use **Media Interface – *Server*** and signaling traffic will use **Signaling Interface – *Server***. The **Endpoint Policy Group** named ***default –low*** (**Step 14**) will be applied to this traffic which specifies that the media is unencrypted. In addition, the Topology Hiding, Interworking, and Routing Profiles defined in **Steps 9 - 13** will be applied where applicable. The flow named ***Trunk*** specifies that all traffic to or from any URI Group will be allowed to the server named ***Trunk*** (remote Avaya SES). Media traffic will use **Media Interface – *Phone*** and signaling traffic will use **Signaling Interface – *Phone***. The **Endpoint Policy Group** named ***default –low*** (**Step 14**) will be applied to this traffic which specifies that the media is unencrypted. In addition, the Topology Hiding, Interworking, and Routing Profiles defined in **Steps 9 - 13** will be applied where applicable. 

7. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager using SIP trunking. This section covers the general test approach and the test results.

7.1. General Test Approach

The general test approach was to make calls between the two sites using various codec settings and exercising common PBX features.

7.2. Test Results

IPCS passed compliance testing. The following features and functionality were verified.

- Successful registrations of endpoints at both sites.
- Calls from both SIP and non-SIP endpoints between sites.
- G.711u and G.729A codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls. For more information on FNEs, please refer to [4].
- Proper system recovery after an IPCS restart and loss of IP connection.

8. Verification Steps

The following steps may be used to verify the configuration:

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

9. Support

For technical support on IPCS, contact Sipera support at www.sipera.com/support.

10. Conclusion

Sipera IPCS 310 passed compliance testing. These Application Notes describe the procedures required to configure Sipera IPCS 310 to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support SIP trunking between enterprise locations as shown in **Figure 1**.

11. Additional References

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

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

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

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

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

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

[7] *IPCS210_310 Installation Guide (230-5210-31)*.

[8] *IPCS Administration Guide (010-5310-31).*

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

Product documentation for IPCS can be obtained from Sipera. Contact Sipera using the contact link at http://www.sipera.com.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.