Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Quintum Tenor AS VoIP MultiPath Switch as a Back-To-Back User Agent in Support of SIP Endpoints and Local Survivability with Avaya Communication Manager and Avaya SIP Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Quintum Tenor AS VoIP MultiPath Switch as a back-to-back user agent (B2BUA) in support of SIP endpoints and local survivability with Avaya Communication Manager and Avaya SIP Enablement Services.

With the B2BUA functionality disabled, the Quintum Tenor AS VoIP MultiPath Switch serves as a gateway between analog telephones at a branch location and a VoIP infrastructure at a main location using the Session Initiation Protocol (SIP). The Tenor supports failover to a PSTN connection for external calls if the data WAN connection fails.

When the B2BUA functionality is enabled, the Tenor will also support SIP telephones at the branch location by performing as an Outbound Proxy. The B2BUA functionality also allows both analog and SIP phones to continue to make internal calls if the data WAN connection fails. This is referred to as local survivability. Emphasis of the testing was placed on SIP interoperability with the B2BUA enabled. 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.

1. Introduction

These Application Notes describe the procedure for configuring the Quintum Tenor AS VoIP MultiPath Switch as a back-to-back user agent (B2BUA) in support of SIP endpoints and local survivability with Avaya Communication Manager and Avaya SIP Enablement Services (SES).

With the B2BUA functionality disabled, the Quintum Tenor AS VoIP MultiPath Switch serves as a gateway between analog telephones at a branch location and a VoIP infrastructure at a main location using the Session Initiation Protocol (SIP). The Tenor supports failover to a PSTN connection for external calls if the data WAN connection fails.

When the B2BUA functionality is enabled, the Tenor has all the functionality previously described plus provides support for SIP telephones at the branch location by performing as an Outbound Proxy. The B2BUA functionality also allows both analog and SIP phones to continue to make internal calls if the data WAN connection fails. This is referred to as local survivability. The compliance testing was performed with the B2BUA enabled and focused on SIP interoperability.

The Tenor registers with the Avaya SES as a SIP endpoint for each analog telephone connected to it. When a call is placed from an analog telephone, the Tenor will send SIP signaling messages to the Avaya SES to setup the call. Once the call has been setup, the Tenor converts the analog signal from the analog telephone to a series of voice samples sent in data packets over the data network using the Real Time Protocol (RTP).

Quality of Service was achieved through the use of Layer-3 (DiffServ) parameter configuration on the Tenor.

1.1. Configuration

Figure 1 illustrates the configuration used in these Application Notes. In the sample configuration, two sites are connected via an IP network. The main site has an Avaya S8300 Media Server running Avaya Communication Manager in an Avaya G350 Media Gateway and an Avaya SES. Endpoints include an Avaya 4600 Series IP Telephone (with SIP firmware), an Avaya 4600 Series IP Telephone (with H.323 firmware) and an Avaya 6408D Digital Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN.

The branch site has a Quintum Tenor AS MultiPath Switch with two analog telephones and a fax machine connected to it. For the purposes of testing, only two extensions were configured on the Tenor. The fax machine shared one extension with one of the analog telephones; thus, the fax machine and second telephone were never connected to the Tenor at the same time. The branch site also has two Avaya 4600 Series IP Telephones (with SIP firmware), two generic SIP telephones and a Windows PC running the Tenor Configuration Manager application. The Tenor connects the branch site to the PSTN via an FXO (POTS) trunk.

All SIP telephones and analog telephones at both sites are registered to Avaya SES and are administered as Outboard Proxy SIP (OPS) stations in Avaya Communication Manager. However, the SIP telephones at the branch site are configured to use the Tenor IP address as the call server and/or outbound proxy IP address. Thus, all SIP traffic between the endpoint and the Avaya SES will pass through the Tenor.

The two DID numbers of the ISDN-PRI trunk to the Main Site are each mapped to a telephone extension at the Main Site. The DID number of the POTS line is mapped to an extension at the Branch Site.

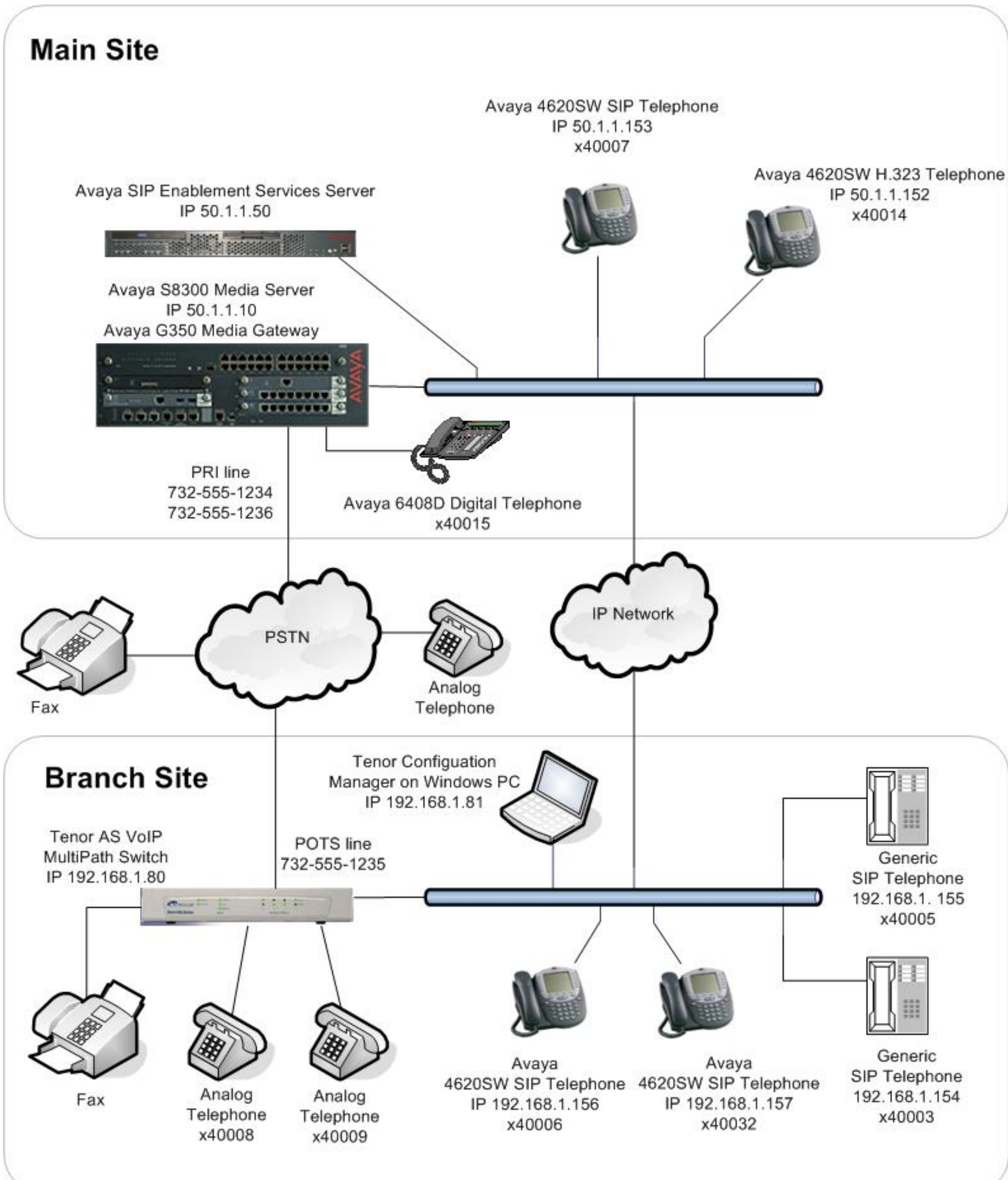


Figure 1: Tenor Test Configuration

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 SIP Enablement Services (SES)	3.1 (build 18)
Avaya 4620SW IP Telephones	SIP version 2.2.2 H.323 version 2.3
Avaya 6408D Digital Telephone	-
Analog Telephones	-
Analog Fax Machines	-
Generic SIP Telephone	-
Quintum Tenor AS VoIP MultiPath Switch	P105-03-00
Quintum Tenor Configuration Manager running on Windows XP	Tenor_Client_CM105.01.00_053006

3. Configure Avaya Communication Manager

The communication between Avaya Communication Manager and Avaya SES is via a SIP trunk group. All SIP signaling for calls between Avaya Communication Manager and the Tenor passes through Avaya SES via this trunk group. This section describes the steps for configuring this trunk group, and associated signaling group. In addition, this section describes the configuration of stations as OPS stations, which is required for each analog telephone or fax machine connected to the Tenor.

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.

Step	Description
1.	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. In this solution, each analog endpoint at the branch counts as a SIP telephone. 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.)
```

Step	Description
2.	Use the **change node-name ip** command to assign the node name and IP address for Avaya SES at the enterprise site. 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                          .   .   .
```

Step	Description
3.	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 6. 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 **Audio PHB Value** is ***46,*** which translates to a DiffServ header value of 0xb8. This same value will be configured on the Tenor in Section 5, Step 24.
- 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
```

Step	Description

4.	Use the **change ip-codec-set *n*** command, where ***n*** is the codec set value specified in Step 3, to enter the supported audio codecs for calls routed to Avaya SES. Multiple codecs can be listed in priority order to allow the codec to be negotiated during call establishment. The list should include the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. 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>

5.	On Page 2, set the **FAX Mode** field to *t.38-standard*.
	<pre>change ip-codec-set 1 Page 2 of 2
	
	                          IP Codec Set
	
	                              Allow Direct-IP Multimedia? n
	
	                    Mode Redundancy
	    FAX t.38-standard 0
	    Modem off 0
	    TDD/TTY US 3
	    Clear-channel n 0</pre>

Step	Description
6.	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 2. 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 3. This defines which IP network region contains the Avaya SES server. If the **Far-end Network Region** field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the inter-region connectivity for the pair of network regions. ▪ Enter the domain name of Avaya SES in the **Far-end Domain** field. In this configuration, the domain name is ***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
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>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 6.
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. In this solution, each analog endpoint at the branch counts as a SIP telephone.
The default values may be retained for the other fields.

<pre>
add trunk-group 1   Page   1 of 21
                                TRUNK GROUP

Group Number: 1   Group Type: sip   CDR Reports: y
  Group Name: To SES 50.1.1.50   COR: 1   TN: 1   TAC: 101
   Direction: two-way   Outgoing Display? n
 Dial Access? n   Night Service:
Queue Length: 0
Service Type: tie   Auth Code? n

                                                     Signaling Group: 1
                                                   Number of Members: 24
</pre></td></tr>
<tr><td>8.</td><td>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.

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

Step	Description
9.	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 7. 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
```

Step	Description
10.	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 the Avaya SES. This includes the dialing scenarios performed in the compliance test. 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
 6: y y y y y n  n            rest                                            none
```

Step	Description

11.	Use the **change locations** command to assign the default SIP route pattern to the location. In the compliance test, all SIP endpoints whether at the main or branch site 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:`

12.	All SIP stations are configured as OPS stations on Avaya Communication Manager. This includes the analog telephones and the fax machine connected to the Tenor, which appear as SIP stations to 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 and analog telephones at the branch office 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

13.	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.
	<pre>add station 40008 Page 1 of 4
	                                     STATION
	
	Extension: 40008 Lock Messages? n BCC: 0
	     Type: 6408D+ Security Code: TN: 1
	     Port: X Coverage Path 1: COR: 1
	     Name: Tenor 1 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</pre>

14.	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. The example below shows the configuration of one of the analog phones connected to the Tenor. The analog phones used in the compliance test were configured with two call appearances.
	<pre>add station 40008 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: 7:
	 4: 8:</pre>

Step	Description

15.	Map the Avaya Communication Manager extension to the Avaya SES media server extension defined in Section 4, Step 8 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.
	
	<pre>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
	 40008 OPS - 40008 1 1
	                                -</pre>

16.	On Page 2, set the **Call Limit** to the number of call appearances set on the station form in Step 14. Verify that the **Mapping Mode** is set to ***both***.
	
	<pre>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
	 40008 2 both all both</pre>

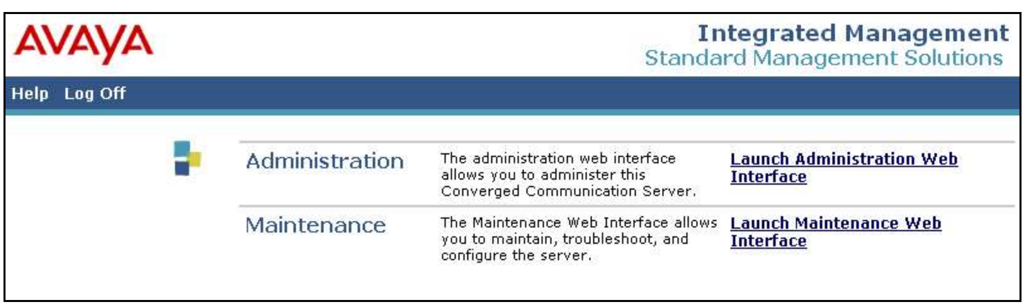
17.	Repeat Steps 13 -16 for each remaining station located at the branch office. The branch office has six stations: two analog telephones connected to the Tenor (x40008 and x40009), two Avaya 4600 Series SIP Telephones (x40006 and x40032) and two generic SIP telephones (x40003 and x40005). In the compliance test, the fax machine at the branch replaced one of the analog telephones above when necessary. Thus, it did not require the configuration of a separate extension.

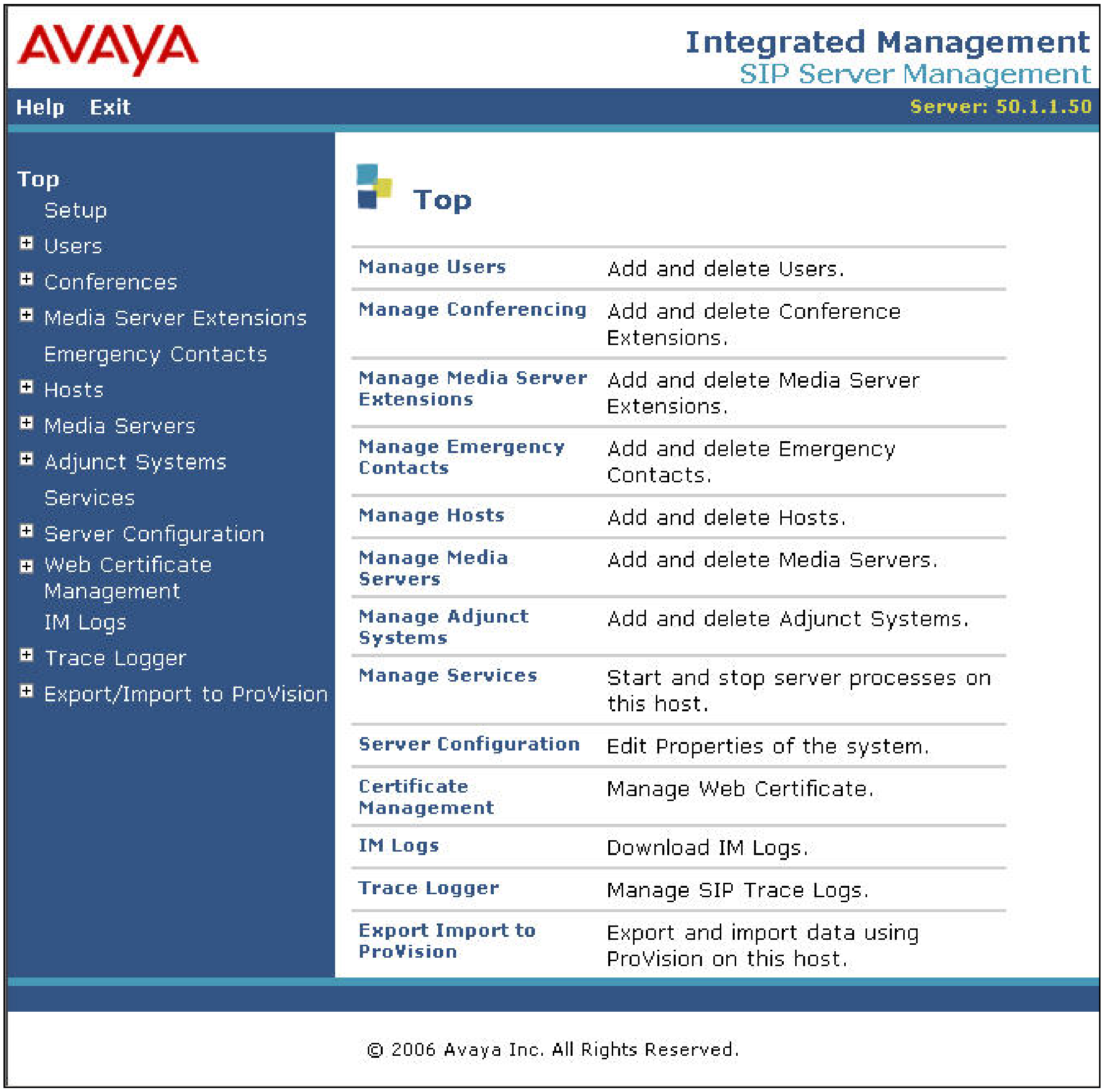
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>18.</td><td>To map a DID number to a station at the main or branch office, use the change inc-call-handling-trmt trunk-group n command, where n is the trunk group number connected to the PSTN from the Avaya G350 Media Gateway. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows three incoming 11-digit numbers being deleted and replaced with the extension number of the desired station.
<pre>
change inc-call-handling-trmt trunk-group 2   Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/   Called   Called   Del Insert
 Feature   Len   Number
 tie   11 17325551234   11   40007
 tie   11 17325551235   11   40008
 tie   11 17325551236   11   40015
</pre></td></tr>
</table>

4. Configure Avaya SES

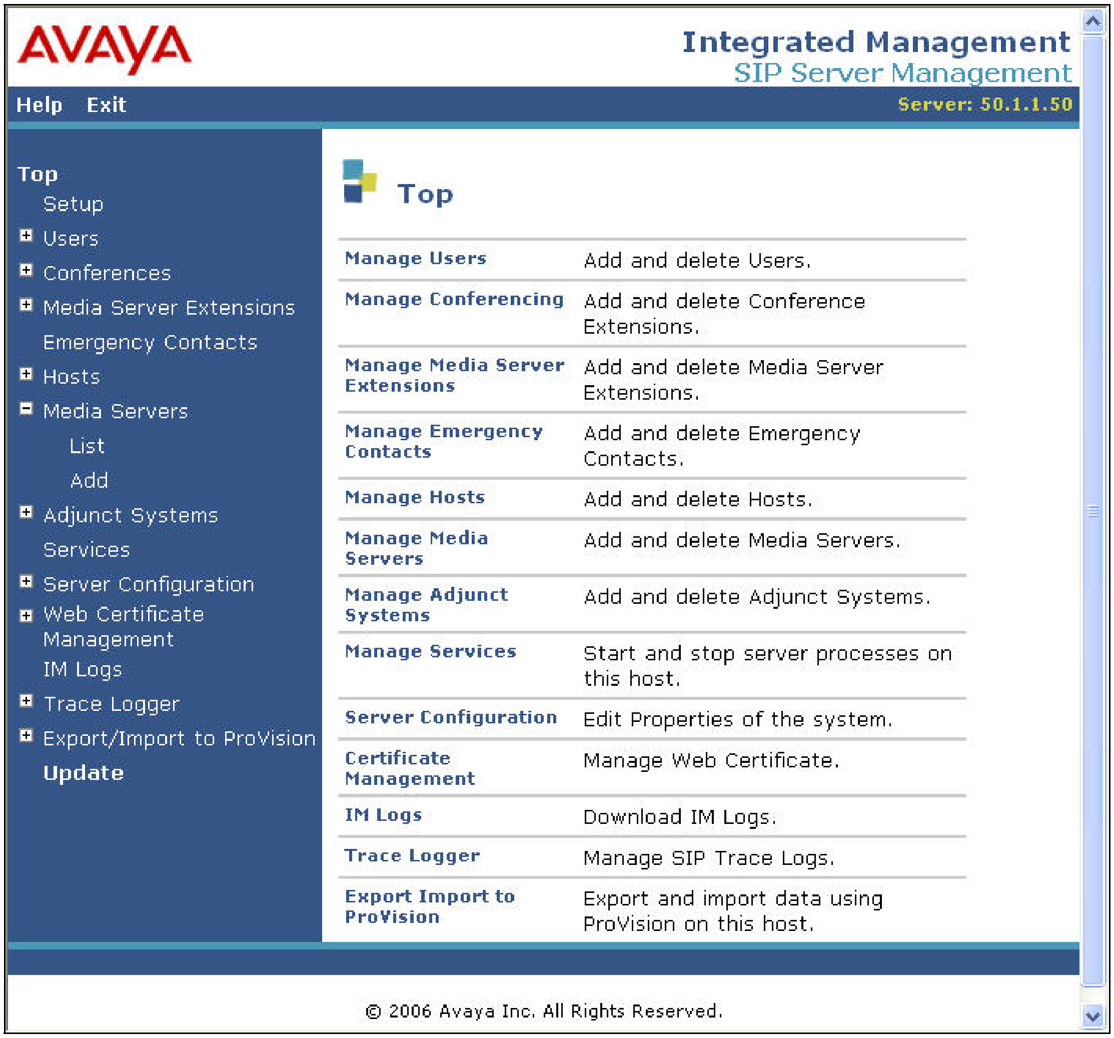
This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that Avaya SES software and the license file have already been installed on the server. During the software installation, the installation script is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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Access the Avaya SES administration web interface by entering http://<<i>ip-addr</i>>/admin as the URL in an Internet browser, where <<i>ip-addr</i>> 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.

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

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

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.

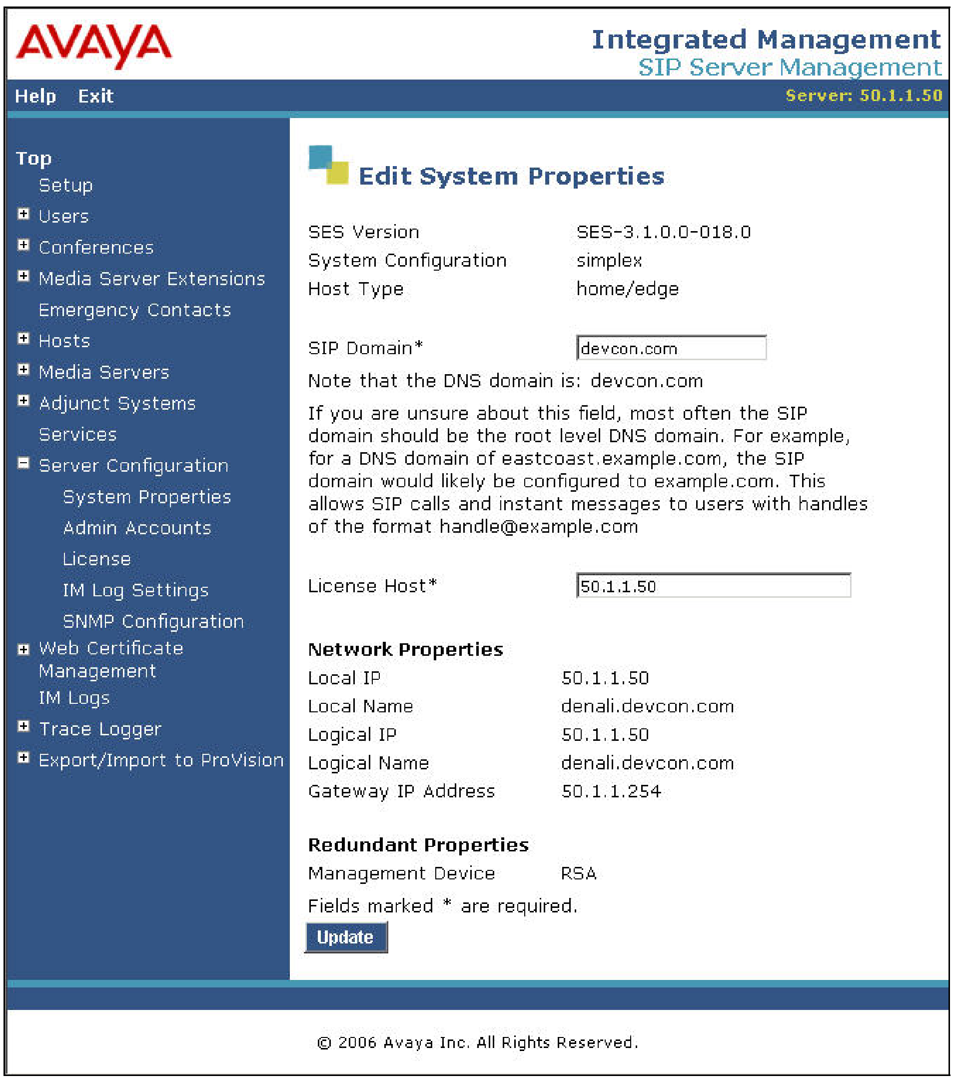


<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

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, Step 3.
- Enter the **License Host** field. This is the host name, the fully qualified domain name, or the IP address of the SIP proxy server that is running the WebLM application and has the associated license file installed.
- After configuring the **Edit System Properties** page, click the **Update** button.

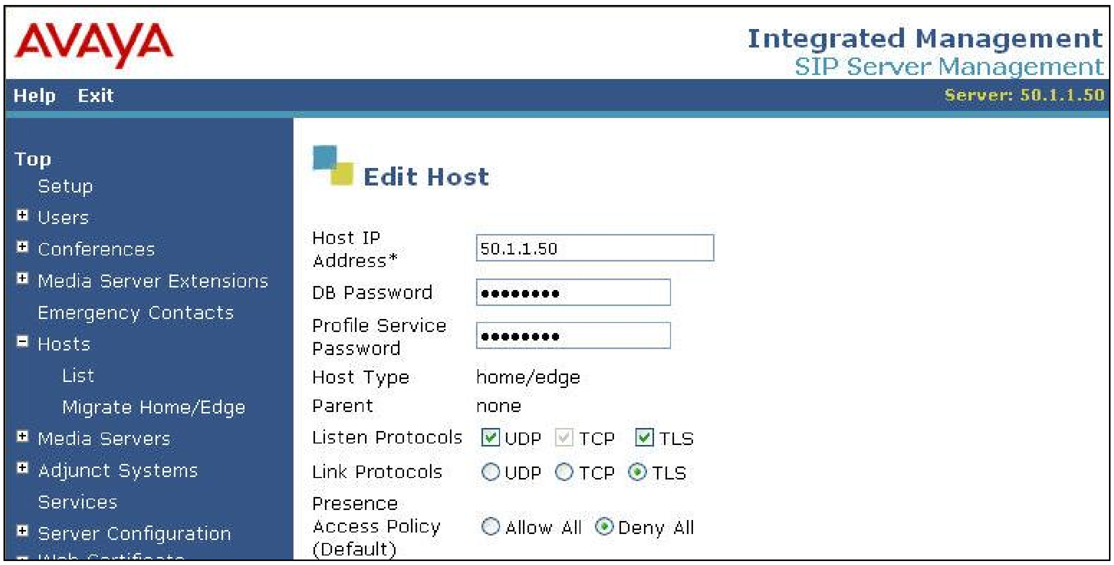


</td></tr>
</table>

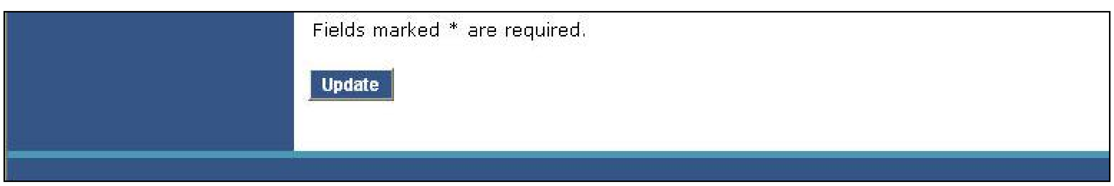
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>
After setting up the domain on the Edit System Properties page, create a host computer entry for Avaya SES. The following example shows the Edit Host page since the host had already been added to the system.

The Edit Host page shown below is accessible by clicking on the Hosts link in the left pane and then clicking on the Edit link under the Commands section of the subsequent page that is displayed.

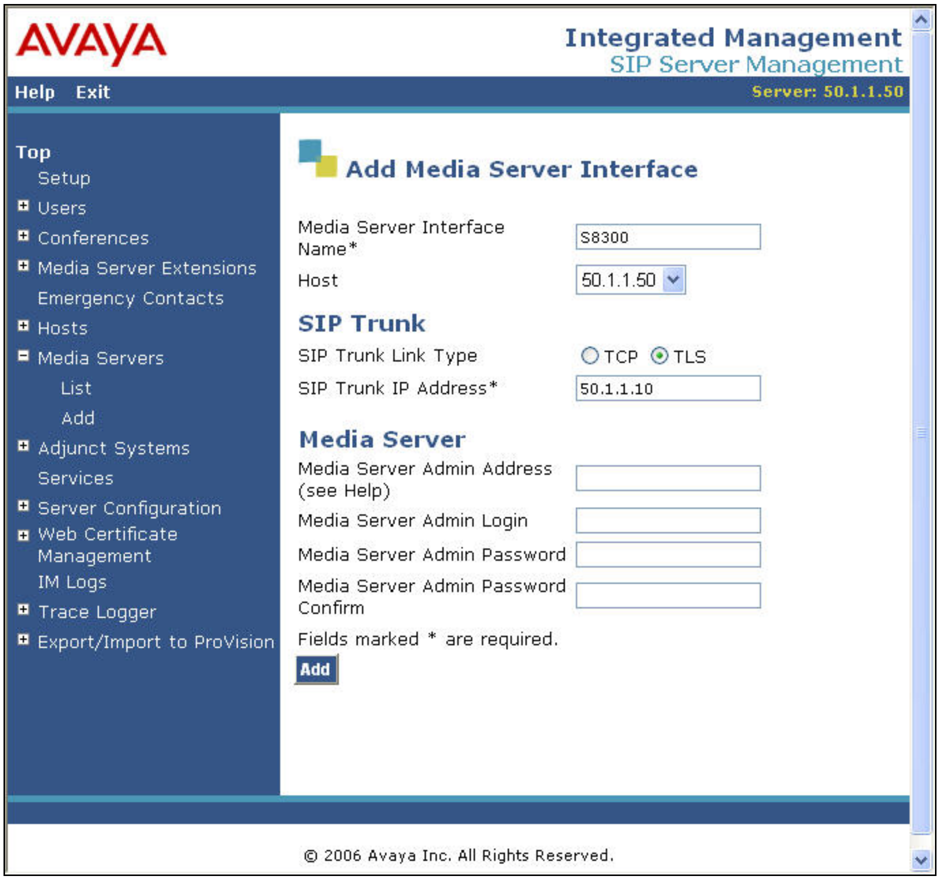
In the Host IP Address field, enter the Logical IP or Logical Name of this server as shown in Step 4.
Enter the DB Password that was specified during the system installation.
The default values for the other fields may be used.



Scroll down to the bottom of the page and click the Update button.



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

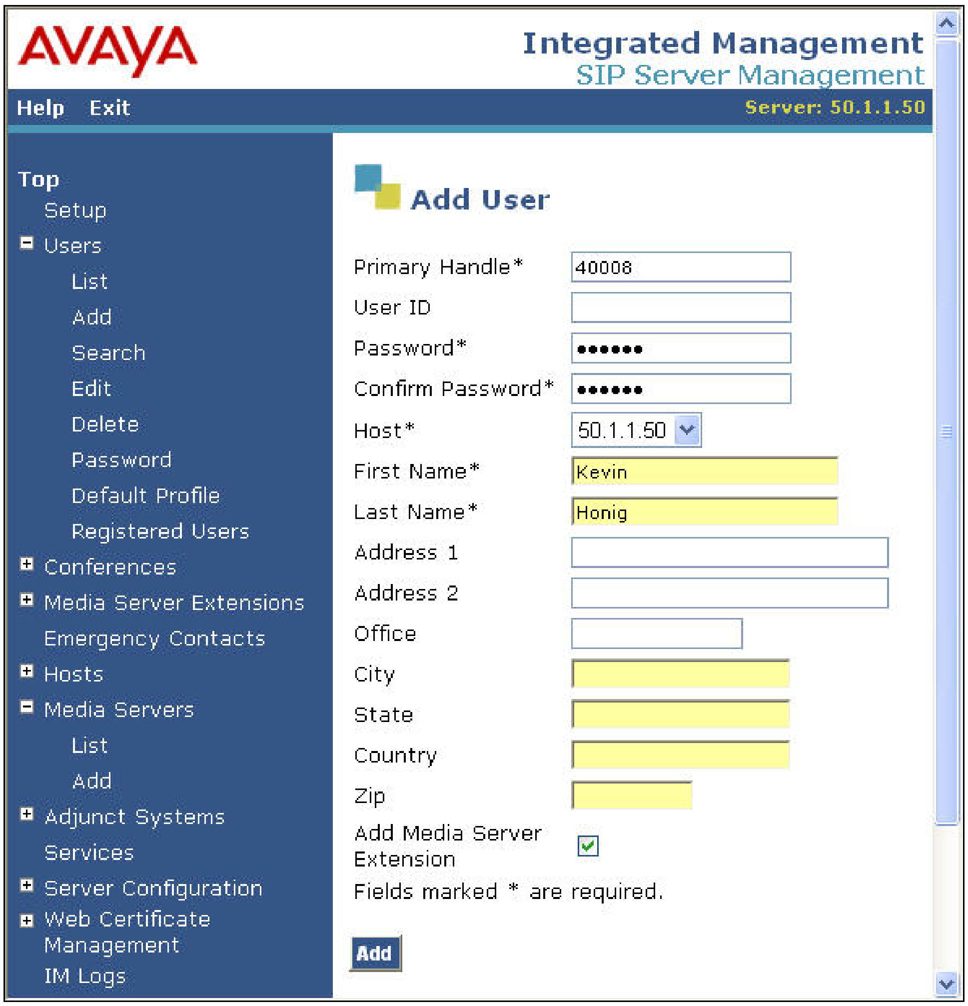
Step	Description
6.	From the left pane of the administration web interface, expand the **Media Server** option and select **Add** to add the Avaya Media Server to the list of media servers known to Avaya SES. Adding the media server will create the Avaya SES side of the SIP trunk previously created in Avaya Communication Manager. On the **Add Media Server Interface** page, enter the following information: ▪ 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** page, click the **Add** button. 

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

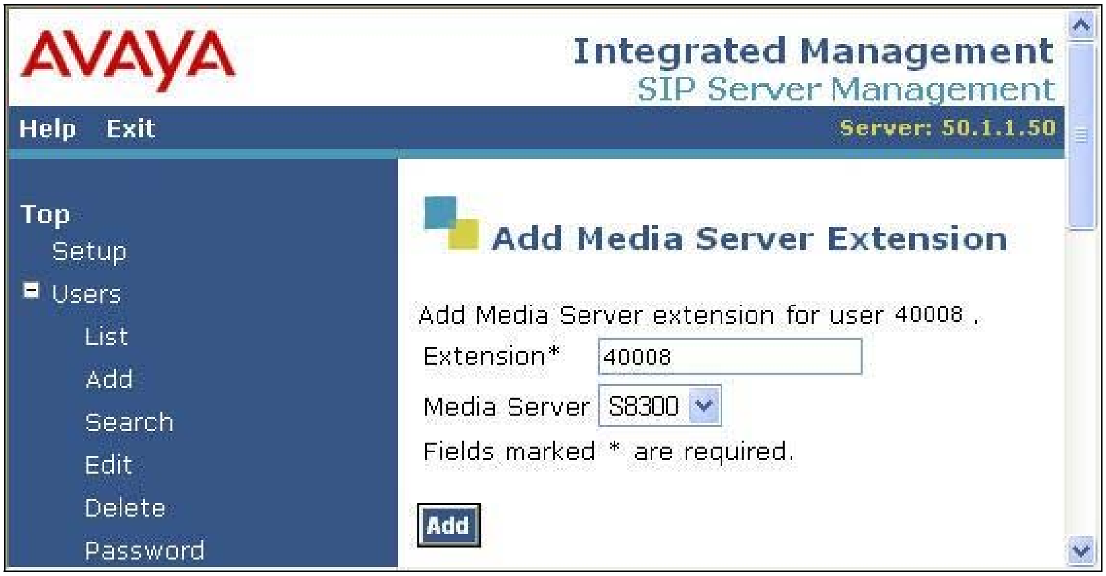
A user must be added on Avaya SES for each of the extensions at the branch office created on Avaya Communication Manager in Section 3, Steps 13 - 17. From the left pane, navigate to **Users → Add**. Enter the values as shown below.

- **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.

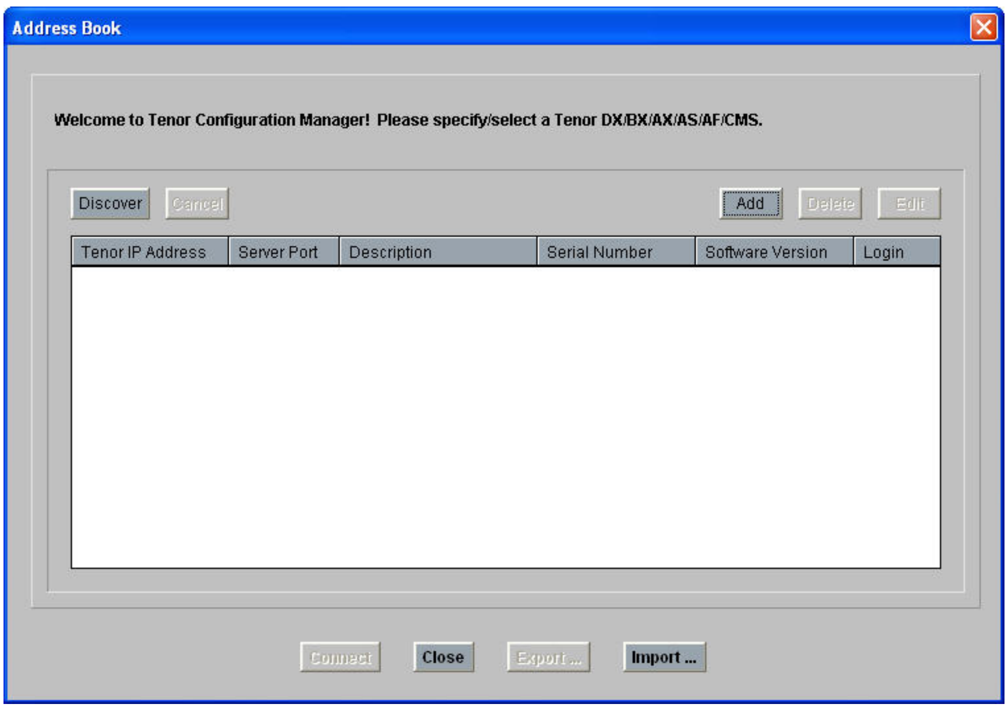


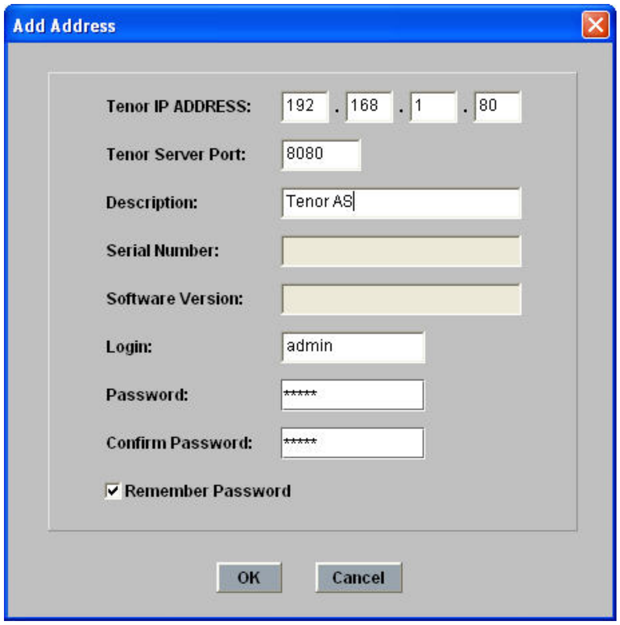
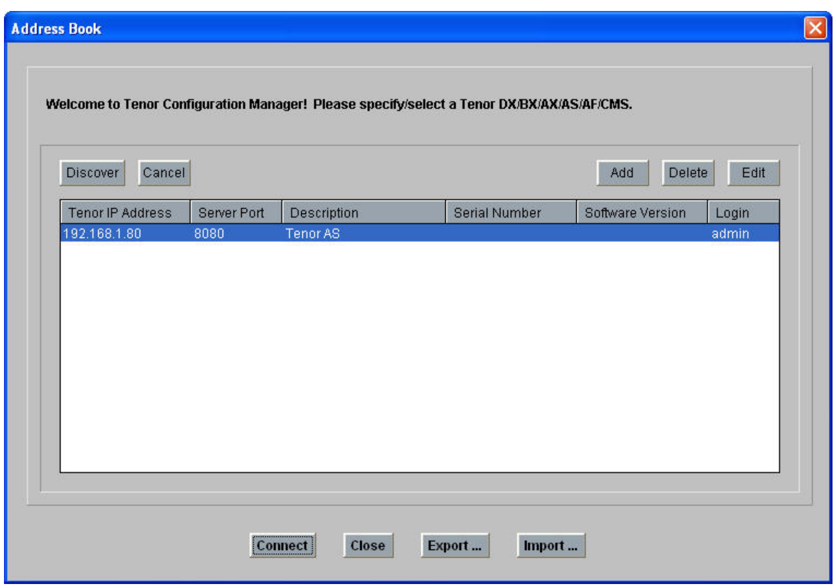
</td></tr>
</table>

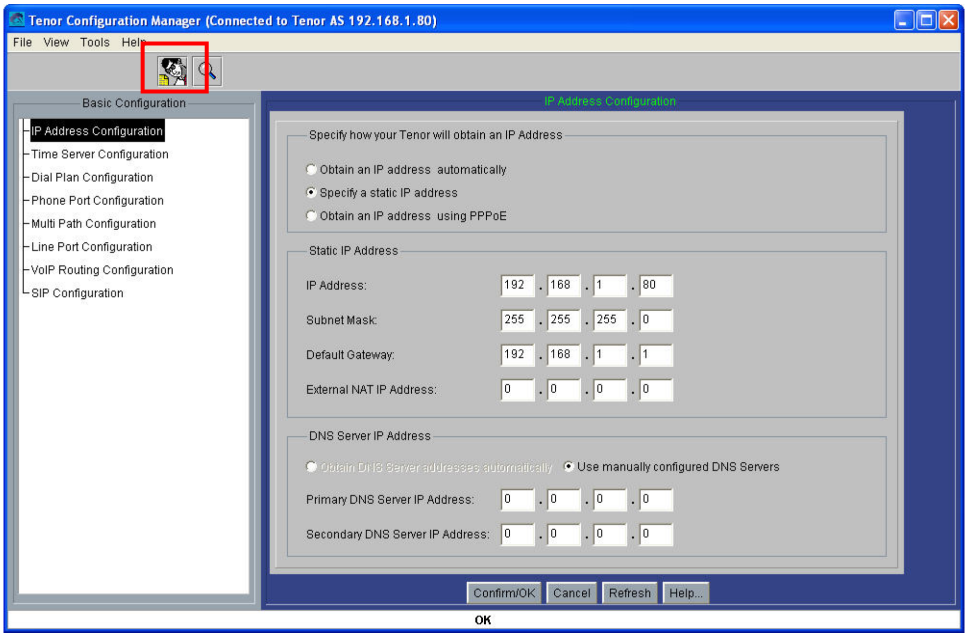
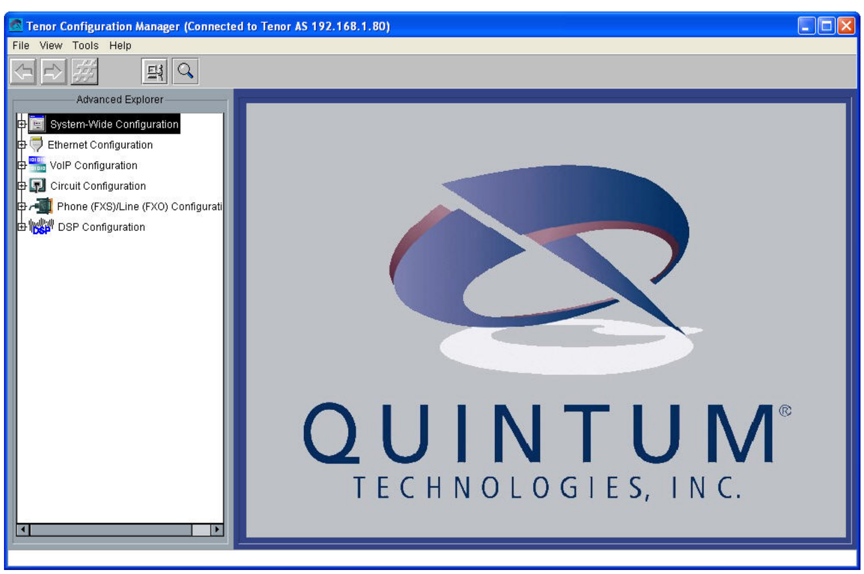
Step	Description
8.	The **Add Media Server Extension** page will appear. In the **Extension** field, enter the same extension used in the previous step. In the **Media Server** field, select from the pull-down menu the name of the media server added in Step 6. Click the **Add** button to complete the operation. 
9.	Repeat Steps 7 - 8 for each of the remaining stations at the branch office.

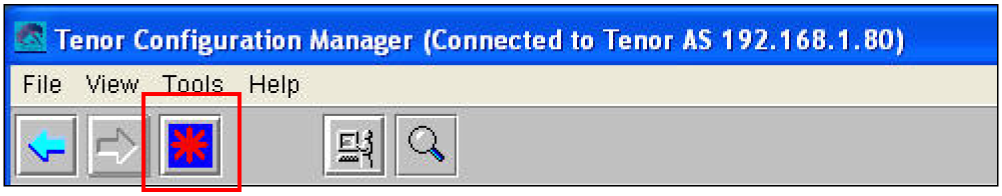
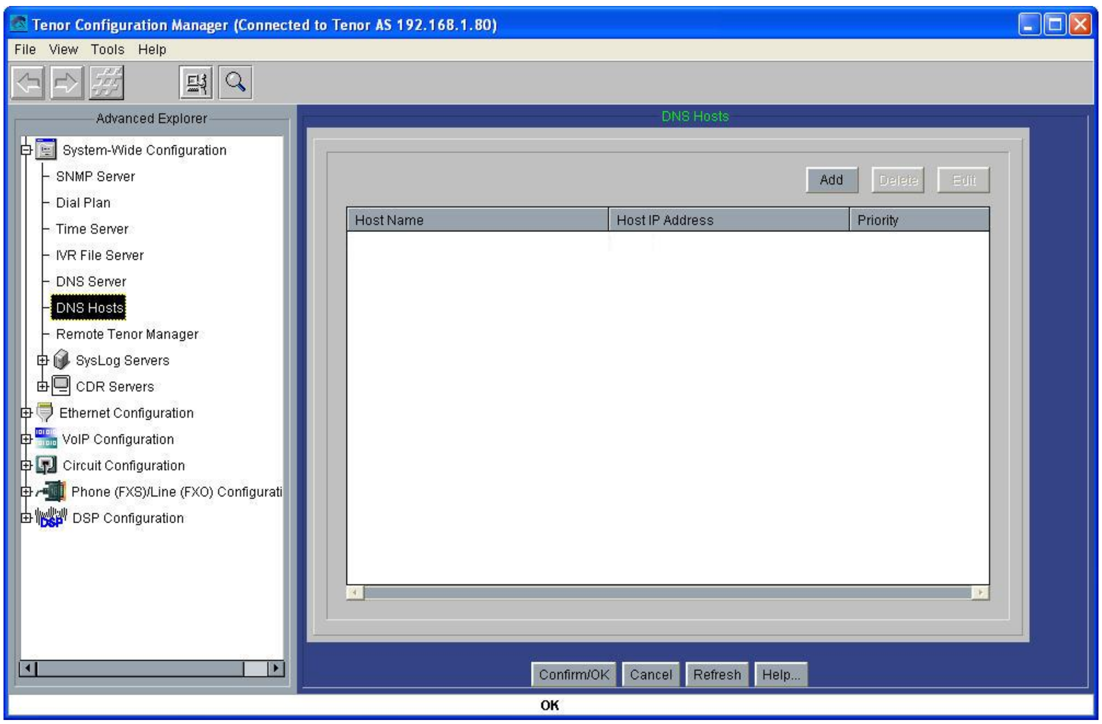
5. Configure the Tenor AS MultiPath Switch

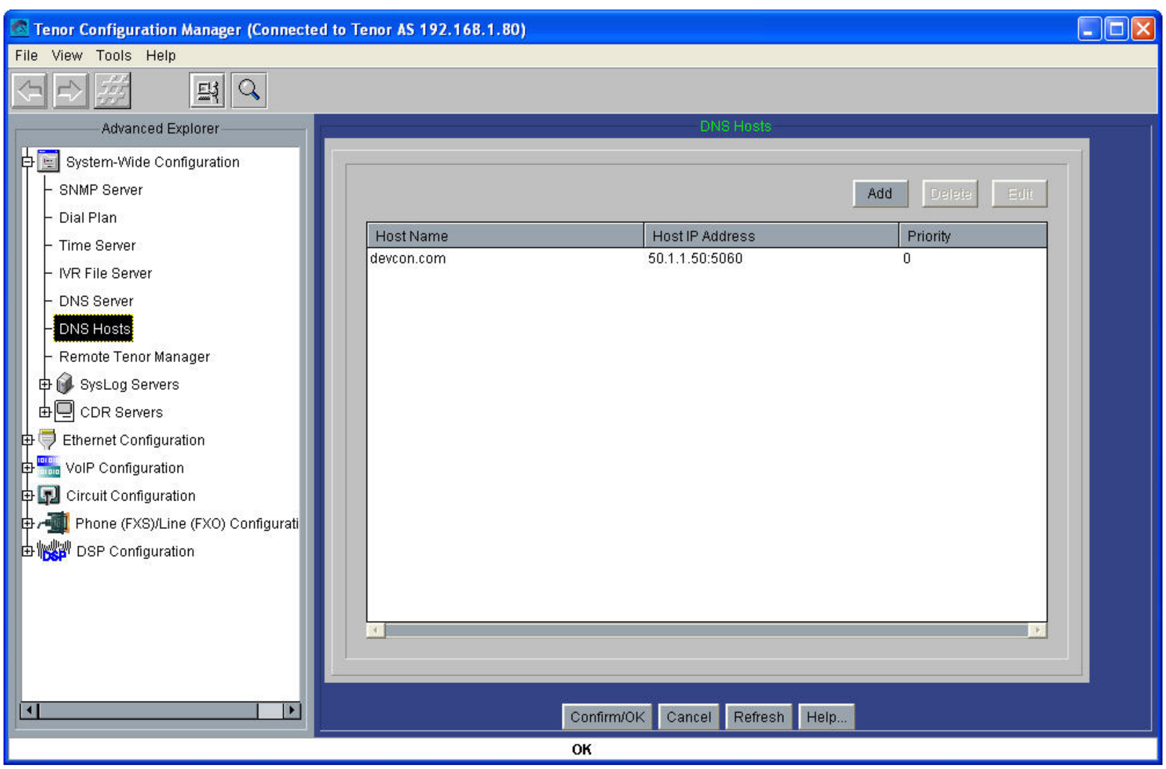
This section describes the procedure for configuring the Tenor AS VoIP MultiPath Switch with the B2BUA functionality. This procedure assumes the Tenor has already been configured with an IP address. All Tenor configuration described in this section is performed using the Tenor Configuration Manager. The Tenor Configuration Manager is a software application that runs on a Windows PC. For detailed information on installing and running Tenor Configuration Manager, consult references [7] and [8].

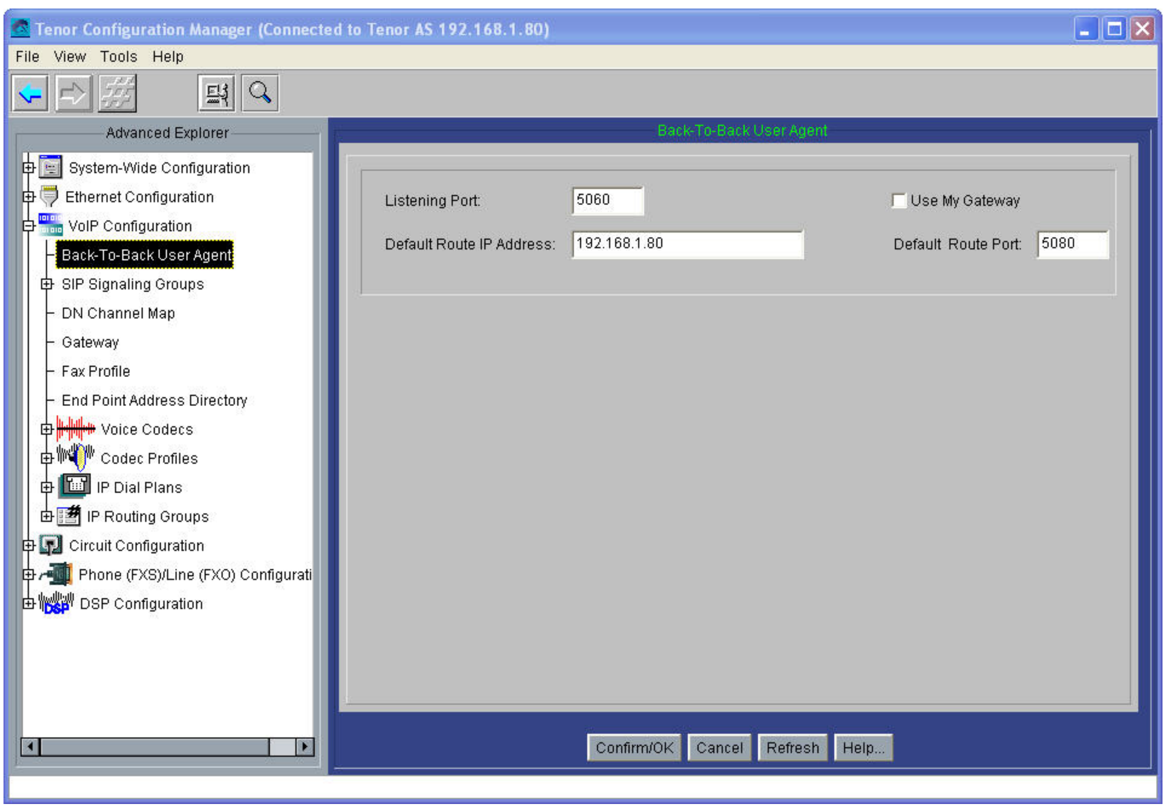
Step	Description
1.	Launch the Tenor Configuration Manager from the Windows Start Menu by navigating to **All Programs → Quintum Tenor Configuration Manager → Tenor Config Manager.** An **Address Book** window will appear. The address of the Tenor must be initially added to the Tenor Configuration Manager's Address Book. Click **Add** to continue. 

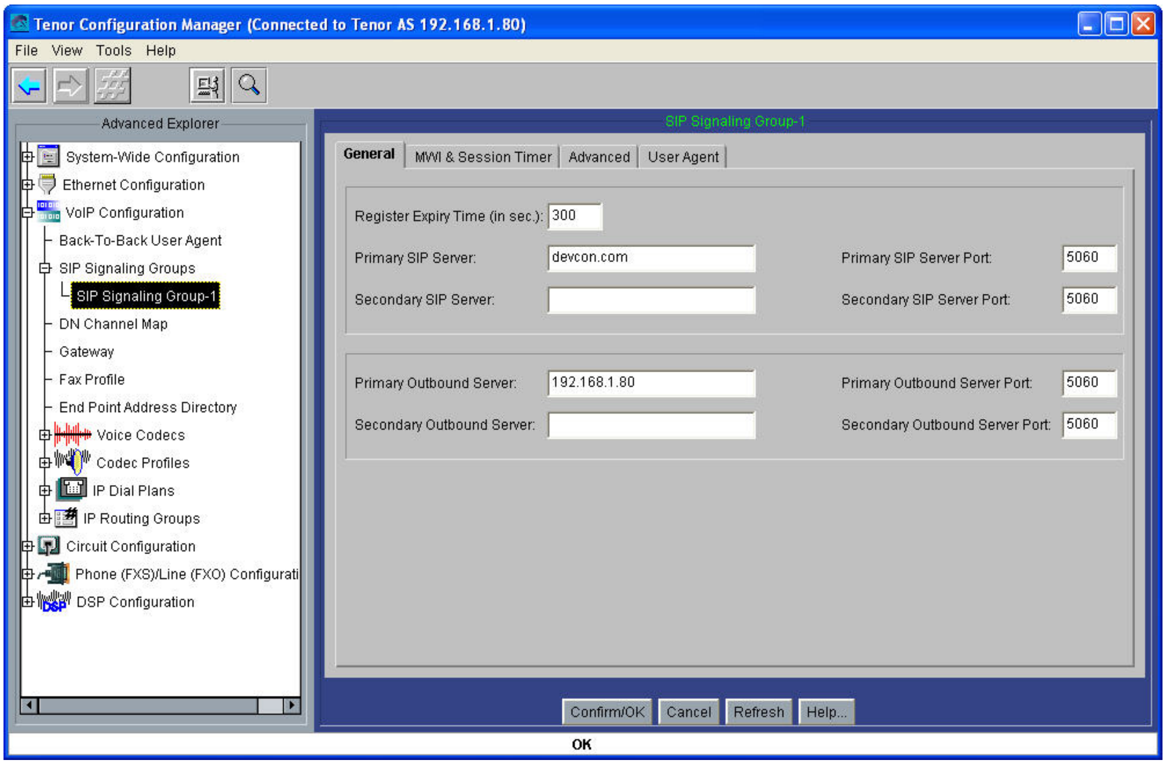
Step	Description
2.	The **Add Address** window appears. Enter the Tenor IP address where indicated. Use the default value for the **Tenor Server Port**. Enter a descriptive name in the **Description** field. Use the admin login and password in the **Login** and **Password** fields. The default values may be for all other fields. Click **OK**. 
3.	The new entry for the Tenor will now appear in the Address Book. To establish a connection from the Tenor Configuration Manager to the Tenor, highlight the entry in the Address Book and click the **Connect** button. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>The initial screen displays the Basic Configuration menu tree in the left pane of the window. The right pane displays the top page of the tree – IP Address Configuration. The following procedures use the Advanced Explorer menu to configure the Tenor. To change the menu tree in the left pane from Basic Configuration to Advanced Explorer, click the Advanced Explorer button at the top of the page. This button is highlighted in the example below.

</td></tr>
<tr><td>5.</td><td>The Advanced Explorer menu tree appears in the left pane of the window. Each entry in the tree can be expanded to reveal additional sub-menu options by clicking on the + next to an entry. This interface will be used to navigate to each window requiring configuration.

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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>When changes are pending, a sunburst button will appear in the menu bar at the top of the window as shown below. Click the sunburst button to submit the pending changes.

</td></tr>
<tr><td>7.</td><td>Assign a host name to the Avaya SES server IP address for use by the Tenor. From the Advanced Explorer menu tree, navigate to System-Wide Configuration → DNS Hosts. Click Add to display the Add DNS Host pop-up window.

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

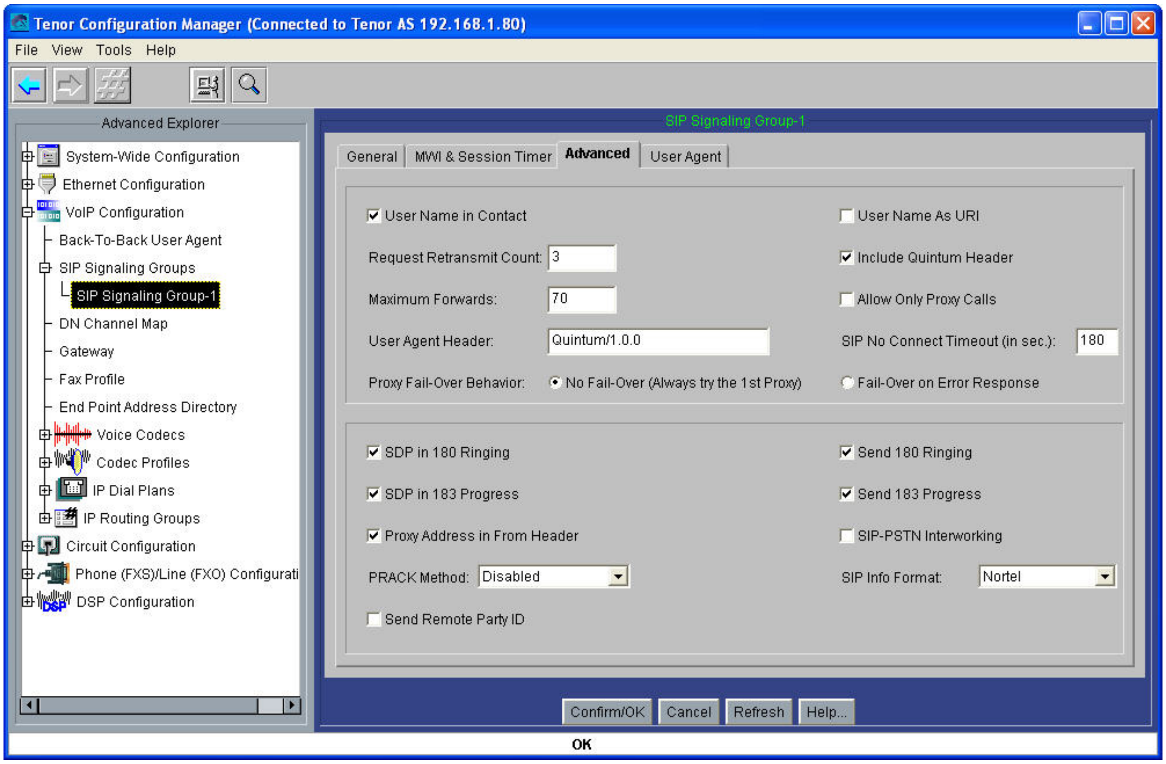
Step	Description
8.	In the **Host Name** field, enter the SIP domain of the Avaya SES. In the **IP Address** field, enter the IP address and port number of the Avaya SES server. The Avaya SES server uses port 5060, which is the standard port for SIP. Click **OK** to complete. 
9.	The newly created entry appears in the DNS Hosts table. Click the **Confirm/OK** button. The sunburst button will appear in the tool bar. Click on the sunburst button to submit the changes. 

Step	Description
10.	Configure the back-to-back user agent. From the Advanced Explorer menu tree, navigate to **VoIP Configuration → Back-To-Back User Agent**. Enter the default SIP listening port 5060 in the **Listening Port** field. To access the PSTN when the data WAN fails, a default route must be configured that the back-to-back user agent will use in this situation. The default route is one of the SIP user agents in the gateway function of the Tenor. Any of the gateway user agents can be used for this function, since they all have access to the PSTN connection. To configure this default route, uncheck the box next to **Use My Gateway**. In the **Default Route IP Address** field, enter the IP address of the Tenor since the gateway function resides in the same device as the back-to-back agent. In the **Default Route Port** field, enter the SIP listening port for one of the gateway user agents configured in Steps 14 -15. For the compliance test, the user agent for port 1 (e.g. UA 101) was selected as the default route. User agent 101 uses listening port 5080 as shown in Step 14. Click the **Confirm/OK** button. The sunburst button will appear in the tool bar. Click on the sunburst button to submit the changes. 

Step	Description
11.	Configure the SIP parameters of the gateway functionality. From the Advanced Explorer menu tree, navigate to **VoIP Configuration → SIP Signaling Groups → SIP Signaling Group-1**. On the **Signaling Group-1** form, select the **General** tab. In the **Primary SIP Server** field, enter the host name given the Avaya SES in Step 8. Verify the **Primary SIP Server Port** is set to *5060*. In the **Primary Outbound Server** field, enter the IP address of the B2BUA. Entering a value in this field enables the B2BUA functionality. Verify the **Primary Outboard Server Port** is set to *5060*. The default values may be used for all other fields. 

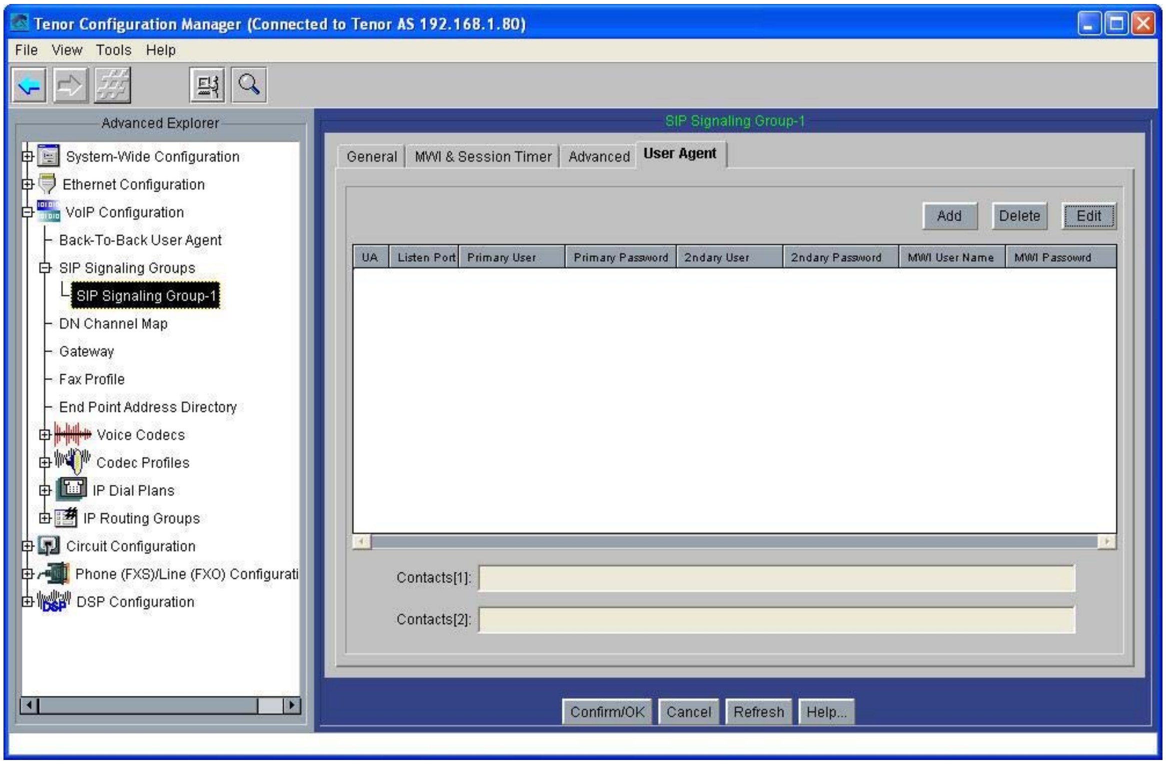
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>12.</td><td>

On the **Advanced** tab, set the **Request Retransmit Count** to *3*. This is the number of times the gateway attempts to reach the Avaya SES server before switching to the PSTN connection.



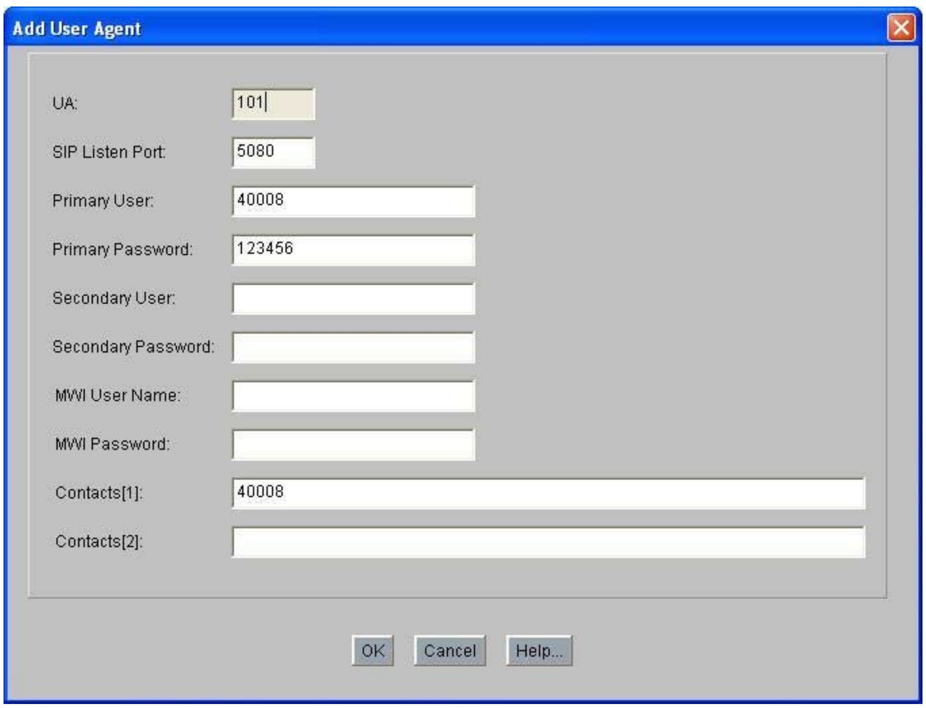
</td></tr>
</table>

Step	Description
13.	Each analog device (phone or fax) connected to the Tenor requires a SIP user agent. To add a SIP user agent, select the **User Agent** tab and click the **Add** button to display the **Add User Agent** pop-up window.



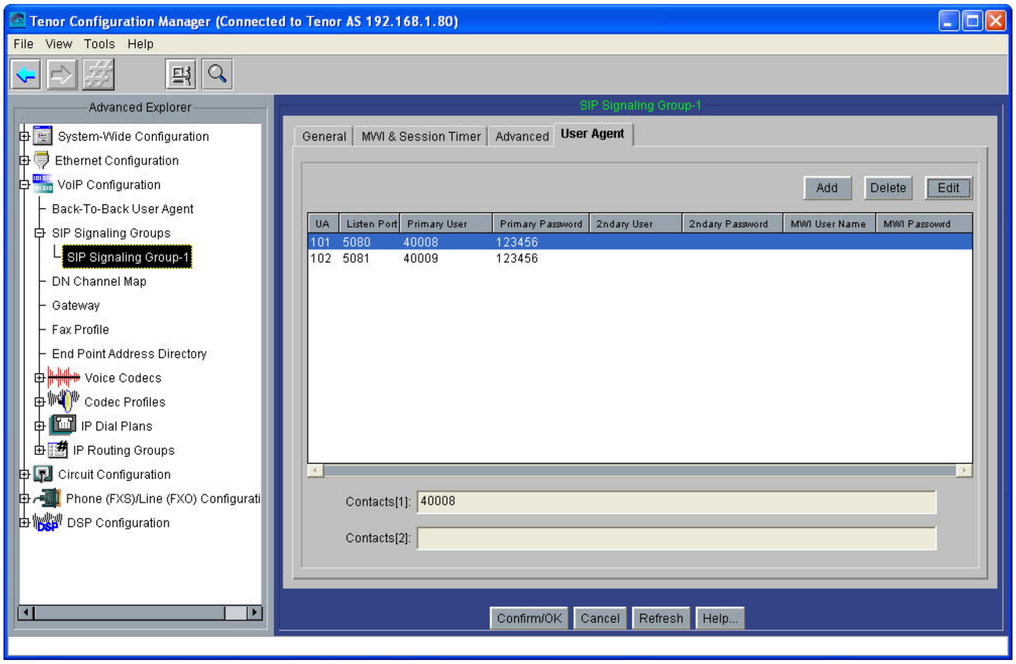
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>14.</td><td>In the Add User Agent pop-up window, enter the following information:

Primary User: A user/station configured on Avaya SES that corresponds to an analog phone connected to the Tenor.
SIP Listen Port: A valid TCP port other than the standard SIP port of 5060. The Primary Outbound Server is using port 5060 as configured in Step 10.
Primary Password: The password defined on Avaya SES for the above user.
Contacts[1]: Same as the Primary User.

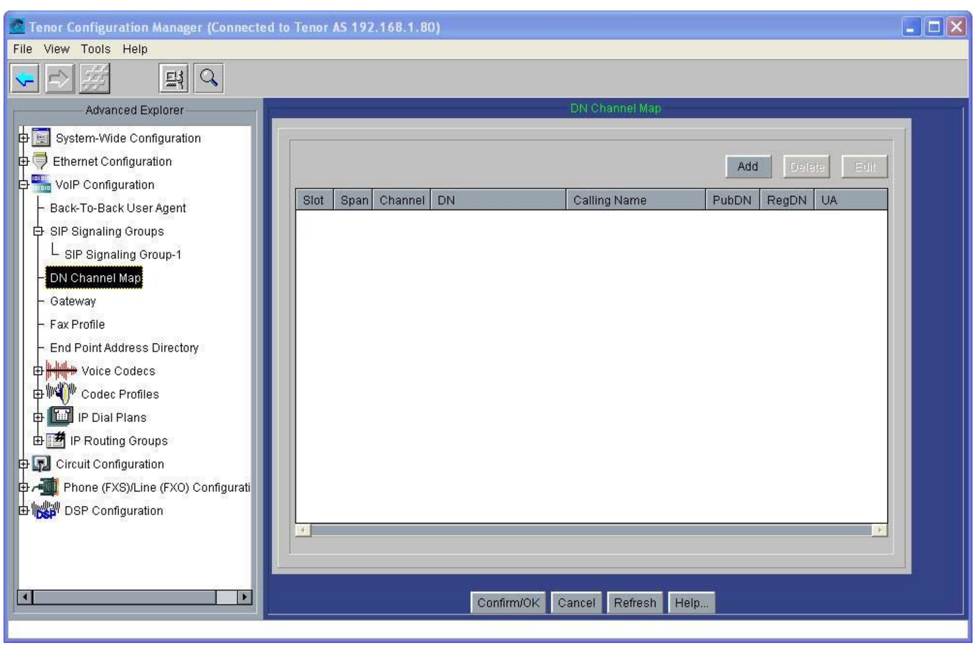
The default values may be retained for all other fields. Click OK to continue.


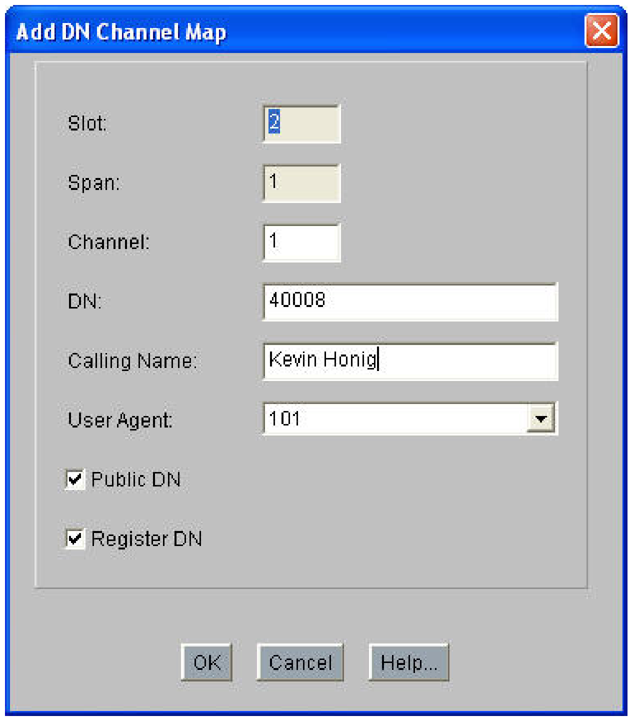
</td></tr>
<tr><td>15.</td><td>Repeat Steps 13 – 14 for each analog device (phone or fax) connected to the Tenor.</td></tr>
</table>

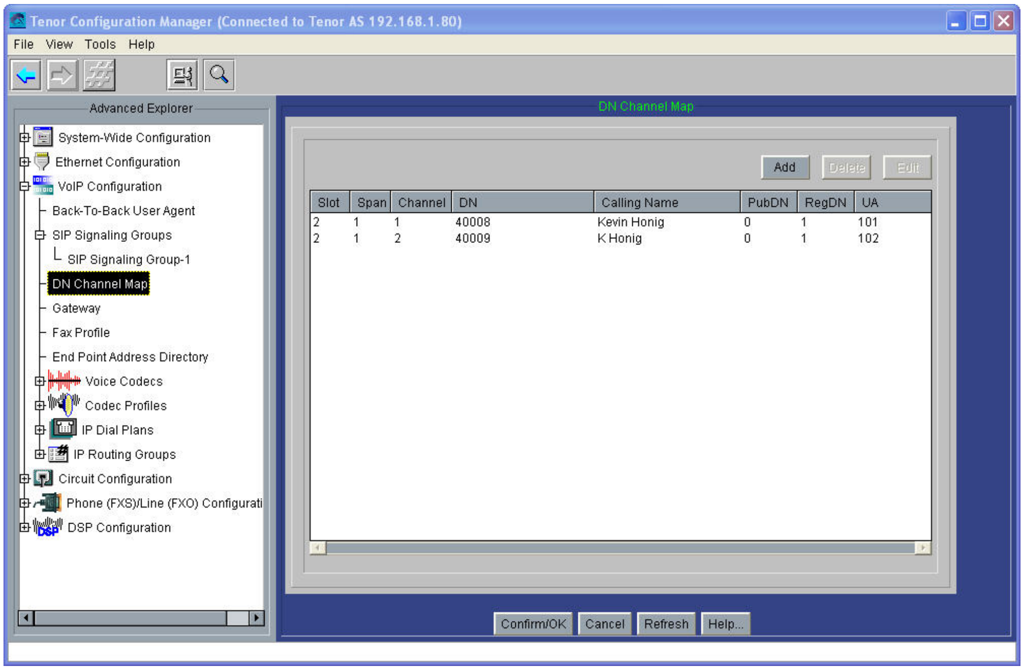
Step	Description
16.	The newly created entries appear in the SIP Signaling Group-1 table. Click the **Confirm/OK** button. The sunburst button will appear in the tool bar. Click on the sunburst button to submit the changes.

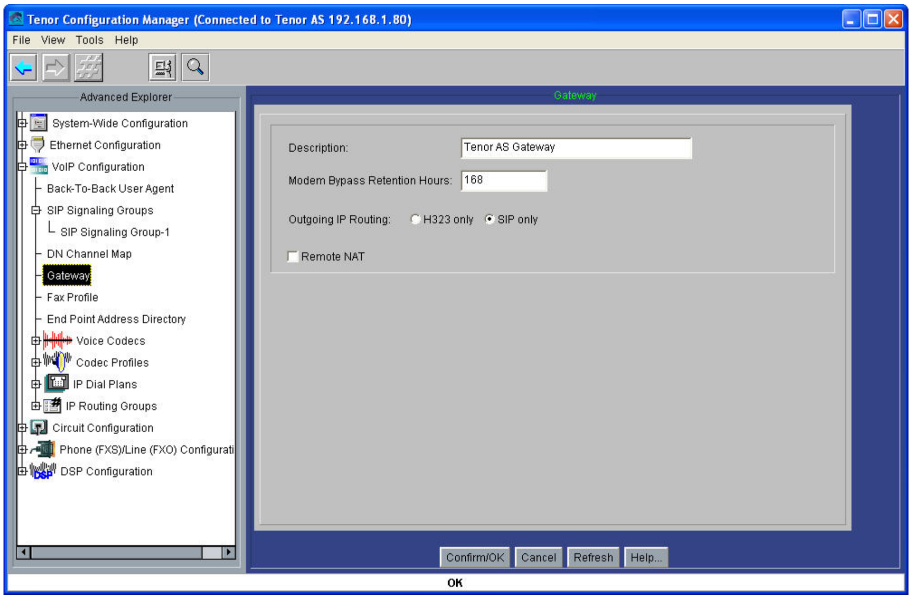


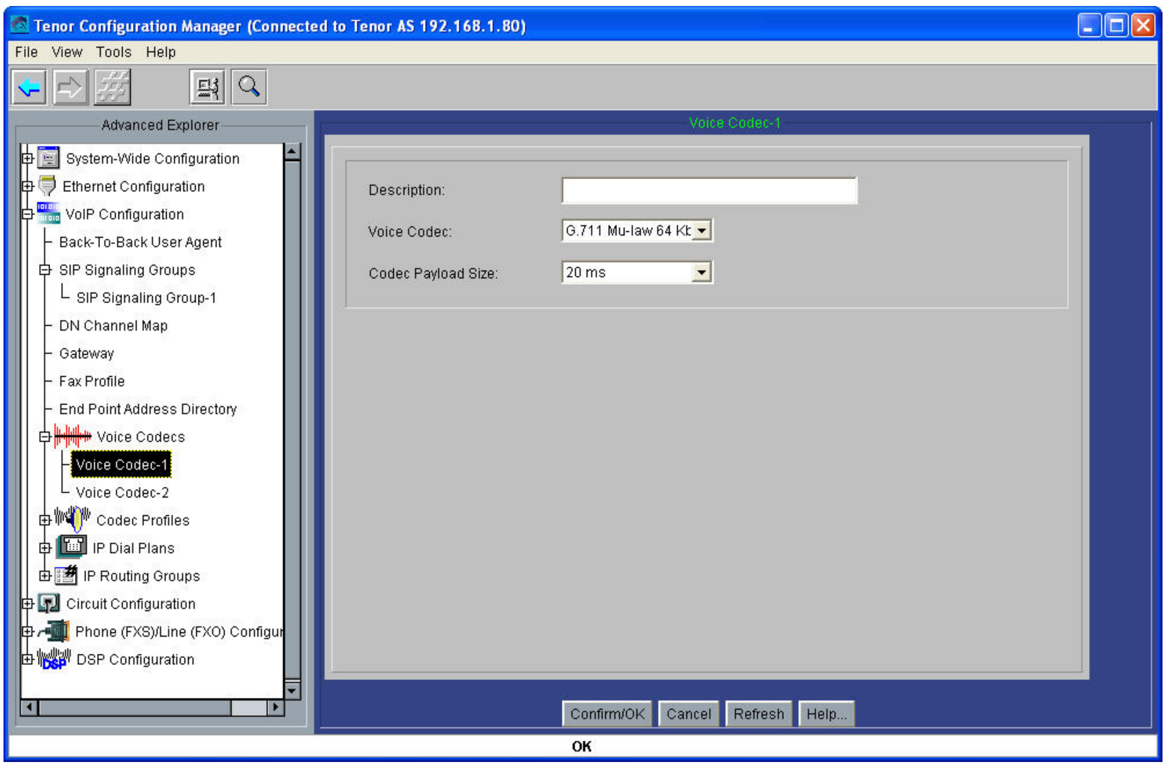
Step	Description
17.	Each user agent created in Steps 13 - 15 must be associated with a physical port/channel on the Tenor. In the Advanced Explorer menu tree, navigate to **VoIP Configuration → DN Channel Map**. Click the **Add** button to display the **Add DN Channel Map** pop-up window.

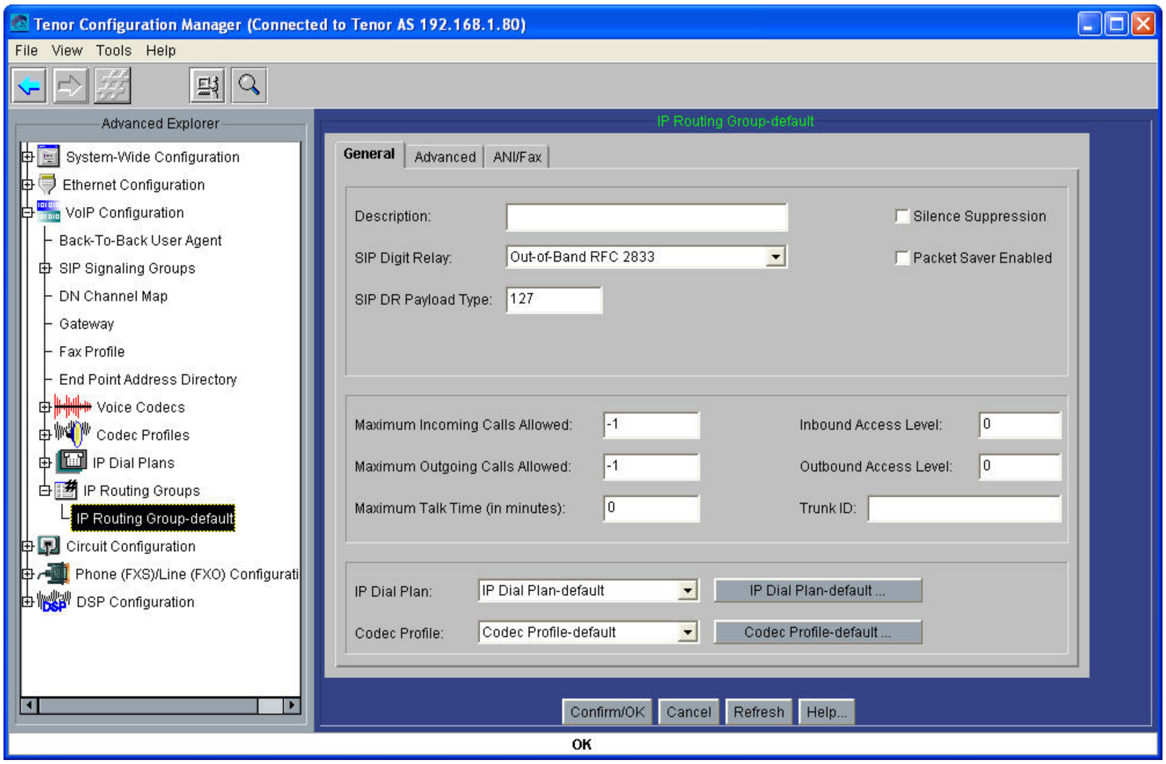


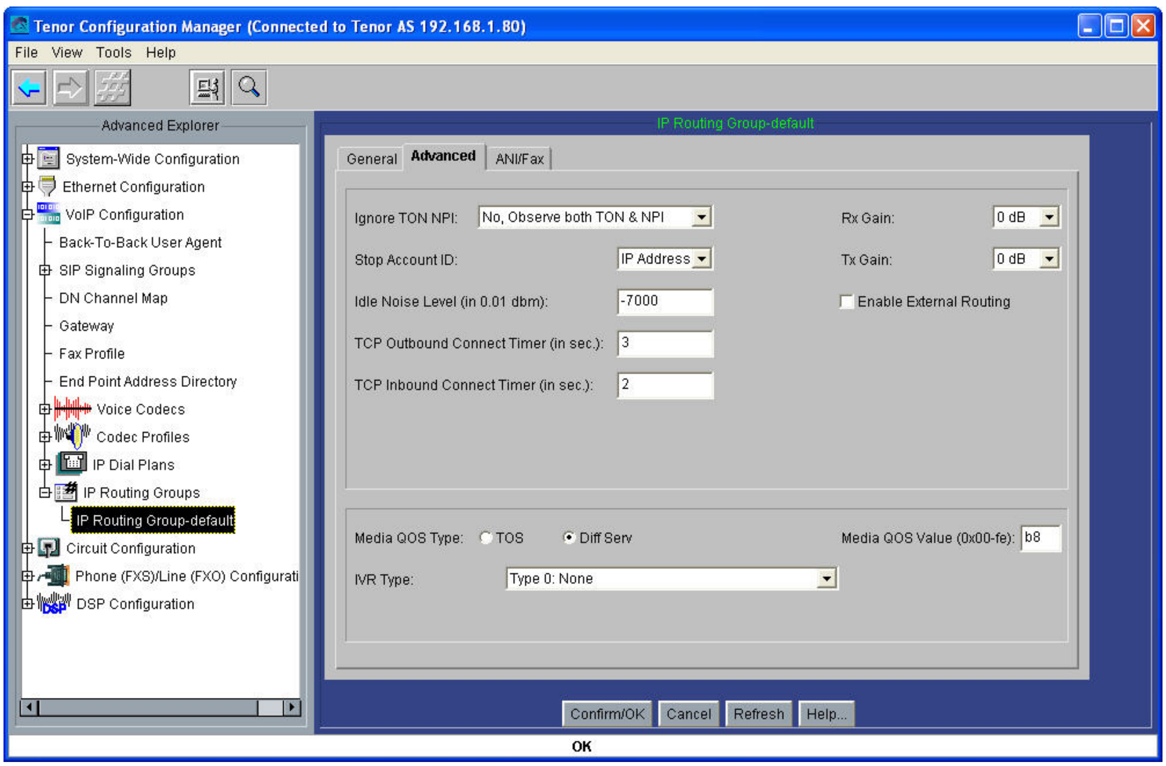
Step	Description
18.	In the **Add DN Channel Map** window, enter the following information: ▪ **Channel:** The port number on the Tenor to which the analog phone or fax is connected. ▪ **DN:** The extension of the analog phone. ▪ **Calling Name:** Any descriptive name. ▪ **User Agent:** The user agent defined for this extension. Check the checkboxes next to **Public DN** and **Register DN**. Click **OK** to continue. 
19.	Repeat Steps 17 – 18 for each user agent created.

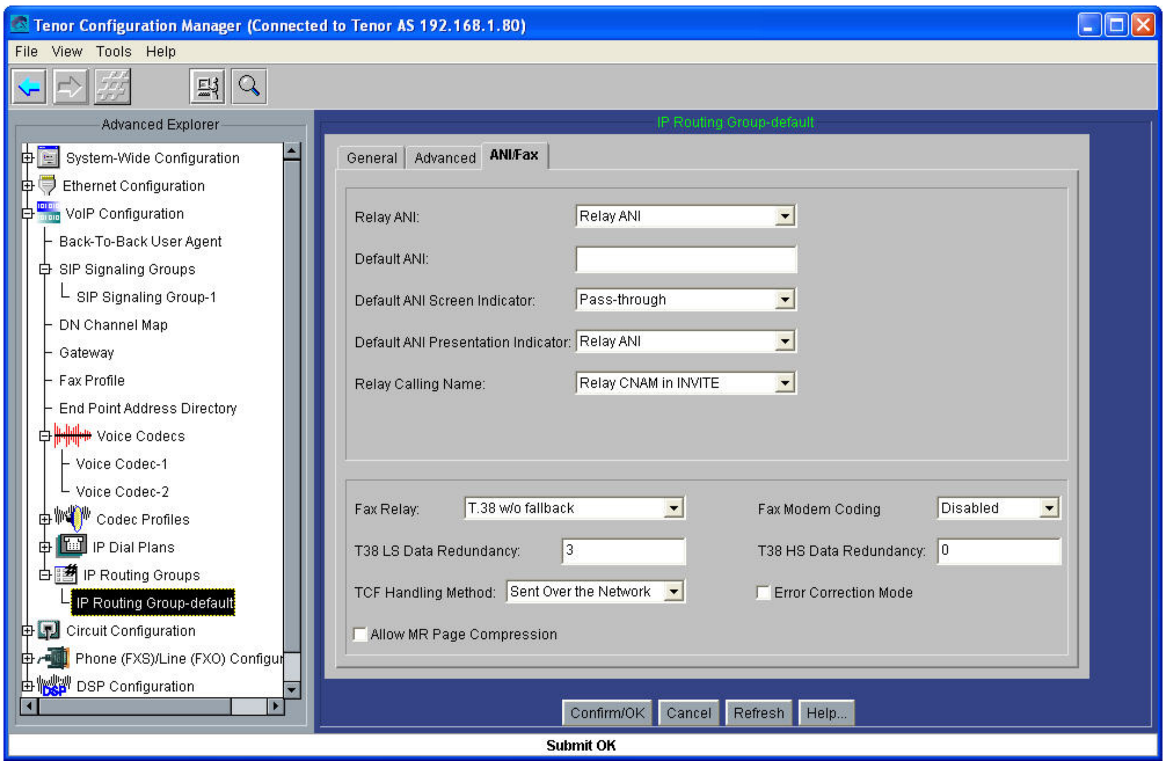
Step	Description
20.	The newly created entries appear in the DN Channel Map table. Click the **Confirm/OK** button. The sunburst button will appear in the tool bar. Click on the sunburst button to submit the changes. 

Step	Description
21.	Configure the gateway functionality to use SIP. From the **Advanced Explorer** menu tree, navigate to **VoIP Configuration → Gateway**. Enter a description in the **Description** field. Check the **SIP only** radio button for the **Outgoing IP Routing** field. The default values may be used for the other fields. Click the **Confirm/OK** button followed by the sunburst button on the menu bar to submit the changes. 

Step	Description
22.	Define the codecs that the gateway will use. From the **Advanced Explorer** menu tree, navigate to **VoIP Configuration → Voice Codecs → Voice Codec-1**. **Voice Codec-1** is the preferred codec. Select the desired **Voice Codec** from the drop-down menu. The compliance test used ***G.711 Mu-law 64 Kb***. From the **Advanced Explorer** menu tree, navigate to **VoIP Configuration → Voice Codecs → Voice Codec-2**. **Voice Codec-2** is the second codec in the list. Select the desired **Voice Codec** from the drop-down menu. The compliance test used ***G.729AB*** for **Voice Codec-2**. The default values may be used for the other fields. Click the **Confirm/OK** button and then the sunburst button on the menu bar to submit the changes. 

Step	Description
23.	Configure additional SIP related parameters in the IP Routing Group. From the **Advanced Explorer** menu tree, navigate to **VoIP Configuration → IP Routing Groups → IP Routing Group-default**. Select the **General** tab. From the **SIP Digit Relay** drop-down menu, select ***Out-of-Band RFC 2833***. Verify the **SIP DR Payload Type** is set to *127*. Uncheck the box next to **Silence Suppression**. The default values may be used for all other fields. 

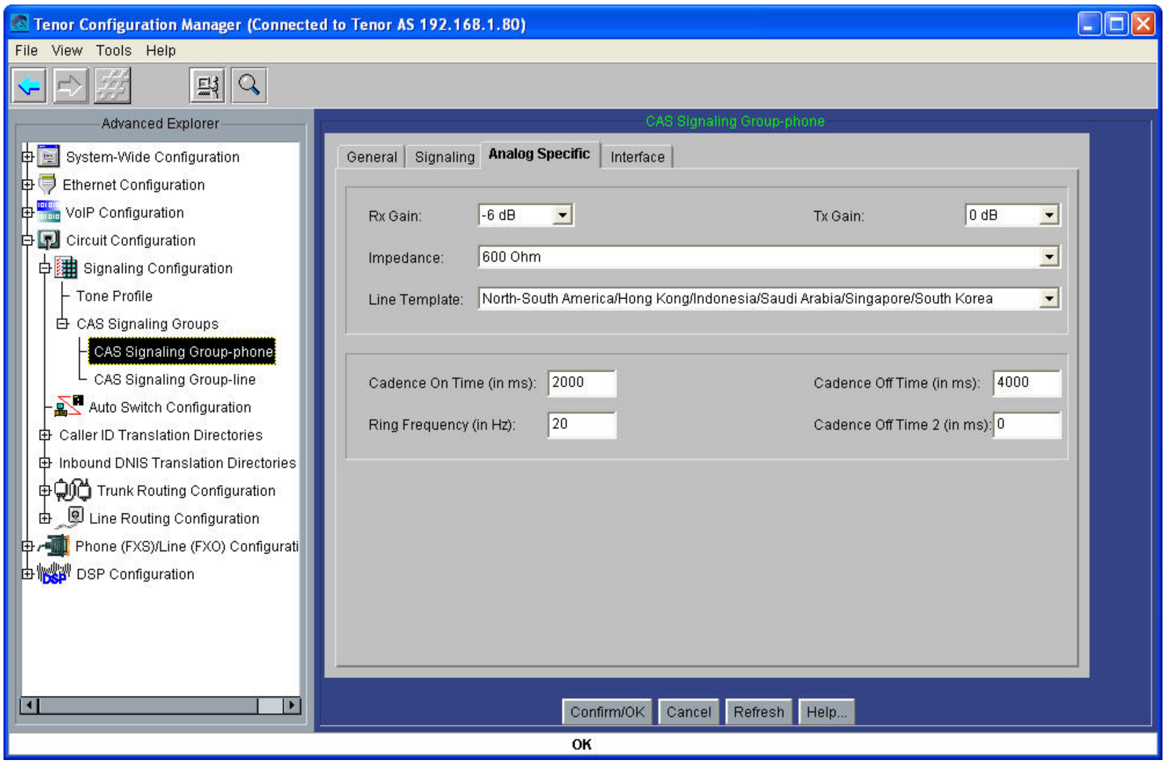
Step	Description
24.	To support Quality of Service (QOS) for the audio streams, configure a DiffServ value that will be inserted in the IP header of the RTP packets. The network could then be configured to give priority to packets with this DiffServ value. Select the **Advanced** tab. Select the **DiffServ** radio button for the **Media QOS Type** field. Change the **Media QOS Value** to ***b8***. This configures the DiffServ value in the RTP packets to be 0xb8. This value corresponds with the value entered on Avaya Communication Manager in Section 3, Step 3. To optimize the voice quality, select *0 db* from the **Rx Gain** and the **Tx Gain** pull-down menus. 

Step	Description
25.	Configure the ANI and Fax parameters. Select the **ANI-Fax** tab. Configure the following information. ▪ **Relay ANI**: ***Relay ANI***. ▪ **Relay Calling Name**: ***Relay CNAM in INVITE***. ▪ **Fax Relay**: ***T.38 w/o fallback*** The default values may be used for all other fields. Click **Confirm/OK** and then the sunburst button on the menu bar to implement the change. 

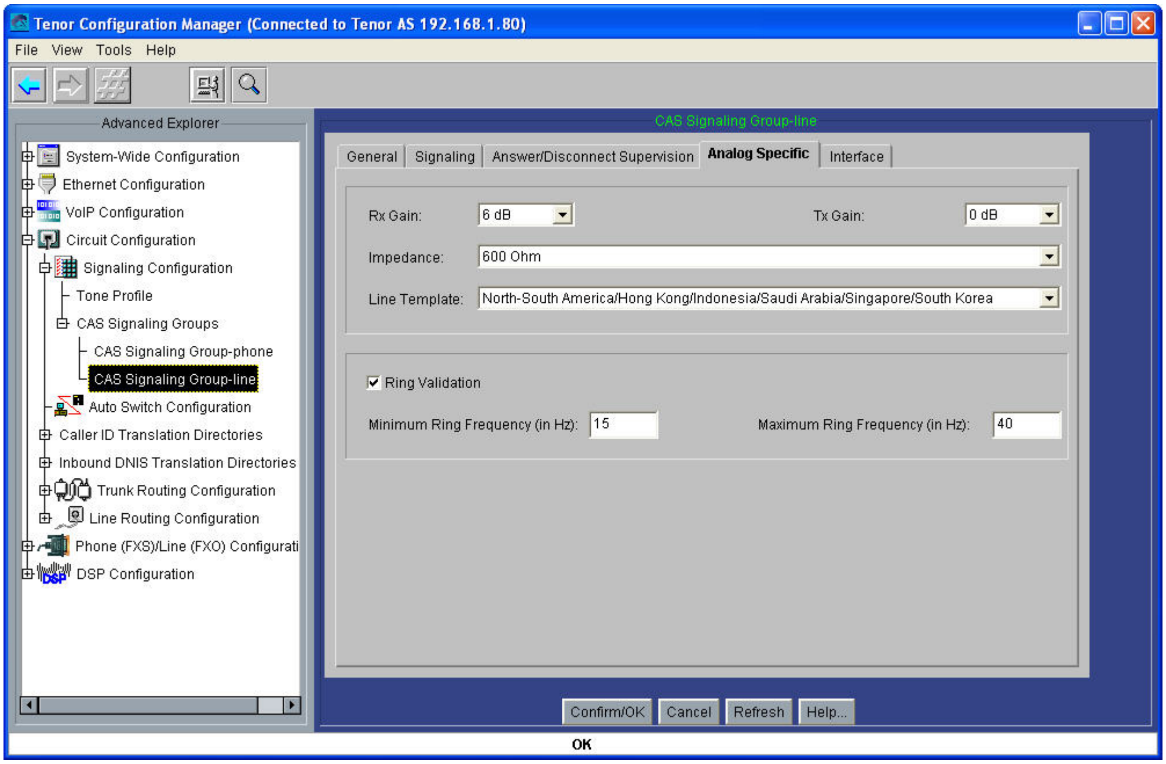
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>26.</td><td>

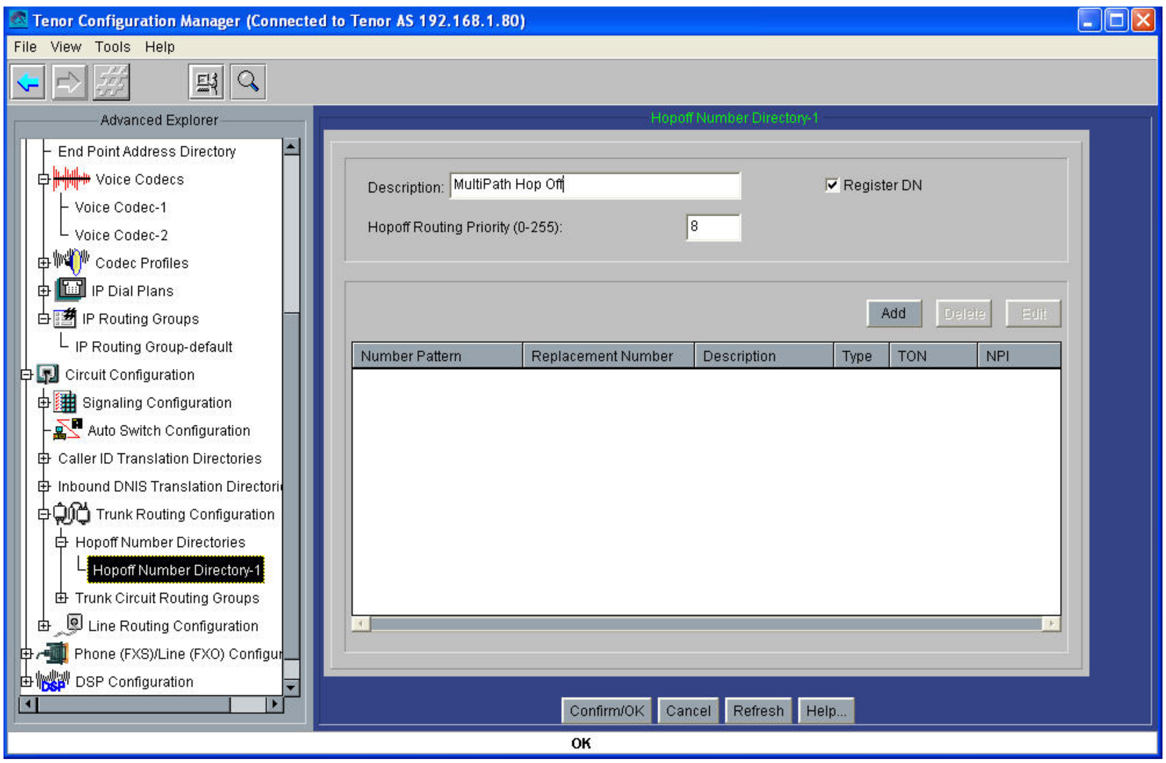
Configure the CAS Signaling parameters to be used for the analog phones connected to the gateway. In general, all default values can be used except for the Rx Gain and Tx Gain values. From the **Advanced Explorer** menu tree, navigate to **Circuit Configuration → Signaling Configuration → CAS Signaling Groups → CAS Signaling Group-phone**. Select the **Analog Specific** tab. From the appropriate drop-down menu, select *-6 db* for the **RX Gain** field and *0 db* for the **Tx Gain** field.

Click **Confirm/OK** and then the sunburst button on the menu bar to submit the change.



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

Step	Description
27.	Configure the CAS Signaling parameters to be used for the PSTN connected to the gateway. In general, all default values can be used except for the Rx Gain and Tx Gain values. From the **Advanced Explorer** menu tree, navigate to **Circuit Configuration → Signaling Configuration → CAS Signaling Groups → CAS Signaling Group-line**. Select the **Analog Specific** tab. From the appropriate drop-down menu, select *6 db* for the **RX Gain** field and *0 db* for the **Tx Gain** field. Click **Confirm/OK** and then the sunburst button on the menu bar to submit the change. 

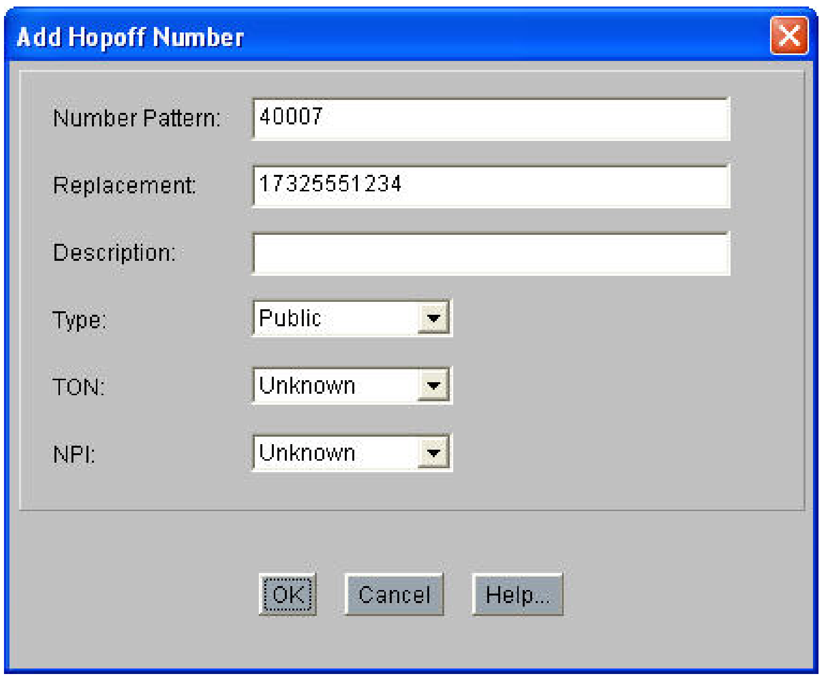
Step	Description
28.	If the data WAN fails, external calls are rerouted over the PSTN but only if the dialed digits match an entry in the Hopoff Number Directory. A replacement number can be supplied to convert any dialed string to a full PSTN routable number. For the compliance test, extensions 40007 and 40015 at the main site were mapped to replacement numbers which were the DID numbers associated with these extensions. Also, an entry was created to reroute all numbers beginning with a 1 to the PSTN during a data WAN failure. Presumably, numbers beginning with a 1 are already PSTN routable numbers. To add entries to the Hopoff directory, navigate to **Circuit Configuration → Trunk Routing Configuration → Hopoff Number Directories → Hopoff Number Directory-1** from the **Advanced Explorer** menu tree. Enter a description in the **Description** field. The default values may be used for the other fields. Click on **Add** to display the **Add Hopoff Number** pop-up window. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>29.</td><td>
In the Add Hopoff Number pop-up window, enter the following information:

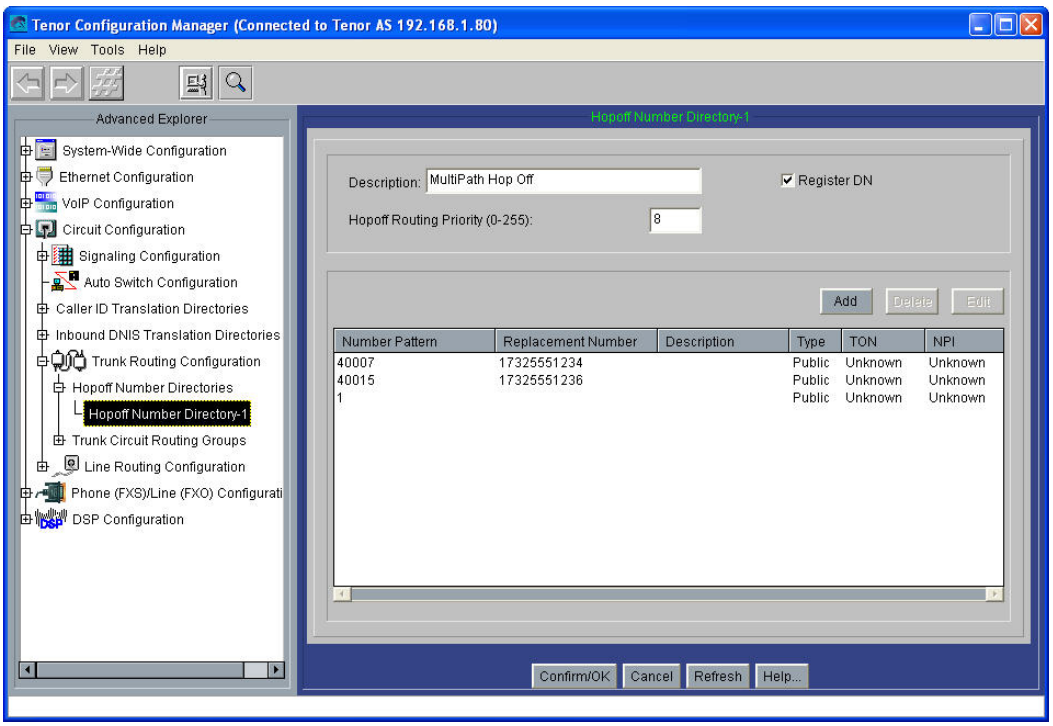
Number Pattern: A number pattern to be matched against the dialed digits of a call to determine if the call should be rerouted to the PSTN, when the data WAN is down.
Replacement: The PSTN routable number that will replace the dialed digits of the call. If no number is provided, the dialed digits are used to place the call.

The example below shows the entry that allows extension 40007 at the main site to still be reached when the data WAN fails. The call is allowed to be rerouted across the PSTN using the DID number 17325551234 associated with this extension.

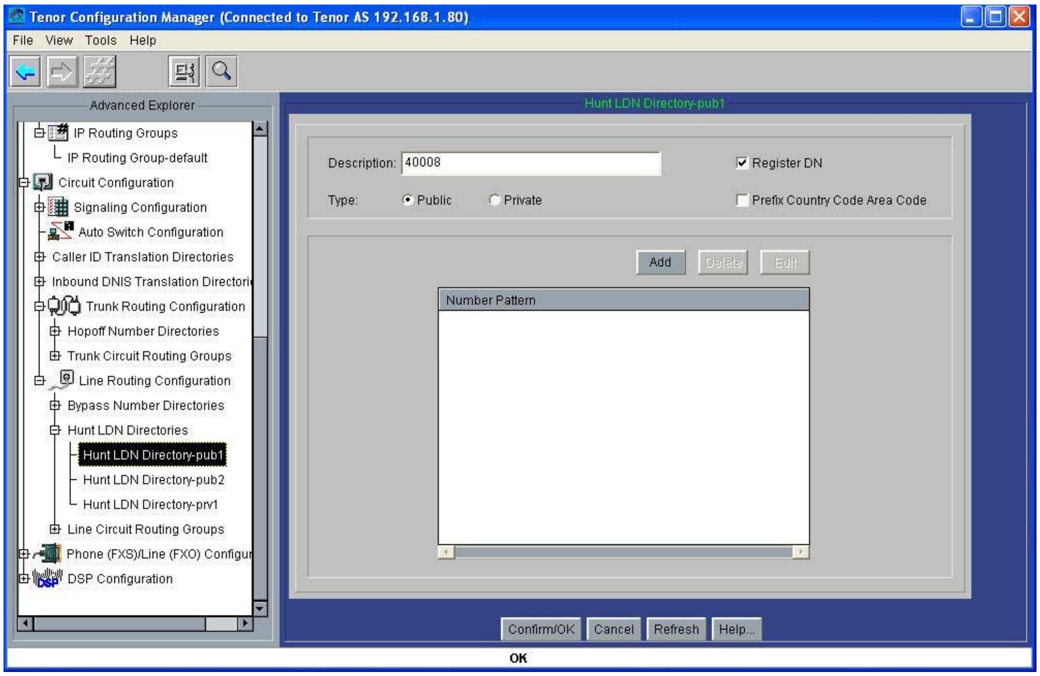
The default values may be used for the other fields. Click OK to continue.



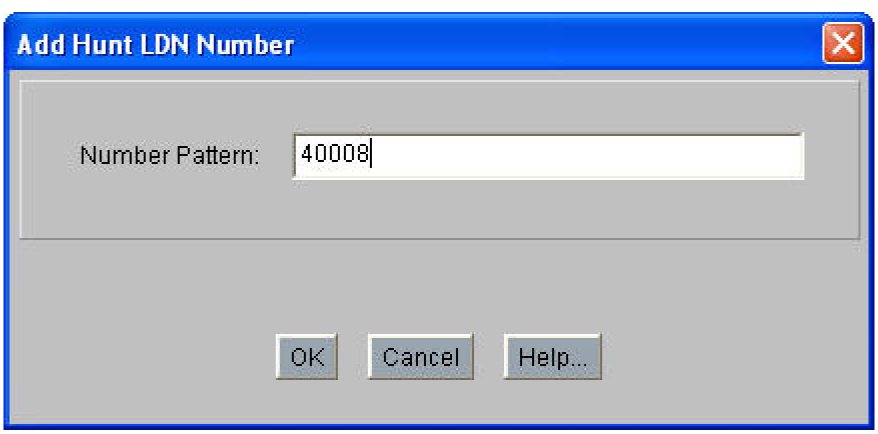
</td></tr>
</table>

Step	Description
30.	Repeat Steps 28 - 29 for any remaining number patterns that are to be rerouted. For the compliance test, two more number patterns were added as shown: ▪ **Number Pattern**: ***40015*** Matches another extension at the main site ▪ **Replacement**: ***17325551236*** DID number for extension 40015 ▪ **Number Pattern**: ***1*** Matches any dialed string beginning with a 1. ▪ **Replacement**: Leave this field blank, so no replacement is done. Click **Confirm/OK**, and then the sunburst button on the menu bar to submit the changes. The example below shows the values used for the compliance test. 

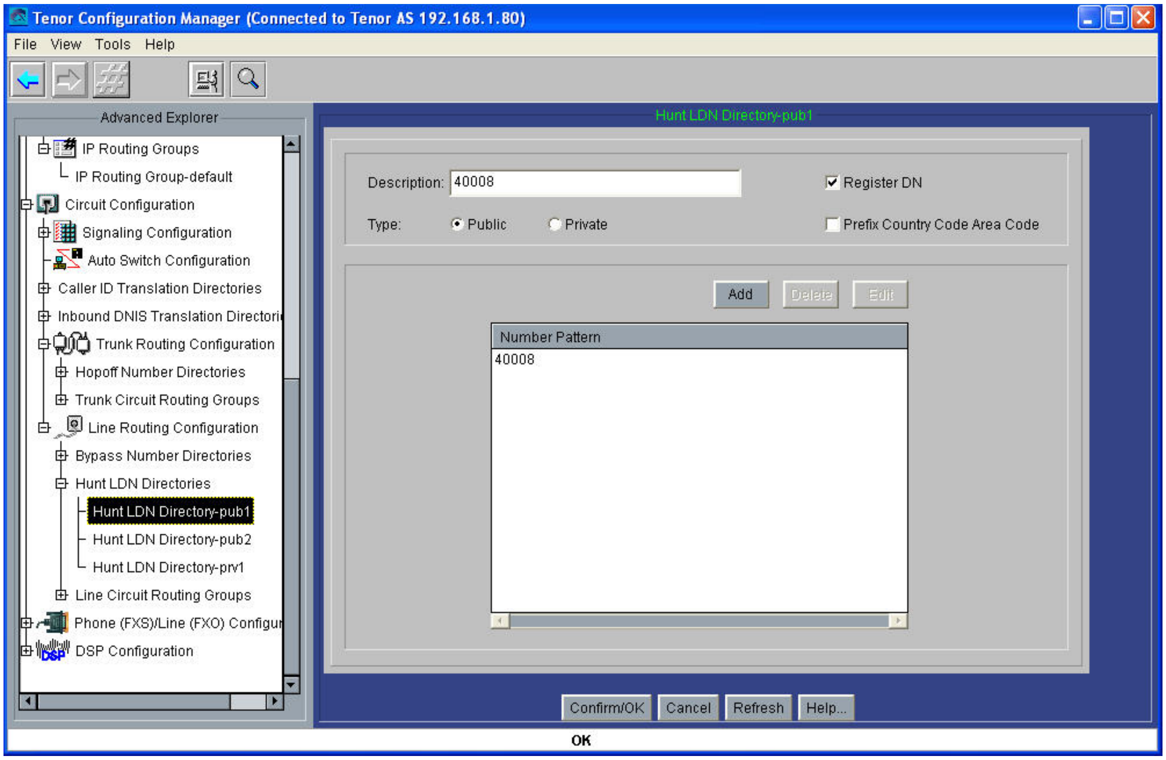
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>31.</td><td>Multiple numbers may be associated with a physical port and are contained in a directory called the Hunt LDN Directory. The association between the directory and the port will be done through the Line Routing Group in Step 37. To add numbers to the Hunt LDN Directory, navigate to Circuit Configuration → Line Routing Configuration → Hunt LDN Directories → Hunt LDN Directory-pub1 from the Advanced Explorer menu tree. Enter a Description for this directory. Click on Add to add a number to the directory.

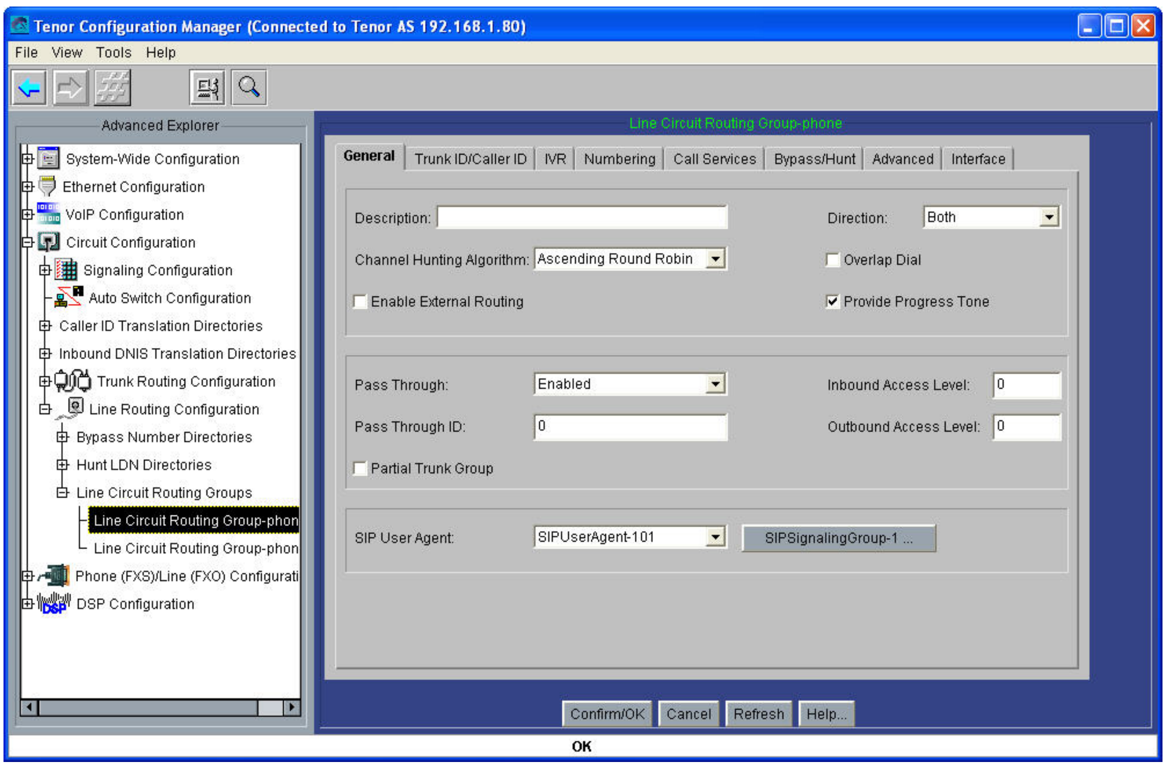


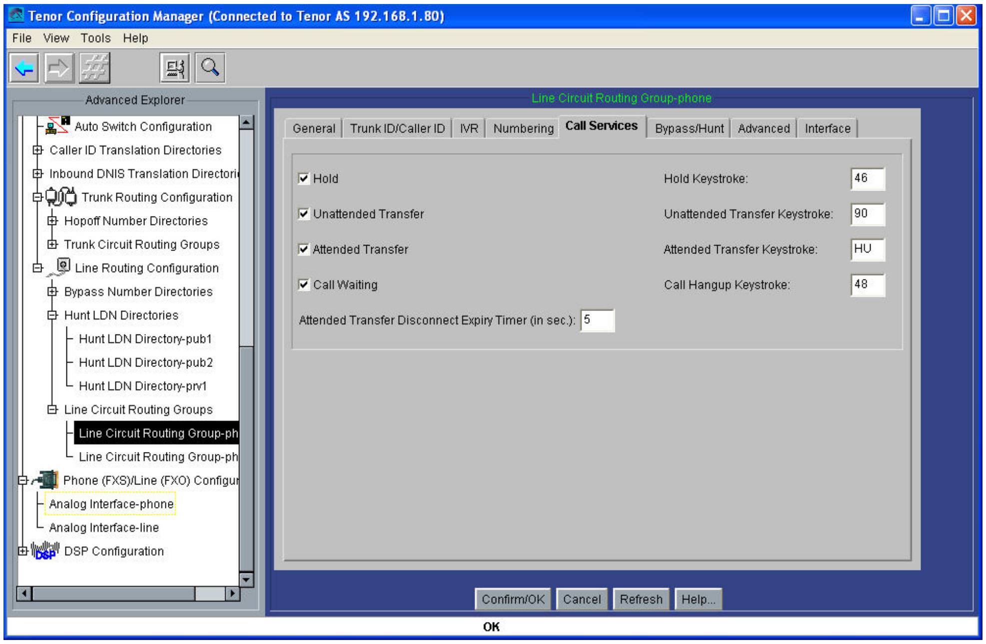
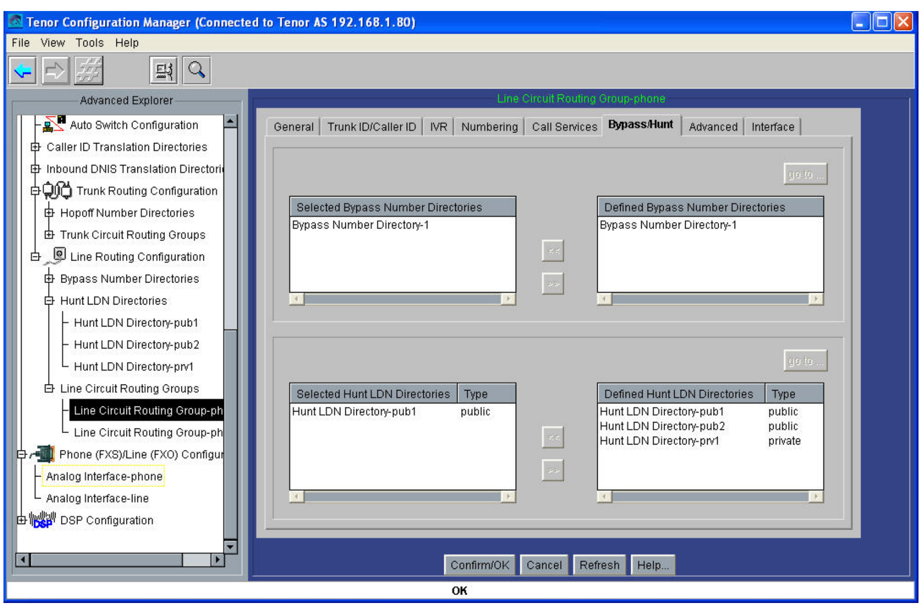
</td></tr>
<tr><td>32.</td><td>In the Add Hunt LDN Number pop-up window, enter the Number Pattern for an extension at the Branch Site. Click OK to continue.

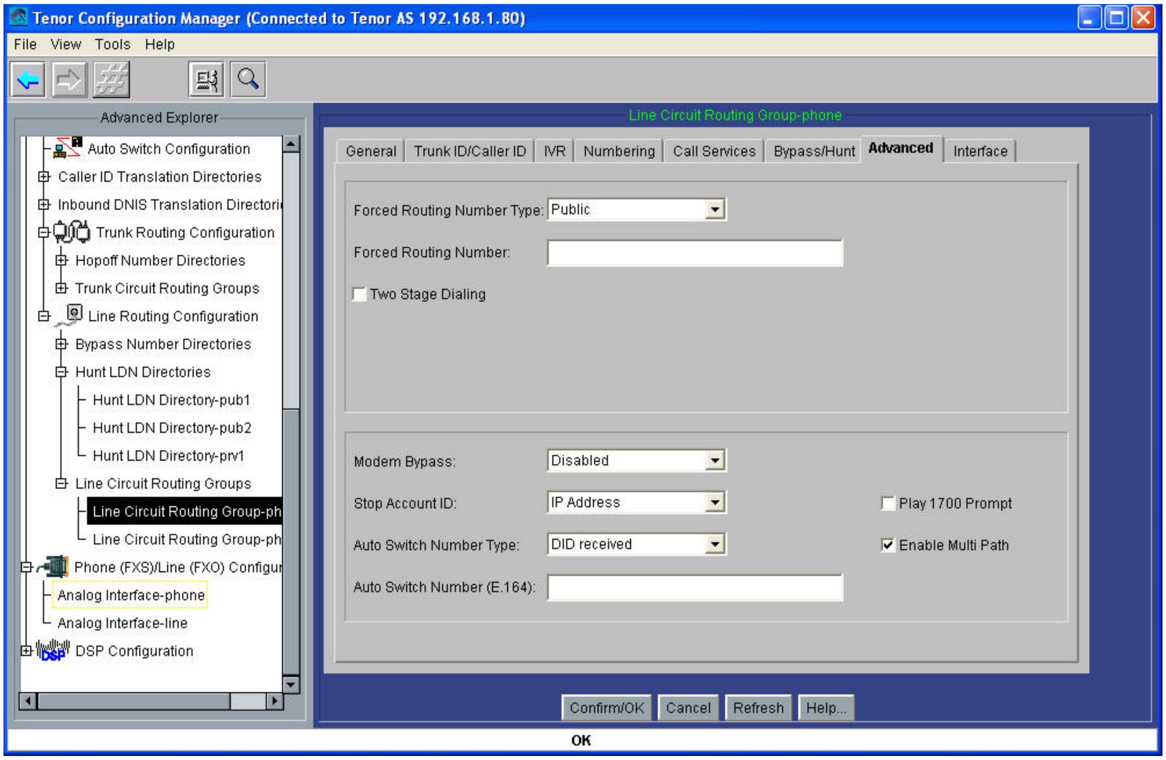


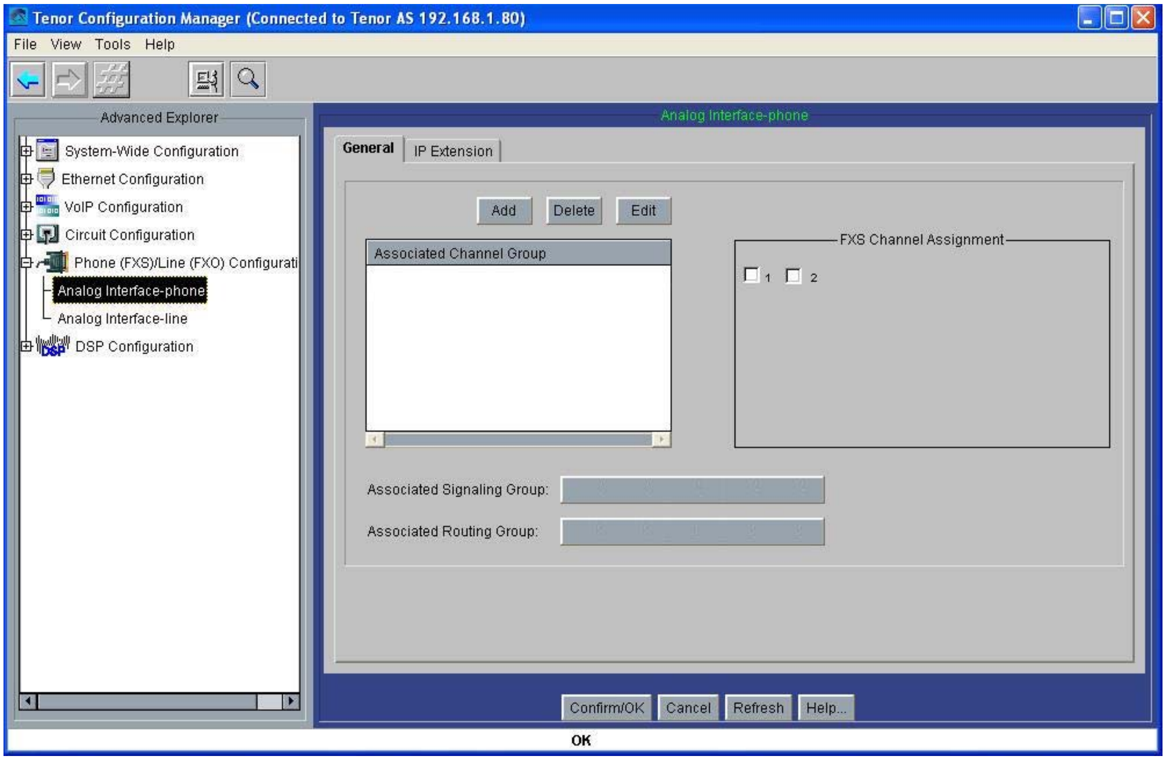
</td></tr>
</table>

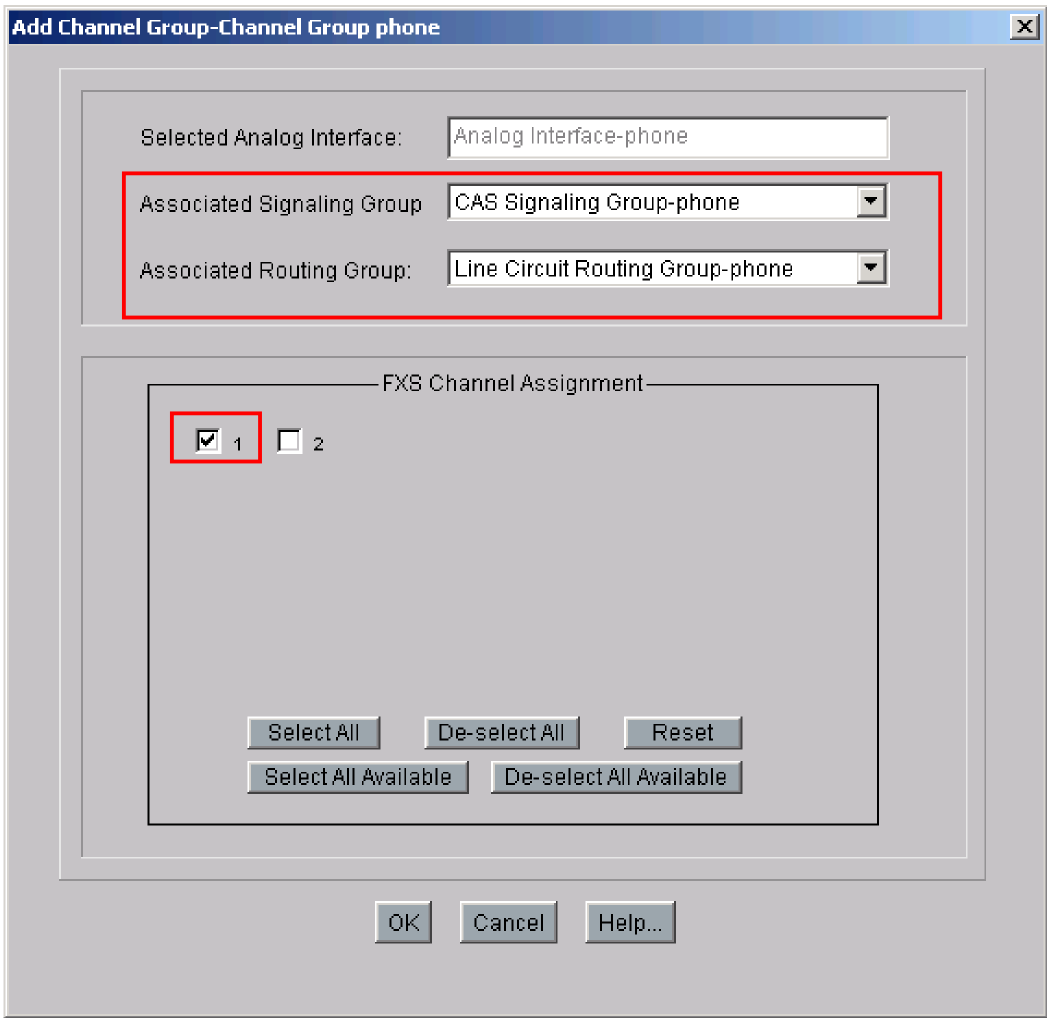
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>33.</td><td>The newly added extension is displayed in the Number Pattern list. For the compliance test, only a single number was assigned to each Hunt LDN directory and ultimately to each port. Click on Confirm/OK in the Hunt LDN Directory-pub1 panel and click on the sunburst button on the menu bar to implement the change.

</td></tr>
<tr><td>34.</td><td>Repeat Steps 31 - 33 for the second analog extension (40009) used in the compliance test. Use Hunt LDN Directory-pub2 for this extension.</td></tr>
</table>

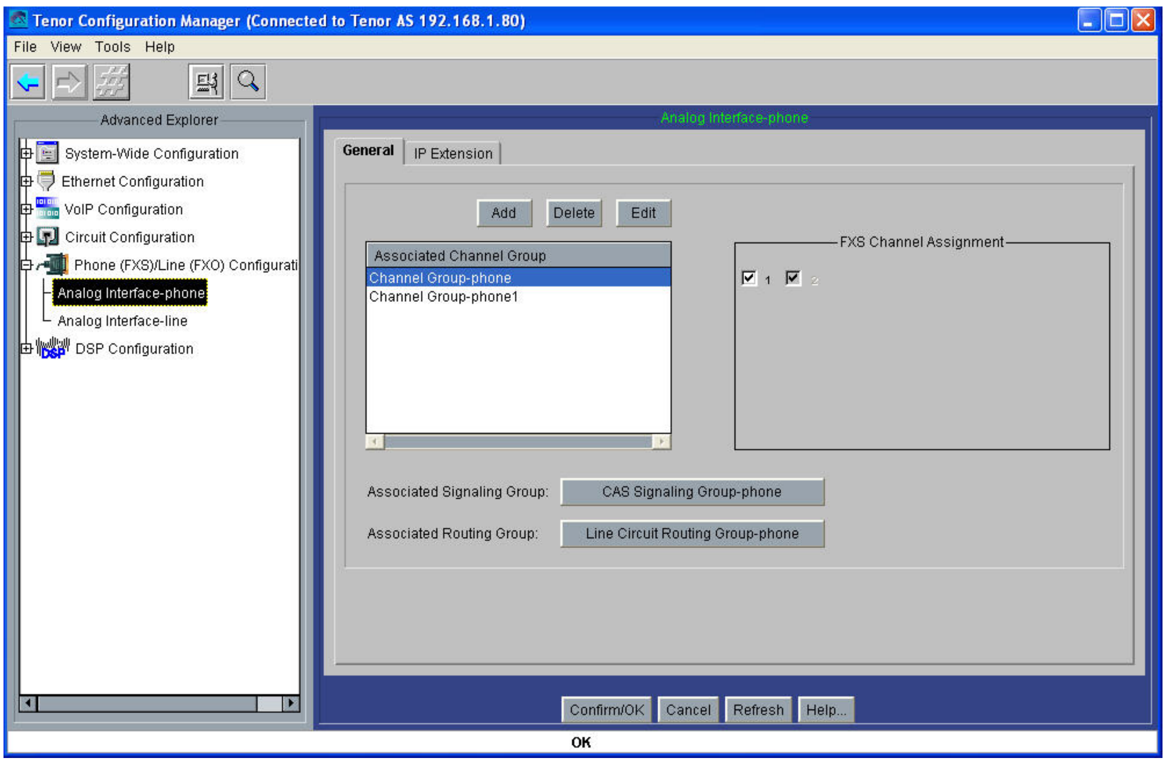
Step	Description
35.	Define the line routing parameters for each physical port. The example below shows the values for port 1 (x40008). The association between these parameters and port 1 will be done in a later step. From the **Advanced Explorer** menu tree, navigate to **Circuit Configuration → Line Routing Configuration → Line Circuit Routing Groups → Line Circuit Routing Group-phone**. Select the **General** tab in the **Line Circuit Routing Group-phone** panel on the right. From the **Pass Through** drop-down menu, select ***Enabled***. From the **SIP User Agent** drop-down menu, select ***SIPUserAgent-101***. This **SIP User Agent** name was automatically assigned by the system in Section 5, Step 14. Select the **Call Services** tab. 

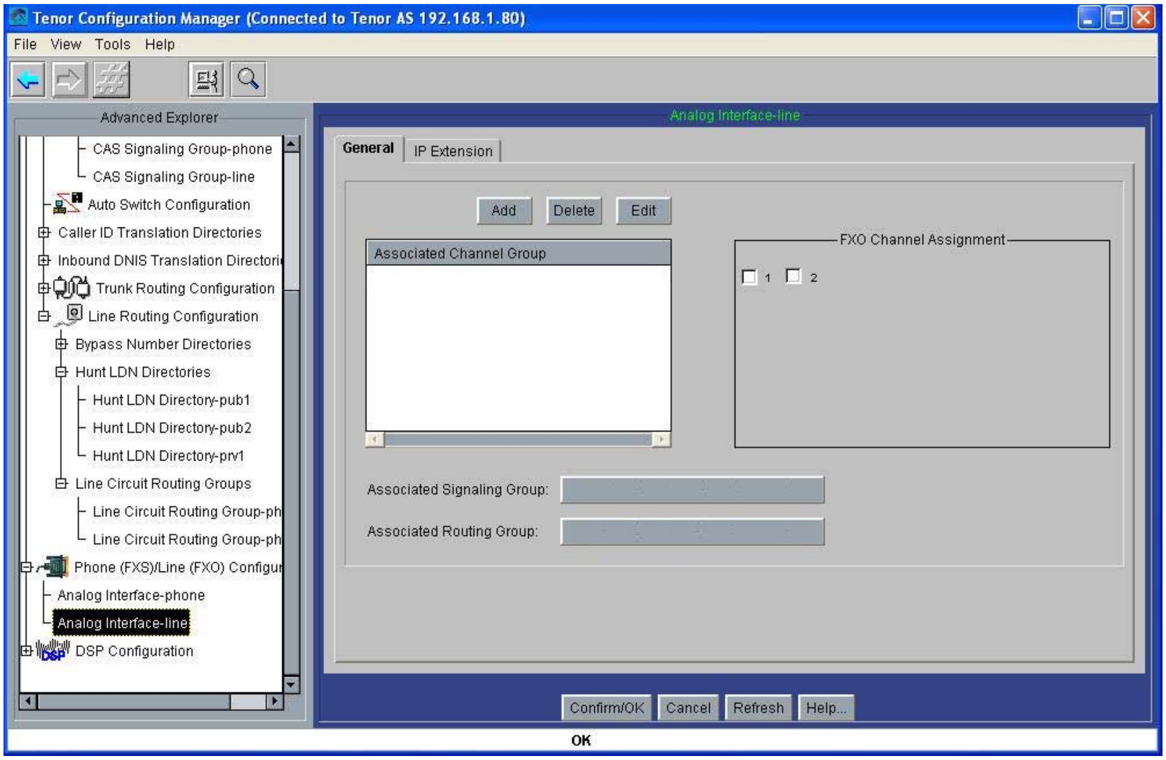
Step	Description
36.	In the **Call Services** tab, verify the appropriate services are enabled for the analog phone. To enable a service, check the check box next to the service name. The test configuration had **Hold**, **Unattended Transfer**, **Attended Transfer**, and **Call Waiting** checked. Next, select the **ByPass/Hunt** tab. 
37.	In the **Bypass/Hunt** tab, select the **Hunt LDN Directory-pub1** field in the lower right window, this will make active the << button. Click on the **<<** button to move **Hunt LDN Directory-pub1** to the lower left window. This will make an association between this Line Circuit Routing Group and **Hunt LDN Directory-pub1.** Next**,** select the **Advanced** tab. 

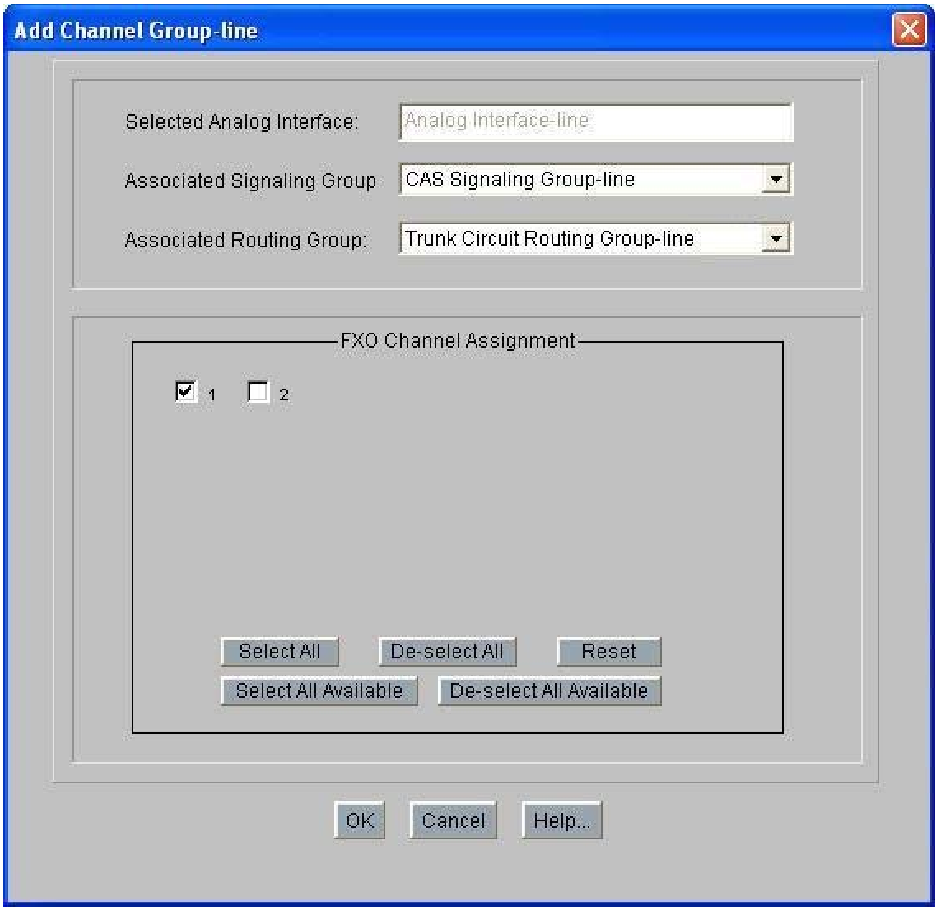
Step	Description
38.	In the **Advanced** tab, check the radio button for **Enable Multi Path**. This will allow the routing of calls to the PSTN in the case of a data WAN failure. Click **Confirm/OK** and then the sunburst button on the menu bar to implement the change. 
39.	Repeat Steps 35 – 38 for the second Line Circuit Routing Group (**Line Circuit Routing Group-phone1**). All configuration is the same as before with the exception of the following: ▪ Use ***SIPUserAgent-102*** for the **SIP User Agent** in Step 35. ▪ Select ***Hunt LDN Directory-pub2*** for the **Selected Hunt LDN Directories** in Step 37.

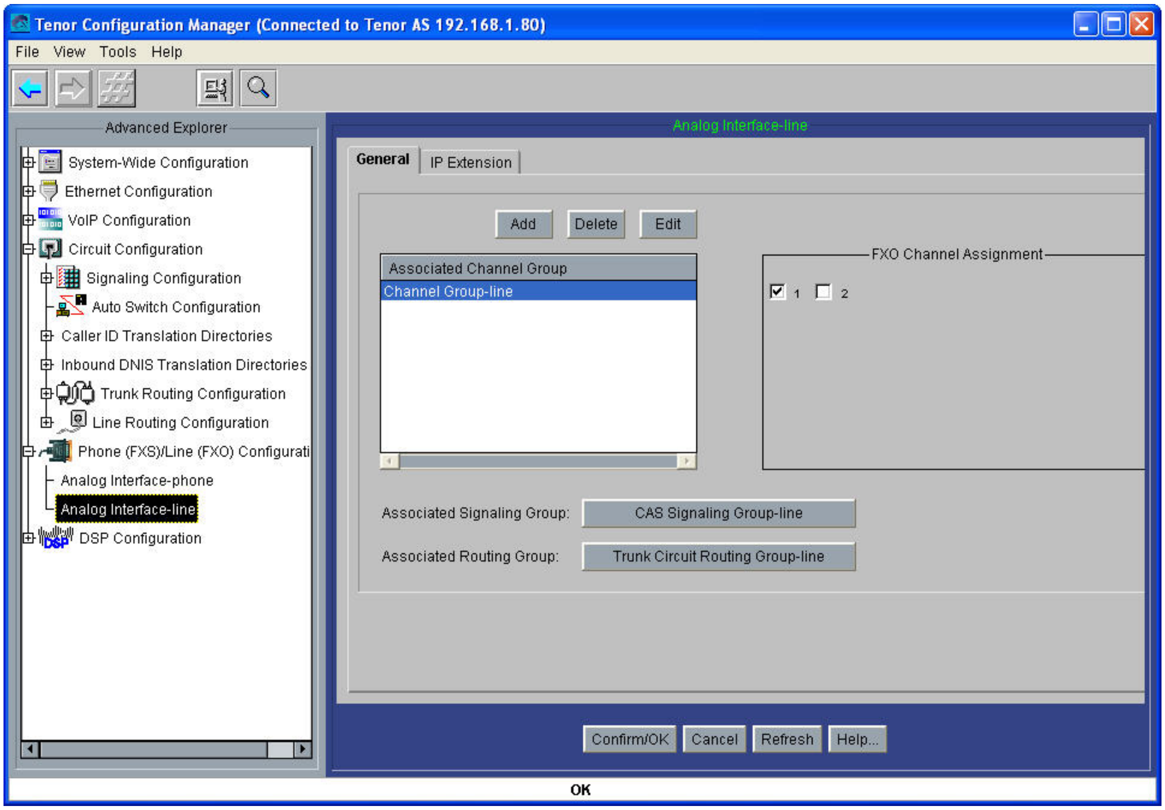
Step	Description
40.	Configure the physical ports for the analog phones. From the **Advanced Explorer** menu tree, navigate to **Phone (FXS)/Line (FXO) Configuration →Analog Interface-phone.** In the **Analog Interface-phone** panel on the right, click **Add**. 
41.	In the pop-up window that appears, enter a description for the **Channel Group** and click **OK** to continue. 

Step	Description
42.	In the **Add Channel Group-Channel Group phone** pop-up window, configure the following information. This configuration will associate physical FXS port 1 with this channel group, as well as a particular signaling and routing group. **Associated Signaling Group:** *CAS Signaling Group-phone* **Associated Routing Group:** *Line Circuit Routing Group-phone* **FXS Channel Assignment:** check the radio button for **1** Click **OK** to complete. 

Step	Description
43.	Repeat Steps 40 - 42, creating a second channel group for physical FSX port 2. Specify a descriptive name for the Channel Group name and enter the following information on the **Add Channel Group** window in Step 42. **Associated Signaling Group:** ***CAS Signaling Group-phone*** **Associated Routing Group:** ***Line Circuit Routing Group-phone1*** **FXS Channel Assignment:** check radio button for **2** The example below shows the Analog Interface-phone panel after both phones/fax have been configured. There is no difference in the configuration of the port whether it is used for an analog telephone or fax machine. Click **Confirm/OK** and then the sunburst button on the menu bar to submit the changes. 

Step	Description
44.	Configure the physical port for the POTS line. From the **Advanced Explorer** menu tree, navigate to **Phone (FXS)/Line (FXO) Configuration → Analog Interface-line**. Click **Add** under the **Analog Interface-line** panel on the right. 

Step	Description
45.	In the **Add Channel Group-line** pop-up window, configure the following information. This configuration will associate physical FXO port 1 with this channel group, as well as a particular signaling and routing group. **Associated Signaling Group:** ***CAS Signaling Group-line*** **Associated Routing Group:** ***Trunk Circuit Routing Group-line*** **FXO Channel Assignment:** ***1*** (The port where the POTS line is connected) Click **OK** to continue. 

Step	Description
46.	In the **Analog Interface-line** panel, click **Confirm/OK,** and then the sunburst button on the menu bar to implement the change. The example below shows the Analog Interface-line panel after the POTS line has been configured. 

6. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability between the Quintum Tenor AS, Avaya Communication Manager and Avaya SIP Enablement Services (SES). 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 Tenor at the branch site using various codec settings and exercising common PBX features. This testing included the analog telephones, Avaya SIP telephones, and generic SIP telephones. The SIP telephones at the branch site use the IP address of the Tenor as the call server/outbound proxy. The calls were made to/from the main site, the PSTN and within the branch site. The same test cases, where applicable, were repeated with a simulated data WAN outage.

6.2. Test Results

The Quintum Tenor successfully passed compliance testing. The following features and functionality were verified during the interoperability compliance test. Each feature was tested with an analog telephone, Avaya SIP telephone and generic SIP telephone, where applicable, unless stated otherwise below:

- Calls to/from the main site
- Calls to/from the PSTN
- Failover to the POTS line to complete calls to the main site and PSTN when a simulated data WAN failure was introduced (multipath switching). Incoming calls to the branch are limited to the single POTS number assigned to the branch.
- Intra-branch calls
- Intra-branch calls with a simulated data WAN failure (local survivability)
- G.711mu and G.729AB codec support
- Proper recognition of DTMF transmissions
- Local device support for Hold, Transfer, and Call Waiting
- Conferencing (SIP phones only)
- T.38 fax support (Tenor analog ports only)
- Proper system recovery after a Tenor restart

The following features and functionality were also verified during the interoperability compliance test but these features are only applicable when the data WAN is functioning. This is because these features require support from Avaya Communication Manager and/or Avaya SES.

- Proper operation of voicemail with message waiting indicators (MWI). For the analog phones, MWI was provided via stutter dial tone.
- Call Forwarding provided by Avaya Communication Manager or locally by the SIP telephones is not supported when the data WAN has failed.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions such as Call Park, Call Pickup, Automatic Redial and Send All Calls. For more details, please refer to [6].

The following observations were made during the compliance test:

- For proper operation of conferencing during a data WAN outage, the preferred codec configured on the Tenor must be the same as the preferred codec used by the SIP telephones.
- During a data WAN outage, a different DiffServ value is transmitted in the RTP packets than the value configured on the Tenor.
- During a data WAN outage, several seconds of delay occurs between dialing and ringback.
- During a data WAN outage, several seconds of delay occurs before voice cut-through following a transfer operation.

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.
- 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 behind the Tenor, both analog and SIP, are registered with the Avaya SES.
- Verify that calls can be placed to/from the analog and SIP endpoints behind the Tenor.
- Verify that calls can be placed from the analog and SIP endpoints behind the Tenor when a simulated data WAN failure is introduced.

8. Support

For technical support on the Quintum Tenor AS in the US, contact Quintum toll-free at (877) 435-7553 and from outside the US, call (732) 460-9399. Support can also be obtained from www.quintum.com.

9. Conclusion

These Application Notes describe the procedures required to configure the Quintum Tenor AS VoIP MultiPath Switch with a B2BUA in support of SIP endpoints and local survivability 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] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005 Release 3.0
[4] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005
[5] *Installing and Administering SIP Enablement Services R3.1*, Doc# 03-600768, Issue 1.5, February 2006
[6] *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
[7] *Tenor AS VoIP MultiPath/Gateway Switch Product Guide*, P/N 480-0059-00-13
[8] *Tenor Configuration Manager/Tenor Monitor Product Guide.* P/N 480-0028

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

Product documentation for Quintum Tenor AS VoIP MultiPath Switch products may be found at http://www.quintum.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 Developer*Connection* Program at devconnect@avaya.com.