Configuring the NexTone Multiprotocol Session Exchange iServer to Provide Connectivity between a Public Network and the Avaya Meeting Exchange S6800 Conferencing Server via Avaya SIP Enablement Services - Issue 1.0

Abstract

These Application Notes describe a compliance-tested solution comprised of the Avaya Meeting Exchange S6800 Conferencing Server, Avaya SIP Enablement Services and the NexTone Multiprotocol Session Exchange (MSX) iServer. The NexTone Multiprotocol Session Exchange (MSX) iServer is utilized to manage both signaling (SIP) and media (Audio-RTP) between a public network and a private network containing Avaya SIP Enablement Services and the Avaya Meeting Exchange S6800 Conferencing Server. Avaya SIP Enablement Services is configured as a SIP redirect server and routes calls between the Avaya Meeting Exchange S6800 Conferencing Server and the public network. This configuration provides a rich set of conferencing options available on the Avaya Meeting Exchange S6800 Conferencing Server to participants associated with a public network.

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 a compliance-tested solution comprised of the Avaya Meeting Exchange S6800 Conferencing Server, Avaya SIP Enablement Services and the NexTone Multiprotocol Session Exchange (MSX) iServer. The NexTone Multiprotocol Session Exchange (MSX) iServer is utilized to manage both signaling (SIP) and media (Audio-RTP) between a public network and a private network containing Avaya SIP Enablement Services and the Avaya Meeting Exchange S6800 Conferencing Server. Avaya SIP Enablement Services is configured as a SIP redirect server and routes calls between the Avaya Meeting Exchange S6800 Conferencing Server and the public network. This configuration provides a rich set of conferencing options available on the Avaya Meeting Exchange S6800 Conferencing Server to participants associated with a public network.

Figure 1 illustrates the network configuration utilized for this compliance-tested solution.

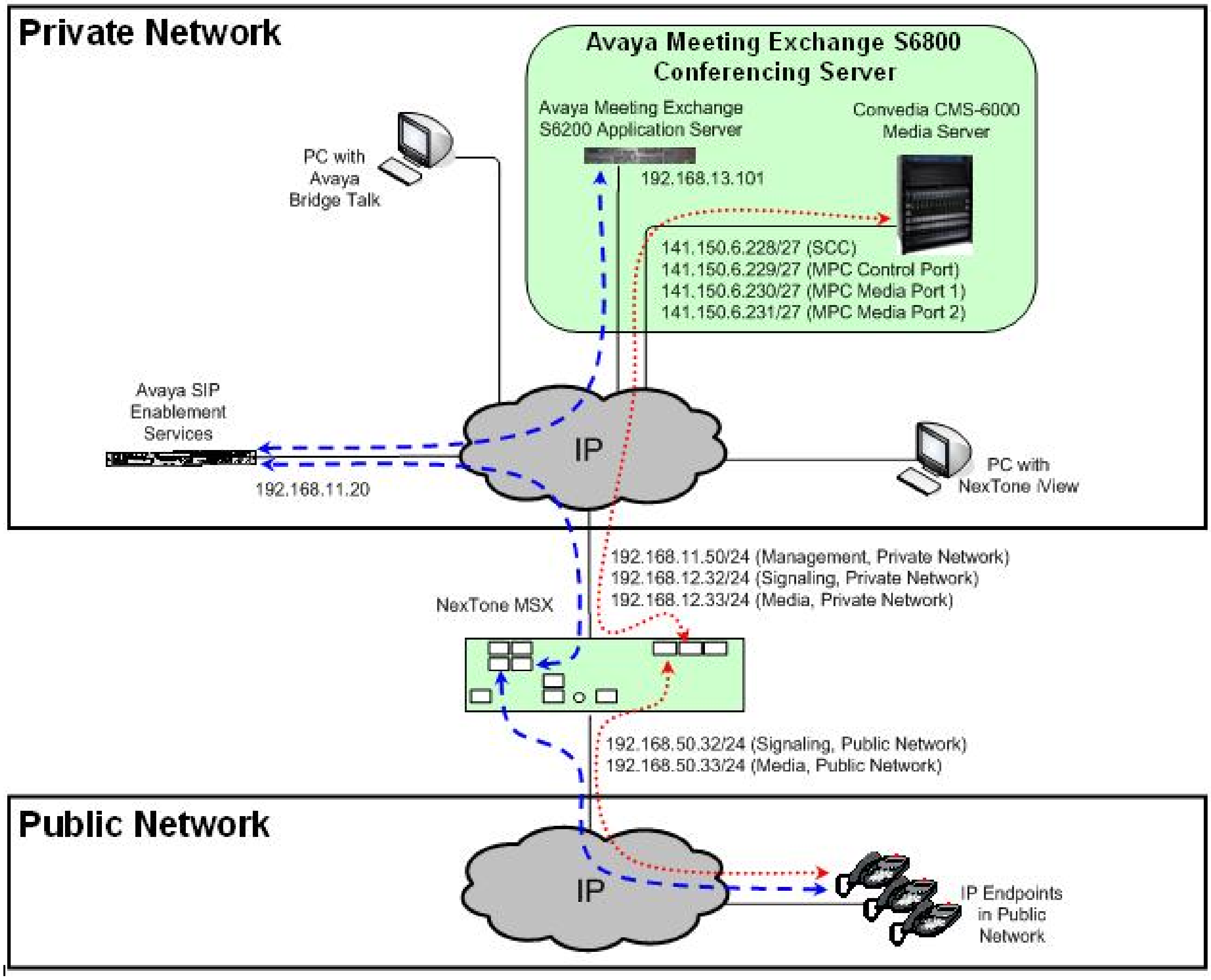


Figure 1: Network Configuration

Signaling (SIP) connectivity between the public and private networks traversed the following Path (blue dashed line).

- SIP/UDP between a public network to the NexTone MSX iServer.
- SIP/UDP between the NexTone MSX iServer and Avaya SIP Enablement Services.
- SIP/UDP between Avaya SIP Enablement Services and the Avaya Meeting Exchange S6200 Application Server.

Media (Audio-RTP) connectivity between the public and private networks traversed the following Path (red dotted line).

- RTP/UDP between a public network and the NexTone MSX iServer.
    - RTP/UDP between the NexTone MSX iServer and the Convedia CMS-6000 Media Server.

1.1. Avaya Meeting Exchange S6800 Conferencing Server

The Avaya Meeting Exchange S6800 Conferencing Server is a SIP-based voice conferencing solution that extends Avaya's conferencing applications including reservation-less, attended, event, mobile to support various IP network implementations. The following capabilities are supported by the Avaya Meeting Exchange S6800 Conferencing Server:

- RFC 2833 DTMF support.
- In-band DTMF support.
- Up to 2016-user and 115-operator conferences.
- Support for up to four digitally recorded music sources.
- Support for one recorded music channel and up to four connection based (FDAPI) music channels.
- Any combination of G.711 a-law or u-law, G.729, G723, G726-16, G726-24, G726-32, or G726-40 codecs.

Figure 2 illustrates the configuration for the Avaya Meeting Exchange S6800 Conferencing Server, which is composed of the following:

- Up to four Avaya Meeting Exchange S6200 server(s) configured as Application Server(s), e.g., call signaling processes are managed by the S6200(s). For these Application Notes, one Avaya Meeting Exchange S6200 server is utilized as an Application Server.
- A Convedia CMS-6000 Media Server, containing the following cards:
    - One Media Processor Card (MPC).
    - One Shelf Control Card (SCC).
- Signaling between the Avaya Meeting Exchange Application Server(s) and the Convedia CMS-6000 Media Server is SIP.

Figure 2: Avaya Meeting Exchange S6800 Conferencing Server

1.2. Avaya SIP Enablement Services

Avaya SIP Enablement Services can perform proxy, registration and redirection functions associated with SIP applications. For these Application Notes, Avaya SIP Enablement Services is configured as A SIP redirect server.

1.3. NexTone MSX iServer

The NexTone MSX iServer is composed of a Multi-protocol Session Controller (MSC) and a Multi-protocol Signaling Switch (MSW). The NexTone MSX iServer (MSC and MSW) is a server that facilitates all calls initiated in a VoIP network by authenticating and routing the calls between IP endpoints. This server is the repository for all IP addresses and phone numbers of all endpoints registered on it. Administrative access is via TCP/IP network connection. The iServer is also a repository of hop-off points or gateways to other private or public telephone networks.

Figure 3 illustrated the back panel of the NexTone MSX iServer.

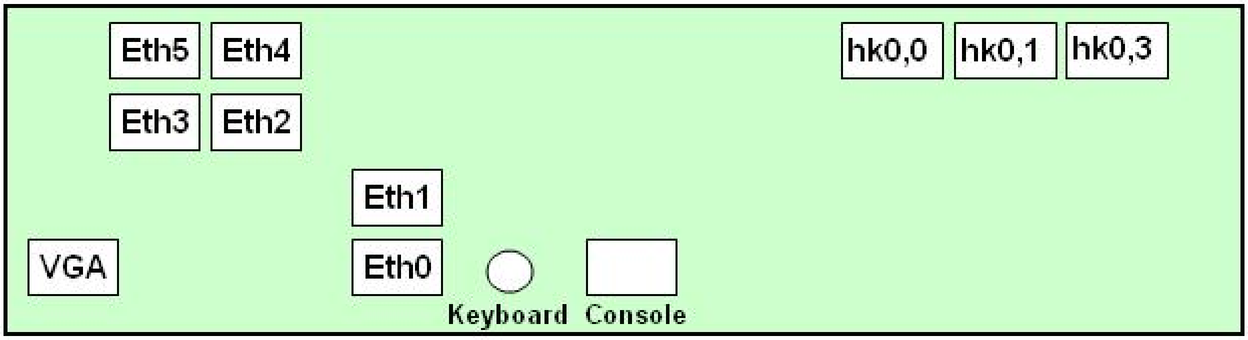


Figure 3: NexTone MSX iServer Hardware Configuration

The NexTone MSX iServer uses CAT6 for the Ethernet (Eth) and GigE for the HotKnife (HK) connections. The Ethernet connections are used for signaling and management. The HotKnife connections are used for media. The following network connections were configured on the NexTone MSX iServer for these Application Notes.

- Eth0 – Connected to the management LAN (CAT6).
- Eth2 – Signaling interface connected to the private network (CAT6).
- Eth3 – Signaling interface connected to a public network (CAT6).
- Eth5 – Console connection to a services PC to provide initial configuration.
- hk0,0 – Media interface connected to a public network (GigE Fiber).
- hk0,1 – Media interface connected to the private network (GigE fiber).

2. Equipment and Software Validated

The following equipment and software versions were used for the sample configuration provided in these Application Notes.

Equipment	Software
Avaya Meeting Exchange S6800 Conferencing Server	
• Avaya Meeting Exchange S6200 Application Server	
o Software version	40103_00_01
o IPCB build version	mx7_1.3.00-86
• Convedia™ CMS-6000 Media Server	
o SCC2 (slot 1)	4.8.0.16
o MPC2 (slot 2)	4.8.0.16
Avaya Bridge Talk	4.1.01b
Avaya SIP Enablement Services	3.1.1 (SES-3.1.1.0-114.0)
NexTone MSX iServer	
• Configuration Server	v4.0c3-18
• Cmd Execution Server	v4.0.c3-18
• GIS Directory Server	v4.0.c3-18
• Replication Server	v4.0.c3-18
NexTone iView	v4.1c5

Table 1: Hardware and Software Versions

3. Configure the Avaya Meeting Exchange S6800 Conferencing Server

This section describes the steps for configuring the Avaya Meeting Exchange S6800 Conferencing Server to interoperate with a public network via Avaya SIP Enablement Services and the NexTone MSX iServer (see **Section 1**, **Figure 1**).

3.1. Configure the Avaya Meeting Exchange S6200 Application Server

The following steps describe the administrative procedures for configuring the Avaya Meeting Exchange S6200 Application Server to originate/terminate calls utilizing the Convedia CMS-6000 Media Server.

Step	**Description**
3.1	Log in to the Avaya Meeting Exchange S6200 Application Server console to access the Command Line Interface (CLI) with the appropriate credentials.

Step	Description
3.2	Configure settings that enable SIP connectivity between the Avaya Meeting Exchange S6200 Application Server and other SIP User Agent(s) by editing the **system.cfg** file as follows: • cd to **/usr/ipcb/config** • Edit the **system.cfg** file with a text editor, e.g., vi. • Add a line to identify the IP address of the Avaya Meeting Exchange S6200 Application Server (as defined in the /etc/hosts file): o **IPAddress=192.168.13.101** • Add a line to populate the From Header Field in SIP INVITE messages from the Avaya Meeting Exchange S6200 Application Server: o **MyListener=sip:001s6800@192.168.13.101** ***Note****: The user field* ***001s6800****, defined for this SIP URI must conform to the RFC 3261. For consistency, it is selected to match the user field provisioned for the* ***respContact*** *entry (****see below****).* • Add a line to provide SIP User Agent(s) a Contact address to use for Acknowledging SIP messages from the Avaya Meeting Exchange S6200 Application Server: o **respContact=<sip:001s6800@192.168.13.101:5060;transport=udp>** ***Note****: The user field* ***001s6800****, defined for this SIP URI must conform to the RFC 3261 and is selected to uniquely identify this server. E.g., the user field* ***001s6800*** *will be inserted in the From header field of SIP INVITE messages from this Avaya Meeting Exchange S6200 Application Server (see* ***Step 7.11****). The intention is for* ***001s6800*** *to display on a participant's User Agent Client (UAC) when Dial-Out procedures from the Avaya Meeting Exchange S6200 Application Server are invoked. This allows end-user's to identify a call from this server.* • Add the following lines to set the Min-SE timer to **1800** seconds in SIP INVITE messages from the Avaya Meeting Exchange S6200 Application Server: o **sessionRefreshTimerValue= 1800** o **minSETimerValue= 1800** ***Note****: The values for the* ***sessionRefreshTimerValue*** *and the* ***minSETimerValue*** *are defined in seconds and should be provisioned to be greater than or equal to the value used by SIP User Agent(s) connecting to the Avaya Meeting Exchange S6200 Application Server, e.g., the SIP User Agent on the public network. This setting is necessary to enable Dial-Out from the Avaya Meeting Exchange S6200 Application Server to the public network via Avaya SIP Enablement Services and the NexTone MSX iServer.*

Step	Description
3.3	To associate incoming calls to the Avaya Meeting Exchange S6200 Application Server with different call flows, edit the **UriToTelnum.tab** file to extract both Automatic Number Identification (ANI) and Direct Inward Dial (DID, also known as DDI in Europe) values as follows: • cd to **/usr/ipcb/config** • Edit the **UriToTelnum.tab** file with a text editor, e.g., vi. • Add a line to match the pattern of the To header field in SIP INVITE messages from the public network to the Avaya Meeting Exchange S6200 Application Server. If a match occurs, the DID is extracted from the To header field and the ANI is extracted from the From header field: ○ **"*<sip:*@*" $2** Where the pattern **"*<sip:*@*"** matches: ▪ To: **<sip:556@192.168.50.32:5060>** and **$2** utilizes **556** (the variable contained in the second *****) as the DID value for the call. *__Note__: The IP address (__192.168.50.32__) in the To header field is the IP address defined for the public signaling interface on the NexTone MSX (see __Step 5.49__).* ▪ From: **<sip:56014@192.168.12.32>** and **$2** utilizes **56014** (the variable contained in the second *****) as the ANI for the call (see **Step 7.9**). *__Note__: The IP address (__192.168.12.32__) in the From header field is the IP address defined for the private signaling interface on the NexTone MSX (see __Step 5.50__).* • Enable an undefined caller to receive a prompt for operator assistance by administering for the condition of an unmatched SIP INVITE message by adding a wildcard entry as the last line in this file: ○ *** $0** *__Note__: Entries in this file are read sequentially, therefore, the line __* $0__ must be the last line in the file. Otherwise, all calls to the Avaya Meeting Exchange S6200 Application Server would match the wildcard and thus receive a prompt for operator assistance.*

Step	Description
3.4	To enable Dial-Out from the Avaya Meeting Exchange S6200 Application Server to the public network via Avaya SIP Enablement Services and the NexTone MSX iServer, edit the **telnumToUri.tab** file as follows: • cd to **/usr/ipcb/config** • Edit the **telnumToUri.tab** file with a text editor, e.g., vi. • Add a line to the file to route outbound calls from the Avaya Meeting Exchange S6200 Application Server to Avaya SIP Enablement Services: o **5???? sip:$0@192.168.11.20:5060;transport=udp** Where the pattern **5????** matches any five digit number with a leading "**5**" and routes the call to Avaya SIP Enablement Services (**192.168.11.20**) via SIP/UDP. To enable SIP connectivity utilizing UDP, the entry contains: **5060** and **transport=udp**. The Avaya Meeting Exchange S6200 Application Server will substitute **$0** with the dialed number in outgoing SIP INVITE messages, e.g., if **56011** is dialed, the Avaya Meeting Exchange S6200 Application Server will send a SIP INVITE message with: **sip:56011@192.168.11.20:5060;transport=udp** in the SIP URI and To header field (see **Step 7.11**). ***Note****: Alternatively, routing to Avaya SIP Enablement Services could have been enabled with a wildcard entry:* • ***sip:$0@192.168.11.20:5060;transport=udp*** *Where* ******* *routes any dialed digits to Avaya SIP Enablement Services (****192.168.11.20****) via SIP/UDP.*

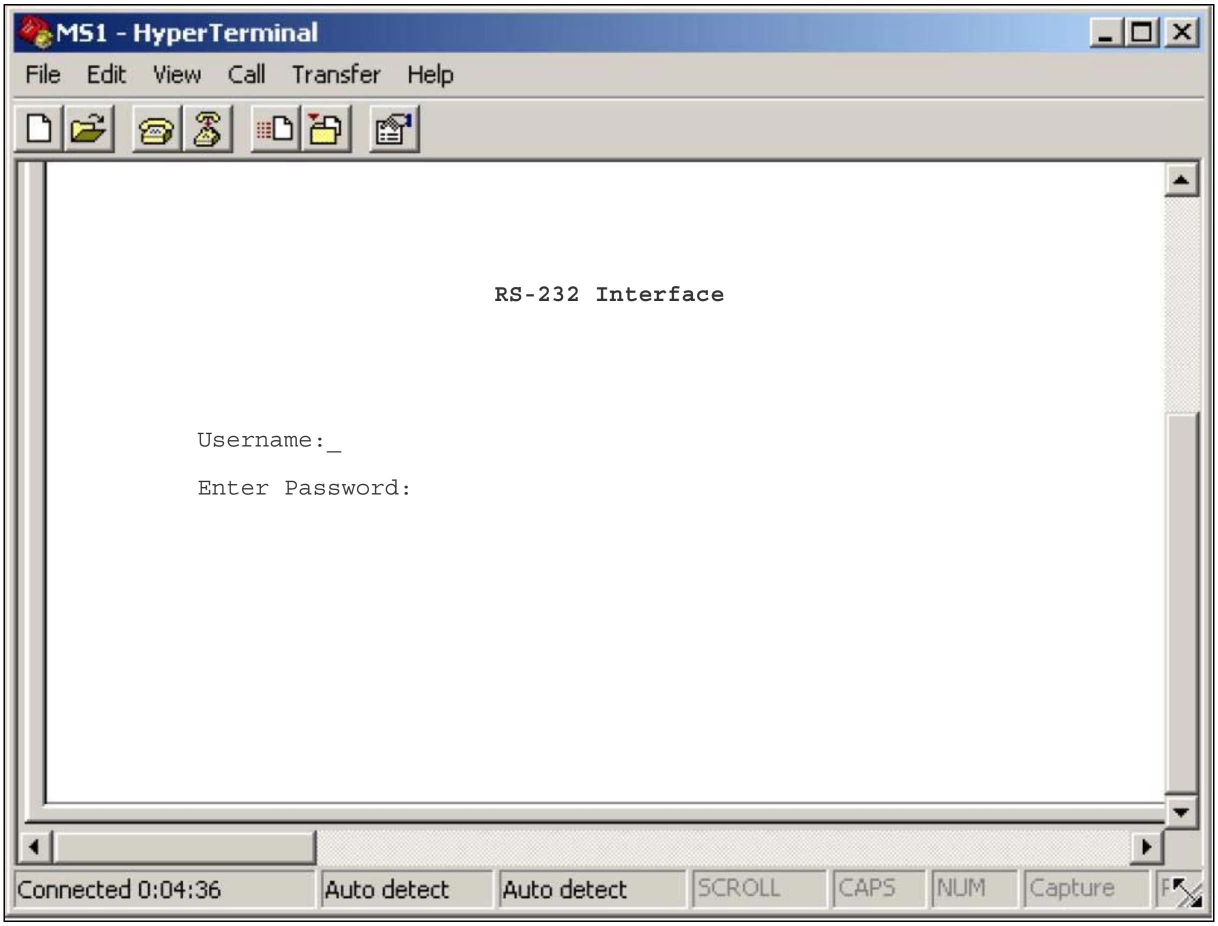
Step	Description
3.5	To configure the Avaya Meeting Exchange S6200 Application Server to utilize MPC resources on the Convedia CMS-6000 Media Server, edit the **processTable.cfg** file as follows: • cd to **/usr/ipcb/config** • Edit the **processTable.cfg** file with a text editor, e.g., vi. • Add an **ipAddress** for each corresponding **proccessName** in this file. ***Note**: The **processTable.cfg** for these Application Notes contains IP Addresses of **0.0.0.0**, where **0.0.0.0** is defined as a global IP address on the Avaya Meeting Exchange S6200 Application Server. Alternatively, the IP address of the Avaya Meeting Exchange S6200 Application Server (as defined in the /etc/hosts file) could have been entered in the **ipAddress** for each **proccessName**.*

```
# processes file, enumerates the number of processes in the network.
# will have the name of the process   Key ID and the IP address
#
# The default configuration is a single MPC board system. There are
# two commented out entries for a second and third MPC board. If more
# than 1 board is needed for the system then uncomment out the appropriate
# line(s). The last thing on the line correlates to the _* entry in the
# mediaServerInterface.cfg. For example, for the 1st mediaServer line that
# ends with a 1. The _1 entries in the mediaServerInterface.cfg are used.
#
proccessName      ipcKeyNumber   ProcessExe                     ipAddress
route                                           ProcessArgs
initipcb          110            noexecute                      0.0.0.0
bridget700        100            noexecute                      0.0.0.0
dspEvents/msDispatcher,netEvents/sipAgent
commsProcess      111            /usr/dcb/bin/serverComms       0.0.0.0
sipAgent          101            /usr/dcb/bin/sipagent          0.0.0.0
dspEvents/msDispatcher,appEvents/bridget700
msDispatcher      102            /usr/dcb/bin/msdispatcher      0.0.0.0
netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer
mediaServer       103            /usr/dcb/bin/convMS            0.0.0.0
appEvents/msDispatcher,netEvents/msDispatcher   1
#mediaServer      104            /usr/dcb/bin/convMS            0.0.0.0
appEvents/msDispatcher,netEvents/msDispatcher  2
#mediaServer      105            /usr/dcb/bin/convMS            0.0.0.0
appEvents/msDispatcher,netEvents/msDispatcher  3
```

3.2. Configure the Convedia CMS-6000 Media Server

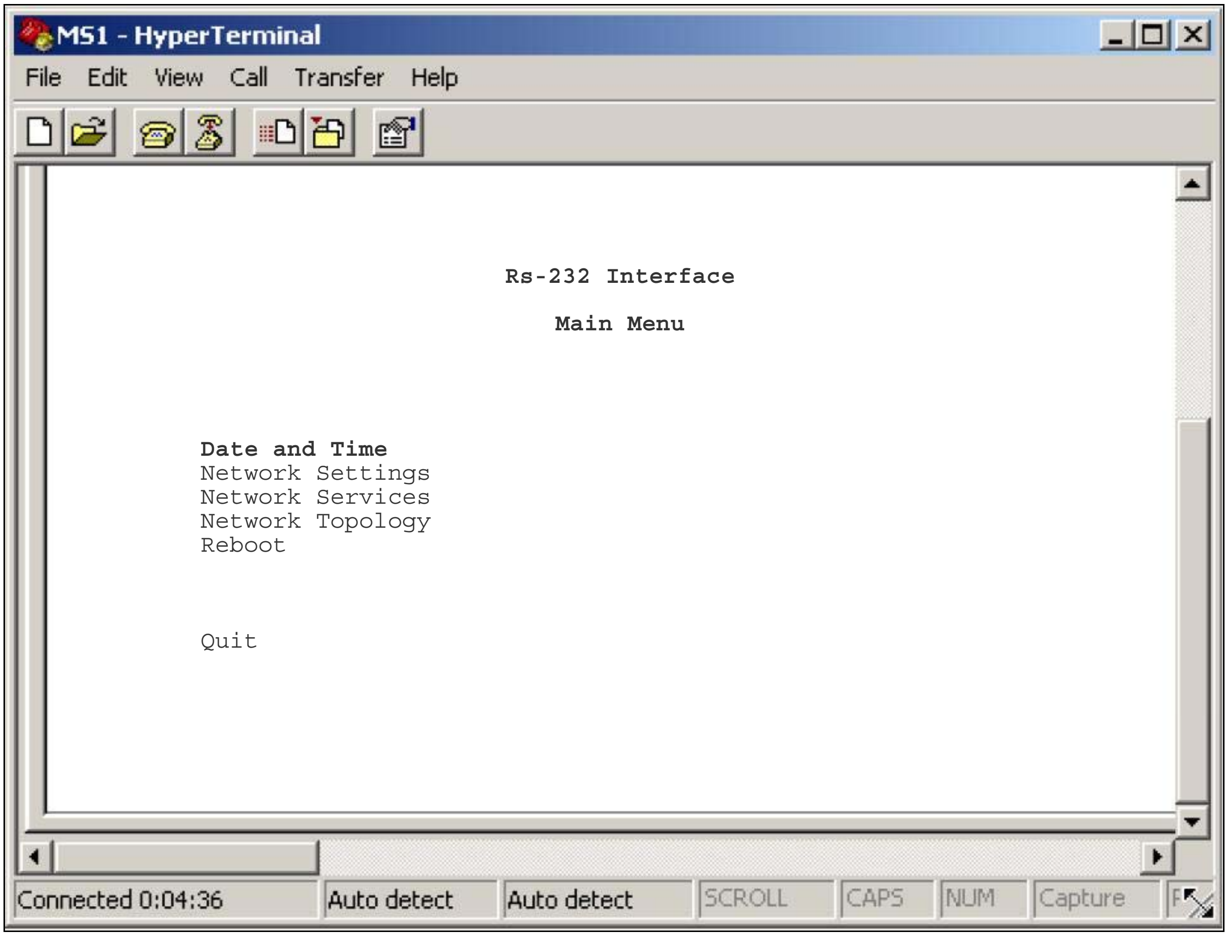
The following steps describe the administrative procedures for configuring the Convedia CMS-6000 Media Server to enable collaboration with the Avaya Meeting Exchange S6200 Application Server. For additional information regarding configuring the Convedia CMS-6000 Media Server, see **Section 9**, **Reference 2**.

Step	Description
3.6	Provision the SCC on the Convedia CMS-6000 Media Server as follows: • Establish an RS-232 connection from a services PC to the Convedia CMS-6000 Media Server by connecting a serial cable to the front of the SCC card (slot 1). • Start a terminal server application, e.g., HyperTerminal on the services PC with the following settings: o Speed: 9600 bps. o Data bits: 8 bits. o Parity: No parity. o Stop bit: 1 bit. o Flow control: none. • Wait for the system to establish the connection, or press <Enter>.

Step	Description
3.7	From the **RS-232 Interface** login screen that is displayed, log in to the Convedia CMS-6000 Media Server craft interface with the appropriate credentials. 

```
RS-232 Interface

Username:_
Enter Password:
```

Step	Description
3.8	From the **RS-232 Interface Main Menu** screen that is displayed, select **Date and Time** and press <Enter>.



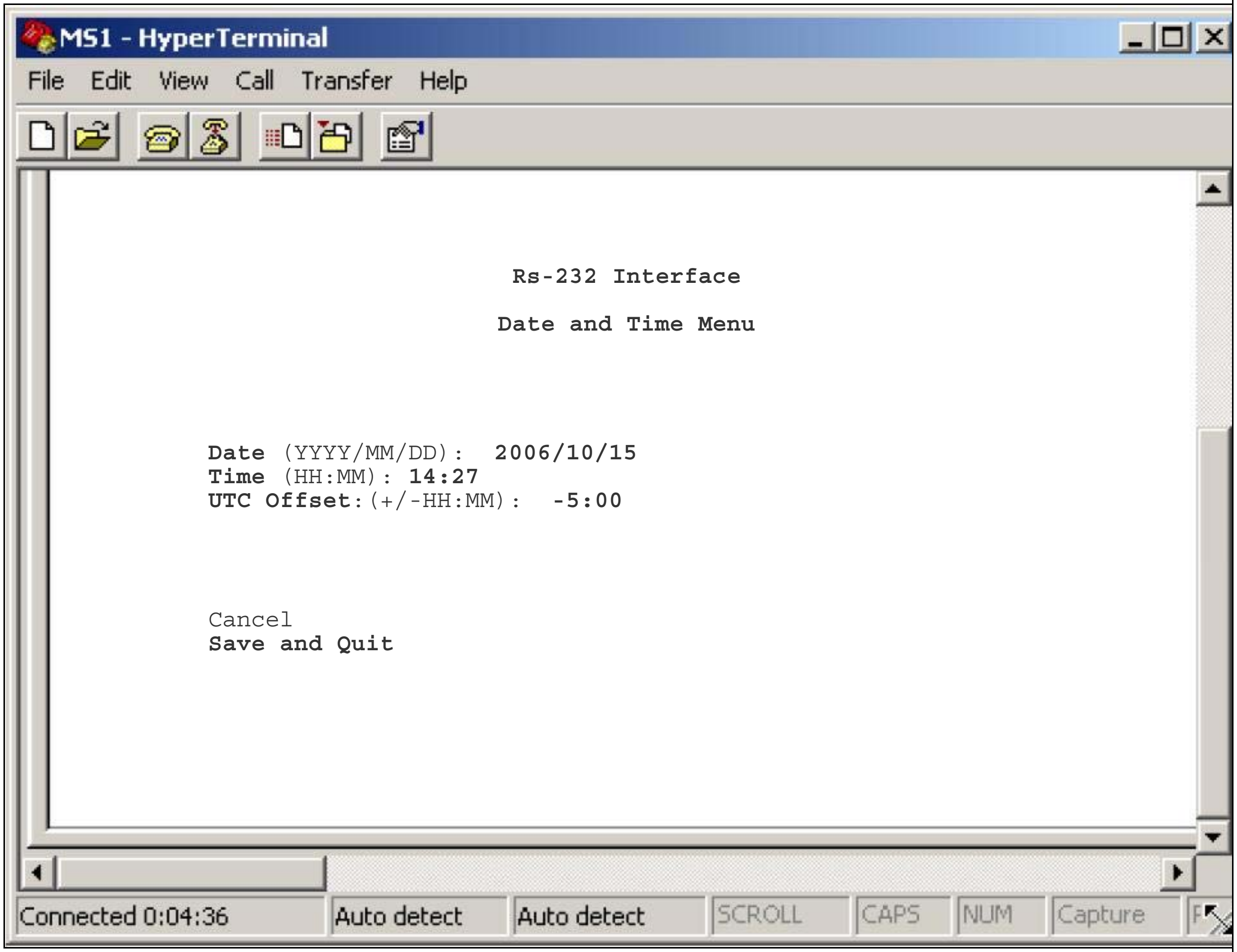
```
                              Rs-232 Interface

                                 Main Menu



          Date and Time
          Network Settings
          Network Services
          Network Topology
          Reboot



          Quit
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.9</td><td>

From the **RS-232 Interface Date and Time Menu** that is displayed, configure settings for the date and time as follows.

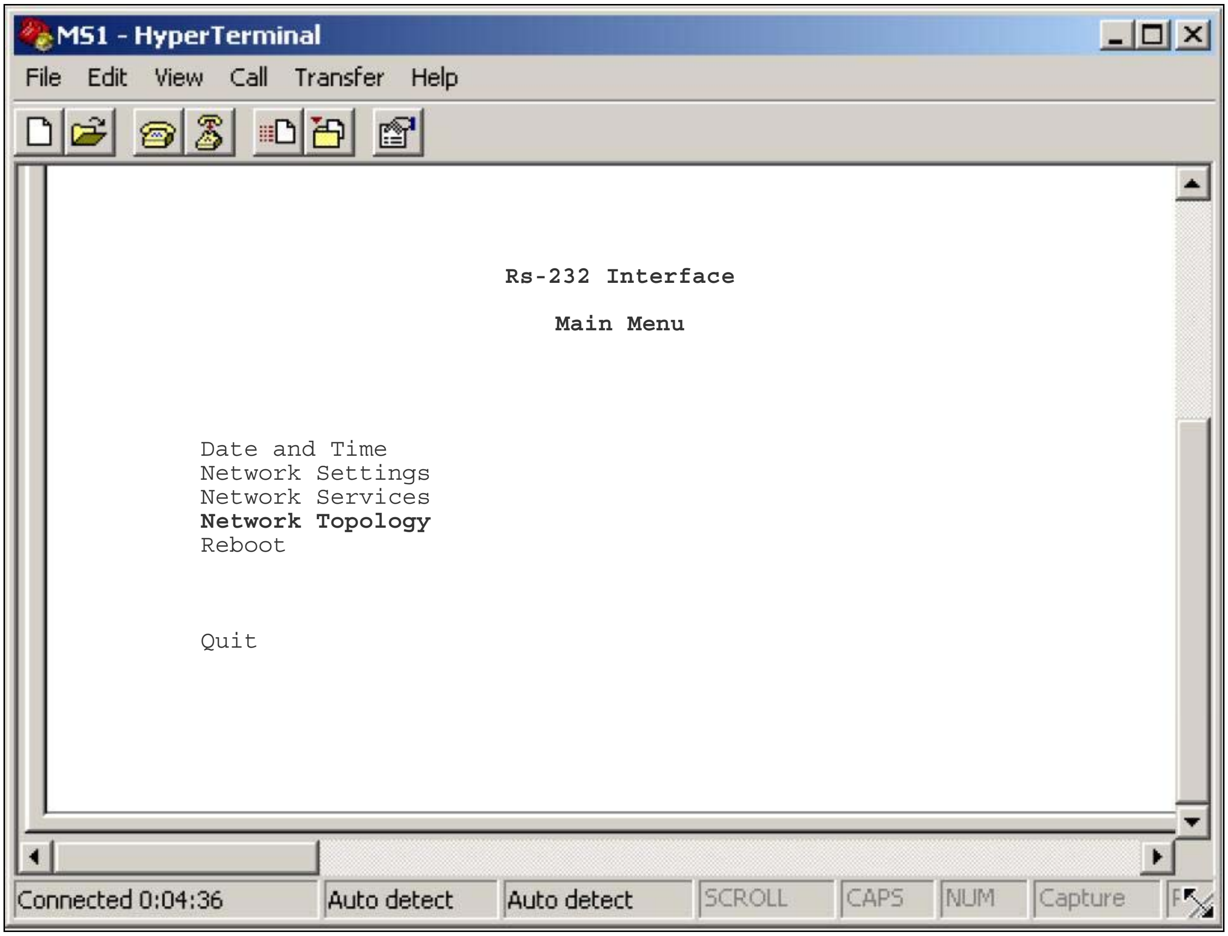
- Set the **Date** to the current date.
- Set the **Time** to the current time.
- Set the **UTC Offset** to compensate for the location of the Convedia CMS-6000 Media Server relative to the Universal Time Clock (UTC) or Greenwich Mean Time (GMT).

  > ***Note***: *The* ***UTC Offset*** *is derived from the location of Convedia CMS-6000 Media Server relative to the UTC/GMT. Format is +|–hh:mm, where + represents the number of hours ahead of UTC, – is the number of hours behind UTC. For example, Moscow is +3:00, London is +0:00, New York is –5:00 and Los Angeles is –8:00.*
- Save the settings by using <Tab> to navigate down to **Save and Quit** and press <Enter>.

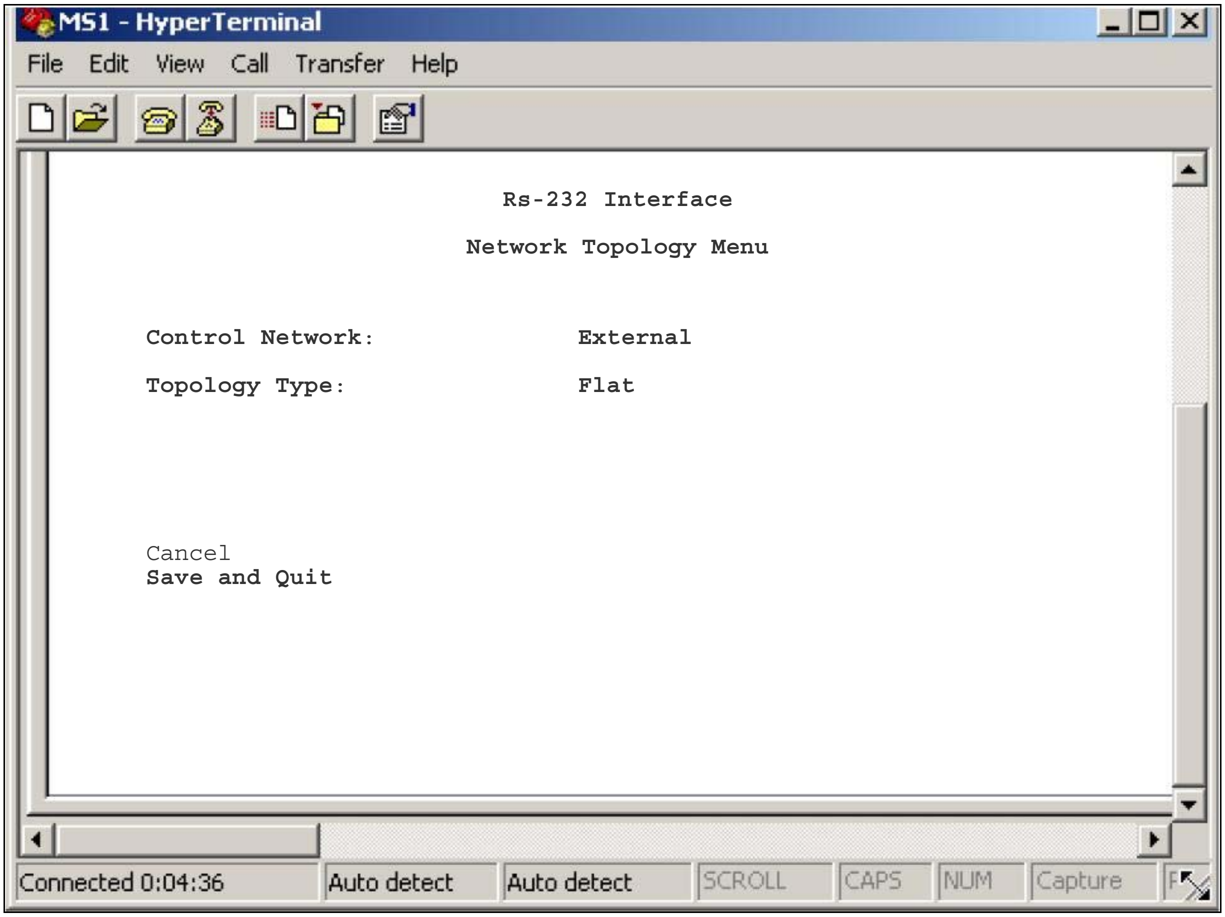


```
                         Rs-232 Interface

                       Date and Time Menu



          Date (YYYY/MM/DD):  2006/10/15
          Time (HH:MM): 14:27
          UTC Offset:(+/-HH:MM):  -5:00



          Cancel
          Save and Quit
```

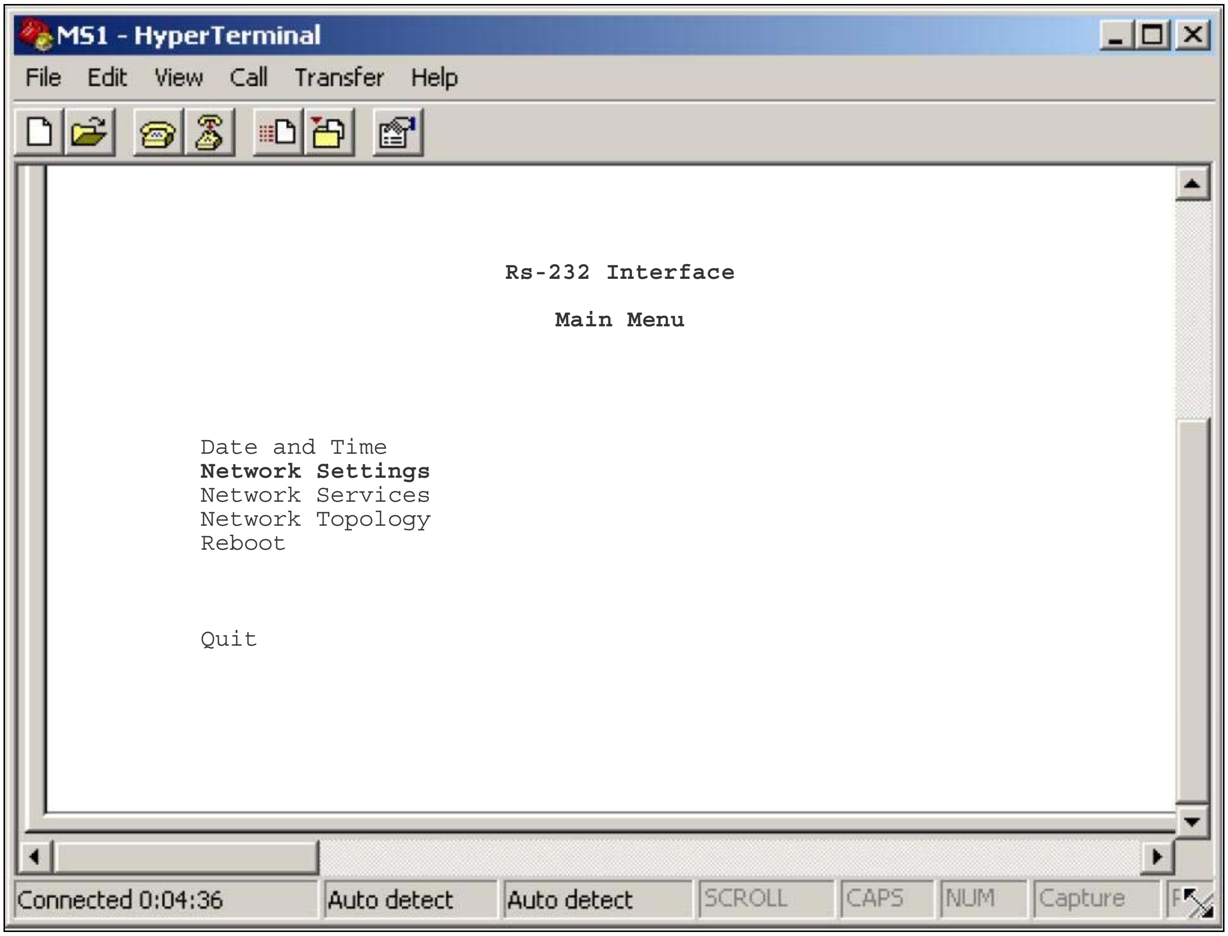
</td></tr>
</table>

Step	Description
3.10	From the **RS-232 Interface Main Menu** screen that is displayed, select **Network Topology** and press <Enter>. 

```
Rs-232 Interface

Main Menu



Date and Time
Network Settings
Network Services
Network Topology
Reboot



Quit
```

Step	Description
3.11	From the **RS-232 Interface Network Topology Menu** that is displayed, configure the network topology as follows. • Set the **Control Network** to **External** by using the spacebar to toggle between values and press <Enter> to accept the value. ***Note**: An **External Control Network** is where MPC control interfaces have IP addresses on the external control subnet. The control agent communicates directly with an MPC through its control interface.* • Set the **Topology Type** to **Flat** by using the spacebar to toggle between values and press <Enter> to accept the value. ***Note**: A **Flat Topology Type** is where control and media share a single network segment.* • Save the settings by using <Tab> to navigate down to **Save and Quit** and press <Enter>. 

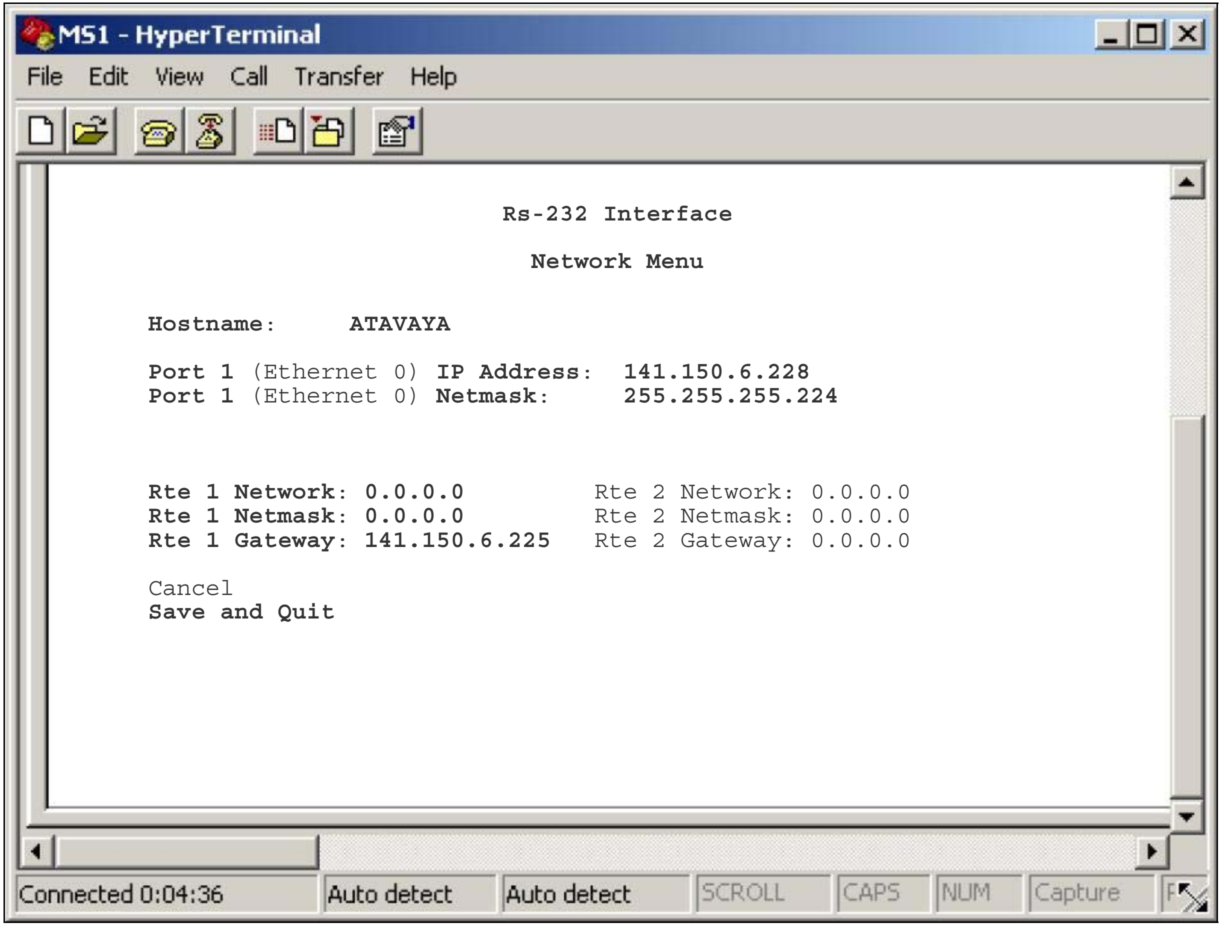
```
Rs-232 Interface

Network Topology Menu


Control Network:              External

Topology Type:                Flat




Cancel
Save and Quit
```

Step	Description
3.12	From the **RS-232 Interface Main Menu** screen that is displayed, select **Network Settings** and press <Enter>. 

Step	Description
3.13	From the **RS-232 Interface Network Menu** that is displayed, configure network settings as follows.

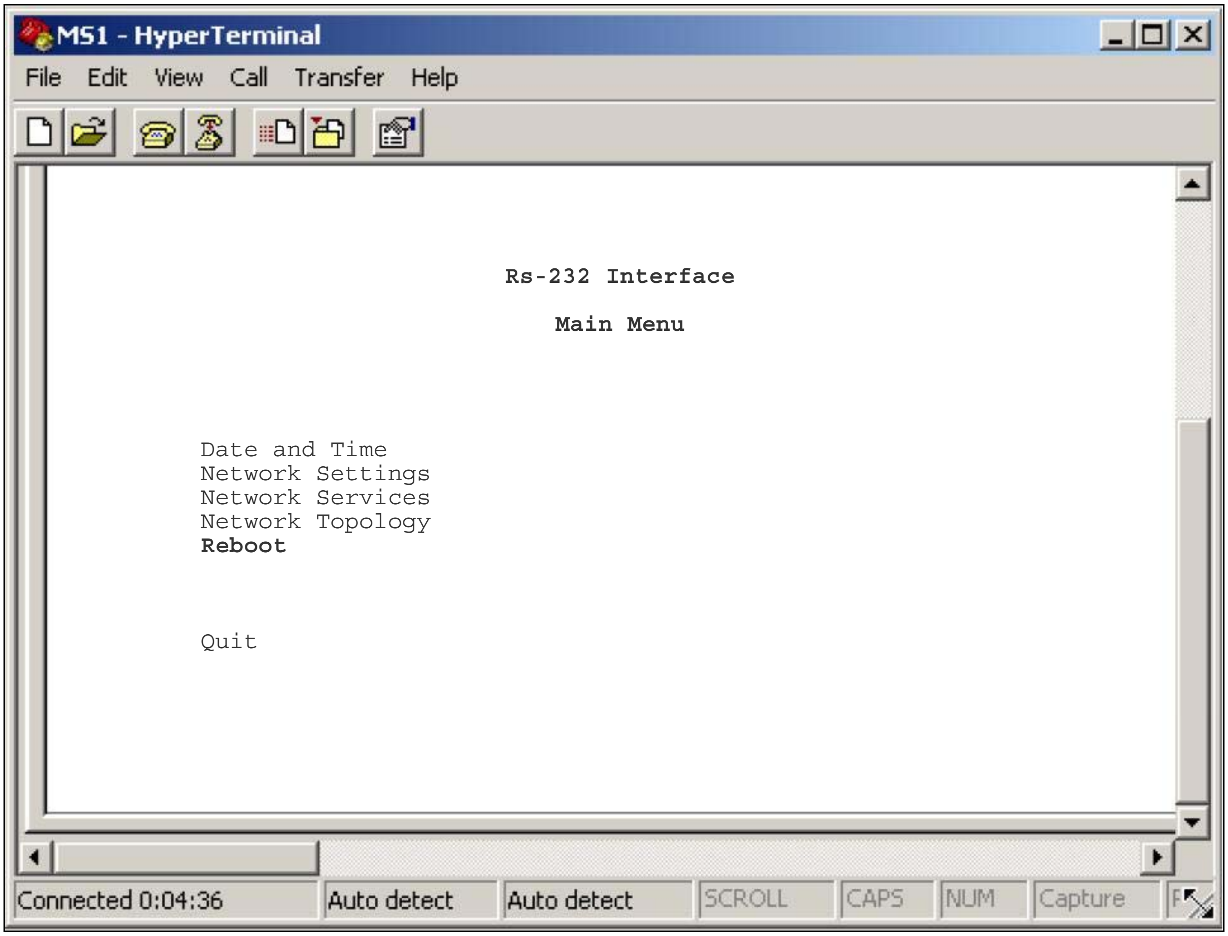
- Administer network parameters used for control and management traffic on the Convedia CMS-6000 Media Server by specifying:
  - A **Hostname** for the Convedia CMS-6000 Media Server.
  - An **IP Address** and **Netmask** for **Port 1**.
- Administer routing parameters used for remote control or management networks on the Convedia CMS-6000 Media Server by specifying:
  - A **Network** IP address, **Netmask** and **Gateway** for **Rte 1**.

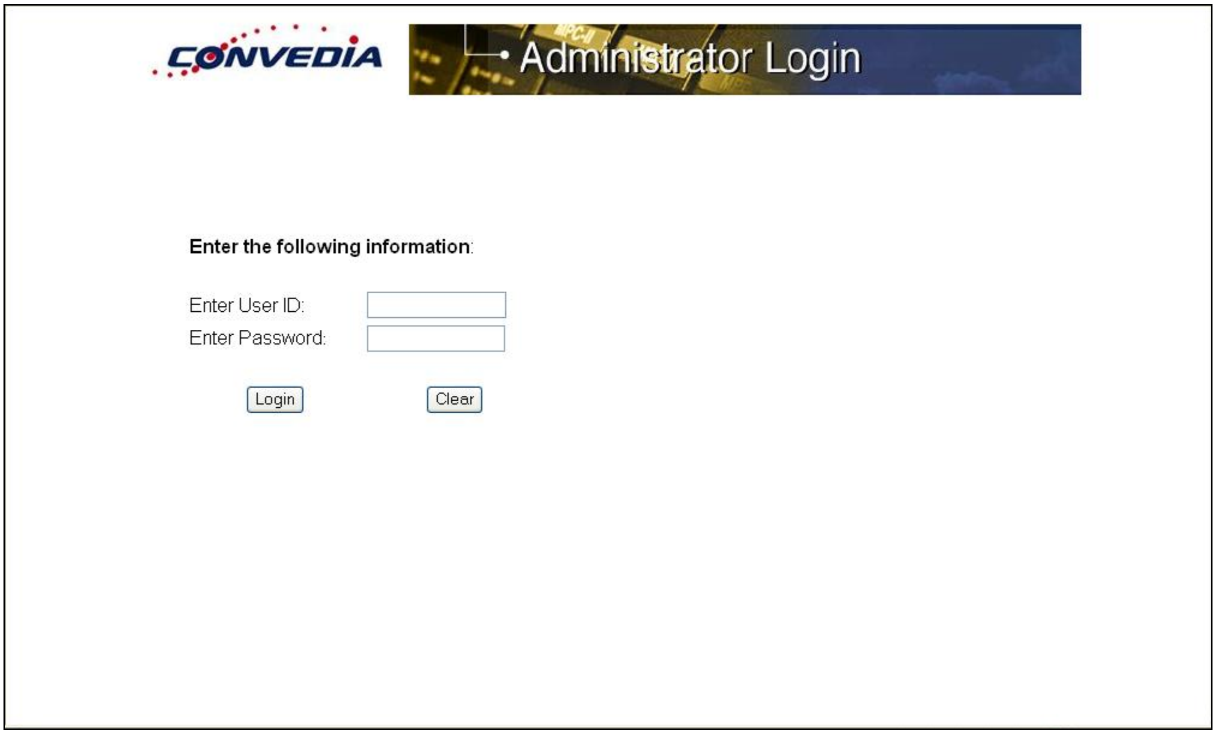
    ***Note**: To indicate the default gateway, leave the **Network** IP address and **Netmask** blank (**0.0.0.0**). The **Gateway** must be on a directly connected network.*
- Save the settings by using <Tab> to navigate down to **Save and Quit** and press <Enter>.



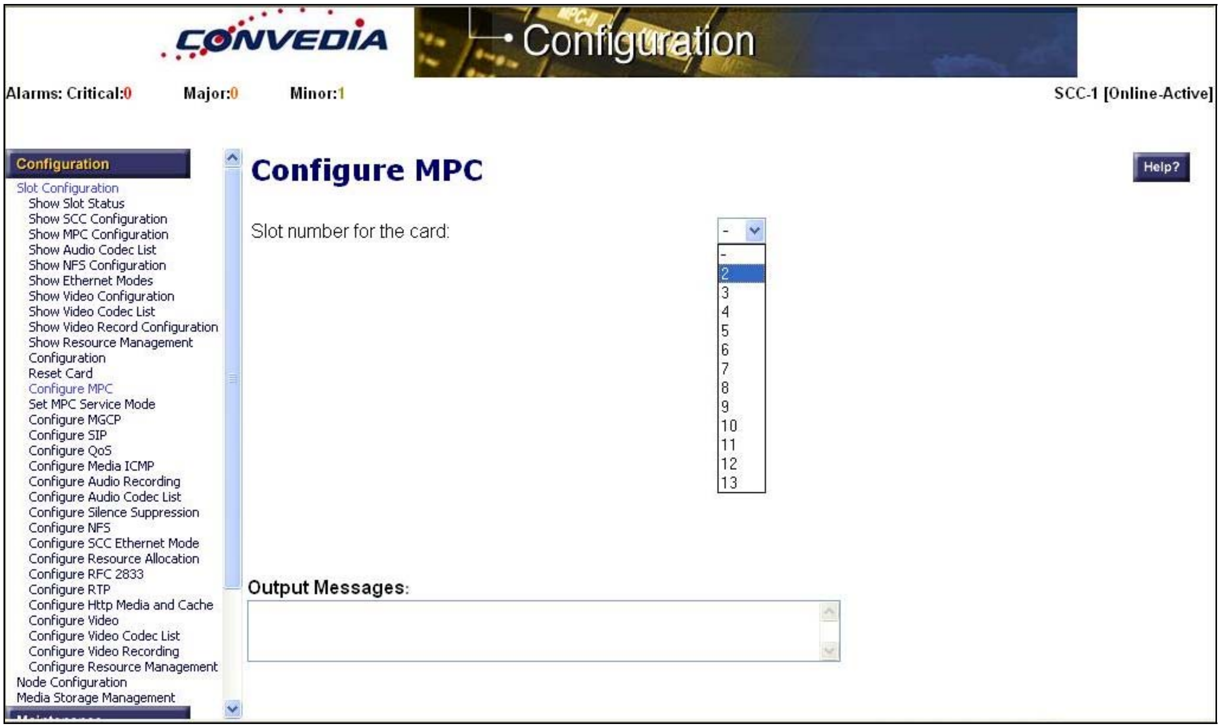
```
                        Rs-232 Interface

                          Network Menu


     Hostname:     ATAVAYA

     Port 1 (Ethernet 0) IP Address:  141.150.6.228
     Port 1 (Ethernet 0) Netmask:     255.255.255.224



     Rte 1 Network: 0.0.0.0         Rte 2 Network: 0.0.0.0
     Rte 1 Netmask: 0.0.0.0         Rte 2 Netmask: 0.0.0.0
     Rte 1 Gateway: 141.150.6.225   Rte 2 Gateway: 0.0.0.0

     Cancel
     Save and Quit
```

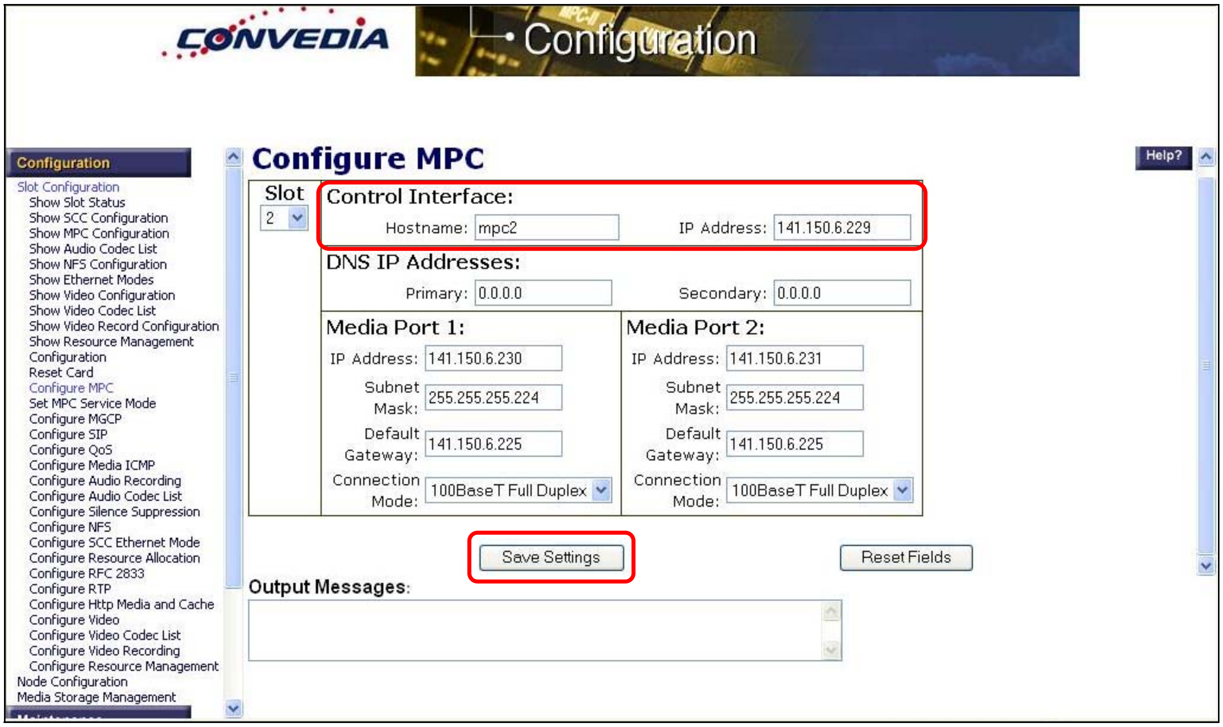
Step	Description

3.14	From the **RS-232 Interface Main Menu** screen that is displayed, preserve the configuration administered in the previous steps by rebooting the Convedia CMS-6000 Media Server.
	• Select **Reboot** and press <Enter>.
	  ○ [***Not Shown***] *A confirmation message displays to confirm the reboot*.
	  ○ [***Not Shown***] *Use the <Tab> key to toggle to the **YES** option and press <Enter>*.
	  ○ [***Not Shown***] *Use the spacebar to toggle to the Choose the **Restart with Current Configuration** option*.
	  ○ [***Not Shown***] *A confirmation message displays to confirm the reboot*.
	  ○ [***Not Shown***] *Use the <Tab> key to toggle to the **YES** option and press <Enter>*.
	• The media server restarts and the network settings are enabled.
	

Step	Description
3.15	Administer settings for Convedia CMS-6000 Media Server via the web GUI as follows: • Open a web browser and enter the following URL: **http://<IP address of Convedia CMS-6000 Media Server >** • Log in to the Convedia CMS-6000 Media Server with the appropriate credentials. 

Step	Description
3.16	Administer settings for Audio Codec(s) on the Convedia CMS-6000 Media Server as follows: • Click **Configuration ➔ Slot Configuration ➔ Configure Audio Codec List**. • Select either the **Slot Number** for the MPC card or **all** (MPC cards) to which this **Audio Codec List** will be applied. • Click **Execute**. ***Note****: Audio Codecs in the* ***Audio Codec List*** *are prioritized from* ***First codec*** *to* ***Tenth codec****.*  **Configure Audio Codec List** Slot number for the card: all First codec: pcmu Second codec: pcma Third codec: g729 Fourth codec: none Fifth codec: none Sixth codec: none Seventh codec: none Eighth codec: none Ninth codec: none Tenth codec: none

Step	Description
3.17	Administer settings for MPC(s) on the Convedia CMS-6000 Media Server as follows: - Click **Configuration** ➔ **Slot Configuration** ➔ **Configure MPC**. - Select the **Slot Number for the** MPC. For these Application Notes, the MPC was placed in **Slot number 2**.  Configure MPC Slot number for the card: 2 Output Messages:

Step	**Description**
3.18	Configure the MPC in slot 2 on the Convedia CMS-6000 Media Server as displayed: • Enter a **Hostname** and **IP Address** for the **Control Interface**. • Enter **IP Address**, **Subnet Mask**, **Connection Mode** and **Default Gateway** information for **Media Ports 1** and **2**. • Click on the **Save Settings** button when finished. ***Note***: *Repeat from* ***Step 3.17*** *to configure each MPC on the Convedia CMS-6000 Media Server. For these Application Notes, there is only one MPC.*  Configure MPC Slot: 2 Control Interface: Hostname: mpc2 IP Address: 141.150.6.229 DNS IP Addresses: Primary: 0.0.0.0 Secondary: 0.0.0.0 Media Port 1: IP Address: 141.150.6.230 Subnet Mask: 255.255.255.224 Default Gateway: 141.150.6.225 Connection Mode: 100BaseT Full Duplex Media Port 2: IP Address: 141.150.6.231 Subnet Mask: 255.255.255.224 Default Gateway: 141.150.6.225 Connection Mode: 100BaseT Full Duplex Output Messages:

3.3. Network File System

The following steps describe the administrative procedures to enable Network File System (NFS) sharing between the Avaya Meeting Exchange S6200 Application Server and the Convedia CMS-6000 Media Server. In this configuration, the Avaya Meeting Exchange S6200 Application Server will function as the NFS server. This will allow playback of audio conference(s) recorded on the Convedia CMS-6000 Media Server from the Avaya Meeting Exchange S6200 Application Server.

3.3.1. Configure NFS on the Avaya Meeting Exchange S6200 Application Server

The following steps describe the administrative procedures to provision NFS on the Avaya Meeting Exchange S6200 Application Server.

Step	Description
3.19	Log in to the Avaya Meeting Exchange S6200 Application Server console to access the CLI with the appropriate credentials.
3.20	The NFS server communicates with the control interface on the Convedia CMS-6000 Media Server MPC. To resolve the IP address for the control interface on the Convedia CMS-6000 Media Server MPC, edit the **hosts** file as follows: • cd to **/etc** • Edit the **hosts** file with a text editor, e.g., vi. • Add a line to the file to resolve the IP address of the control interface to the Convedia CMS-6000 Media Server MPC in slot 2: o **141.150.6.229 mpc2** Where **141.150.6.229** and **mpc2** are the IP address and hostname of the control interface assigned to the Convedia CMS-6000 Media Server MPC in **Step 3.18**.
3.21	To allow the Convedia CMS-6000 Media Server MPC to mount the /usr3/ipcb directory on the Avaya Meeting Exchange S6200 Application Server, edit the **dfstab** file as follows: • cd to **/etc/dfs** • Edit the **dfstab** file with a text editor, e.g., vi. • Add a line to the file to assign read/write (**rw**) privileges to the directory **/usr3/ipcb** for the Convedia CMS-6000 Media Server: o **/usr/sbin/share -F nfs -o rw=mpc2 /usr3/ipcb** Where **mpc2** is the hostname assigned to the Convedia CMS-6000 Media Server MPC in **Step 3.20**.

Step	Description
3.22	To configure the Avaya Meeting Exchange S6200 Application Server as an NFS server, edit the **mediaServerInterface.cfg** file as follows: • cd to **/usr/ipcb/config** • Edit the **mediaServerInterface.cfg** file with a text editor, e.g., vi. • Add a line to the file to assign the Avaya Meeting Exchange Application Server as the NFS server: o **NFSServerIPAddress=192.168.13.101** Where **192.168.13.101** is the IP address assigned to the Avaya Meeting Exchange Application Server. • Add a line to the file to assign the Convedia CMS-6000 Media Server as a media server: o **MediaServerIP_1=141.150.6.229** Where **141.150.6.229** is the IP address of the control interface assigned to the Convedia CMS-6000 Media Server MPC in **Step 3.18**. ***Note**: Multiple MPC cards on the Convedia CMS-6000 Media Server would each require an entry in the **mediaServerInterface.cfg** file. The requirement for successive entries is to increment the MediaServerIP_X variable by 1, e.g., MediaServerIP_2 would correspond to a second MPC, MediaServerIP_3 to a third, etc..* • Add a line to the file to assign a port to the Convedia CMS-6000 Media Server: o **MediaServerInterfaceSipListenPort_1=5050** ***Note**: Multiple MPC cards on the Convedia CMS-6000 Media Server would each require an entry for a unique port in the **mediaServerInterface.cfg** file. The requirement for the successive port entries are to decrease the port number by ten for each MPC card, e.g., the port number for a second MPC would be 5040, a third MPC would have a port entry of 5030, etc..*

```
# This file contains the configuration information for the
# Media Server Interface. This information includes the
# IP Address for the NFS Server (where recordings are stored),
# the IP address of the Media Server(may be more than 1), and
# the udp port that the Media Server Interface code should
# listen for SIP responses.
#
# NFS Server
NFSServerIPAddress=192.168.13.101
#
# MPC 1 on Convedia CMS-6000 Media Server (Control Port)
MediaServerIP_1=141.150.6.229
MediaServerInterfaceSipListenPort_1=5050
```

Step	Description
3.23	From the **/usr3** directory on the Avaya Meeting Exchange S6200 Application Server, verify the following symbolic link is present: **confrp -> /usr3/ipcb/usr3/confrp**.

```
S6200App->pwd
/usr3
S6200App->ls -l
total 4
drwxr-xr-x    3 root     dcb      1024 Jan 17 04:20 BACKUPS
lrwxrwxrwx    1 root     sys        22 Nov 30 19:01 confrp -> /usr3/ipcb/usr3/confrp
drwxr-xr-x    5 root     sys        96 Jun 29  2006 ipcb
drwxrwxrwx   20 root     root     1024 Nov  6 19:03 runtime
drwxrwxr-x    2 root     dcb        96 Oct  5  2005 savedroster
```

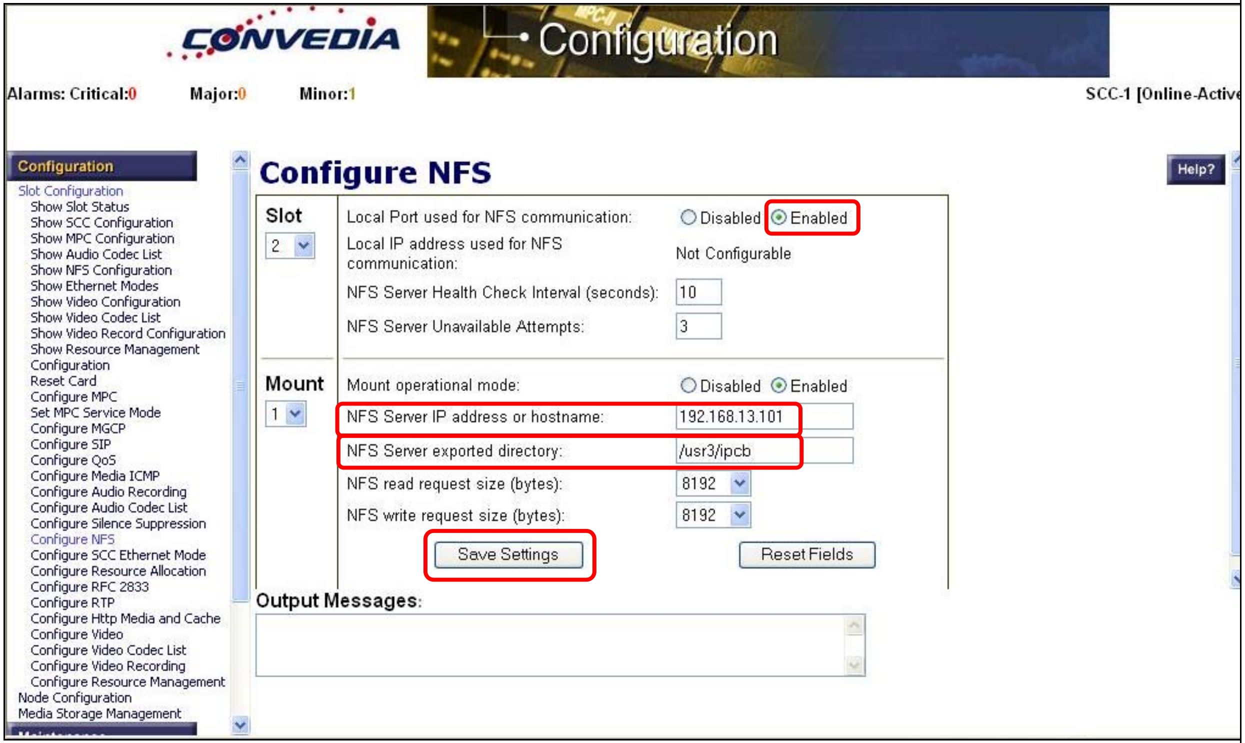
3.24	**Reboot** the Avaya Meeting Exchange S6200 Application Server for changes to take effect. ***Note**: Rebooting the Avaya Meeting Exchange S6200 Application Server is service impacting.*

```
[S6800]> init 6
```

3.3.2. Configure NFS on the Convedia CMS-6000 Media Server

The following steps describe the administrative procedures to provision NFS on the Convedia CMS-6000 Media Server.

Step	Description
3.25	Administer settings for NFS on the Convedia CMS-6000 Media Server MPC(s) via the web GUI as follows: - Click **Configuration ➔ Slot Configuration ➔ Configure NFS**. - Select the **Slot Number for the** MPC to administer settings for NFS. For these Application Notes, the MPC was placed in **Slot number 2**.  Slot number for the card: - Output Messages:

Step	Description
3.26	Configure NFS parameters for the MPC in slot 2 on the Convedia CMS-6000 Media Server as displayed: - Select **Enabled** for the **Local Port used for NFS communication** to enable NFS on this MPC. - Enter the IP address for the NFS server provisioned in Step **3.22** in the **NFS Server IP address or hostname** field. - Enter **/usr3/ipcb** (see **Step 3.21**) in the **NFS Server exported directory** field. - Remaining fields are default settings. - Click on the **Save Settings** button when finished. ***Note****: Repeat from* ***Step 3.25*** *to Configure NFS for each MPC on the Convedia CMS-6000 Media Server. For these Application Notes, there is only one MPC.*  Alarms: Critical:0 Major:0 Minor:1 SCC-1 [Online-Active Configure NFS Slot 2 Local Port used for NFS communication: ○ Disabled ● Enabled Local IP address used for NFS communication: Not Configurable NFS Server Health Check Interval (seconds): 10 NFS Server Unavailable Attempts: 3 Mount 1 Mount operational mode: ○ Disabled ● Enabled NFS Server IP address or hostname: 192.168.13.101 NFS Server exported directory: /usr3/ipcb NFS read request size (bytes): 8192 NFS write request size (bytes): 8192 Output Messages:

Step	Description
3.27	Reset the Convedia CMS-6000 Media Server MPC in slot 2 for changes to take effect as follows: • Click **Configuration → Reset Card**. • Select the slot number for the MPC to reset. For these Application Notes, the MPC was placed in slot number **2**. • Select **Forced** for the **Type of reset operation**. • Click **Execute**. ***Note****: If there is only one MPC in the Convedia CMS-6000 Media Server chassis, resetting the MPC is service impacting. If more than one MPC is present, resetting a single MPC would not be service impacting, as all traffic on the MPC being reset would fail over to an active MPC.*  Slot number for the card: 2 Type of reset operation: Forced Output Messages: `Action in progress...`

3.4. CBUTIL Utility

The following steps provide examples of how to provision DIRECT and SCAN call functions by utilizing the cbutil utility on the Avaya Meeting Exchange S6200 Application Server. DID values (obtained from procedures in **Step 3.3**) are associated with call functions to access conferences provisioned on the Avaya Meeting Exchange S6200 Application Server.

Step	Description
3.28	To map DID values obtained in **Step 3.3** to DNIS entries, run the **cbutil** utility as follows: • If not already logged on, log in to the Avaya Meeting Exchange S6200 Application Server console to access the CLI with the appropriate credentials. • At the command prompt enter **tcsh** to set the UNIX shell on the Avaya Meeting Exchange S6200 Application Server. • At the command prompt run the **cbutil** utility to verify DNIS entries provisioned on the Avaya Meeting Exchange S6200 Application Server. ***Note**: A command line utility, **cbutil** enables administrators to assign a specific annunciator message, line name, company name, system function, reservation group and prompt sets to a maximum of 30,000 DNIS or DID entries. The Avaya Meeting Exchange S6200 Application Server parses these entries in numerically ascending order, with the wildcard character "?" last in a series. For example, 129? follows 1299. The last entry in the table consists entirely of wildcard characters.*

```
S6200App->cbutil
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.

Usage: cbutil <command> [command-specific args...]
 where <command> may be one of:
  add           Add an entry to the Call Branding table
  remove        Remove an entry from the Call Branding table
  update        Update an entry in the Call Branding table
  lookup        Display an entry in the Call Branding table
  count         Display the number of entries in the Call Branding table
  list          List entries in the Call Branding table
  dnissize      Set system configured max dnis length (1-16)
   Note:  This command should only be used when the bridge is not running.
Use "cbutil<command> -help" to get help on a specific command
```

Step	Description

3.29 Enable Dial-In access (via passcode) to conferences provisioned on the Avaya Meeting Exchange S6200 Application Server as follows:

- Add a DNIS entry for a **scan call function** corresponding to DID **501** by entering the following command at the command prompt:
  cbutil add <**dnis**> <**rg**> <**msg**> <**ps**> <**ucps**> <**func**> [**-l** <**ln**> **-c** <**cn**>], where the variables for add command is defined as follows:
    - <**dnis**> DNIS
    - <**rg**> Reservation Group
    - <**msg**> Annunciator message number
    - <**ps**> Prompt Set number (0-20)
    - <**ucps**> Use Conference Prompt Set (y/n)
    - <**func**> One of: DIRECT/SCAN/ENTER/HANGUP/AUTOVL/FLEX
    - **-l** <"**ln**"> Optional line name to associate with caller
    - **-c** <"**cn**"> Optional company name to associate with caller

```
S6200App->cbutil add 501 0 1 1 n scan
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

3.30 Enable Dial-In access (as moderator, without entering a passcode) to conferences provisioned on the Avaya Meeting Exchange S6200 Application Server by adding a DNIS entry for a **direct call function** corresponding to DID **556**.

```
S6200App->cbutil add 556 0 301 1 n direct
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

3.31 At the command prompt enter **cbutil list** to verify the DNIS entries provisioned in **Step 3.29** and **Step 3.30** were provisioned and entered correctly.

Note*: The last entry in the call brand table is the wild card entry "****???****". This entry captures any wrong number (e.g., unmatched* ***DID*** *values) and places the call into enter queue for operator assistance.*

```
S6200App->cbutil list
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.

DNIS             Grp Msg PS  CP Function Line Name            Company Name
---------------- --- --- --- -- -------- -------------------- -----------------
501              0   1   1   N  SCAN
556              0   301 1   N  DIRECT
???              0   208 1   N  ENTER
```

3.5. Bridge Talk

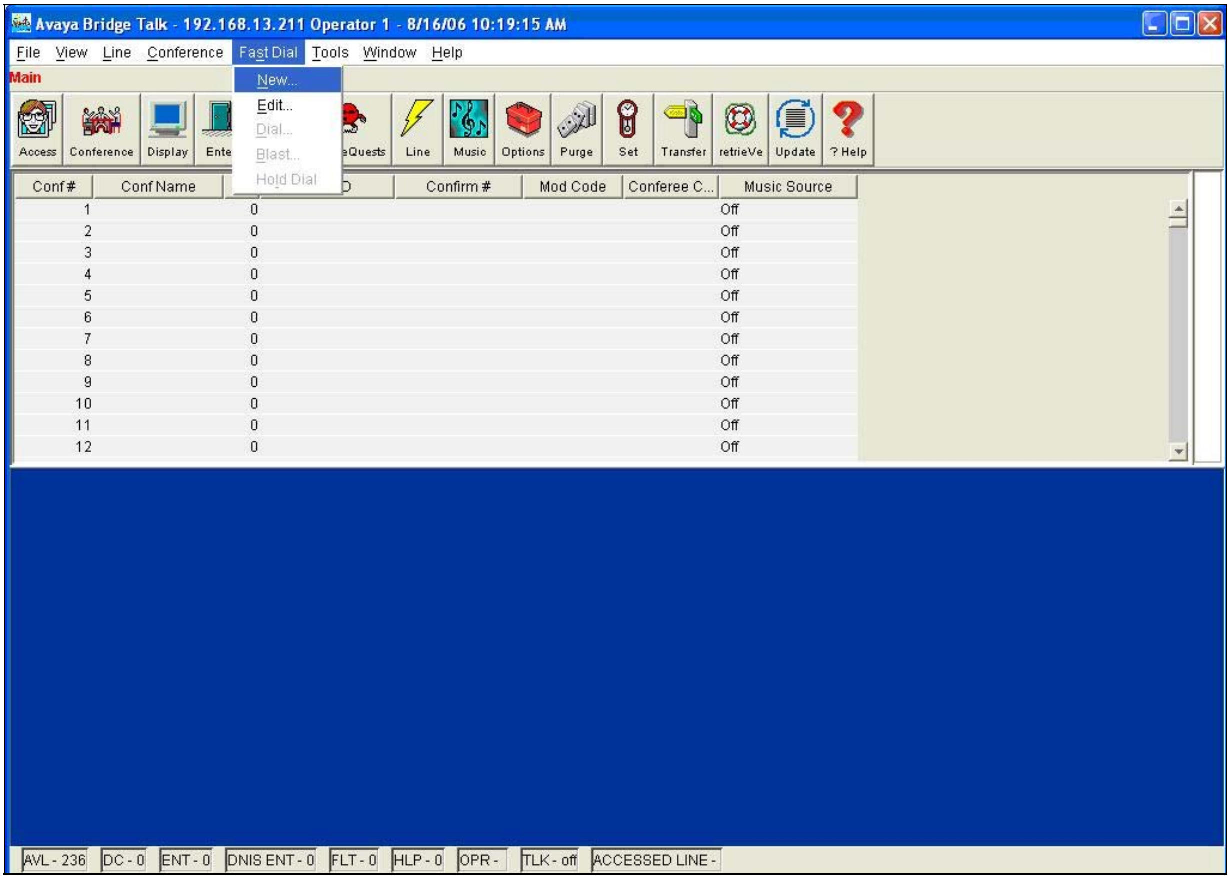
The following steps utilize the Avaya Bridge Talk application to provision a sample conference on the Avaya Meeting Exchange S6200 Application Server. This sample conference is utilized in conjunction with the DIRECT and SCAN call functions provisioned in **Section 3.4** to enable both Dial-In and Dial-Out access to audio conferencing for endpoints on a public network.

***Note**: If any of the features displayed in the Avaya Bridge Talk screen captures are not present, contact an authorized Avaya sales representative to make the appropriate changes.*

Step	**Description**
3.32	Invoke the Avaya Bridge Talk application as follows: • [*Not Shown*] *Double-click on the desktop icon from a PC loaded with the Avaya Bridge Talk application and with network connectivity to the Avaya Meeting Exchange S6200 Application Server*. • Enter the IP address of the Avaya Meeting Exchange S6200 Application Server (**192.169.13.101**) in the **Bridge** field. • Enter the appropriate credentials in the **Sign-In** and **Password** fields.  Operator: Next available

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.33</td><td>Provision a dial list that is utilized for Dial-Out (e.g., Blast dial and Fast Dial) from the Avaya Meeting Exchange S6200 Application Server.

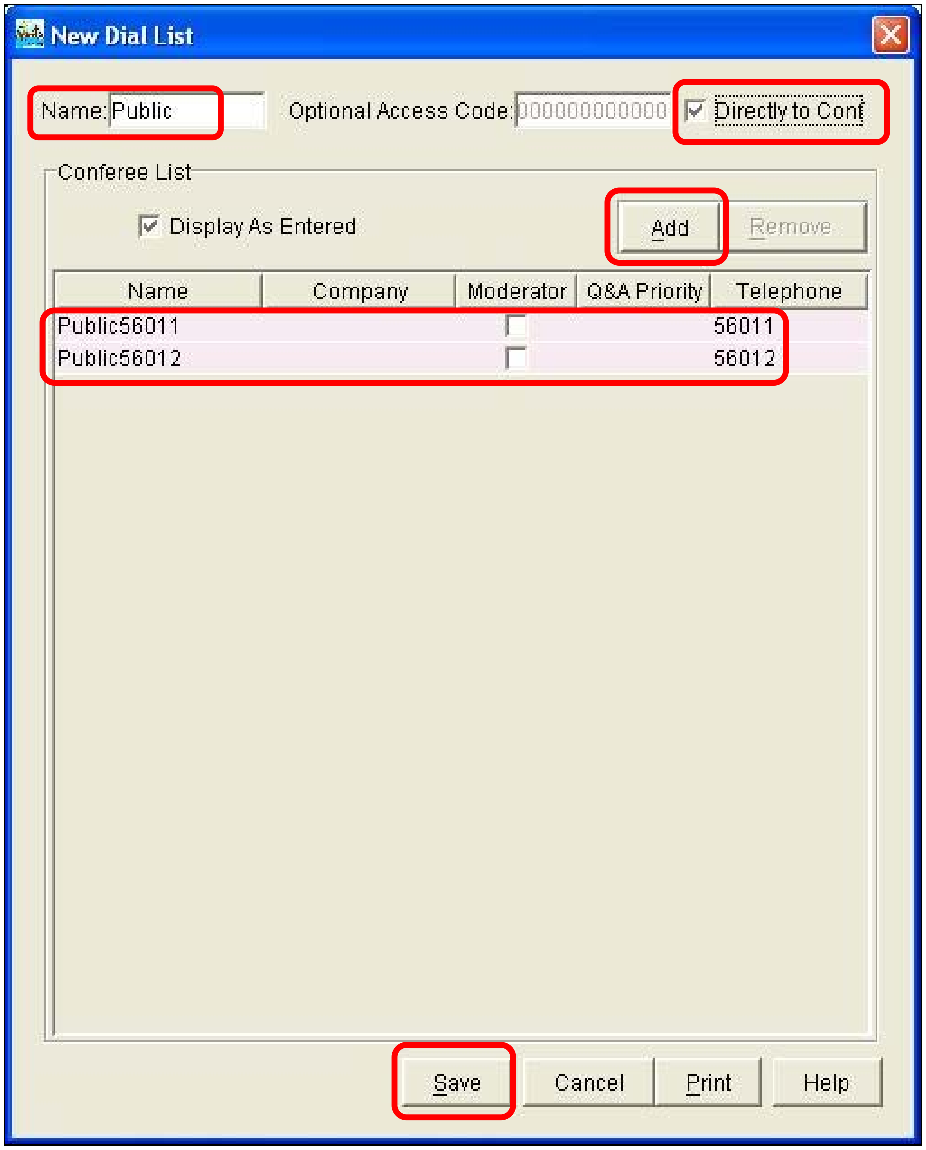
From the Avaya Bridge Talk Menu Bar, click Fast Dial → New.



Avaya Bridge Talk - 192.168.13.211 Operator 1 - 8/16/06 10:19:15 AM

<table>
<tr><th>Conf #</th><th>Conf Name</th><th></th><th>D</th><th>Confirm #</th><th>Mod Code</th><th>Conferee C...</th><th>Music Source</th></tr>
<tr><td>1</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>2</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>3</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>4</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>5</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>6</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>7</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>8</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>9</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>10</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>11</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
<tr><td>12</td><td></td><td>0</td><td></td><td></td><td></td><td></td><td>Off</td></tr>
</table>
</td></tr>
</table>

Step	Description
3.34	From the **New Dial List** window that is displayed: • Enter a descriptive label in the **Name** field. • Enable conference participants on the dial list to enter the conference without a passcode by checking the **Directly to Conf** box as displayed. • Add entries to the dial list by clicking on the **Add** button for each participant. ○ Moderator privileges may be granted to a conference participant by checking the **Moderator** box. • See **Section 9**, **Reference 3** for provisioning the remaining fields in this screen. • When finished, click on the **Save** button on the bottom of the screen.



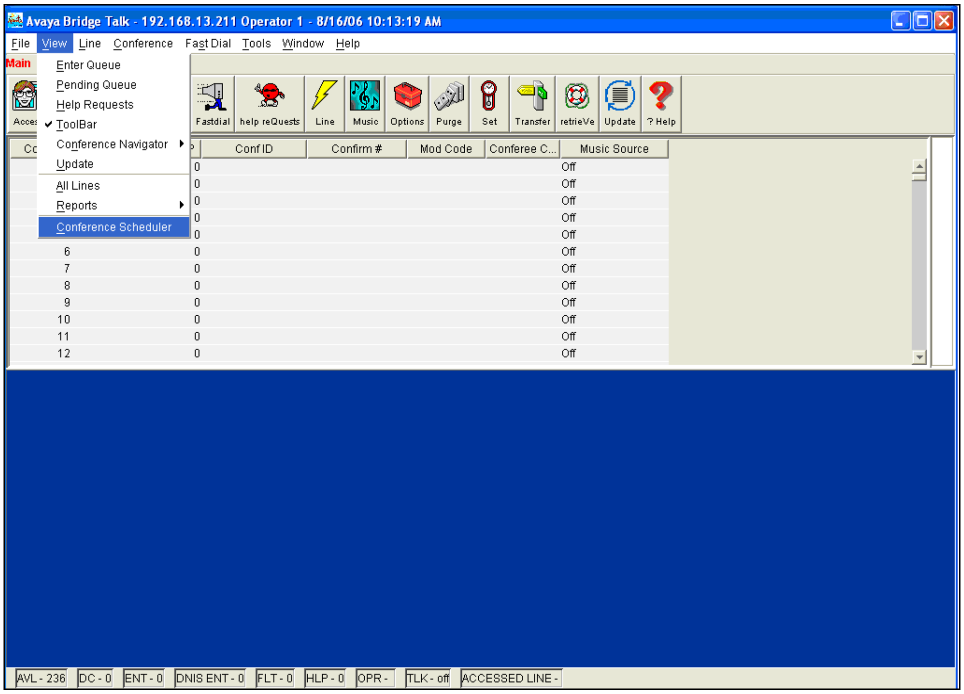
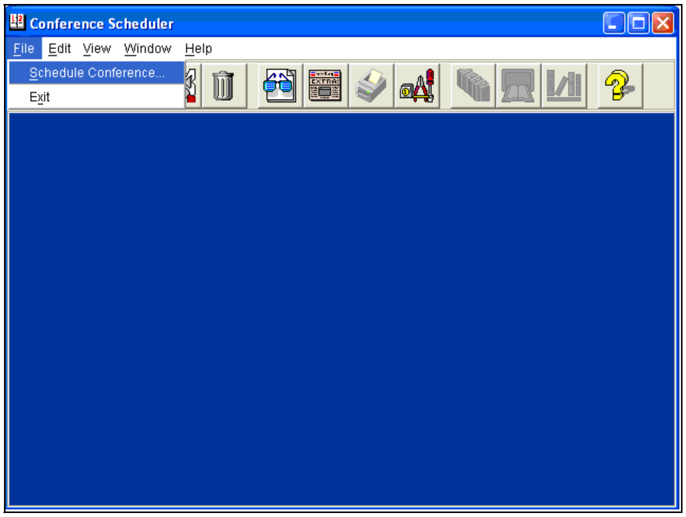
Name: Public

Optional Access Code: 000000000000

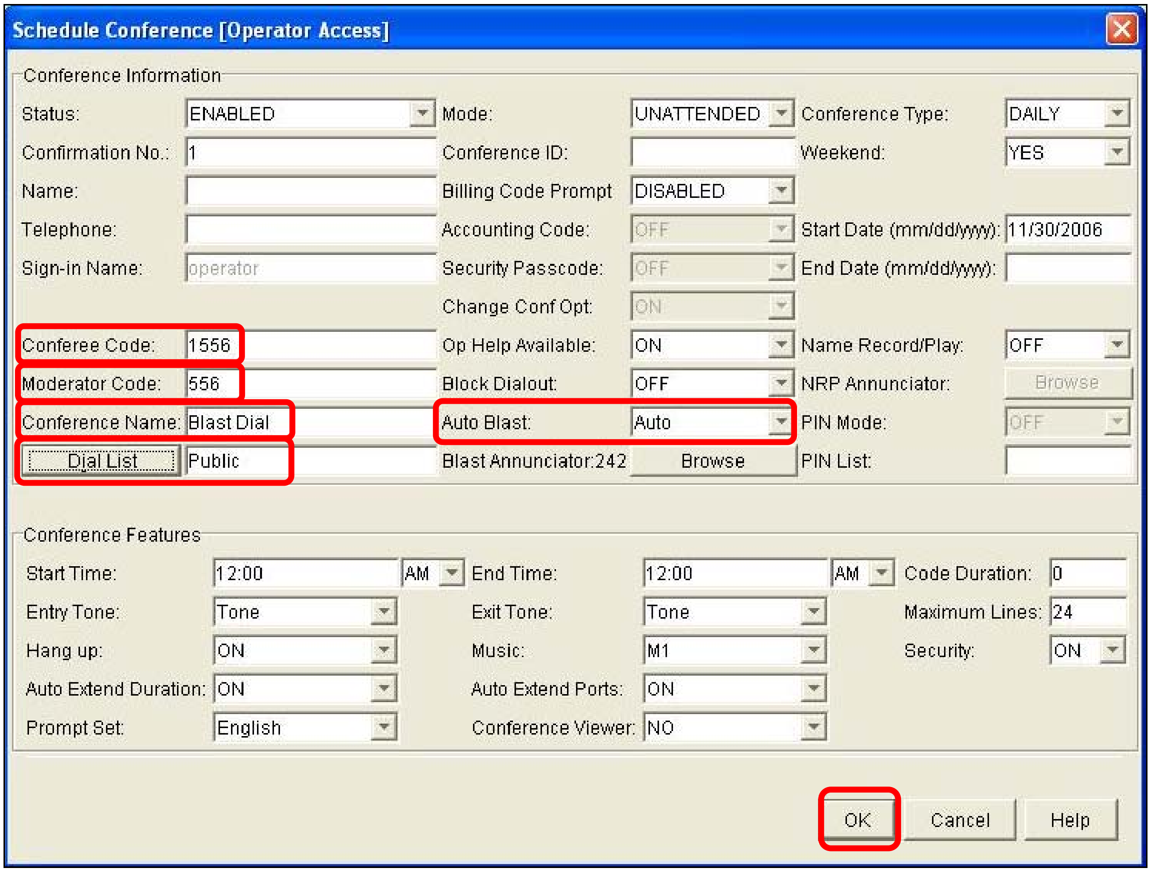
☑ Directly to Conf

☑ Display As Entered

Name	Company	Moderator	Q&A Priority	Telephone
Public56011		☐		56011
Public56012		☐		56012

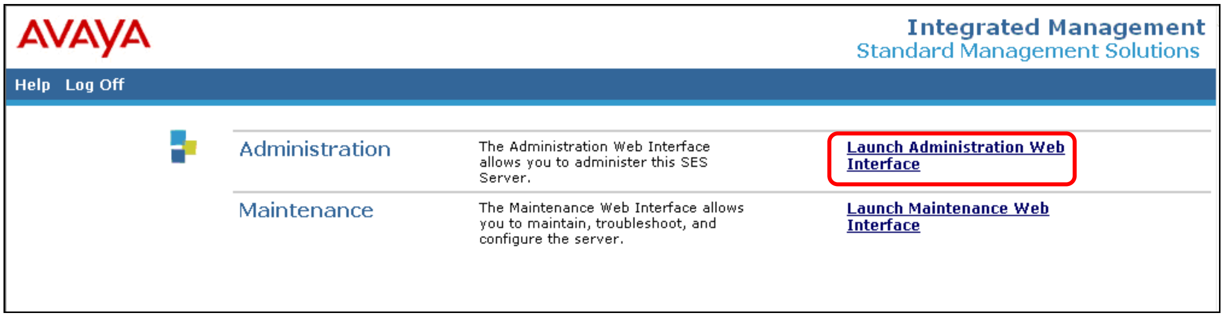
Step	Description
3.35	Provision a conference with Auto Blast enabled. From the Avaya Bridge Talk Menu Bar, click **View** ➔ **Conference Scheduler**. 
3.36	From the **Conference Scheduler** window that is displayed, click **File** ➔ **Schedule Conference**. 

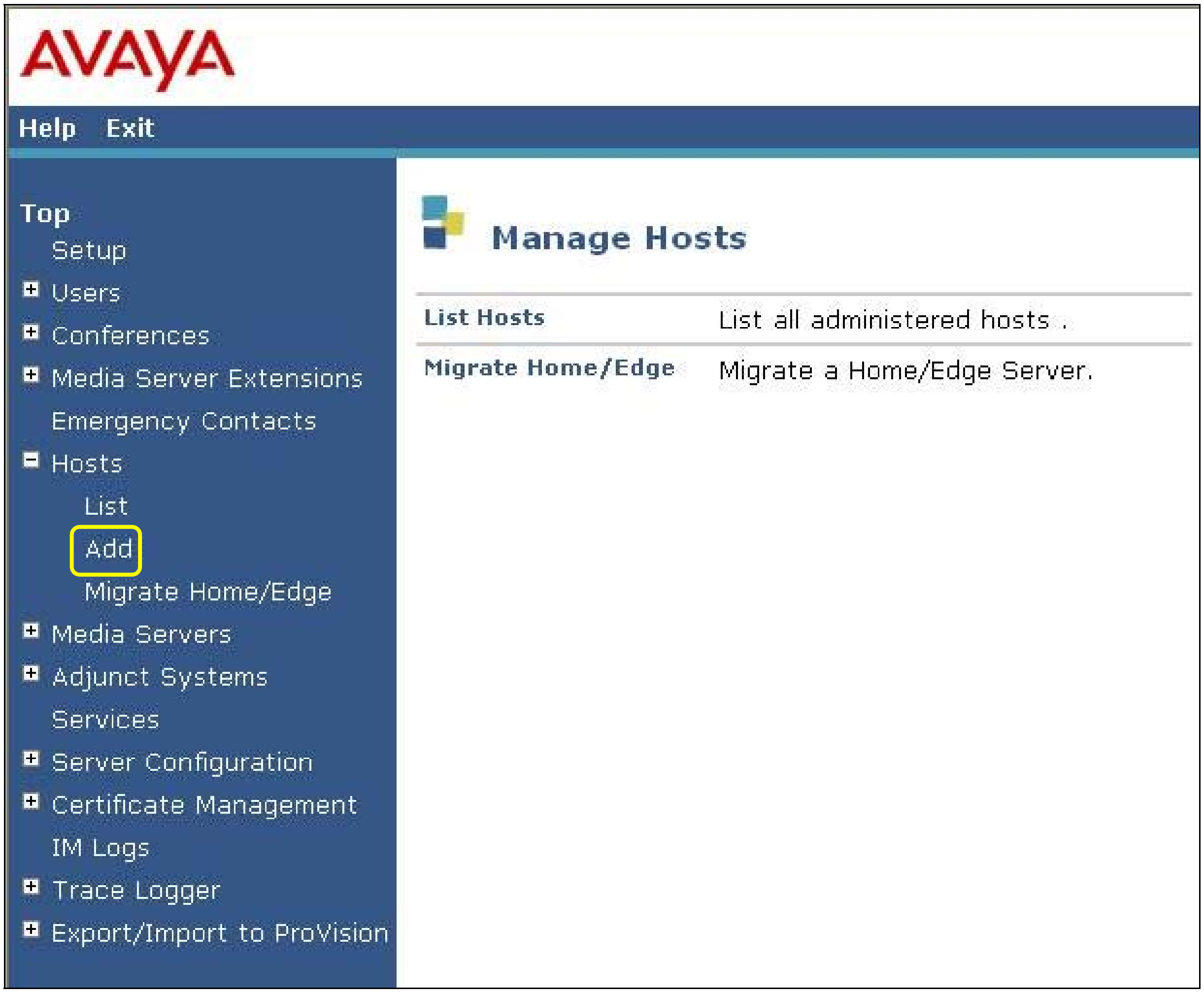
Step	Description

3.37	From the **Schedule Conference** window that is displayed, provision a conference as follows:
	• Enter a unique **Conferee Code** to allow participants access to this conference.
	• Enter a unique **Moderator Code** to allow participants access to this conference with moderator privileges. Enable moderator access without a passcode for this conference call by configuring the following:
	  ○ The **Moderator Code** "**556**" must have an associated **direct call function** provisioned for "**556**" (see **Step 3.30**).
	Note: This conference remains open for participants to enter as either moderator or participant by entering the appropriate code when prompted.
	• Enter a descriptive label in the **Conference Name** field.
	• Administer settings to enable an Auto Blast dial by setting **Auto Blast** to **Auto** and selecting the dial list provisioned in **Step 3.34**.
	  ○ [***Not Shown***] *Select a dial list by clicking on the **Dial List** button ➔ select a dial list from the **Create, Select or Edit Dial List** window that is displayed ➔ click on the **Select** button.*
	• See **Section 9**, **Reference 3** for provisioning the remaining fields in this screen.
	• When finished, click on the **OK** button on the bottom of the screen.
	
	Status: ENABLED
	Mode: UNATTENDED
	Conference Type: DAILY
	Confirmation No.: 1
	Conference ID:
	Weekend: YES
	Name:
	Billing Code Prompt: DISABLED
	Telephone:
	Accounting Code: OFF
	Start Date (mm/dd/yyyy): 11/30/2006
	Sign-in Name: operator
	Security Passcode: OFF
	End Date (mm/dd/yyyy):
	Change Conf Opt: ON
	Conferee Code: 1556
	Op Help Available: ON
	Name Record/Play: OFF
	Moderator Code: 556
	Block Dialout: OFF
	NRP Annunciator: Browse
	Conference Name: Blast Dial
	Auto Blast: Auto
	PIN Mode: OFF
	Dial List: Public
	Blast Annunciator:242 Browse
	PIN List:
	Start Time: 12:00 AM
	End Time: 12:00 AM
	Code Duration: 0
	Entry Tone: Tone
	Exit Tone: Tone
	Maximum Lines: 24
	Hang up: ON
	Music: M1
	Security: ON
	Auto Extend Duration: ON
	Auto Extend Ports: ON
	Prompt Set: English
	Conference Viewer: NO

4. Configure Avaya SIP Enablement Services

This section describes the steps for configuring Avaya SIP Enablement Services to enable SIP connectivity between the Avaya Meeting Exchange S6200 Application Server and the NexTone MSX iServer via Avaya SIP Enablement Services (see **Section 1**, **Figure 1**).

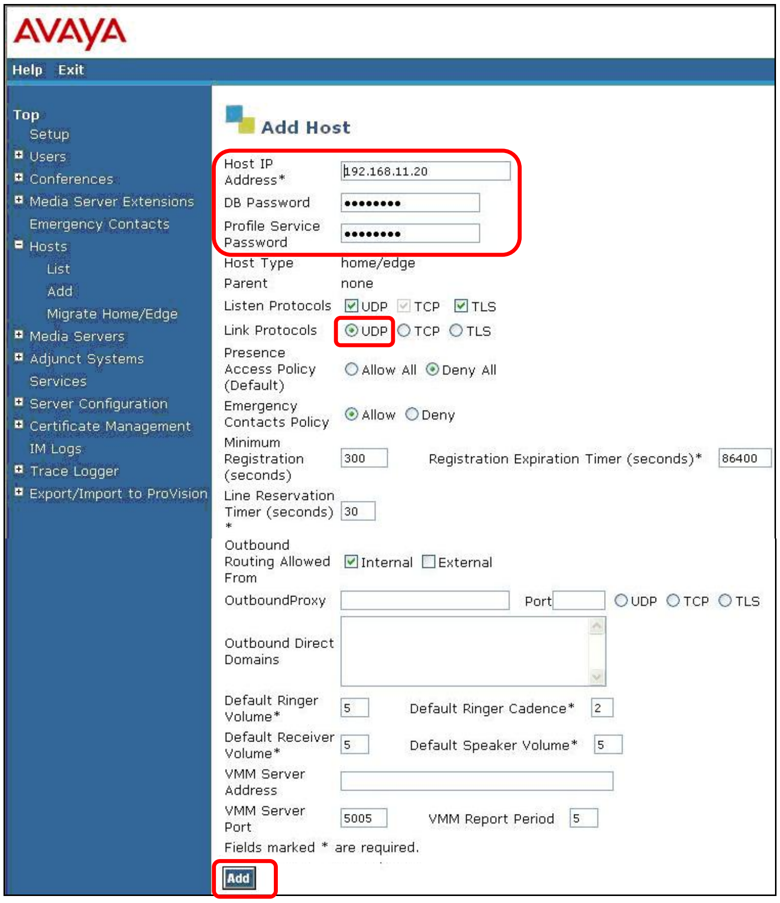
Step	Description
4.1	Administer settings for Avaya SIP Enablement Services as follows: • Open a web browser and enter the following URL: **https://<IP address of Avaya SIP Enablement Services>/admin** • Log in to Avaya SIP Enablement Services with the appropriate credentials. 
4.2	Click **Launch Administration Web Interface**.  The Administration Web Interface allows you to administer this SES Server. The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the server.

Step	Description
4.3	To enable SIP trunking between Avaya SIP Enablement Services and other SIP User Agent(s), add a host corresponding to Avaya SIP Enablement Services as follows. From the Administration Web Interface: • Click on the ⊞ icon to expand the options under **Hosts**. • Click **Add**. 

Step	Description
4.4	The **Add Host** screen is displayed.

Provision host parameters as follows:

- Enter the password assigned to the database at installation in the **DB Password** field.
- Enter a password which uniquely identifies Avaya SIP Enablement Services for intra- and inter-proxy communication in the **Profile Service Password** field.
- Select **UDP** from the available **Link Protocols**, which is consistent with the system.cfg file provisioned for the Avaya Meeting Exchange S6200 Application Server in **Step 3.2**.
- Remaining fields are default settings.
- Click on the **Add** button when finished.
    - [***Not Shown***] *Click on the* ***Continue*** *button on the confirmation screen.*
    - [***Not Shown***] *To apply the administration, click on* ***Update*** *on the left side of the screen. The* ***Update*** *link appears on the current screen whenever updates are outstanding and can be used at any time to save the administration provisioned to that point.*

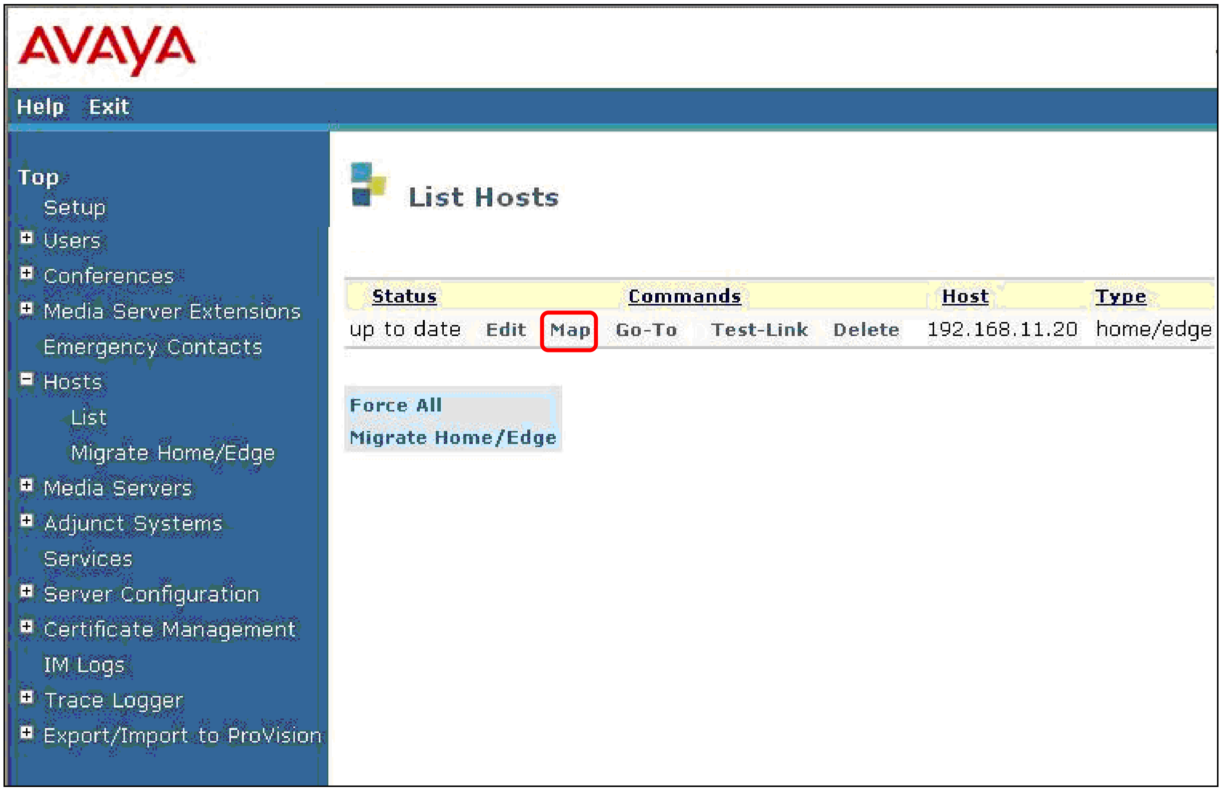


Add Host

Host IP Address*	192.168.11.20		
DB Password	••••••••		
Profile Service Password	••••••••		
Host Type	home/edge		
Parent	none		
Listen Protocols	☑ UDP ☑ TCP ☑ TLS		
Link Protocols	● UDP ○ TCP ○ TLS		
Presence Access Policy (Default)	○ Allow All ● Deny All		
Emergency Contacts Policy	● Allow ○ Deny		
Minimum Registration (seconds)	300	Registration Expiration Timer (seconds)*	86400
Line Reservation Timer (seconds) *	30		
Outbound Routing Allowed From	☑ Internal ☐ External		
OutboundProxy		Port	○ UDP ○ TCP ○ TLS
Outbound Direct Domains			
Default Ringer Volume*	5	Default Ringer Cadence*	2
Default Receiver Volume*	5	Default Speaker Volume*	5
VMM Server Address			
VMM Server Port	5005	VMM Report Period	5

Fields marked * are required.

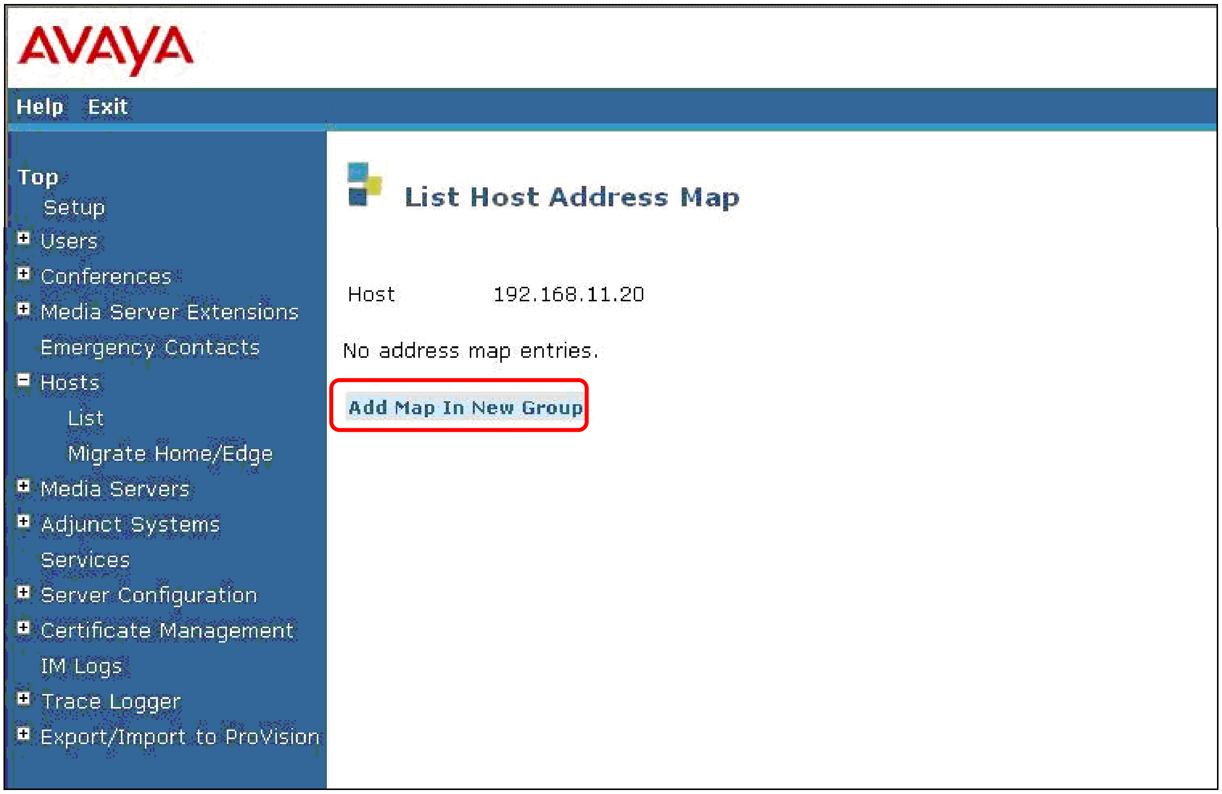
Step	Description
4.5	The **List Hosts** screen is displayed. To manage the address maps this Avaya SIP Enablement Services server uses to redirect calls to other SIP User Agent(s), select **Map** for the host provisioned in **Step 4.4**.



Status	Commands					Host	Type
up to date	Edit	Map	Go-To	Test-Link	Delete	192.168.11.20	home/edge

4.1. Enable Dial-In to the Avaya Meeting Exchange S6800 Conferencing Server

The following steps describe the administrative procedures to enable SIP trunking between Avaya SIP Enablement Services and the Avaya Meeting Exchange S6200 Application Server. This will allow Dial-In to the Avaya Meeting Exchange S6800 Conferencing Server from a public network via the NexTone MSX iServer and Avaya SIP Enablement Services (see **Section 1**, **Figure 1**).

Step	Description
4.6	The **List Host Address Map** screen is displayed. To redirect calls to the Avaya Meeting Exchange S6200 Application Server, provision a host address map for the Avaya Meeting Exchange S6200 Application Server by clicking **Add Map In New Group**. 

List Host Address Map

Host 192.168.11.20

No address map entries.

Step **Description**

4.7 The **Add Host Address Map** screen is displayed.

To match the pattern of incoming SIP INVITE messages destined for the Avaya Meeting Exchange S6200 Application Server, configure settings for the **Host Address Map** as follows:

- Enter a descriptive label in the **Name** field.
- Enter a **Pattern** that corresponds to the following:
  - The call functions provisioned for the Avaya Meeting Exchange S6200 Application Server in **Step 3.29** and **Step 3.30**.
  - The **Calling Plan Route** to the private network provisioned for the NexTone MSX iServer in **Step 5.29**.

  Note*: The* ***Pattern****,* ***^sip:[5][05][0-9]{1}*** *matches the string* ***sip:5*** *(if it occurs at the beginning of the URI), followed by either a* ***0*** *or a* ***5****; then* ***1*** *more digit in the range* ***0*** *through* ***9****.*
- Select **Replace URI** to indicate that the pattern above should be resolved and forwarded by the host shown.
- Click on the **Add** button when finished.
  - [***Not Shown***] *Click on the* ***Continue*** *button on the confirmation screen.*

Add Host Address Map

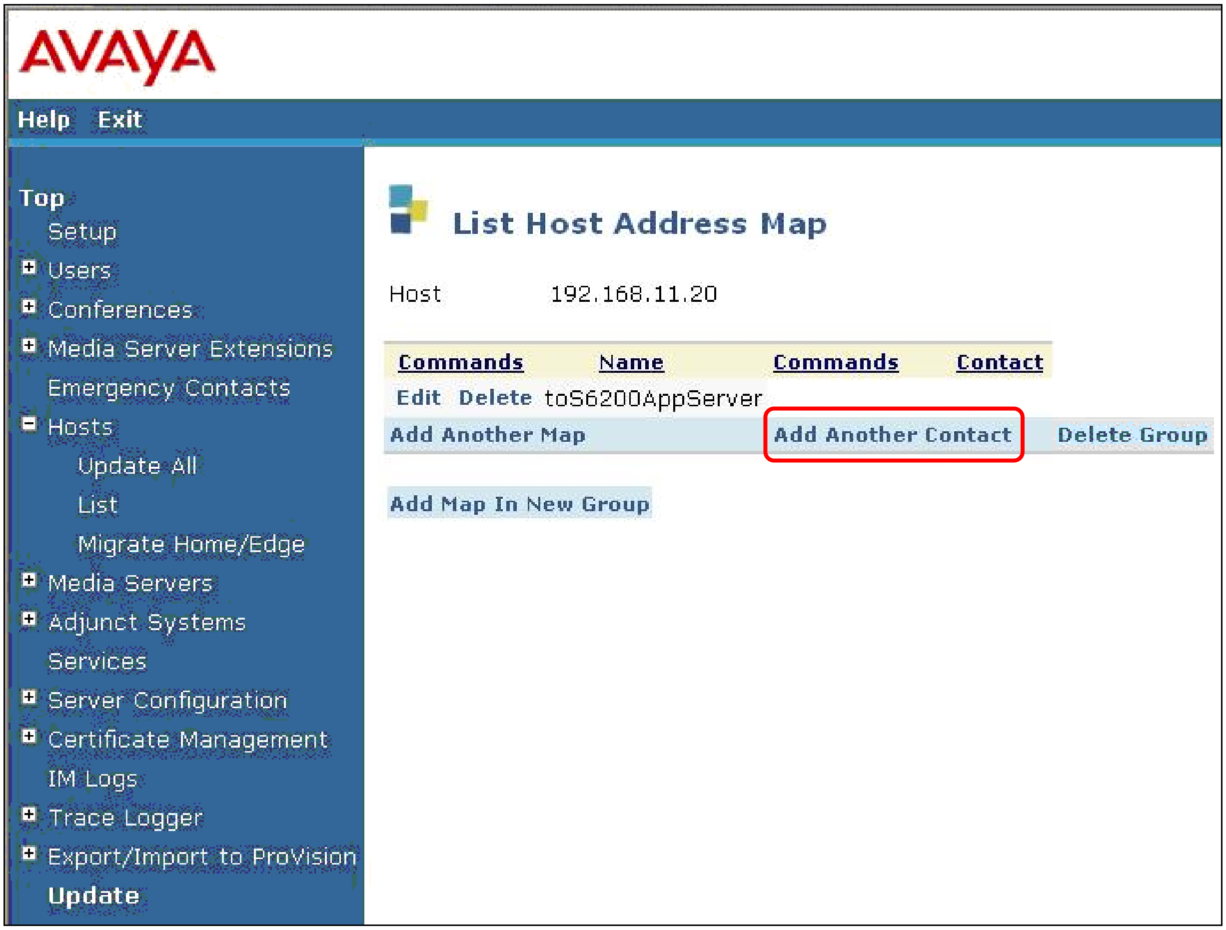
Host 192.168.11.20

Name* toS6200AppServer

Pattern* ^sip:[5][05][0-9]{1}

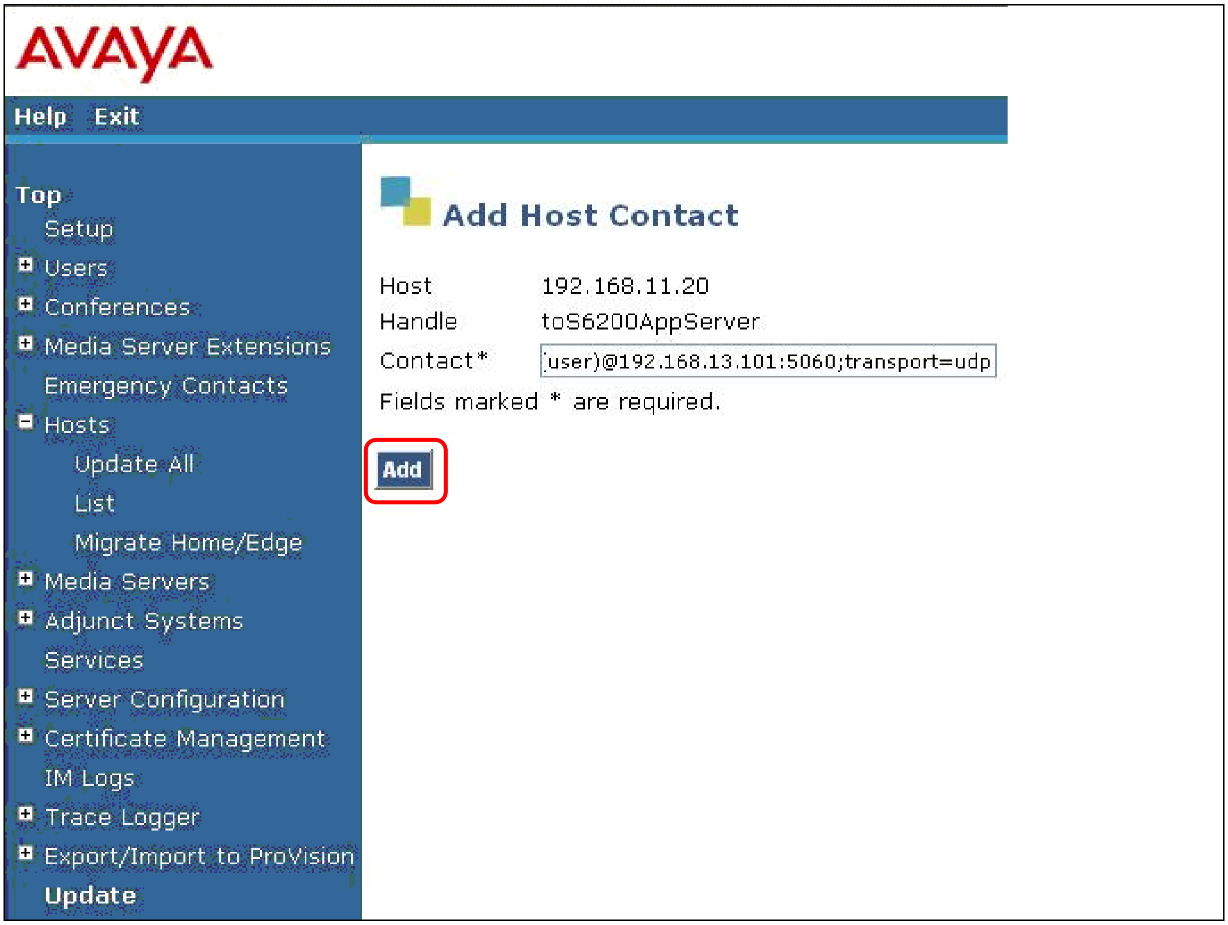
Replace URI ☑

Fields marked * are required.

Step	Description
4.8	The **List Host Address Map** screen is displayed. To specify the contact information for the SIP User Agent that calls are to be redirected to, click on **Add Another Contact** for the address map defined in **Step 4.7**. 

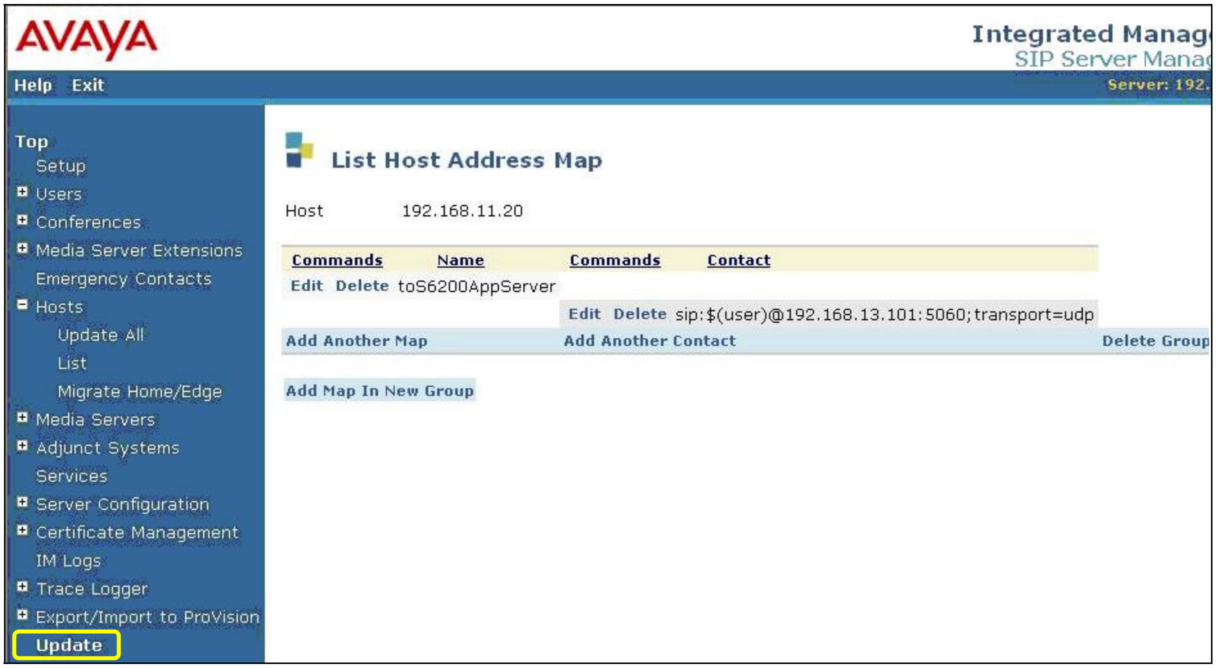
Host 192.168.11.20

Commands	Name	Commands	Contact
Edit Delete	toS6200AppServer		

Step	Description
4.9	The **Add Host Contact** screen is displayed. • To enable SIP connectivity to the Avaya Meeting Exchange S6200 Application Server, enter **sip:$(user)@192.168.13.101:5060;transport=udp** in the **Contact** field. *__Note__: The IP address, port number and transport protocol are consistent with the system.cfg file provisioned for the Avaya Meeting Exchange S6200 Application Server in __Step 3.2__. Avaya SIP Enablement Services substitutes "__$(user)__" with the user field (i.e., the dialed number) in the incoming SIP INVITE message.* • Click on the **Add** button when finished. ○ [***Not Shown***] *Click on the **Continue** button on the confirmation screen.*  Add Host Contact Host 192.168.11.20 Handle toS6200AppServer Contact* user)@192.168.13.101:5060;transport=udp Fields marked * are required.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.10</td><td>
The List Host Address Map screen is displayed.

The host contact is added to the host address map group. To apply the administration in the above steps, click on Update on the left side of the screen.



List Host Address Map

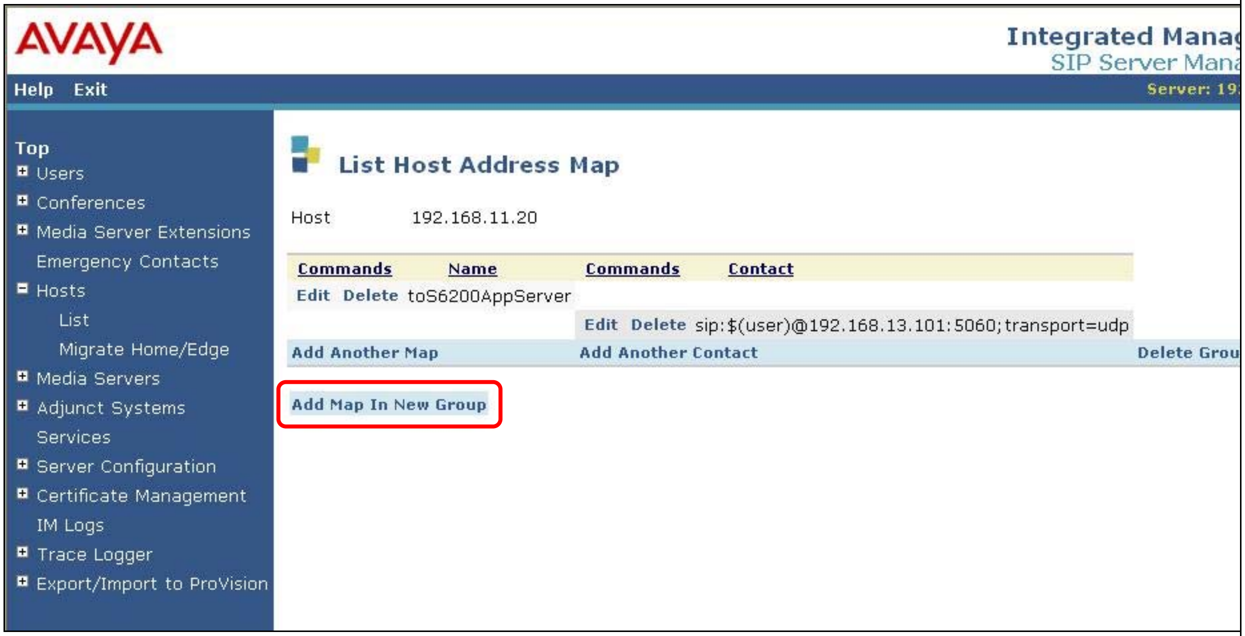
Host 192.168.11.20

<table>
<tr><th>Commands</th><th>Name</th><th>Commands</th><th>Contact</th></tr>
<tr><td>Edit Delete</td><td>toS6200AppServer</td><td></td><td></td></tr>
<tr><td></td><td></td><td>Edit Delete</td><td>sip:$(user)@192.168.13.101:5060;transport=udp</td></tr>
</table>

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

4.2. Enable Dial-Out from the Avaya Meeting Exchange S6800 Conferencing Server

The following steps describe the administrative procedures to enable SIP trunking between Avaya SIP Enablement Services and the NexTone MSX iServer. This will allow Dial-Out from the Avaya Meeting Exchange S6800 Conferencing Server to a public network via Avaya SIP Enablement Services and the NexTone MSX iServer (see **Section 1**, **Figure 1**).

Step	Description
4.11	The **List Host Address Map** screen is displayed. To redirect calls to the NexTone MSX iServer, provision a host address map for the NexTone MSX iServer by clicking **Add Map In New Group**. 

Host 192.168.11.20

Commands	Name	Commands	Contact
Edit Delete	toS6200AppServer		
		Edit Delete	sip:$(user)@192.168.13.101:5060;transport=udp

Step	Description
4.12	The **Add Host Address Map** screen is displayed.

To match the pattern of incoming SIP INVITE messages destined for the NexTone MSX iServer, configure settings for the **Host Address Map** as follows:

- Enter a descriptive label in the **Name** field.
- Enter a **Pattern** that corresponds to the following:
  - The **telnumToUri.tab** file provisioned for the Avaya Meeting Exchange S6200 Application Server in **Step 3.4**.
  - The **Calling Plan Route** to the public network provisioned for the NexTone MSX iServer in **Step 5.28**.

  Note: *The* ***Pattern***, *^****sip:[5][6][0-9]{3}*** *matches the string* ***sip:5*** *(if it occurs at the beginning of the URI), followed by either a* ***0*** *or a* ***5****; then* ***1*** *more digit in the range* ***0*** *through* ***9****.*
- Select **Replace URI** to indicate that the pattern above should be resolved and forwarded by the host shown.
- Click on the **Add** button when finished.
  - [***Not Shown***] *Click on the* ***Continue*** *button on the confirmation screen.*

Add Host Address Map

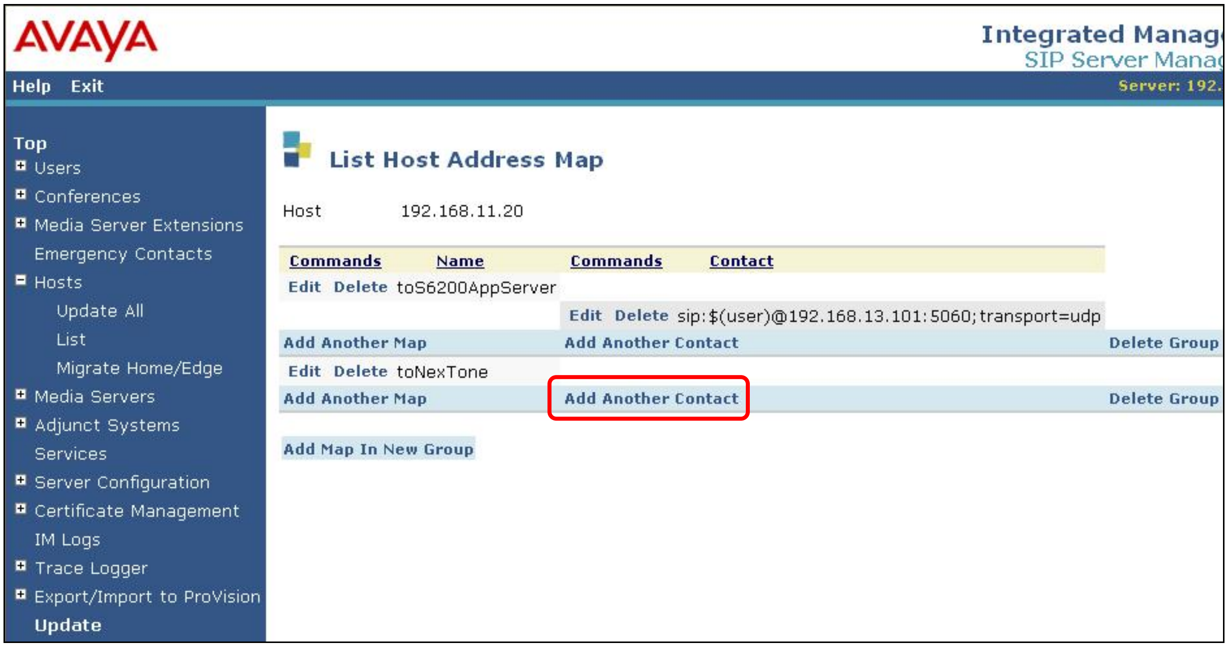
Host 192.168.11.20

Name* toNexTone

Pattern* ^sip:[5][6][0-9]{3}

Replace URI ☑

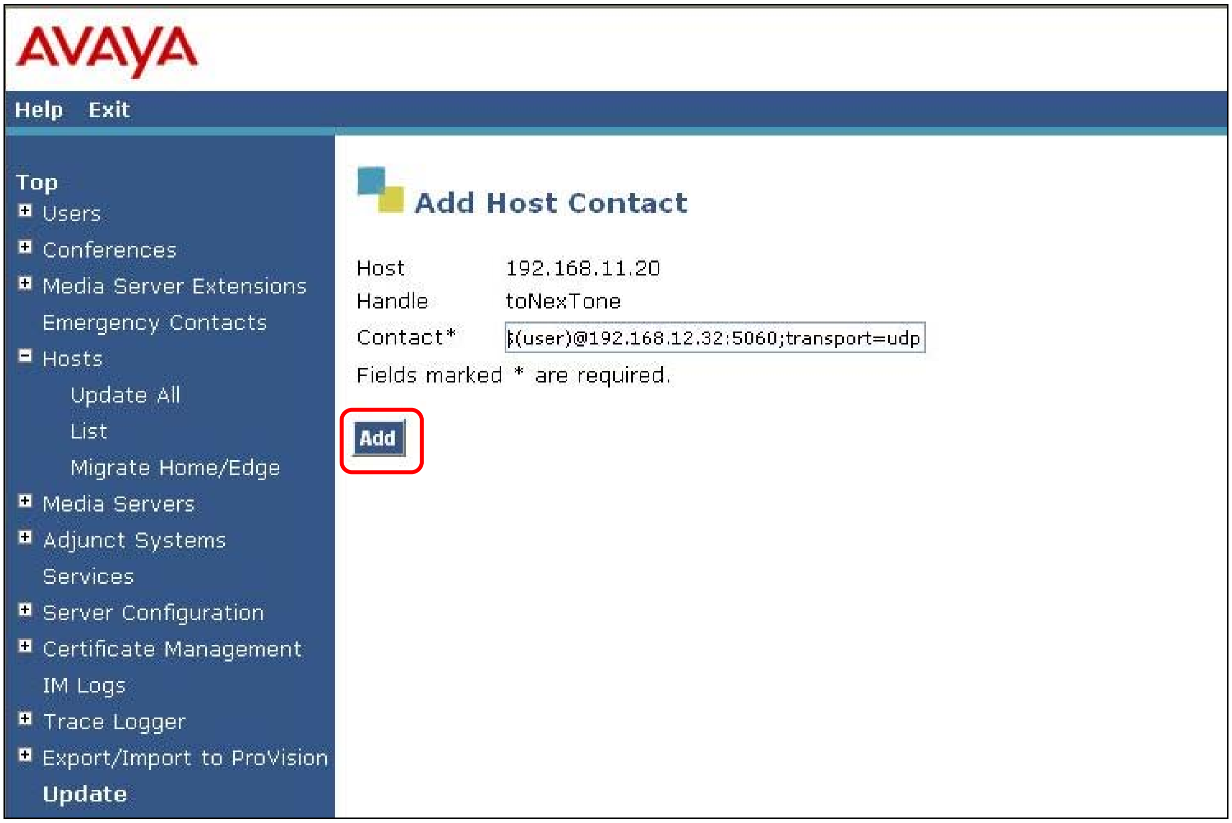
Fields marked * are required.

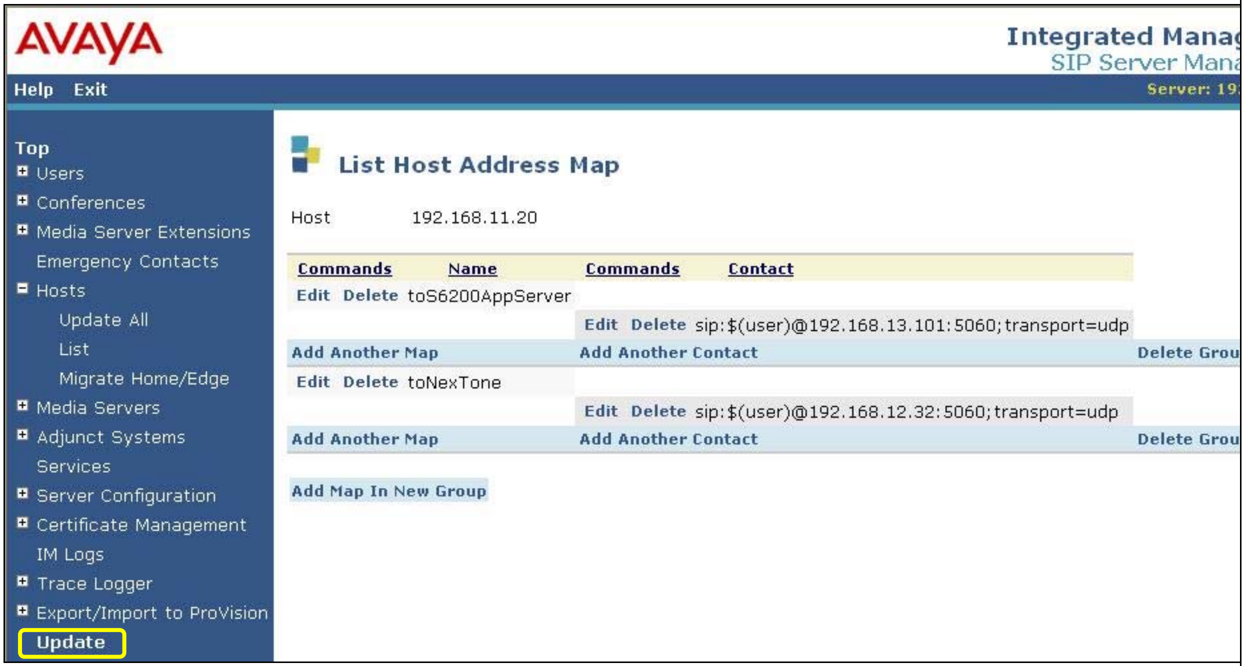
Step	Description
4.13	The **List Host Address Map** screen is displayed. To specify the contact information for the SIP User Agent that calls are to be redirected to, click on **Add Another Contact** for the address map defined in **Step 4.12**. 

List Host Address Map

Host 192.168.11.20

Commands	Name	Commands	Contact
Edit Delete	toS6200AppServer		
		Edit Delete	sip:$(user)@192.168.13.101:5060;transport=udp
Edit Delete	toNexTone		

Step	Description
4.14	The **Add Host Contact** screen is displayed. - To enable SIP connectivity to the private signaling interface (defined in **Step 5.49**) on the NexTone MSX iServer, enter **sip:$(user)@192.168.12.32:5060;transport=udp** in the **Contact** field. *__Note__: The IP address, port number and transport protocol are consistent with the requirements defined by the NexTone MSX iServer (see __Section 9__, __Reference 4__). Avaya SIP Enablement Services substitutes "__$(user)__" with the user field (i.e., the dialed number) in the incoming SIP INVITE message.* - Click on the **Add** button when finished. ○ [***Not Shown***] *Click on the __Continue__ button on the confirmation screen.*  Add Host Contact Host 192.168.11.20 Handle toNexTone Contact* $(user)@192.168.12.32:5060;transport=udp Fields marked * are required.

Step	Description
4.15	The **List Host Address Map** screen is displayed. The host contact is added to the host address map group. To apply the administration in the above steps, click on **Update** on the left side of the screen. 

List Host Address Map

Host 192.168.11.20

Commands	Name	Commands	Contact	
Edit Delete	toS6200AppServer			
		Edit Delete	sip:$(user)@192.168.13.101:5060;transport=udp	
Add Another Map		Add Another Contact		Delete Grou
Edit Delete	toNexTone			
		Edit Delete	sip:$(user)@192.168.12.32:5060;transport=udp	
Add Another Map		Add Another Contact		Delete Grou

Add Map In New Group

Step	Description

4.16 Add the Avaya Meeting Exchange S6200 Application Server as a **trusted host** on Avaya SIP Enablement Services.

All SIP User Agent(s), proxie(s) and/or gateway(s) to which calls can be routed should be administered as trusted host(s) on Avaya SIP Enablement Services. This permits call setup and termination by remote parties to be handled without authentication challenges to a trusted host. This is provisioned at the Avaya SIP Enablement Services command line of the edge server (or as per these Application Notes, at the edge/home server, if only one server is used).

- Log in to the Avaya SIP Enablement Services console with the appropriate credentials.
- Add the Avaya Meeting Exchange S6200 Application Server as a trustedhost by entering the following command:
  trustedhost -a trusted-host-IP-address -n trusting-SES-IP-address [-c 'comment text']

```
SES->trustedhost –a 192.168.13.101 –n 192.168.11.20 –c S6200App
```

- Repeat the **trustedhost –a** command to add the private signaling interface on the NexTone MSX iServer (see **Step 5.49**) as a trusted host.
  Note*: This interface “connected” to Avaya SIP Enablement Services*.
- Verify trusted host entries by entering the following command: **trustedhost -L**

```
SES-> trustedhost -L
Third party trusted hosts.
 Trusted Host IP address  |   SES Host IP address      |         Comment
--------------------------+----------------------------+-------------------------
192.168.13.101            | 192.168.11.20              | S6200App
192.168.12.32             | 192.168.11.20              | NexToneSig
```

4.17 To apply the administration defined in Step **4.16**:

- Open the web browser interface.
- Click on **Update** on the left side of the screen.

5. Configure the NexTone MSX iServer

This section describes how to configure the NexTone MSX iServer to interoperate with a public network and a private network containing the Avaya Meeting Exchange S6800 Conferencing Server and Avaya SIP Enablement Services.

5.1. Configure the Management Interface

The following steps describe the administrative procedures for configuring the management interface (Eth0) on the NexTone MSX iServer. Best practice is to place the management interface to the NexTone MSX iServer on a network reserved for "management" on the private network.

Step	Description
5.1	Provision the management interface (Eth0) on the NexTone MSX iServer as follows: • Establish a connection from a services PC to Eth5 on the NexTone MSX iServer (see **Section 1**, **Figure 3**). In the current version of the NexTone MSX iServer, Eth5 is unused and may be utilized for a console connection to provision initial configuration on the NexTone MSX iServer. o The default IP address/netmask for Eth5 is 10.1.1.1/24. • Log in to the NexTone MSX iServer console to access the CLI with the appropriate credentials.
5.2	From the CLI, enter the command **ifconfig -a** to obtain the **HWaddr** (MAC address) of **Eth0**.

```
nextone-msw:~ # ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0E:0C:77:F9:42
          inet addr:192.168.12.50  Bcast:192.168.12.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe77:f942/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13096 errors:0 dropped:0 overruns:0 frame:0
          TX packets:227757 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1289451 (1.2 Mb)  TX bytes:16329158 (15.5 Mb)
          Base address:0x2440 Memory:fe1a0000-fe1c0000
```

Step	Description
5.3	From the CLI, enter the command **allstat** to verify status of processes running on the NexTone MSX iServer. Updating the management interface via the yast utility described in steps starting at **Step 5.6** requires that no processes are running on the NexTone MSX iServer. ***Note****: For brevity, some information is omitted from the screen capture of the* ***allstat*** *command.*

```
nextone-msw:~ # allstat
/usr/local/nextone/bin ~

Process Status:
---------------
  PID TTY      STAT   TIME  MAJFL   TRS   DRS  RSS %MEM COMMAND
11895 pts/1    S<     0:01      0  4295 823964 503676 12.1 gis
11880 pts/1    S<     0:00      0   174 14085  912  0.0 execd
11859 pts/1    S<     0:01      1    42 567537 320868  7.7 java
11809 pts/1    S<     0:00      0   183  2792  848  0.0 pm

NexTone Configuration Server Additional Status:
-----------------------------------------------
Java Version: 1.4.2_11 (Sun Microsystems Inc. 1.4.2_11-b06[Java HotSpot(TM) Server
VM])
Current active user threads: 9
Memory Statistics:
Total: 33488896  Free: 32952992  Used: 535904

Log file: "/var/tmp/jserverlogfile"
Read password string:  ""
Write password string: ""
Compression: off

Server Uptimes:
---------------
Uptime for: NexTone Process Manager v4.0c3-18, 10-13-2006
        1 minute, 20 seconds, 65 milliseconds
Uptime for: NexTone Configuration Server v4.0c3-18, 10-13-2006
        1 minute, 19 seconds, 389 milliseconds
Uptime for: NexTone GIS Directory Server v4.0c3-18, 10-13-2006
        1 minute, 18 seconds, 894 milliseconds
```

Step	Description
5.4	Enter the command **allstop** to stop processes on the NexTone MSX iServer.

```
nextone-msw:~ # allstop
/usr/local/nextone/bin ~
Stopping NexTone Process Manager, pid=[11809].

Stopping NexTone Configuration Server, pid=[11859].
Stopping NexTone GIS Directory Server, pid=[11895].

Stopping NexTone Cmd Execution Server, pid=[11880].
```

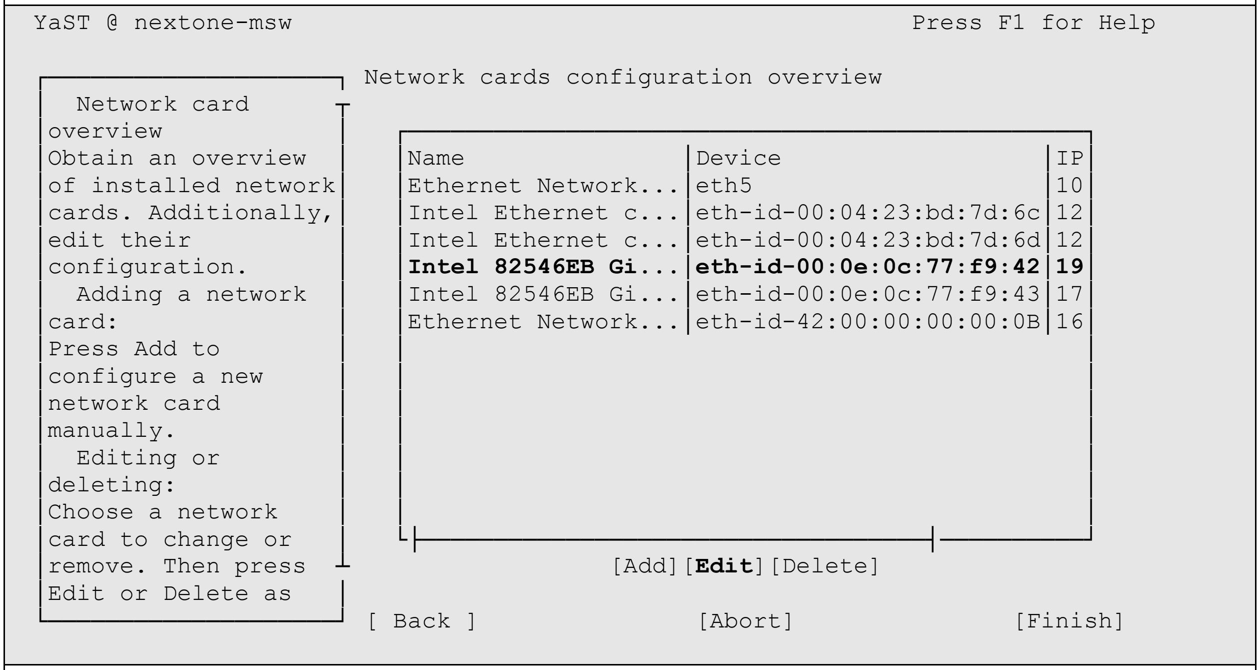
Step	Description
5.5	From the CLI, enter the command **allstat** to verify no processes are running on the NexTone MSX iServer.

```
nextone-msw:~ # allstat
/usr/local/nextone/bin ~
pm: No such process
execd: No such process
gis: No such process
iServer not running
```

Step	Description
5.6	From the CLI, enter **yast lan** to edit the interface for management network (Eth0); then <Tab> to **Change...** and press <Enter>.

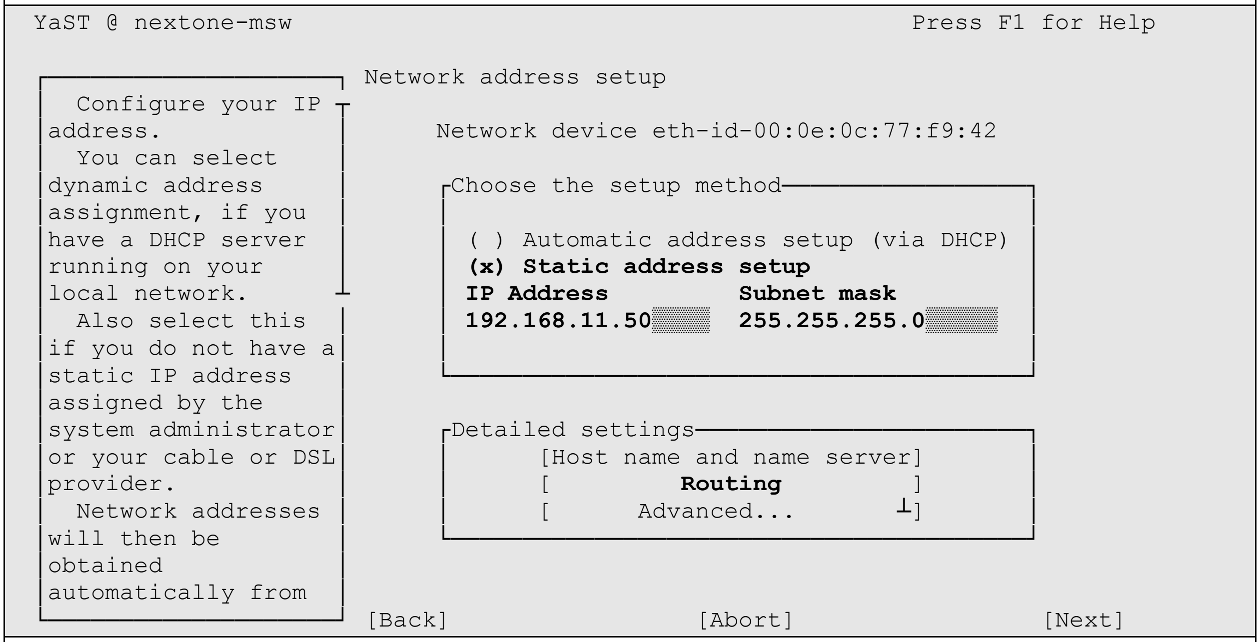
```
nextone-msw:~ # yast lan

 YaST @ nextone-msw                                          Press F1 for Help

┌────────────────────┐ Network cards configuration
│  Network card setup┬   ┌Network cards to configure──────────────────┐
│                    │   │┌Available are:───────────────────────────┐│
│Configure your      │   ││Intel Ethernet controller                ││
│network card here.  │   ││Intel Ethernet controller                ││
│  Adding a network  │   ││Other (not detected)                     ││
│card:               │   ││                                         ││
│Choose a network    │   ││                                         ││
│card from the list  │   │└─────────────────────────────────────────┘│
│of detected network │   │                             [Configure...]│
│cards. If your      │   └───────────────────────────────────────────┘
│network card was not│
│autodetected, select│   ┌───────────────────────────────────────────┐
│Other (not detected)│   │Already configured devices:                I
│then press Configure│   │ *  Ethernet Network Card                  │
│.                   ┴   │    Configured with Address 10.1.1.1       │
│  Editing or        │   │ *  Intel Ethernet controller              │
│Deleting:           │   │    Configured with Address 127.1.1.2      │
│If you press Change,│   └───────────────────────────────────────────┘
│an additional dialog│                                         [Change...]
└────────────────────┘ [ Back ]              [Abort]              [Finish]
```

Step	Description
5.7	From the CLI, select the entry with the MAC address obtained (from the ifconfig –a command) in **Step 5.2** (**eth-id-00:0e:0c:77:f9:42**); then <Tab> to **Edit** and press <Enter>.



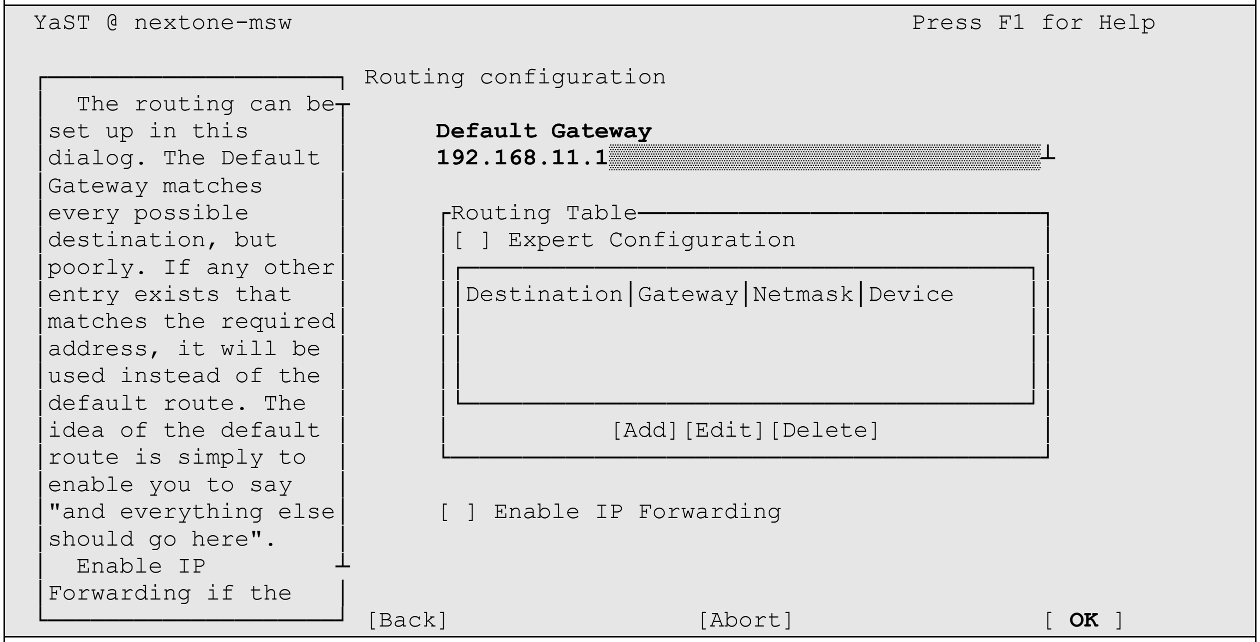
```
 YaST @ nextone-msw                                          Press F1 for Help

┌─────────────────────┐ Network cards configuration overview
│  Network card       ┬
│overview             │
│Obtain an overview   │   ┌────────────────────────────────────────────────┐
│of installed network│   │Name                │Device                   │IP│
│cards. Additionally,│   │Ethernet Network...│eth5                     │10│
│edit their           │   │Intel Ethernet c...│eth-id-00:04:23:bd:7d:6c│12│
│configuration.       │   │Intel Ethernet c...│eth-id-00:04:23:bd:7d:6d│12│
│  Adding a network   │   │Intel 82546EB Gi...│eth-id-00:0e:0c:77:f9:42│19│
│card:                │   │Intel 82546EB Gi...│eth-id-00:0e:0c:77:f9:43│17│
│Press Add to         │   │Ethernet Network...│eth-id-42:00:00:00:00:0B│16│
│configure a new      │   │                                                │
│network card         │   │                                                │
│manually.            │   │                                                │
│  Editing or         │   │                                                │
│deleting:            │   │                                                │
│Choose a network     │   │                                                │
│card to change or    │   └├────────────────────────────────────┤───────────┘
│remove. Then press   ┴              [Add][Edit][Delete]
│Edit or Delete as    │
└─────────────────────┘ [ Back ]               [Abort]               [Finish]
```

Step	Description
5.8	From the CLI, select **Static address setup** and enter an **IP Address** and **Subnet mask** for the management interface; then <Tab> to **Routing** and press <Enter>.



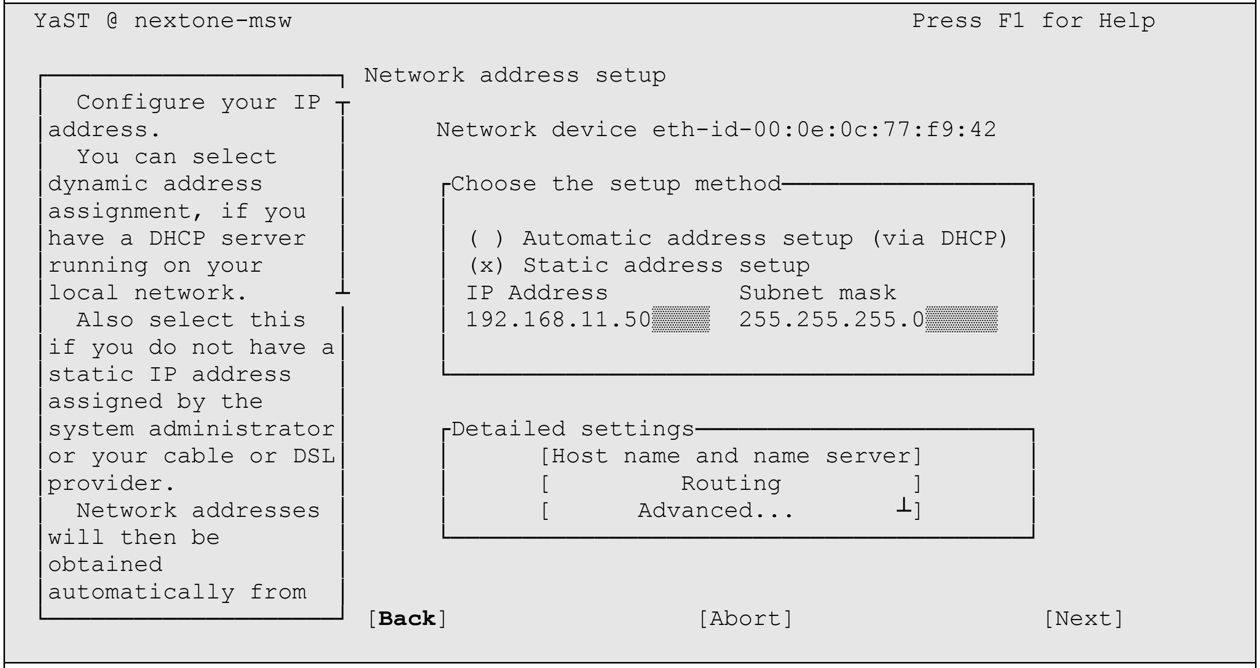
```
 YaST @ nextone-msw                                               Press F1 for Help

┌────────────────────┐ Network address setup
│  Configure your IP ┬
│address.            │     Network device eth-id-00:0e:0c:77:f9:42
│  You can select    │
│dynamic address     │     ┌Choose the setup method───────────────────┐
│assignment, if you  │     │                                          │
│have a DHCP server  │     │ ( ) Automatic address setup (via DHCP)   │
│running on your     │     │ (x) Static address setup                 │
│local network.      ┴     │ IP Address          Subnet mask          │
│  Also select this  │     │ 192.168.11.50       255.255.255.0        │
│if you do not have a│     │                                          │
│static IP address   │     └──────────────────────────────────────────┘
│assigned by the     │
│system administrator│     ┌Detailed settings─────────────────────────┐
│or your cable or DSL│     │      [Host name and name server]         │
│provider.           │     │      [          Routing        ]         │
│  Network addresses │     │      [      Advanced...       ┴]         │
│will then be        │     └──────────────────────────────────────────┘
│obtained            │
│automatically from  │
└────────────────────┘ [Back]                 [Abort]                 [Next]
```

5.9	From the CLI, enter a **Default Gateway**; then <Tab> to **OK** and press <Enter>.



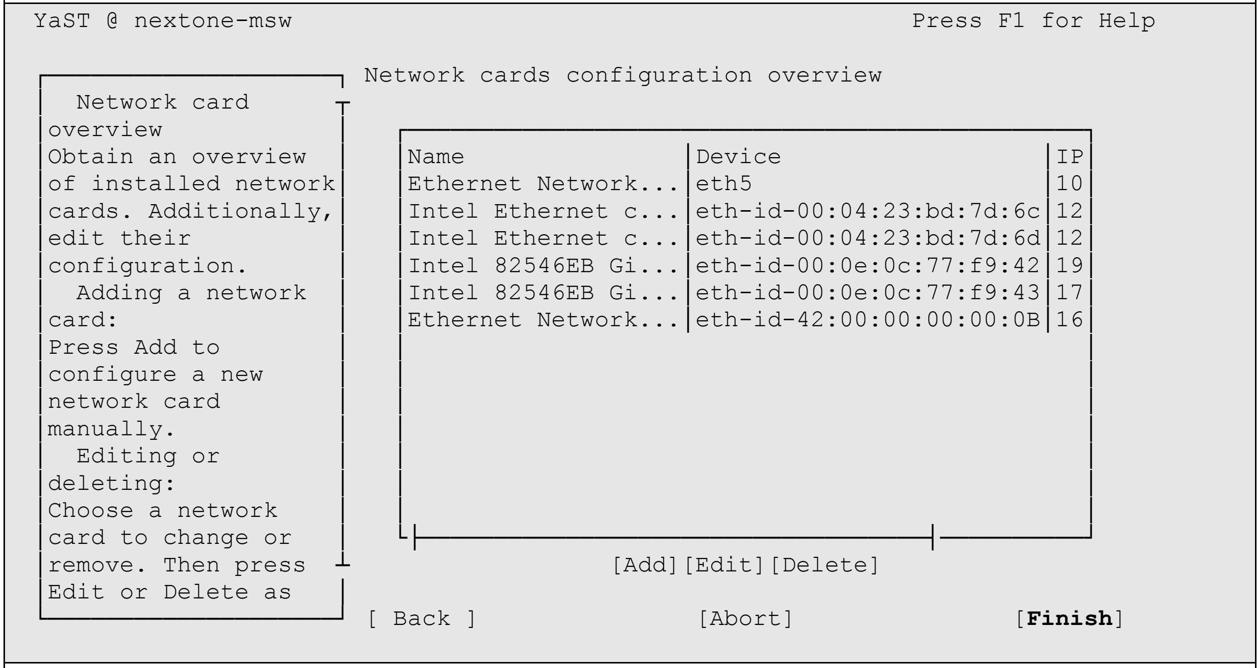
```
 YaST @ nextone-msw                                               Press F1 for Help

┌────────────────────┐ Routing configuration
│  The routing can be┬
│set up in this      │     Default Gateway
│dialog. The Default │     192.168.11.1                              ┴
│Gateway matches     │
│every possible      │     ┌Routing Table─────────────────────────────┐
│destination, but    │     │[ ] Expert Configuration                  │
│poorly. If any other│     │                                          │
│entry exists that   │     │ ┌──────────────────────────────────────┐ │
│matches the required│     │ │Destination│Gateway│Netmask│Device    │ │
│address, it will be │     │ │                                      │ │
│used instead of the │     │ │                                      │ │
│default route. The  │     │ └──────────────────────────────────────┘ │
│idea of the default │     │          [Add][Edit][Delete]             │
│route is simply to  │     └──────────────────────────────────────────┘
│enable you to say   │
│"and everything else│     [ ] Enable IP Forwarding
│should go here".    │
│  Enable IP         ┴
│Forwarding if the   │
└────────────────────┘ [Back]                 [Abort]                 [ OK ]
```

Step	Description
5.10	From the CLI, <Tab> to **Back** and press <Enter>.



```
 YaST @ nextone-msw                                            Press F1 for Help

 ┌────────────────────┐ Network address setup
 │  Configure your IP ┬
 │address.            │    Network device eth-id-00:0e:0c:77:f9:42
 │  You can select    │
 │dynamic address     │   ┌Choose the setup method────────────────┐
 │assignment, if you  │   │                                        │
 │have a DHCP server  │   │ ( ) Automatic address setup (via DHCP) │
 │running on your     │   │ (x) Static address setup               │
 │local network.      ┴   │ IP Address          Subnet mask        │
 │  Also select this  │   │ 192.168.11.50▒▒▒▒   255.255.255.0▒▒▒▒▒ │
 │if you do not have a│   │                                        │
 │static IP address   │   └────────────────────────────────────────┘
 │assigned by the     │
 │system administrator│   ┌Detailed settings──────────────────────┐
 │or your cable or DSL│   │      [Host name and name server]       │
 │provider.           │   │      [         Routing         ]       │
 │  Network addresses │   │      [      Advanced...       ┴]       │
 │will then be        │   └────────────────────────────────────────┘
 │obtained            │
 │automatically from  │
 └────────────────────┘ [Back]                [Abort]                [Next]
```

Step	Description
5.11	From the CLI, <Tab> to **Finish** and press <Enter>.



```
 YaST @ nextone-msw                                            Press F1 for Help

 ┌────────────────────┐ Network cards configuration overview
 │  Network card      ┬
 │overview            │  ┌──────────────────────────────────────────────────┐
 │Obtain an overview  │  │Name                │Device                 │IP  │
 │of installed network│  │Ethernet Network... │eth5                   │10  │
 │cards. Additionally,│  │Intel Ethernet c... │eth-id-00:04:23:bd:7d:6c│12 │
 │edit their          │  │Intel Ethernet c... │eth-id-00:04:23:bd:7d:6d│12 │
 │configuration.      │  │Intel 82546EB Gi... │eth-id-00:0e:0c:77:f9:42│19 │
 │  Adding a network  │  │Intel 82546EB Gi... │eth-id-00:0e:0c:77:f9:43│17 │
 │card:               │  │Ethernet Network... │eth-id-42:00:00:00:00:0B│16 │
 │Press Add to        │  │                                                  │
 │configure a new     │  │                                                  │
 │network card        │  │                                                  │
 │manually.           │  │                                                  │
 │  Editing or        │  │                                                  │
 │deleting:           │  │                                                  │
 │Choose a network    │  │                                                  │
 │card to change or   │  └┤────────────────────────────────────┤────────────┘
 │remove. Then press  ┴              [Add][Edit][Delete]
 │Edit or Delete as   │
 └────────────────────┘ [ Back ]              [Abort]              [Finish]
```

Step	Description
5.12	From the CLI, verify that the **/usr/local/nextone/bin/server.cfg** file utilizes the management IP address provisioned in **Step 5.8**. If not, edit the file with a text editor, (e.g., vi) to make the update. ***Note****: For brevity, some information is omitted from the screen capture of the* ***/usr/local/nextone/bin/server.cfg*** *file.*

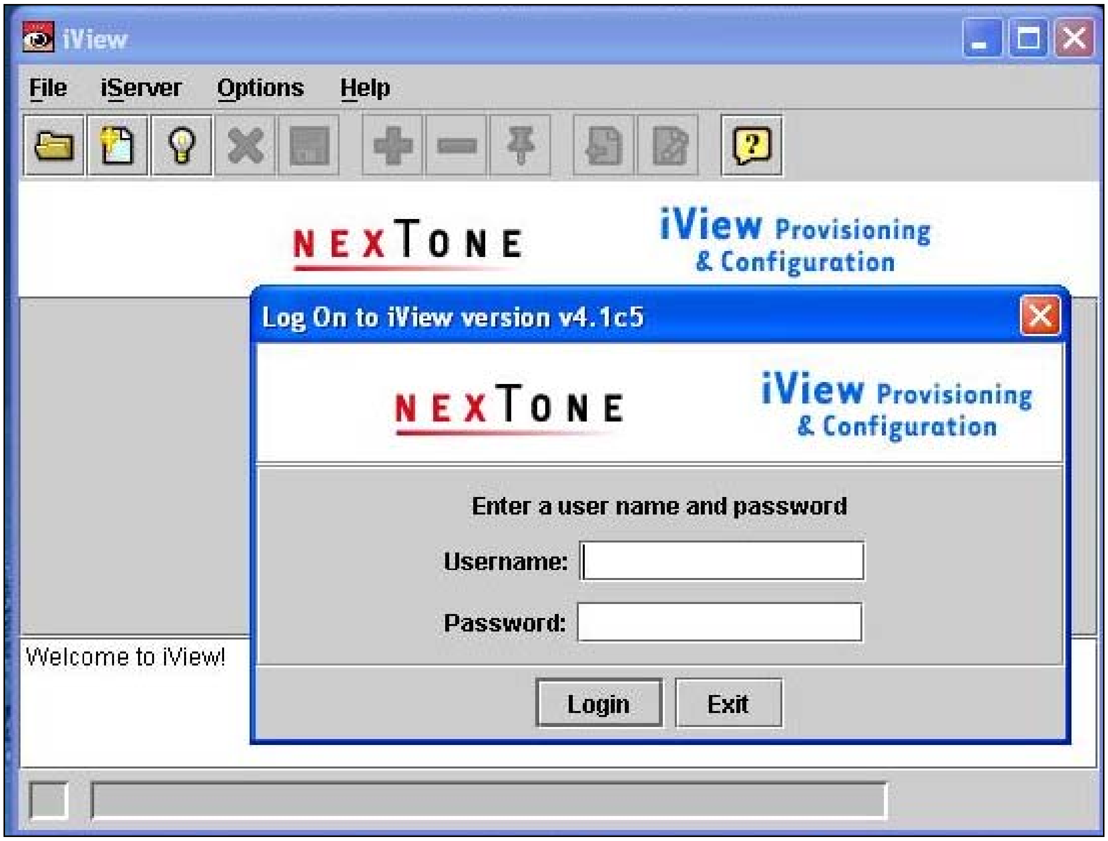
```
mgmt_interface {
        mgmt_ip "192.168.11.50"
}
```

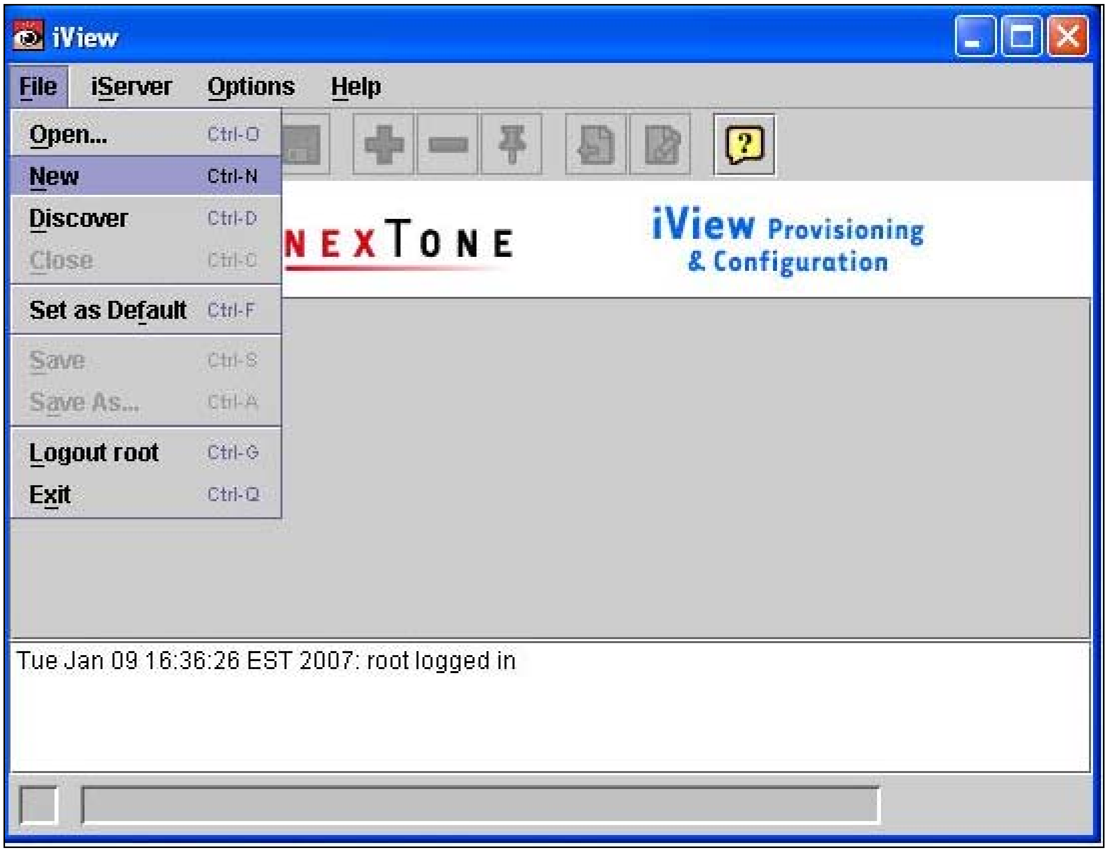
Step	Description
5.13	From the CLI, verify that the **/etc/hosts** file utilizes the management IP address provisioned in **Step 5.8**. If not, edit the file with a text editor, (e.g., vi) to make the update.
5.14	From the CLI, restart the server with **allstart**; then verify that processes are up with allstat.

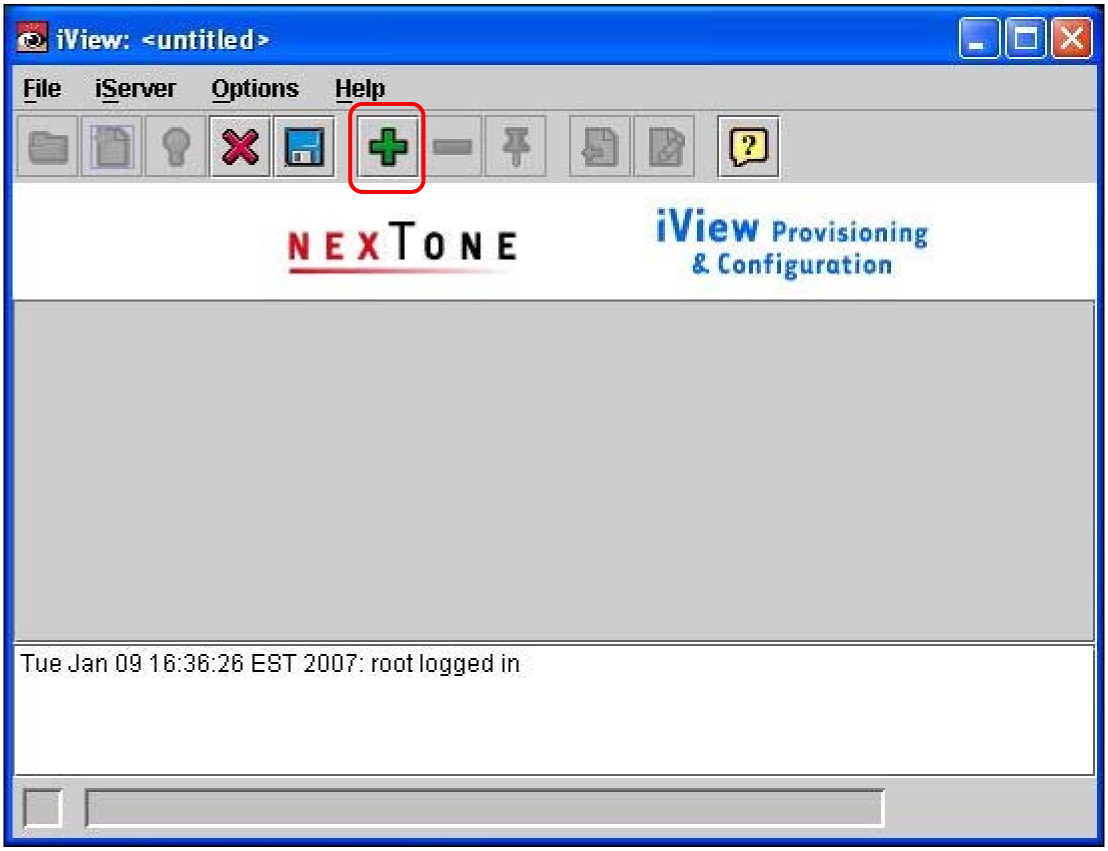
```
nextone-msw:~ # allstart
/usr/local/nextone/bin ~
Ramdisk version = HKRAM_3_2_t6
Unloading enp2611 drivers PM3386 devices stopped
SPI3 bridge stopped
.
Ramdisk version = HKRAM_3_2_t6
Loading enp2611 drivers Using ./spi3br.o
Using ./pm338x.o
Using ./TejaDrv_radisys.o
Using ./halMeDrv.o
Using ./meIrq.o
SPI3 bridge started
PM3386 devices started
Packets cleared
MtHood Static Route Initialization Done
Start your microengines
Port0->Port1, Port1->Port2, Port2->Port0
.
kernel/core_uses_pid = 1
Unable to open socket to statserver
Unable to open socket to statserver
Control_2611 Ver: c2611-3_2-c2-22 - Oct 11 2006
Statistics Server Ver: stat_1_1_d37
Nextone iServer is being started
```

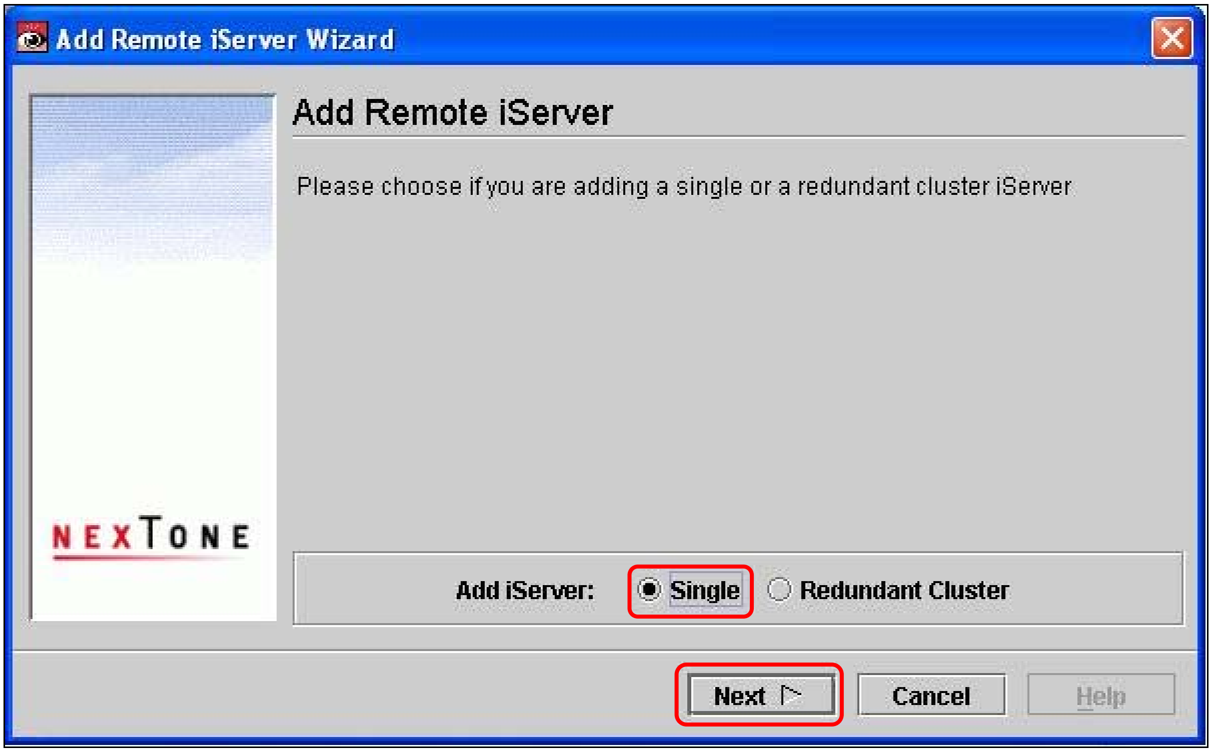
5.2. Configure the iView Application to Manage the NexTone MSX iServer

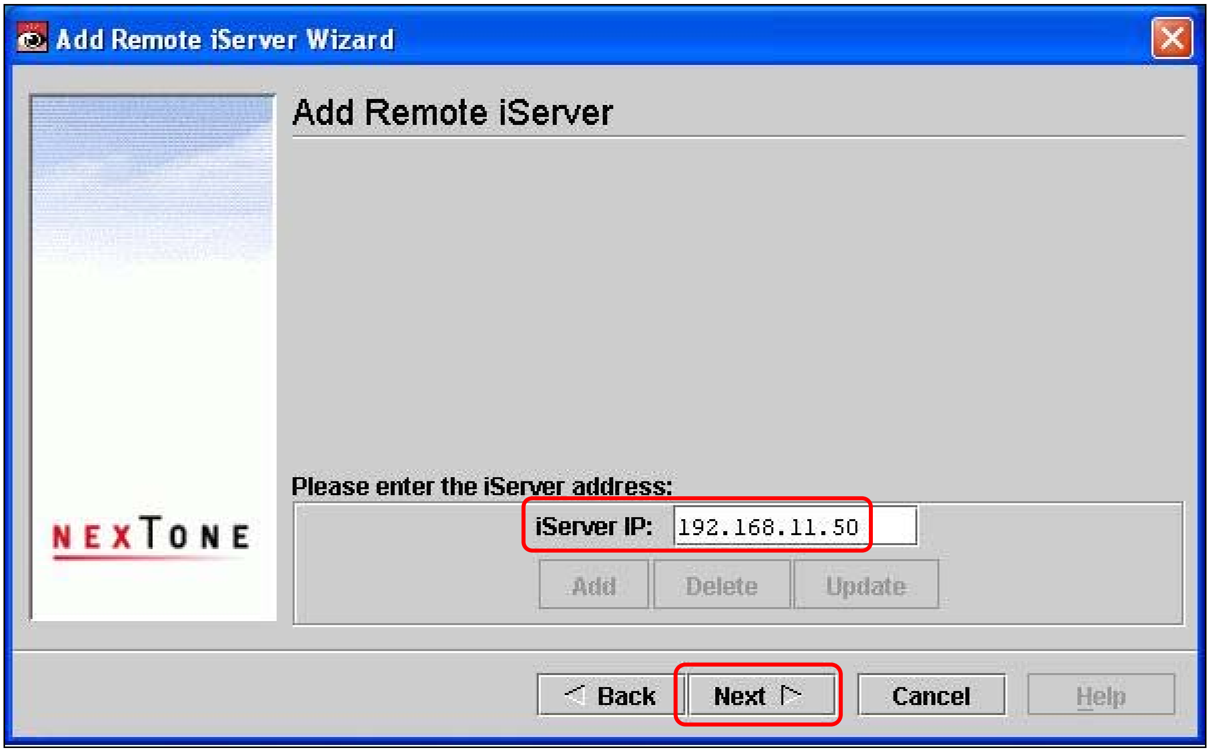
The following steps describe the administrative procedures for configuring the NexTone iView application to manage the NexTone MSX iServer. NexTone iView is client software that is utilized for provisioning the NexTone MSX iServer and is loaded on a PC that has layer 3 connectivity to the management interface on the NexTone MSX iServer.

Step	**Description**
5.15	To manage the NexTone MSX iServer via the iView application, add the NexTone MSX iServer to the iView application as follows: • Open the NexTone iView application. • Log in to NexTone iView with the appropriate credentials.  Enter a user name and password Welcome to iView!

Step	Description
5.16	From the NexTone iView Menu Bar, click **File** → **New**.  Tue Jan 09 16:36:26 EST 2007: root logged in

Step	Description
5.17	Click on the **+** icon to add a new NexTone MSX iServer to the NexTone iView application.  Tue Jan 09 16:36:26 EST 2007: root logged in

Step	Description
5.18	Add a Remote NexTone MSX iServer as either a single (stand alone) or redundant cluster. For these Application Notes, a **Single** iServer was used. Click **Next** to continue.  Add Remote iServer Wizard Add Remote iServer Please choose if you are adding a single or a redundant cluster iServer Add iServer: ● Single ○ Redundant Cluster

Step	Description
5.19	Enter the management IP address provisioned in **Step 5.8** for the **iServer IP** entry; then click **Next** to continue.  Add Remote iServer Please enter the iServer address: iServer IP: 192.168.11.50

Step	Description
5.20	Click **Finish** to add the iServer to the iView application.  Add Remote iServer iServer Type: Single iServer Address: /192.168.11.50

5.3. Configure Call Processing

The following call processing configuration of the NexTone MSX iServer is provisioned using the NexTone iView application. Call processing is defined as the configuration utilized by the NexTone MSX iServer to support both media and signaling between public and private networks.

The NexTone MSX iServer uses the following parameters to process SIP calls:

- **Calling Plan –** A calling plan is a name given to one or a group of call routes.
- **Call Route –** Call routes are rules for matching and routing a call based on incoming digits.
- **Call Bindings –** Call bindings is where a call route is associated with a calling plan.
- **Vnet –** A Vnet is a logical interface associated with a physical interface.
- **Media Pools –** Media pools are logical, named groupings of firewall resources available for realm-based media routing.
- **Realm –** Realms are utilized for keeping networks logically separated, so that traffic originating and destined for them is correctly routed. This is accomplished by associating dedicated signaling and media addresses (e.g., physical hardware interfaces, Eth2, hk0,0, etc.) with logical entities on the NexTone MSX iServer (e.g., signaling/media Vnet(s) and media pool(s), see **Figure 4** and **Figure 5**).
- **Endpoint –** An endpoint is a source or destination IP address of a call.

Figure 4 displays the schema regarding a Realm and a Signaling Vnet.

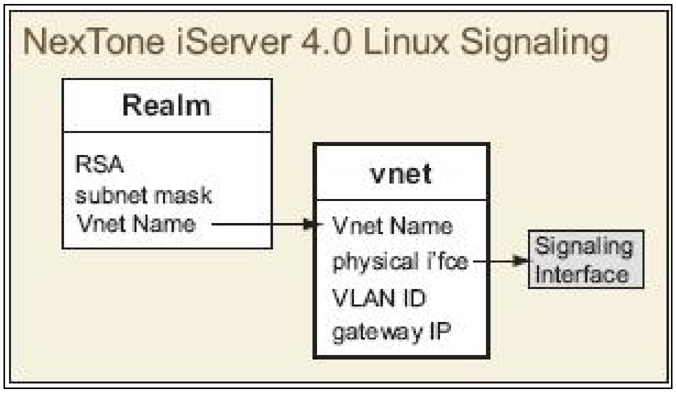


Figure 4: Schema for Realm and Signaling Vnet

Figure 5 displays the schema regarding a Realm and a Media Pool/Vnet.

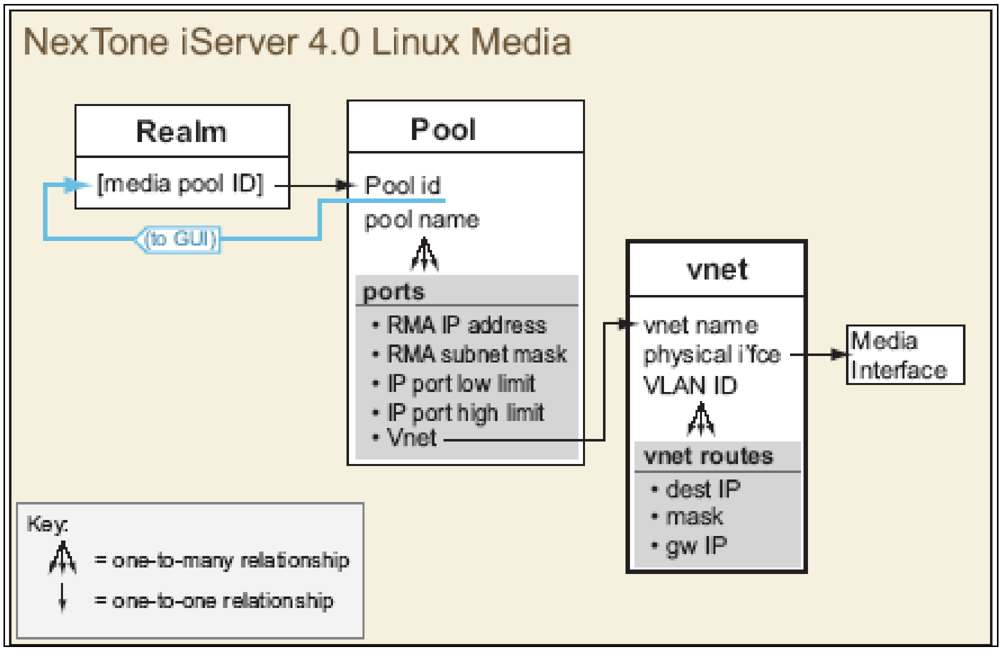
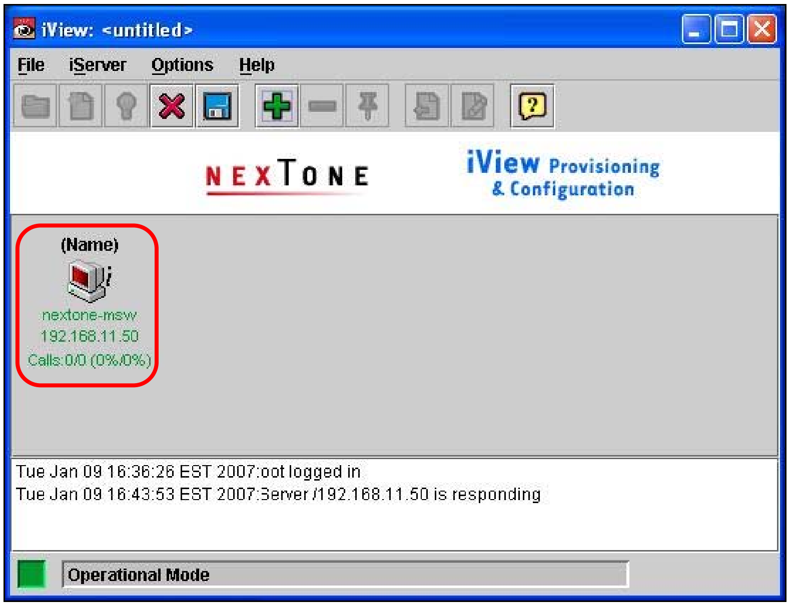
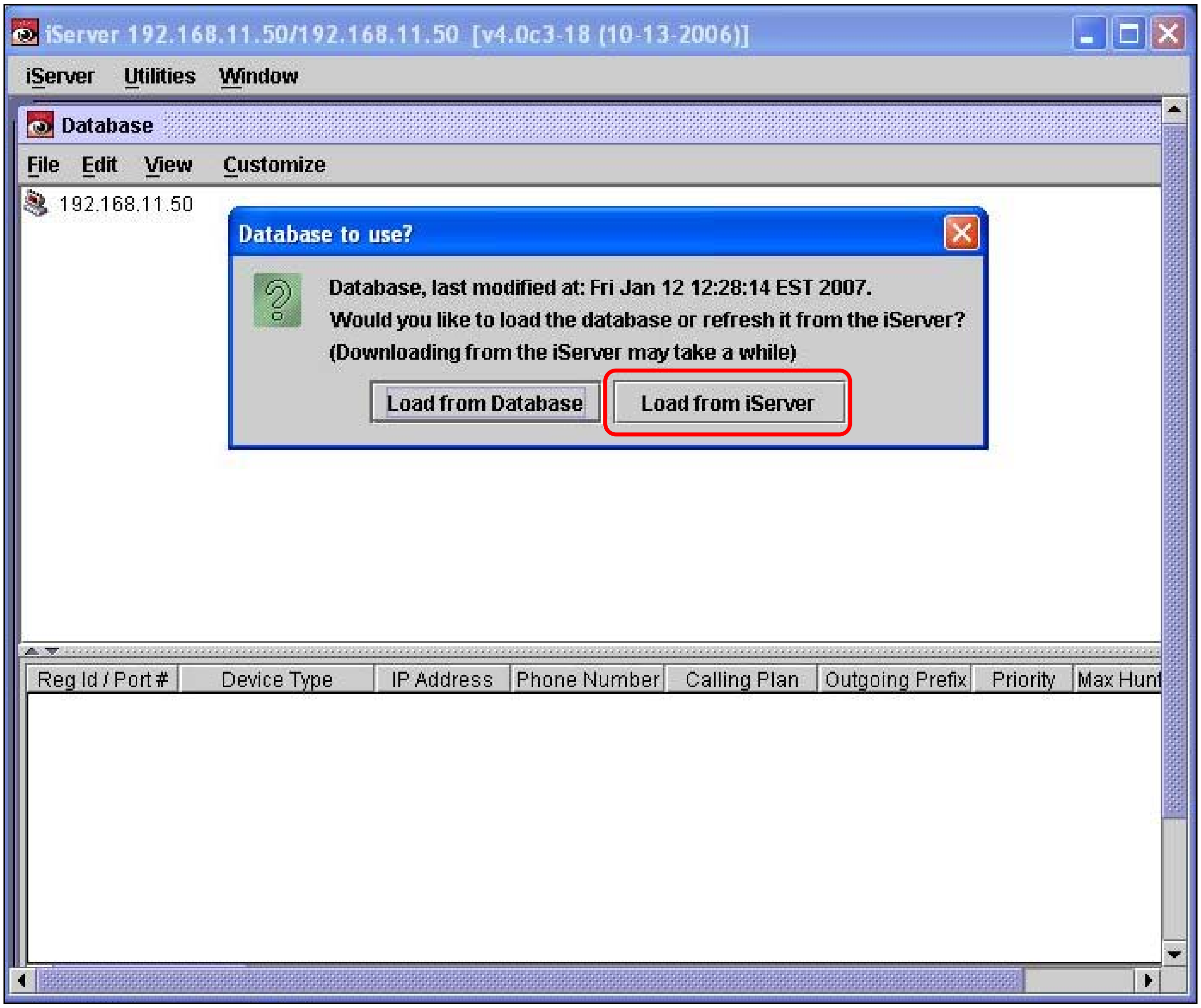
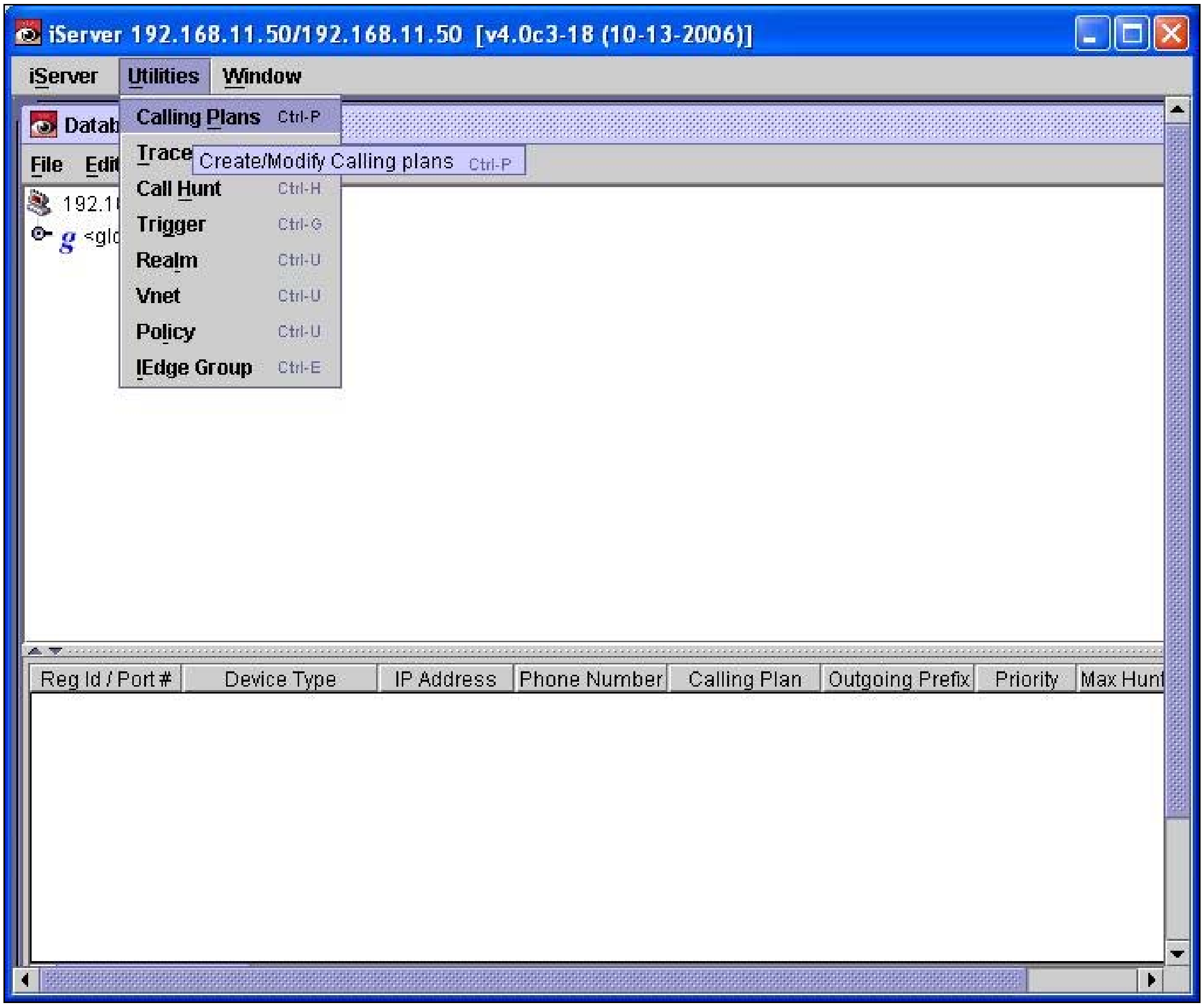
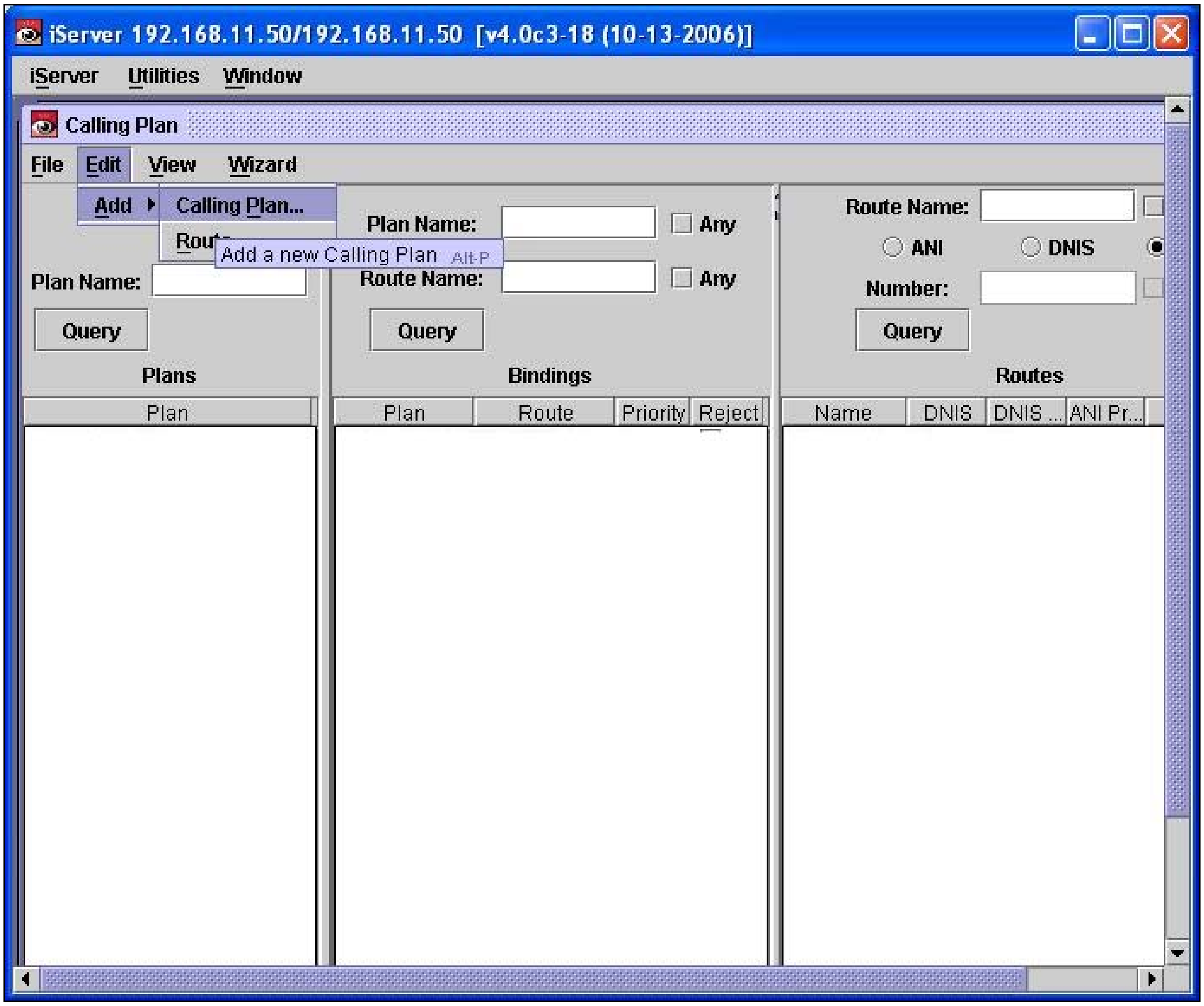


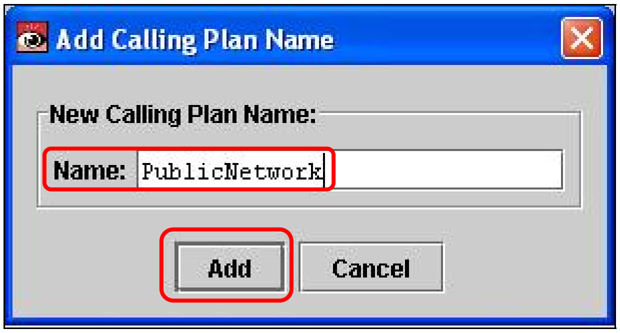
Figure 4: Schema for Realm and Media Pool/Vnet

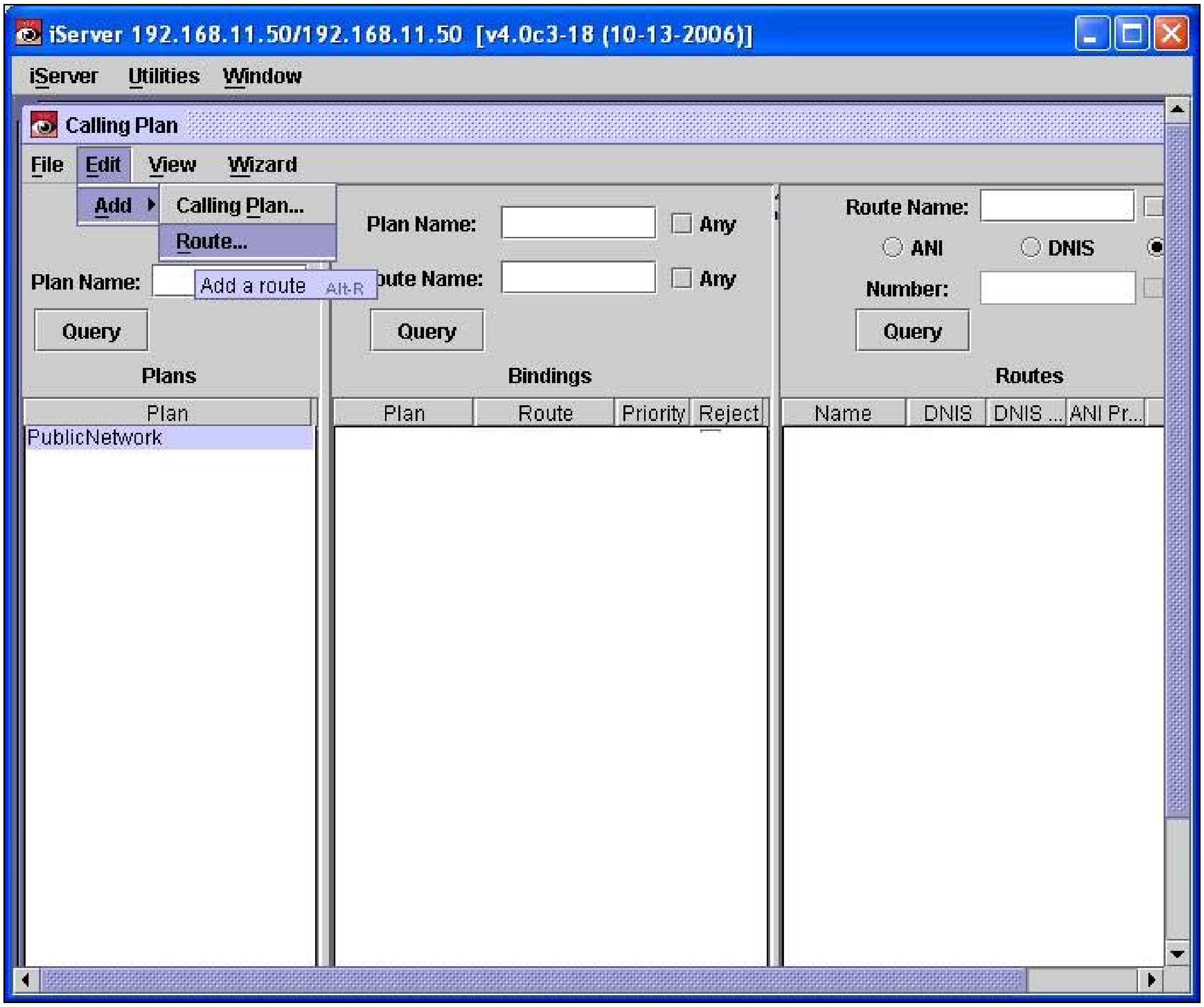
Step	**Description**
5.21	From the iView application, double click on the icon for the newly added NexTone MSX iServer.  Tue Jan 09 16:36:26 EST 2007:oot logged in Tue Jan 09 16:43:53 EST 2007:Server /192.168.11.50 is responding Operational Mode

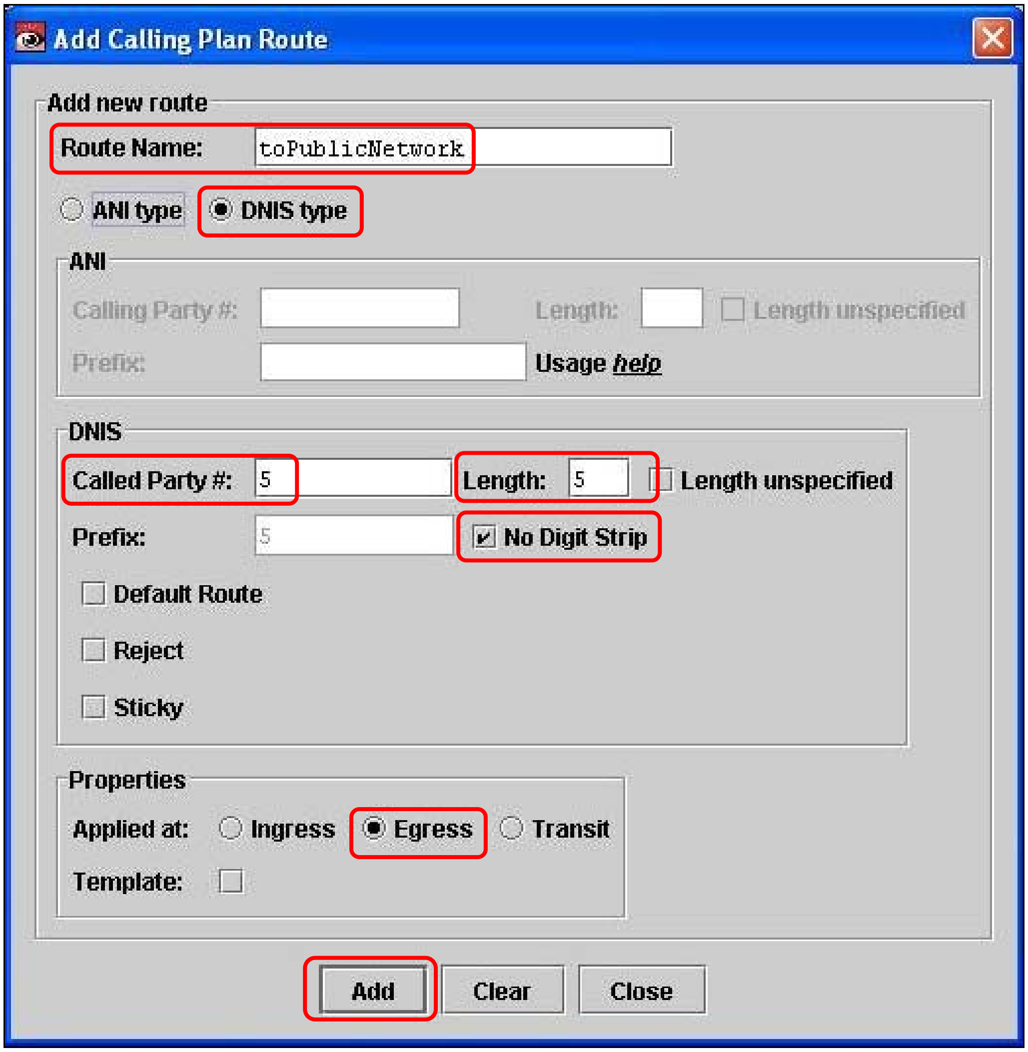
Step	Description
5.22	Load the database from the iServer by selecting **Load from iServer** from the pop-up window that is displayed. [***Not Shown***] Click yes to confirm the request to load the database from the NexTone MSX iServer.  Database, last modified at: Fri Jan 12 12:28:14 EST 2007. Would you like to load the database or refresh it from the iServer? (Downloading from the iServer may take a while)

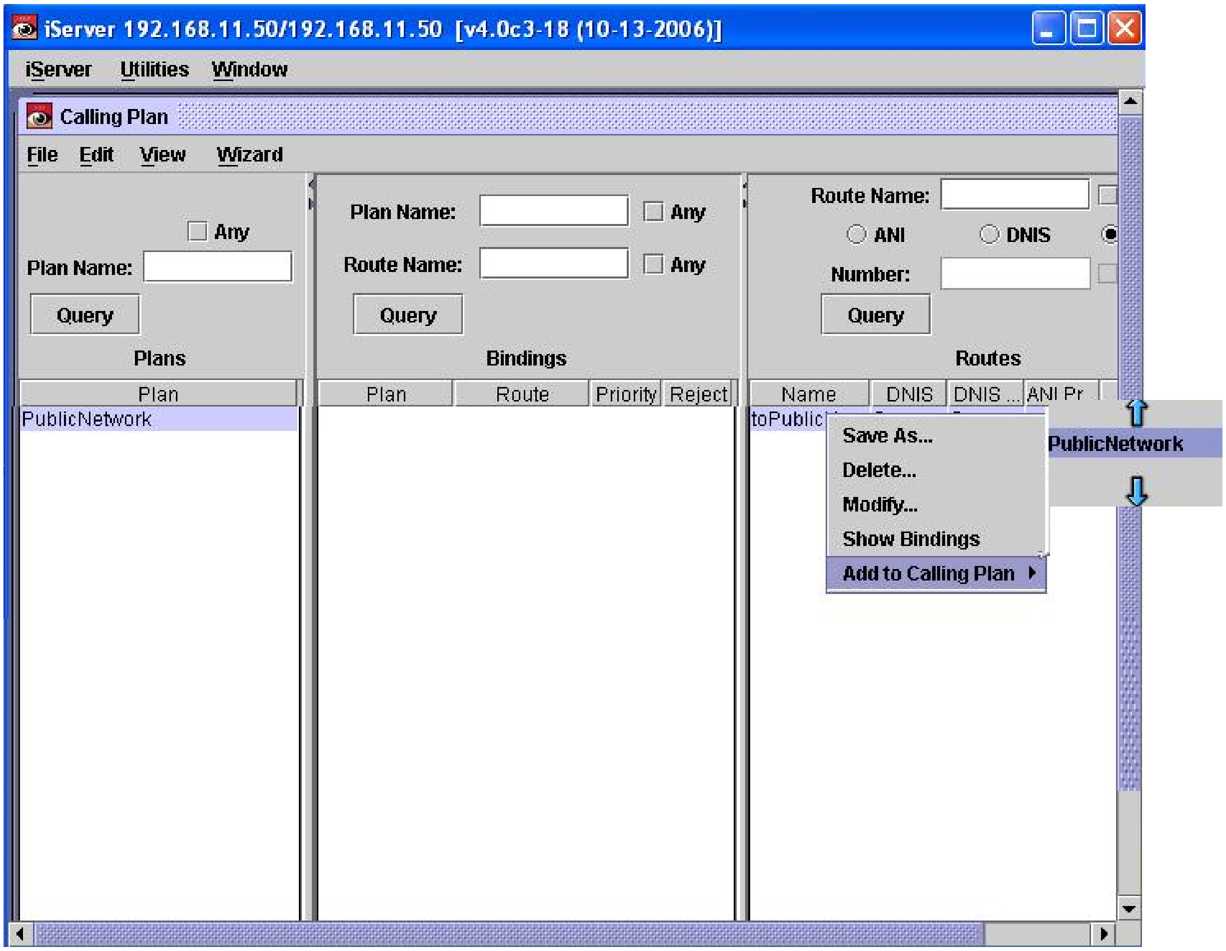
Step	Description
5.23	To specify the preferences and policies for incoming and outgoing calls, provision a calling plan by clicking **Utilities** ➔ **Calling Plans**. 

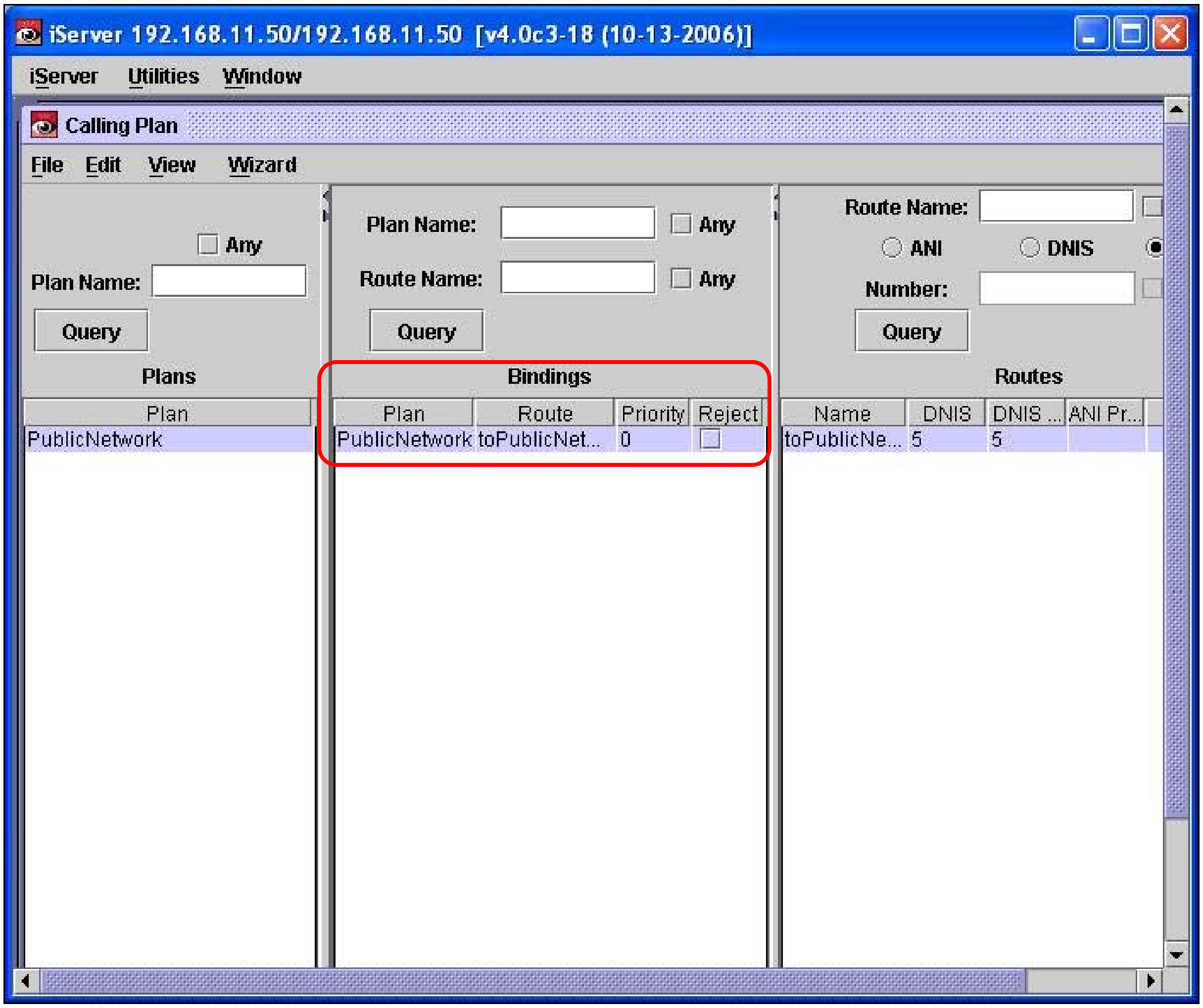
Step	Description
5.24	From the **Calling Plan** window that is displayed, add a calling plan for the public network by clicking **Edit** ➔ **Add** ➔ **Calling Plan**. 

Step	Description
5.25	From the **Add Calling Plan Name** window that is displayed, add a calling plan name as follows. • Enter a descriptive label in the **Name** field. • Click on the **Add** button when finished.  Name: PublicNetwork
5.26	Repeat **Step 5.24** and **Step 5.25** to create a calling plan name (**PrivateNetwork**) for the private network.

Step	Description
5.27	From the **Calling Plan** window that is displayed, add a route for the public network by clicking **Edit → Add → Route**. 

Step	Description
5.28	From the **Add Calling Plan Route** window that is displayed, configure a route to the public network as follows. • Enter a descriptive label in the **Route Name** field. • Select **DNIS type** to route calls according to the dialed number. • Configure the **Called Party #** and **Length** fields to support dial-out to the public network from the Avaya Meeting Exchange S6800 Conferencing Server via Avaya SIP Enablement Services (see **Step 3.4** and **Step 4.12**). • Select **No Digit Strip**. *__Note__: The Prefix and No Digit Strip is used in conjunction with the Prefix entry to prepend optional digits to the number sent to the egress gateway.* • Select **Egress** to apply these route **Properties** on calls to the public network. • Click on the **Add** button when finished.  Add Calling Plan Route Add new route Route Name: toPublicNetwork ○ ANI type ● DNIS type ANI Calling Party #: Length: ☐ Length unspecified Prefix: Usage help DNIS Called Party #: 5 Length: 5 ☐ Length unspecified Prefix: 5 ☑ No Digit Strip ☐ Default Route ☐ Reject ☐ Sticky Properties Applied at: ○ Ingress ● Egress ○ Transit Template: ☐ Add Clear Close

Step	Description
5.29	Repeat **Step 5.27** and **Step 5.28** to create a route to the private network with the following settings: • Enter **toPrivateNetwork** in the **Route Name** field. • Select **DNIS type** to route calls according to the dialed number. • Set the **Called Party #** to **5**. • Set the **Length** to **3**. • Select **No Digit Strip**. • Select **Egress** to apply these route **Properties** on calls to the private network.
5.30	To associate the public route with the public calling plan name, bind the two together by right clicking on the route and selecting the calling plan name to bind to. ***Note****: A calling plan name can have any number of routes bound to it. Also, a route can belong to any number of calling plans.* 

Step	Description
5.31	The public calling plan name and route to the public network are bound. 
5.32	Repeat **Step 5.30** to bind the private calling plan name with the route to the private network

Plans

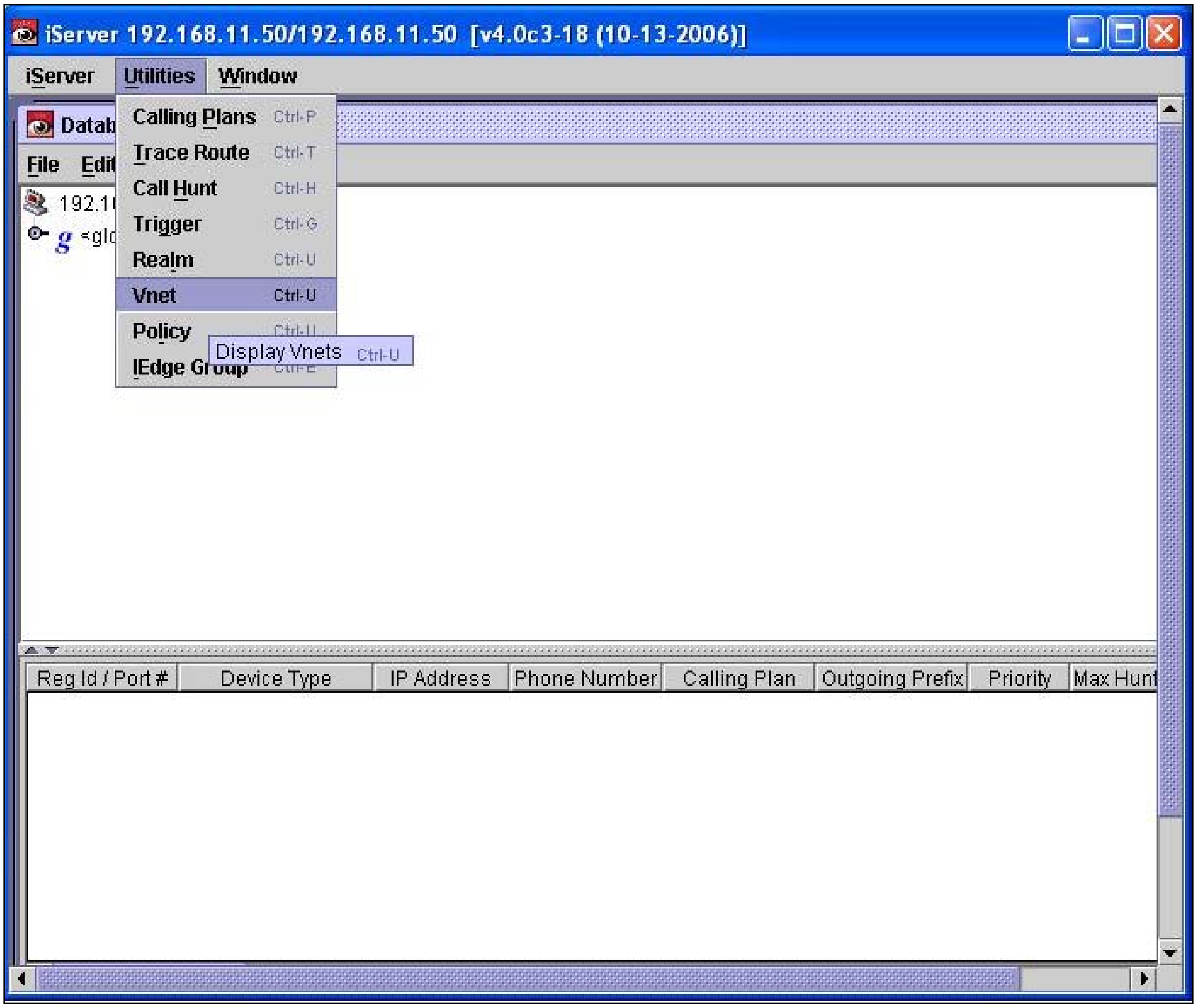
Plan
PublicNetwork

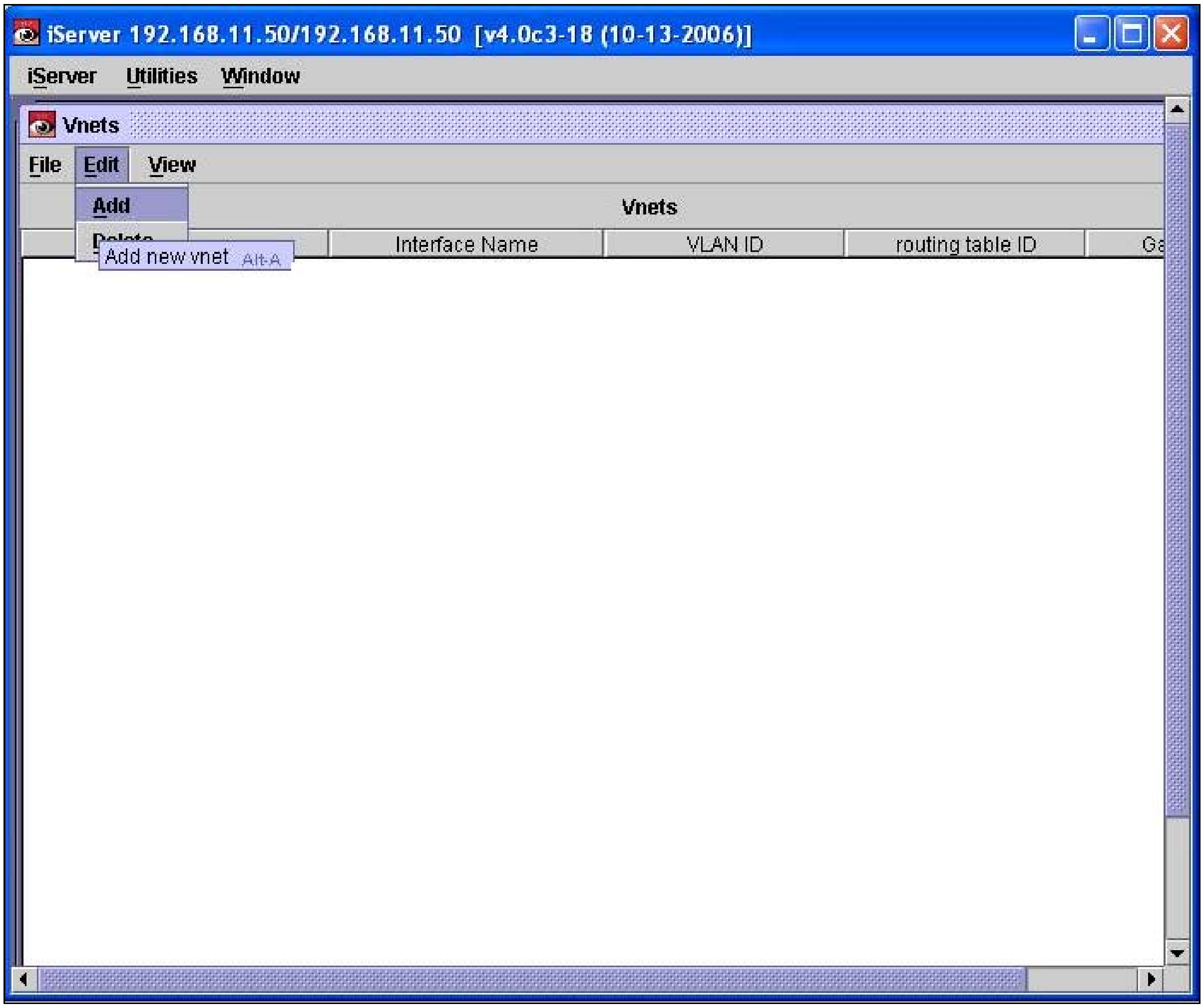
Bindings

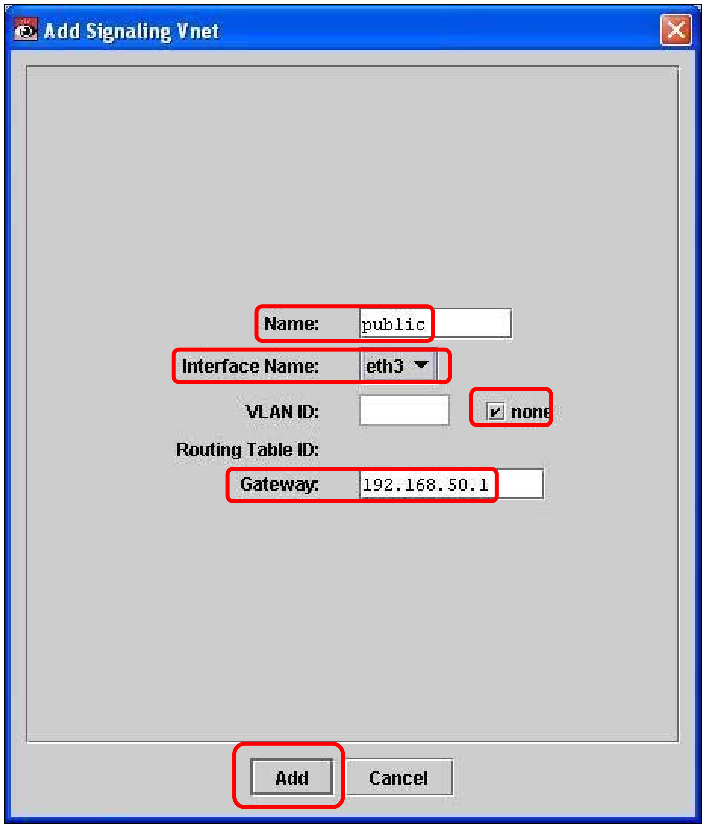
Plan	Route	Priority	Reject
PublicNetwork	toPublicNet...	0	☐

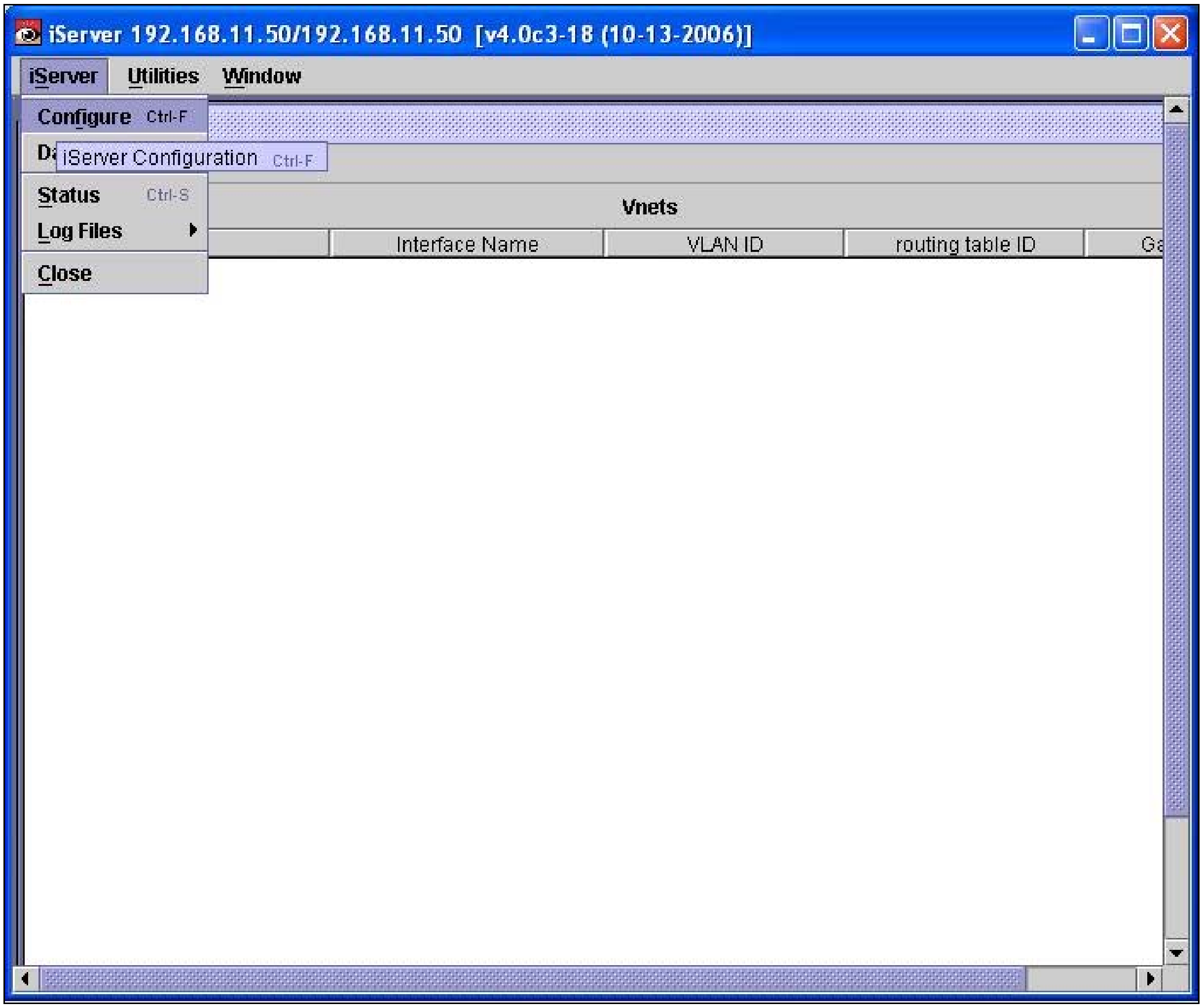
Routes

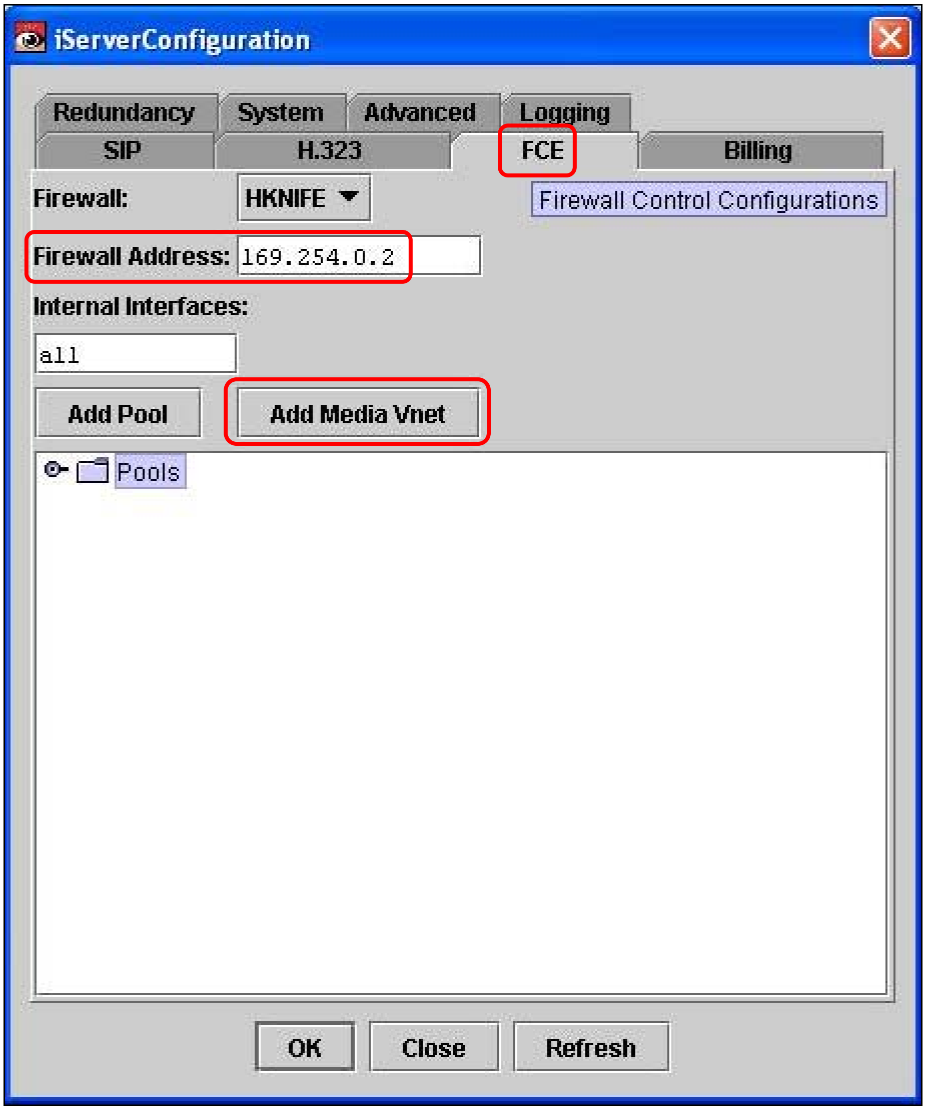
Name	DNIS	DNIS ...	ANI Pr...
toPublicNe...	5	5	

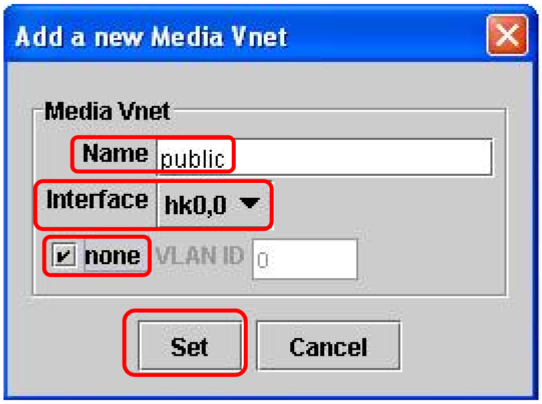
Step	Description
5.33	To associate physical interfaces on the NexTone MSX iServer with public and private (signaling) networks, provision Virtual Network Interface(s) (Vnet) for signaling by clicking **Utilities → Vnet**. 

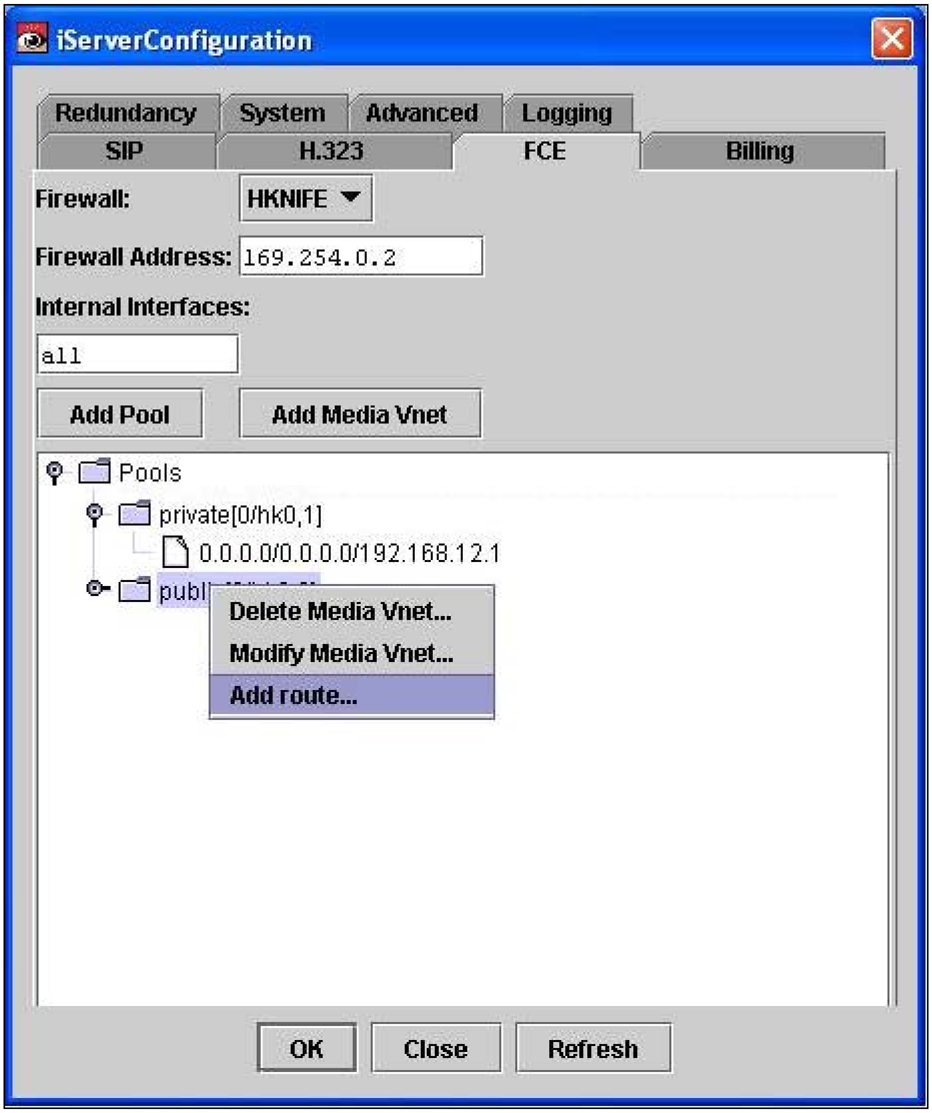
Step	Description
5.34	From the **Vnets** window that is displayed, add a signaling Vnet by clicking **Edit** → **Add**. 

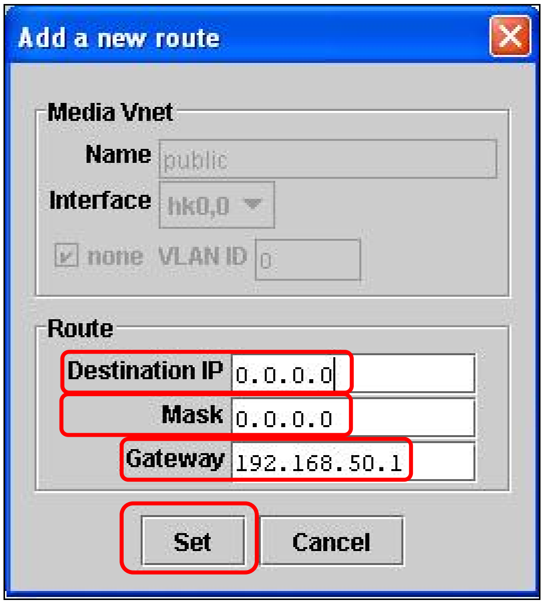
Step	Description
5.35	From the **Add Signaling Vnet** window that is displayed, configure a signaling Vnet to connect to the public network as follows. • Enter a descriptive label in the **Name** field. • Select the interface connected to the public network for the **Interface Name**. • Enter a valid 802.1q VID in the **VLAN ID** field (from 1 through 4094), or select **none**. • Enter the IP address of the gateway for the public network in the **Gateway** field. • Click on the **Add** button when finished.  Name: public Interface Name: eth3 VLAN ID: ☑ none Routing Table ID: Gateway: 192.168.50.1
5.36	Repeat **Step 5.34** and **Step 5.35** to create a signaling Vnet to connect to the private network with the following settings: • Enter **private** in the **Name** field. • Select the interface connected to the private network (**eth2**) for the **Interface Name**. • Select **none** for the **VLAN ID**. • Enter the IP address of the gateway for the private network (**192.168.12.1**) in the **Gateway** field.

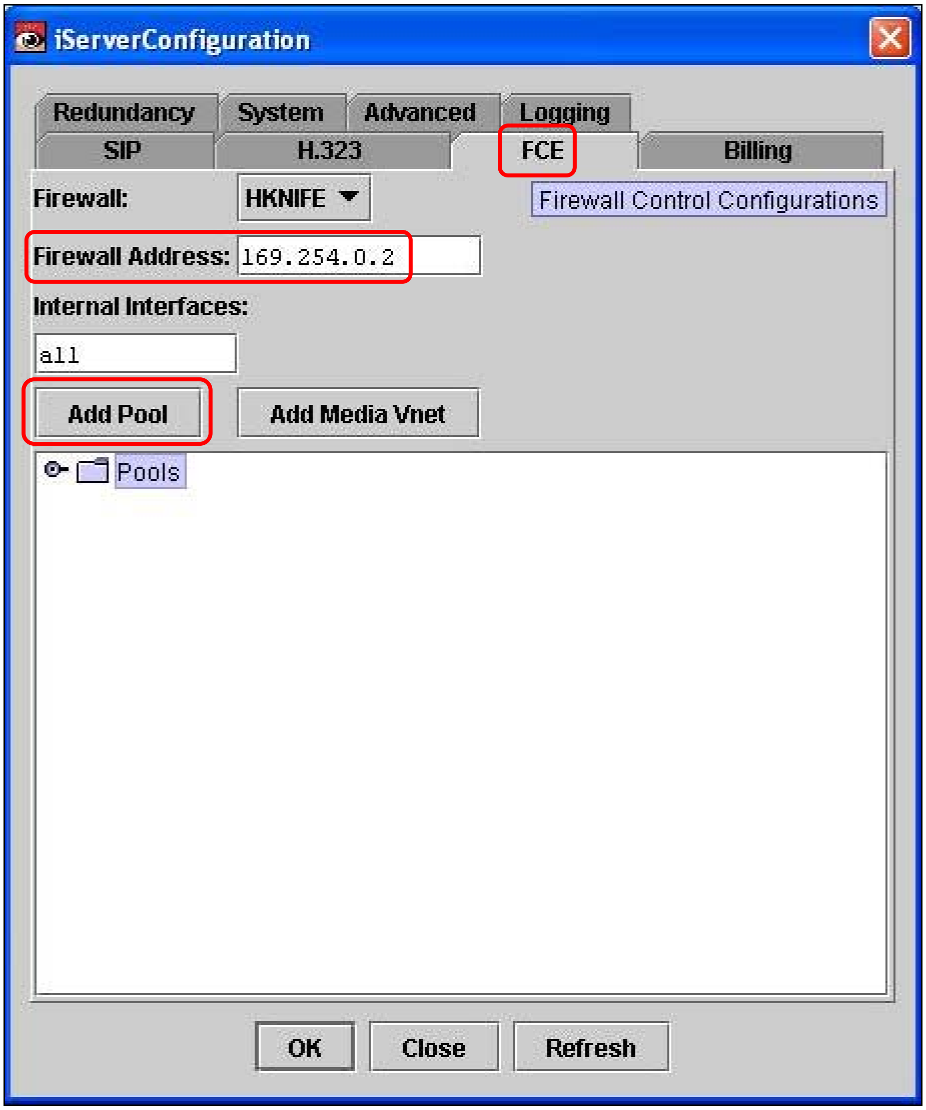
Step	Description
5.37	To associate physical interfaces on the NexTone MSX iServer with public and private (media) networks, provision Virtual Network Interface(s) (Vnet) and pools for media by clicking **iServer → Configure**. 

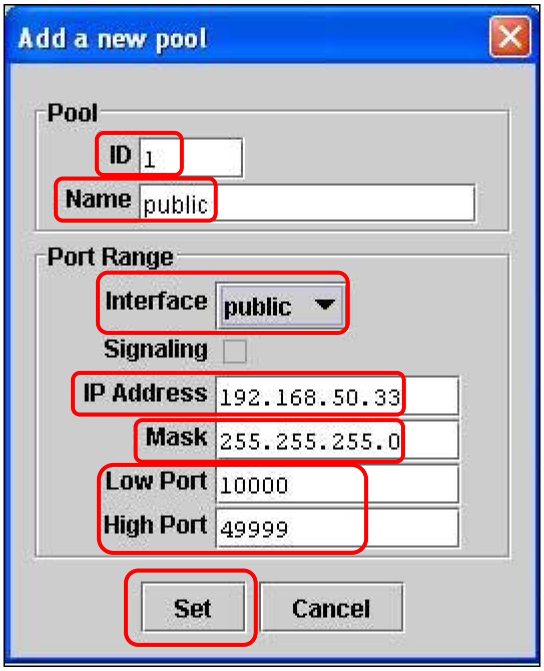
Step	Description
5.38	To manage media on the NexTone MSX iServer, add Media Vnet(s) to the Firewall Control Configuration (FCE) by clicking on the **FCE** tab, then **Add Media Vnet**. *__Note__: The Firewall Address is the address of the MSC's IP interface into the NSF-NP card, __169.254.0.2__. The NexTone MSX iServer OS and the NSF-NP OS communicate with each other via fixed, non-routable IP addresses as follows*: • *The iServer sees the NSF-NP board at 169.254.0.2.* • *The NSF-NP board sees the iServer at 169.254.0.1.*  Firewall: HKNIFE Firewall Address: 169.254.0.2 Internal Interfaces: all

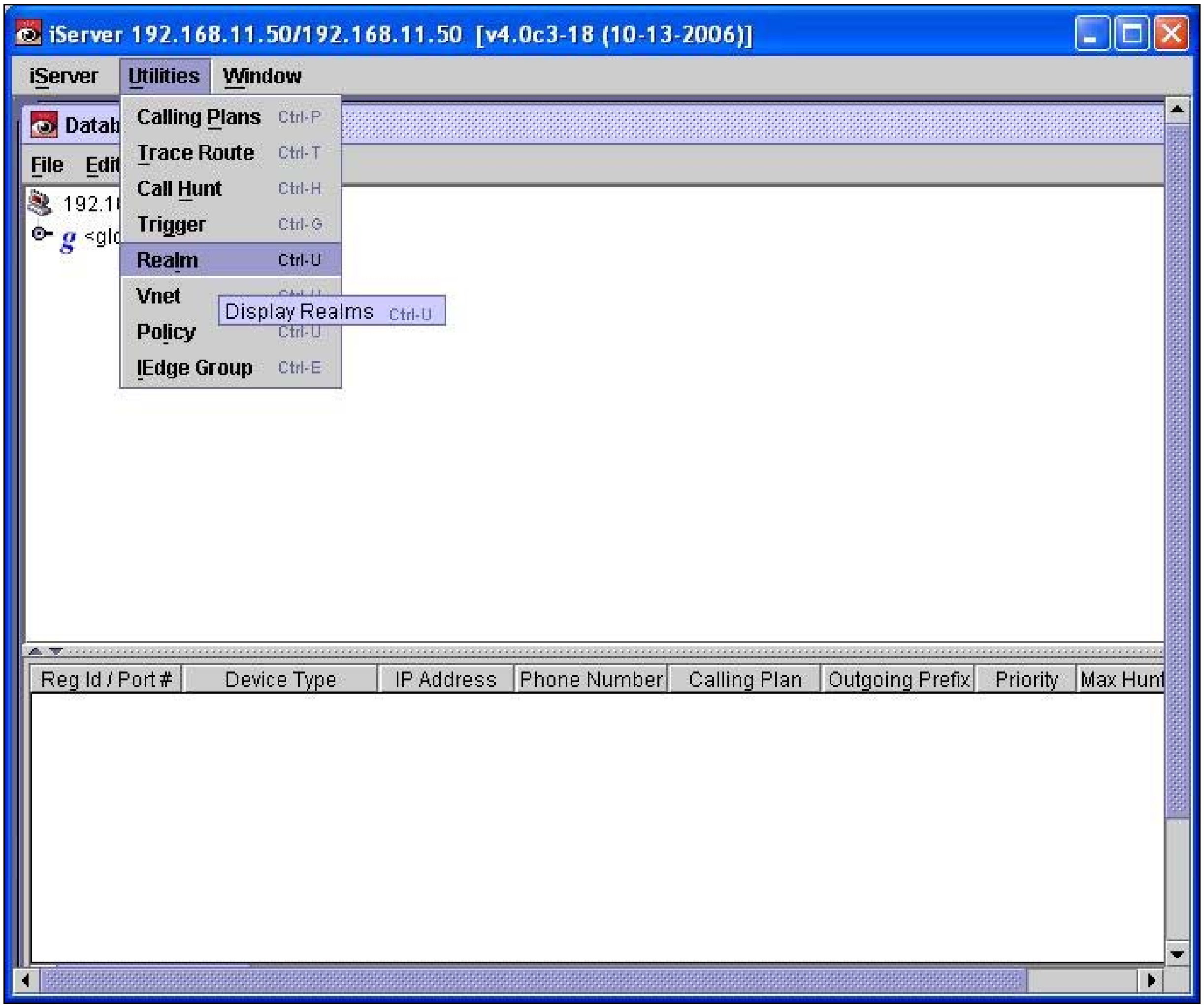
Step	Description
5.39	From the **Add a new Media Vnet** window that is displayed, configure a media Vnet to connect to the public network as follows. • Enter a descriptive label in the **Name** field. • Select the interface connected to the public network for the **Interface**. • Enter a valid 802.1q VID in the **VLAN ID** field (from 1 through 4094), or select **none**. • Click on the **Set** button when finished.  Add a new Media Vnet Media Vnet Name public Interface hk0,0 ☑ none VLAN ID 0 Set Cancel
5.40	Repeat **Step 5.38** and **Step 5.39** to create a media Vnet to connect to the private network with the following settings: • Enter **private** in the **Name** field. • Select the interface connected to the private network (**hk0,1**) for the **Interface**. • Select **none** for the **VLAN ID**.

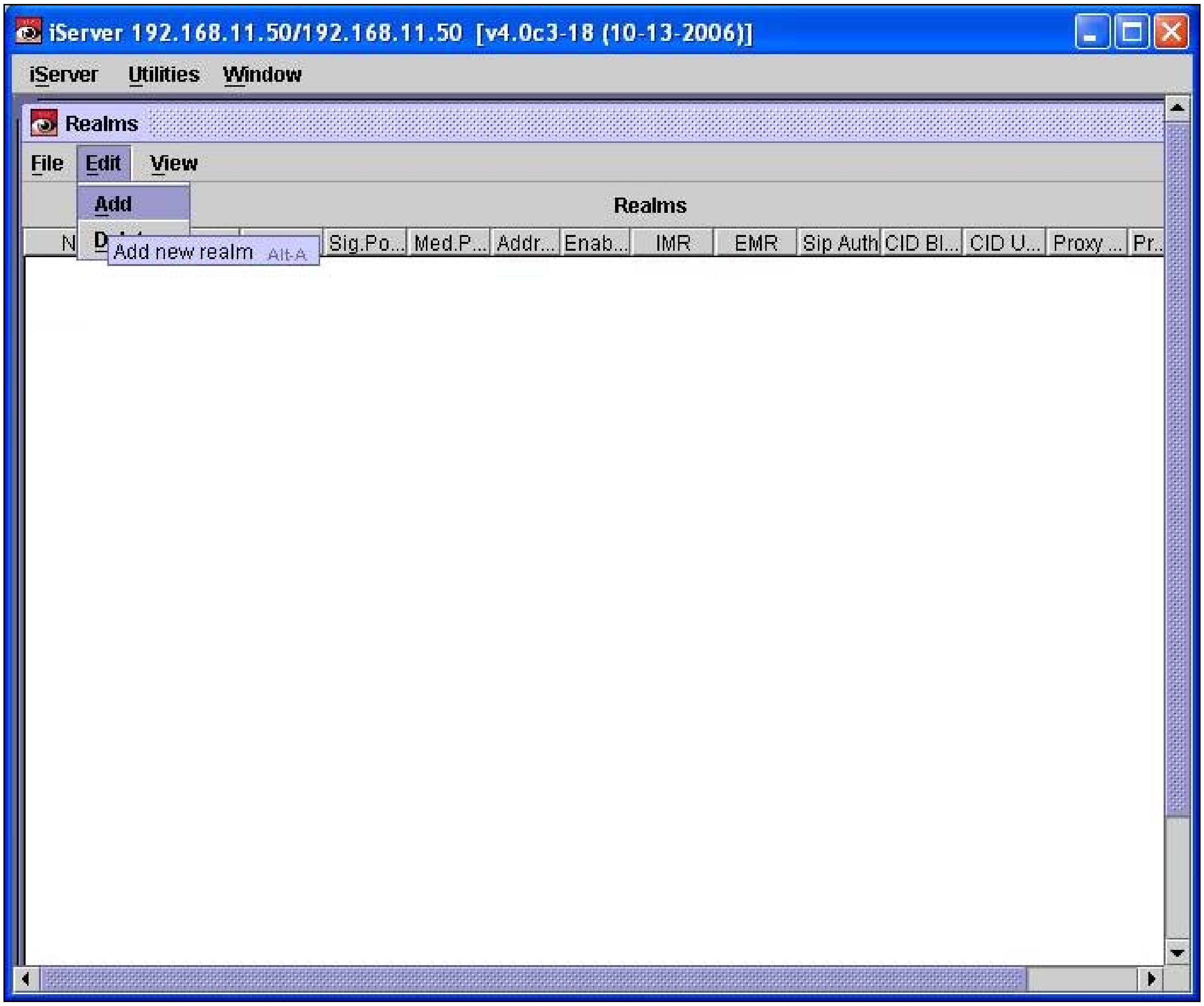
Step	Description
5.41	From the **FCE** tab, add route(s) to the media Vnets provisioned in **Steps 5.38 - 5.40**, as follows: • Select a Media Vnet from the Pools list. • Right click on it and choose **Add route**.  Firewall: HKNIFE Firewall Address: 169.254.0.2 Internal Interfaces: all Pools private[0/hk0,1] 0.0.0.0/0.0.0.0/192.168.12.1

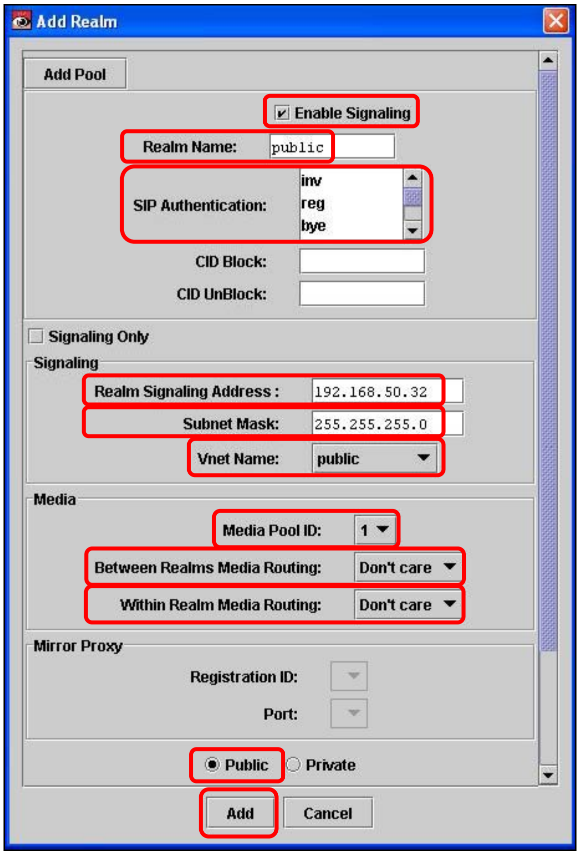
Step	Description
5.42	From the **Add a new route** window that is displayed, configure routing for the public media Vnet to route to the public network as follows: • Enter an IP address/mask for the public network in the **Destination IP** and **Mask** fields. • Enter the IP address of the gateway for the public network in the **Gateway** field. • Click on the **Set** button when finished.  Media Vnet Name: public Interface: hk0,0 ☑ none VLAN ID: 0 Route Destination IP: 0.0.0.0 Mask: 0.0.0.0 Gateway: 192.168.50.1
5.43	Repeat **Step 5.41** and **Step 5.42** to add routing to the private network with the following settings: • Enter **0.0.0.0** in the **Destination IP** and **Mask** fields. • Enter **192.168.12.1** in the **Gateway** field.

Step	Description
5.44	To manage media on the NexTone MSX iServer, add Pool(s) to the Firewall Control Configuration (FCE) by clicking on the **FCE** tab, then **Add Pool**. *__Note__: The Firewall Address is the address of the MSC's IP interface into the NSF-NP card, __169.254.0.2__. The NexTone MSX iServer OS and the NSF-NP OS communicate with each other via fixed, non-routable IP addresses as follows*: • *The iServer sees the NSF-NP board at 169.254.0.2.* • *The NSF-NP board sees the iServer at 169.254.0.1.*  Firewall: HKNIFE Firewall Address: 169.254.0.2 Internal Interfaces: all

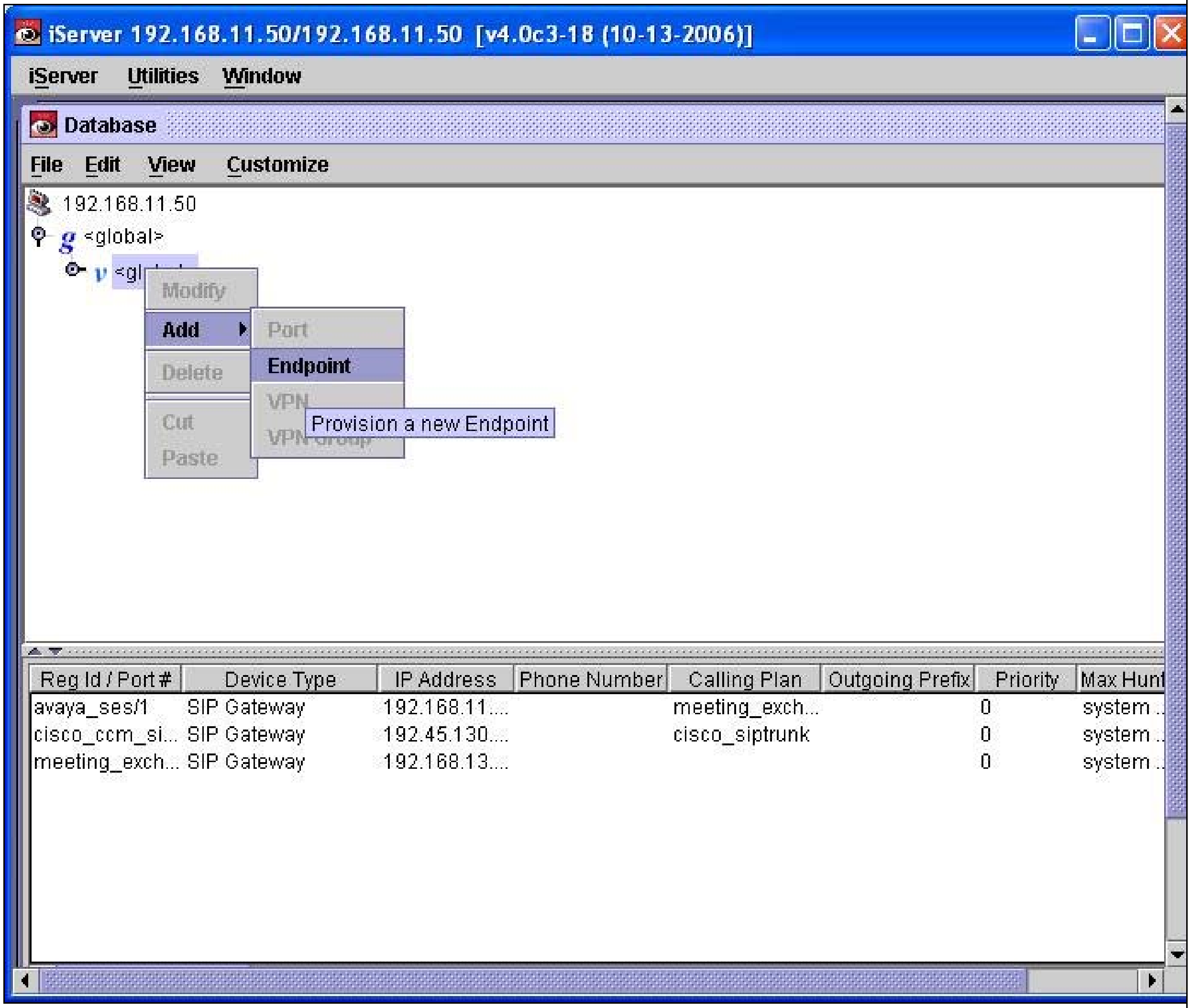
Step	Description
5.45	From the **Add a new pool** window that is displayed, configure a pool to connect to the public network as follows. • The **ID** field is pre-populated with a pool ID number that is not already in use. • Enter a descriptive label in the **Name** field. • Select the public media Vnet provisioned in Step **5.39** for the **Interface**. • Enter the **IP Address** and **Mask** for the Realm Media Address (RMA) to be used by this **Port Range**. • Enter the first port in the range for this IP address in the **Low Port** field. • Enter the first port in the range for this IP address in the **High Port** field. • Click on the **Set** button when finished.  Add a new pool Pool ID 1 Name public Port Range Interface public Signaling ☐ IP Address 192.168.50.33 Mask 255.255.255.0 Low Port 10000 High Port 49999 Set Cancel
5.46	Repeat **Step 5.44** and **Step 5.45** to add a pool for the private network with the following settings: • Enter **private** in the **Name** field. • Select the private media Vnet for the **Interface**. • Enter the **IP Address** (**192.168.12.33**) and **Mask** (**255.255.255.0**) for the Realm Media Address (RMA) to be used by this **Port Range**. • Enter **10000** in the **Low Port** field. • Enter **49999** in the **High Port** field.

Step	Description
5.47	To associate the Vnets (signaling and media) and the media pools provisioned in the previous steps with endpoints (see provisioning starting with **Step 5.51**), provision realms by clicking **Utilities → Realm**. 

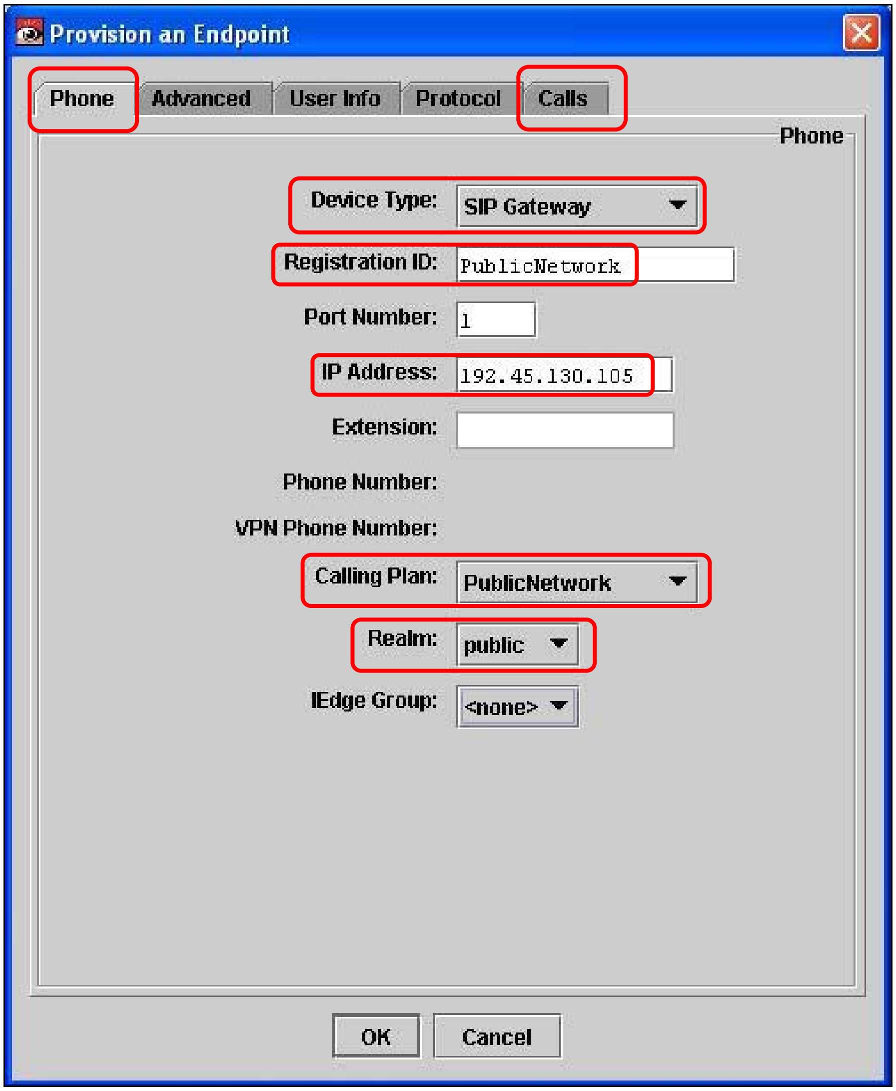
Step	Description
5.48	From the **Realms** window that is displayed, add a realm associated with the public network by clicking **Edit** ➔ **Add**. 

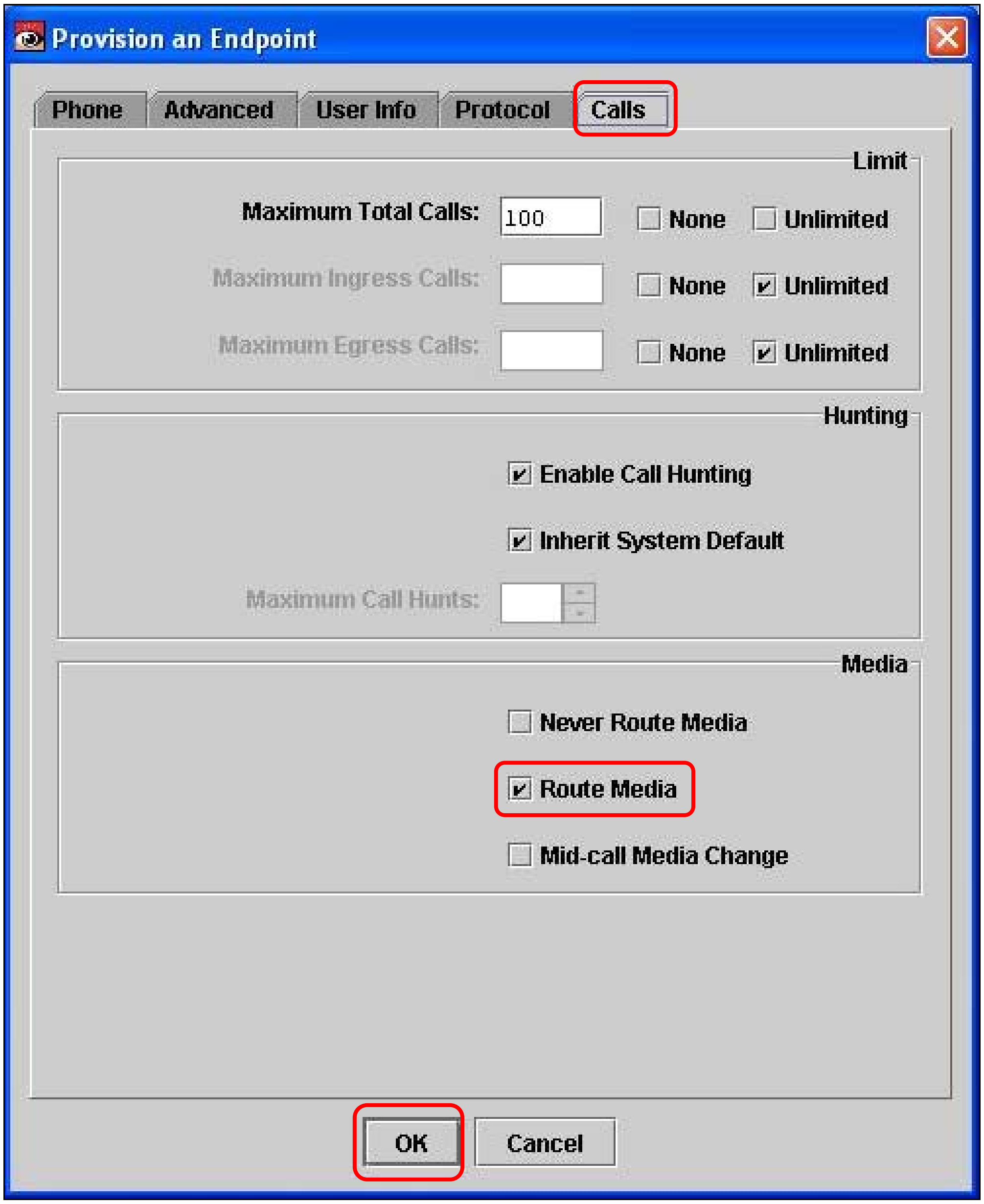
Step	Description
5.49	From the **Add Realm** window that is displayed, configure a realm associated with the public network as follows. • Select **Enable Signaling** to allow call setup for new calls. • Enter a descriptive label in the **Realm Name** field. • Select message types to be subject to **SIP Authentication** rules. For these Application Notes, none were selected. • Enter an IP address and subnet mask for the public network in the **Realm Signaling Address** and **Subnet Mask** fields. • Select the signaling Vnet provisioned for the public network in **Step 5.35** for the **Vnet Name**. • Select the media pool provisioned for the public network in **Step 5.45** for the **Media Pool ID**. • Select **Don’t Care** for **Between Realms Media Routing** and **Within Realm Media Routing**. There were issues found when the selection for **Between Realms Media Routing** was Always On (see **Section 6**, **Test Results**). • Select **Public** which indicates the addresses in this realm are “public” addresses. • Click on the **Add** button when finished.  Add Realm Add Pool ☑ Enable Signaling Realm Name: public SIP Authentication: inv, reg, bye CID Block: CID UnBlock: ☐ Signaling Only Signaling Realm Signaling Address : 192.168.50.32 Subnet Mask: 255.255.255.0 Vnet Name: public Media Media Pool ID: 1 Between Realms Media Routing: Don't care Within Realm Media Routing: Don't care Mirror Proxy Registration ID: Port: ● Public ○ Private Add Cancel

Step	Description
5.50	Repeat **Step 5.48** and **Step 5.49** to create a realm associated with the private network with the following settings: • Select **Enable Signaling** to allow call setup for new calls • Enter **private** in the **Realm Name** field. • Select the interface connected to the private network (**eth2**) for the **Interface Name**. • Select **Enable Signaling** to allow call setup for new calls. • Do not select any message types for **SIP Authentication** • Enter **192.168.12.32** in the **Realm Signaling Address** field • Enter **255.255.255.0** in the **Subnet Mask** field. • Select the signaling Vnet provisioned for the private network for the **Vnet Name**. • Select the media pool provisioned for the private network for the **Media Pool ID**. • Select **Don't Care** for **Between Realms Media Routing** and **Within Realm Media Routing**. There were issues found when the selection for **Between Realms Media Routing** was Always On (see **Section 6**, **Test Results**). • Select **Private** which indicates the addresses in this realm are "private" addresses. • Provision any remaining parameters as per **Step 5.49**.

Step	Description
5.51	To add endpoints for the public and private realms (provisioned in the previous steps), right click ***v*<global> ➔ Add ➔ Endpoint**. 

Reg Id / Port #	Device Type	IP Address	Phone Number	Calling Plan	Outgoing Prefix	Priority	Max Hunt
avaya_ses/1	SIP Gateway	192.168.11....		meeting_exch...		0	system ...
cisco_ccm_si...	SIP Gateway	192.45.130....		cisco_siptrunk		0	system ...
meeting_exch...	SIP Gateway	192.168.13....				0	system ...

Step	Description
5.52	From the **Phone** tab on the **Provision an Endpoint** window that is displayed, configure an endpoint associated with the public network as follows. - Select **SIP Gateway** for the **Device Type**. - Enter a unique ID which is used internally by the NexTone MSX iServer in the **Registration ID** field. - The **Port Number** field is auto generated by the NexTone MSX iServer. - Enter the IP address in this endpoint in the **IP Address** field. - Select the **PublicNetwork** calling plan (see provisioning starting with **Step 5.25**) for the **Calling Plan**. - Select the public realm provisioned in **Step 5.49** for the **Realm**. - Click on the **Calls** tab to provision calling parameters for this endpoint.  Device Type: SIP Gateway Registration ID: PublicNetwork Port Number: 1 IP Address: 192.45.130.105 Extension: Phone Number: VPN Phone Number: Calling Plan: PublicNetwork Realm: public IEdge Group: <none>

Step	Description
5.53	From **Calls** tab on the **Provision an Endpoint** window that is displayed, configure call related parameters for an endpoint associated with the public network as follows: • Select **Route Media** to enable this endpoint to route media to/from other endpoints. • Remaining fields are default settings. • Click on the **OK** button when finished.  Limit Maximum Total Calls: 100 ☐ None ☐ Unlimited Maximum Ingress Calls: ☐ None ☑ Unlimited Maximum Egress Calls: ☐ None ☑ Unlimited Hunting ☑ Enable Call Hunting ☑ Inherit System Default Maximum Call Hunts: Media ☐ Never Route Media ☑ Route Media ☐ Mid-call Media Change

Step	Description
5.54	Repeat **Step 5.51**, **Step 5.52** and **Step 5.53** to create an endpoint associated with the Avaya Meeting Exchange S6800 Conferencing Server (residing in the private network) with the following settings: • From the phone tab: o Select **SIP Gateway** for the **Device Type**. o Enter **AvayaMeetingExchange** in the **Registration ID** field. o Enter the IP address for the Avaya Meeting Exchange S6800 Conferencing Server (**192.168.13.101**) in the **IP Address** field. o Select the calling plan for the private network (**PrivateNetwork**, see provisioning starting with **Step 5.26**) for the **Calling Plan**. o Select the private realm provisioned in **Step 5.50** for the **Realm**. o Provision any remaining parameters as per **Step 5.52**. • From the calls tab: o Select **Route Media** to enable this endpoint to route media to/from other endpoints. o Provision any remaining parameters as per **Step 5.53**.
5.55	Repeat **Step 5.51**, **Step 5.52** and **Step 5.53** to create an endpoint associated with Avaya SIP Enablement Services (residing in the private network) with the following settings: • From the phone tab: o Select **SIP Gateway** for the **Device Type**. o Enter **AvayaSipEnablementServices** in the **Registration ID** field. o Enter the IP address for Avaya SIP Enablement Services (**192.168.11.20**) in the **IP Address** field. o Select the calling plan for the private network (**PrivateNetwork**, see provisioning in **Step 5.26**) for the **Calling Plan**. o Select the private realm provisioned in **Step 5.50** for the **Realm**. o Provision any remaining parameters as per **Step 5.52**. • From the calls tab: o Select **Route Media** to enable this endpoint to route media to/from other endpoints. o Provision any remaining parameters as per **Step 5.53**.

6. Interoperability Compliance Testing

6.1. General Test Approach

The general test approach was to place SIP calls between the private and public networks through the NexTone MSX iServer to/from the Avaya Meeting Exchange S6800 Conferencing Server utilizing the network configuration displayed in **Section1**, **Figure 1**.
The main objectives were to verify the following:

- Dial-In Conferencing:
    - DNIS direct call function, where conference participants enter a conference as moderator, without entering a participant-access-code (passcode).
    - Scan call function, where conference participants enter a conference with a valid passcode.
- Dial-Out Conferencing:
    - Blast dial
        - Auto, where a conference participant enters a conference via a DNIS direct call function and autonomously invokes a Blast dial to a pre-provisioned dial list of one or more participants.
        - Manual, where a conference participant is already in a conference as moderator and invokes a Blast dial (by entering *92) to a pre-provisioned dial list of one or more participants.
    - Originator Dial-Out, where a conference participant is already in a conference as moderator and invokes a Dial-Out (by entering *1) to a single participant
    - Operator Fast Dial, where an operator can Dial-Out to a pre-provisioned dial list of one or more participants.
- Operator Dial-Out to establish an Audio Path.
- Operator Dial-In to establish an Audio Path.
- Dial-Out to an FDAPI channel for audio recording.
- Line Transfer invoked from Avaya Bridge Talk.
- Conference Transfer invoked from Avaya Bridge Talk.
- Touchtone commands {e.g.: *0 Request Help, *2 (as moderator) to start/stop conference recording, *3 to start/stop playback of conference recording, *5 (as moderator) toggle lecture on/off, *6 toggle mute on/off, *7 (as moderator) toggle conference security on/off, *8 play the roster of participant name during conference, *93X (where X is defined from 1 to 9) to invoke a subconference, *930 entered from a subconference to go back to the main conference, *93# entered from a subconference (as moderator) to bring all conference participants back to the main conference, ## (as moderator) to end the conference}.

- The following codecs were verified:
    - G711MU.
- The following SIP feature testing was verified:
    - Call Hold/Resume, invoked from endpoint(s) registered with a public network participating in an active conference call.
    - Call Transfer, imitated from an endpoint registered with a public network participating in an active conference call, transferred to an endpoint registered with a public network.

6.2. Test Results

The test objectives outlined in the general test approach were verified. The following observations were found during testing:

- Due to limitations found when the value for Min-SE timer is negotiated during Dial-Out procedures between the Avaya Meeting Exchange S6200 Application Server and the public network; it is recommended to provision the Min-SE timer on the Avaya Meeting Exchange S6200 Application Server equal to the value utilized on the public network (see **Step 3.2**).
- There were layer-3 network connectivity issues when **Always On** was selected for **Between Realms Media Routing** (see **Step 5.49** and **Step 5.50**). Network connectivity between the NexTone MSX iServer and the **NexthopIP** address (see **Step 7.6**) for the public network would bounce when **Always On** was selected for **Between Realms Media Routing**. The work around was to select **Don't Care** for **Between Realms Media Routing**.

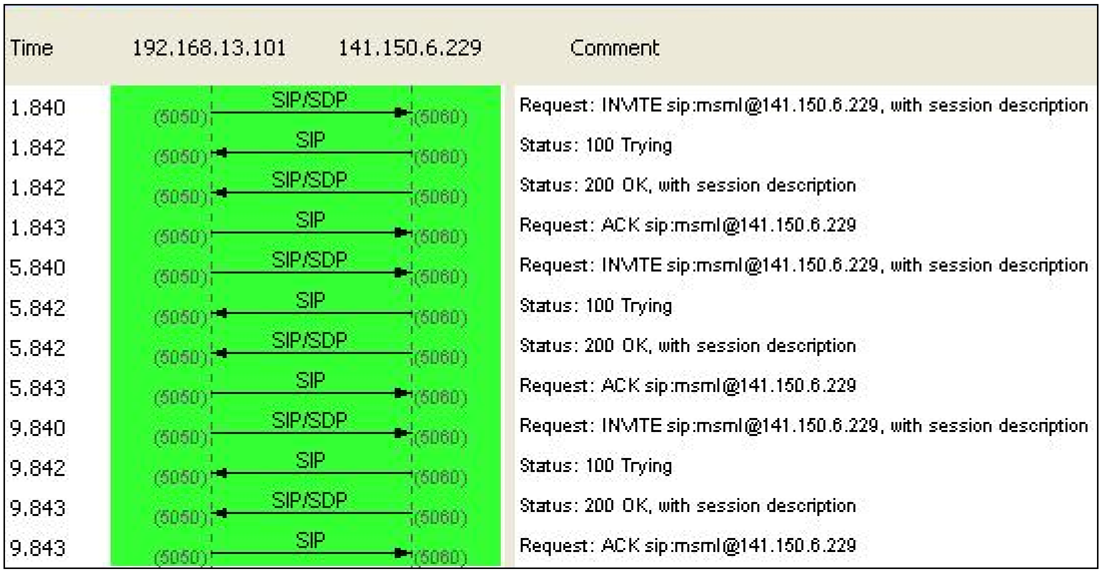
7. Verification Steps

The following steps can be used to troubleshoot network configurations in the field. The verification steps in this section will validate the following:

- The Avaya Meeting Exchange S6800 Conferencing Server configuration as displayed in **Section 1**, **Figure 2** (verified in **Step 7.1** and **Step 7.2**).
- NFS between the Avaya Meeting Exchange S6200 Application Server and the Convedia CMS-6000 Media Server MPC (verified in **Step 7.3 - Step 7.5**).
- Bi-directional end-to-end layer-3 connectivity between the MPC in slot 2 on the Convedia CMS-6000 Media Server and the public network (verified in **Step 7.6**).
- Verify successful inbound and outbound calls between the Avaya Meeting Exchange S6800 Conferencing Server and the public network (verified in **Step 7.7 - Step 7.12**).

Step	Description
7.1	Verify all conferencing related processes are running on the Avaya Meeting Exchange S6800 Conferencing Server as follows: • Log in to the Avaya Meeting Exchange S6200 Application Server console to access the CLI with the appropriate credentials. • cd to **/usr/dcb/bin** • At the command prompt, run the script **dcbps** and confirm all processes are running by verifying an associated Process ID (PID) for each process. ***Note**: The process, **convMS** is running, verifying the Convedia CMS-6000 is functioning as a media server in the Avaya S6800 Conferencing Server architecture (see **Section 1**, **Figure 2**).*

```
S6200App->dcbps
  1783   FP 101 ?        0:00 log
  1773   FP 144 ?        0:05 initdcb
  1784   FP 101 ?        0:00 bridgeTr
  1785   FP 105 ?        0:00 netservi
  1788   FP 129 ?        0:00 timer
  1789   FP 101 ?        0:00 traffic
  1790   FP 104 ?        0:00 chdbased
  1791   FP 101 ?        0:00 startd
  1792   FP 109 ?        0:00 cdr
  1793   FP 101 ?        0:00 modapid
  1794   FP 101 ?        0:00 schapid
  1795   FP 104 ?        0:00 callhand
  1796   FP 139 ?        0:00 initipcb
  1797   FP 139 ?        0:00 sipagent
  1798   FP 139 ?        0:00 msdispat
  1799   FP 139 ?        0:00 convMS
  1800   FP 139 ?        0:00 serverCo
  1556   TS  80 ?        0:00 sqlexecd with 5 children
```

Step	Description
7.2	Verify SIP connectivity between the Avaya Meeting Exchange S6800 Conferencing Server and the Convedia CMS-6000 Media Server. The call flow was captured from a mirrored port of the Avaya Meeting Exchange S6200 Application Server’s Ethernet interface, utilizing a network protocol analyzer and shows the “keep alive” SIP message set that is exchanged between the Avaya Meeting Exchange S6200 Application Server (**192.168.13.101**) and the control port on the Convedia CMS-6000 Media Server MPC in slot 2 (**141.150.6.229**). 

Time	192.168.13.101		141.150.6.229	Comment
1.840	(5050)	SIP/SDP →	(5060)	Request: INVITE sip:msml@141.150.6.229, with session description
1.842	(5050)	← SIP	(5060)	Status: 100 Trying
1.842	(5050)	← SIP/SDP	(5060)	Status: 200 OK, with session description
1.843	(5050)	SIP →	(5060)	Request: ACK sip:msml@141.150.6.229
5.840	(5050)	SIP/SDP →	(5060)	Request: INVITE sip:msml@141.150.6.229, with session description
5.842	(5050)	← SIP	(5060)	Status: 100 Trying
5.842	(5050)	← SIP/SDP	(5060)	Status: 200 OK, with session description
5.843	(5050)	SIP →	(5060)	Request: ACK sip:msml@141.150.6.229
9.840	(5050)	SIP/SDP →	(5060)	Request: INVITE sip:msml@141.150.6.229, with session description
9.842	(5050)	← SIP	(5060)	Status: 100 Trying
9.843	(5050)	← SIP/SDP	(5060)	Status: 200 OK, with session description
9.843	(5050)	SIP →	(5060)	Request: ACK sip:msml@141.150.6.229

Step	Description
7.3	Verify that the NFS server is mounted on the Convedia CMS-6000 Media Server MPC as follows: • Telnet to the Convedia SCC console (**141.150.6.228**, provisioned in **Step 3.13**) and log in to access the SCC CLI with the appropriate credentials. • From the Convedia SCC CLI command prompt: ○ [***Not Shown***] *Enter the command, **telnet mpc2** (the hostname for control interface on the MPC card in slot 2 provisioned in **Step 3.18**) and log in to the console to access the MPC CLI with the appropriate credentials*. • From the Convedia MPC CLI command prompt, change directory to **/mnt** and list files to verify the NFS server is mounted on this Convedia CMS-6000 Media Server MPC.

```
[mpc2]$ cd /mnt
[mpc2]$ ls -l
total 1
lrwxrwxrwx   1 root       23 Jan 16 10:32 192.168.13.101 -> /mnt/pfa_192.168.13.101
drwxrwxrwx   7 root      512 Dec 31  1999 flashdisk
drwxrwxrwx  16 root      512 Dec 20  2005 nvramdisk
drwxr-xr-x   5 root       96 Jun 29  2006 pfa_192.168.13.101
drwxrwxrwx  14 root      512 Nov  6  2006 ramdisk
```

Step	Description
7.4	Verify write privileges to the NFS server from the mount point on the Convedia CMS-6000 Media Server MPC as follows: • [***Not Shown***] *From /mnt, change directory to **pfa_192.168.13.101/usr3/confrp** and list files to verify the directory is empty*. • Create a file that does not already exist on the on the NFS server. • List the files in **pfa_192.168.13.101/usr3/confrp** and verify newly created file is present.

```
[mpc2]$ touch test.NFS
[mpc2]$ ls -l
-rw-r--r--   1 admin           0 Jan 16 15:11 test.NFS
```

Step	Description
7.5	From the NFS server, verify the file created in **Step 7.4** from the mount point on the Convedia CMS-6000 Media Server MPC is present in **/usr3/ipcb/usr3/confrp**.

```
S6200App->pwd
/usr3/ipcb/usr3/confrp
S6200App->ls -l
total 0
-rw-r--r--    1 500      500               0 Jan 16 15:11 test.NFS
```

Step	Description
7.6	Verify bi-directional end-to-end layer-3 connectivity between the MPC in slot 2 on the Convedia CMS-6000 Media Server and the public network using ping or another network diagnostic tool. Bi-directional end-to-end layer-3 connectivity between the MPC in slot 2 on the Convedia CMS-6000 Media Server and the public network implies a bi-directional audio path, e.g., layer-3 connectivity in one direction may imply one-way audio. This procedure accounts for the NexTone MSX iServer securing the public and private networks. First verify that the default gateways for the public and private networks are visible on the NexTone MSX iServer as follows: • Log in to the NexTone MSX iServer console to access the CLI with the appropriate credentials. • From the command prompt, enter the command **tcli**. • Enter **y** to display **ARP Cache**. • The ARP cache should display non-zero **NexthopMAC** addresses for the corresponding **NexthopIP** address entries. ***Note****: For brevity, some information is omitted from this screen capture.*

```
nextone-msw:~ # tcli

Choice:
y
CMD: y

ARP Cache
==========
                                                   L2 Table
NexthopIP       Port   Vlan   NexthopMAC           Index      ExpTime    CurTime
192.168.012.001  1        0   00:04:0d:a4:51:0c     32      1041193.00 1040000.00
192.168.050.001  0        0   00:04:96:1f:a7:27     31      1040681.00 1040000.00 ---
-------------------------------------------
```

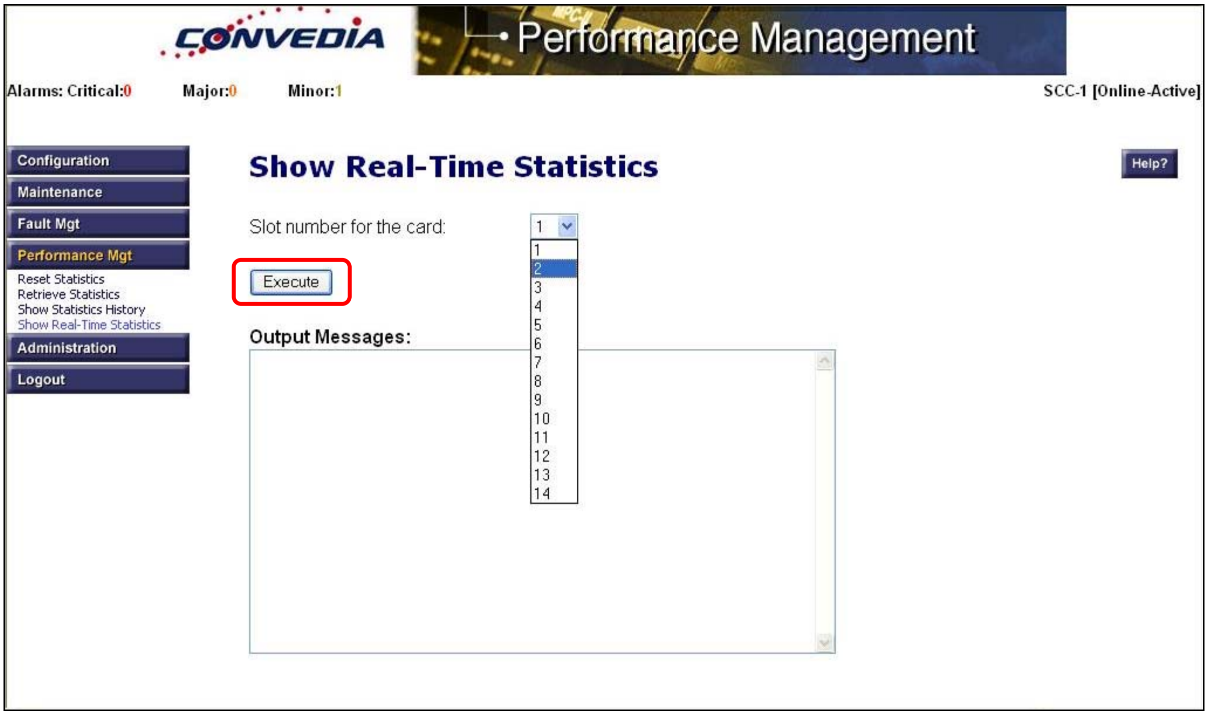
Verify bi-directional layer-3 connectivity between the MPC in slot 2 on the Convedia CMS-6000 Media Server and the public network as follows:

- From the NexTone MSX iServer, verify layer-3 connectivity to both the public (**192.168.50.1**) and private (**192.168.12.1**) networks by pinging the **NexthopIP** address entries from the NexTone MSX iServer.
- Verify layer-3 connectivity from the MPC in slot 2 on the Convedia CMS-6000 to the **NexthopIP** address for the private network.
- Verify layer-3 connectivity to the MPC in slot 2 on the Convedia CMS-6000 from the **NexthopIP** address for the private network.

7.1. Verify Call Routing

The following steps utilize the network configuration displayed in **Section1**, **Figure 1** to verify the general test approach defined in **Section 6**.

Step	Description

7.7	The purpose of this step (and **Step 7.8**) is to obtain a baseline for the number of ports created on the MPC in slot 2 on the Convedia CMS-6000 Media Server prior to the scenario invoked in **Step 7.9**. Verify port utilization on the Convedia CMS-6000 Media Server MPC in slot 2 as follows:
	• [***Optional, Not Shown***] *Reset statistics for the MPC card in slot 2 as follows:*
	    ○ *Click **Configuration** ➔ **Performance Mgt** ➔ **Reset Statistics**.*
	    ○ *Select the **Slot Number for the** MPC. For these Application Notes, the MPC was placed in **Slot number 2**.*
	    ○ *Click **Execute** and wait for the message **Statistics for card in slot 2 have been reset** to display in the **Output Messages** window.*
	• Click **Configuration** ➔ **Performance Mgt** ➔ **Show Real-Time Statistics**.
	• Select the **Slot Number for the** MPC. For these Application Notes, the MPC was placed in **Slot number 2**.
	• Click **Execute**.
	
	Show Real-Time Statistics
	Slot number for the card: 1

Step	Description
7.8	From the **Show Real-Time Statistics** screen that is displayed, note that the number of **Ports Created** for the MPC in slot 2 is **0**. 

Show Real-Time Statistics

Slot number for the card: 2

Output Messages:

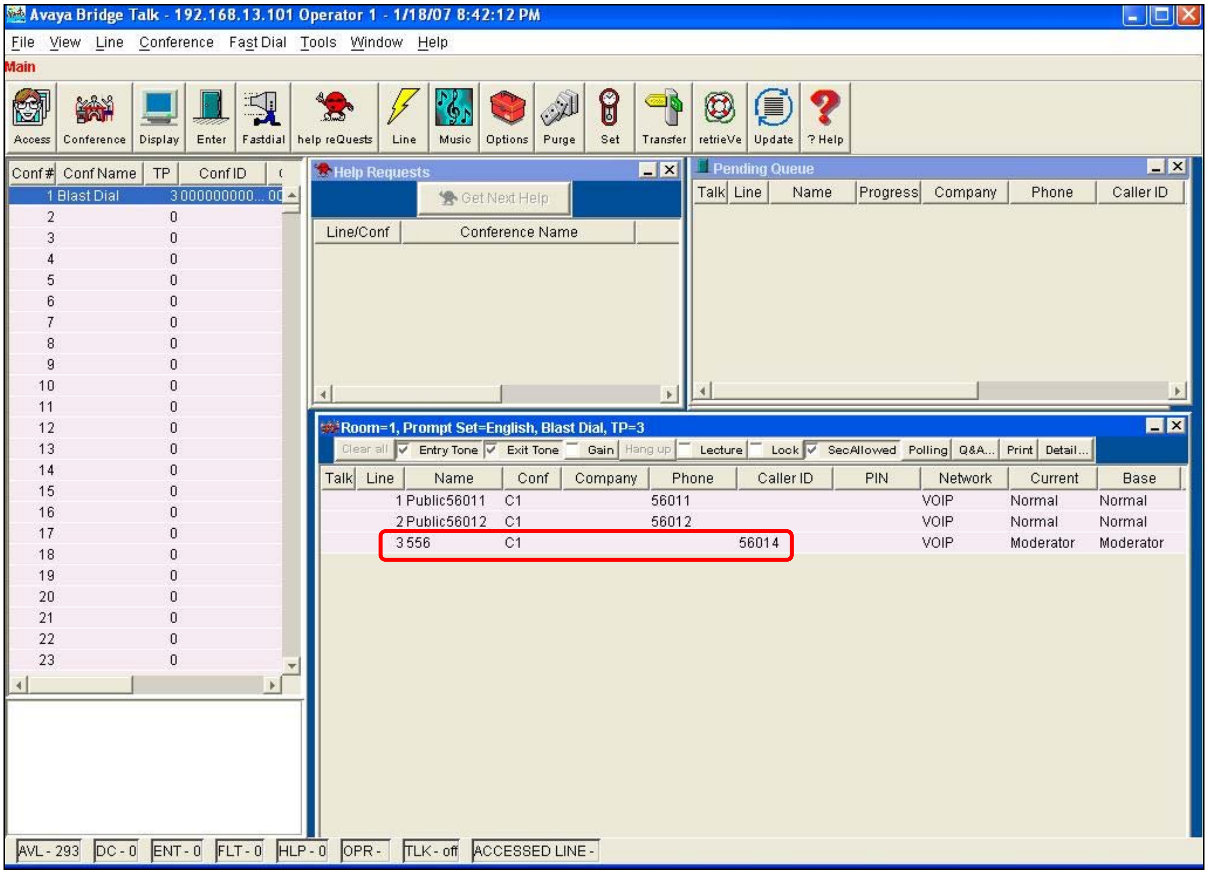
```
Card Statistics
---------------

Max CPU Utilization                          17%
Avg CPU Utilization                          0%
Current CPU Utilization                      0%
Ports Created                                0
Max Announcements                            0
Max Conference Bridges                       0
Max Recordings                               0
Max DTMF Detectors                           0
Port 1 TX Average Bandwidth Utilization      0%
Port 1 RX Average Bandwidth Utilization      0%
Port 1 TX Max Bandwidth Utilization          0%
Port 1 RX Max Bandwidth Utilization          0%
Port 2 TX Average Bandwidth Utilization      0%
```

Step **Description**

7.9 Verify end-to-end signaling/media connectivity between the Avaya Meeting Exchange S6800 Conferencing Server and the public network via Avaya SIP Enablement Services and the NexTone MSX iServer. This is accomplished by placing calls to and from the Avaya Meeting Exchange S6800 Conferencing Server. This step utilizes the Avaya Bridge Talk application to verify calls to and from the Avaya Meeting Exchange S6800 Conferencing Server are managed correctly, e.g., callers are added/removed from conferences. This step will also verify conferencing applications provisioned in **Section 3**.

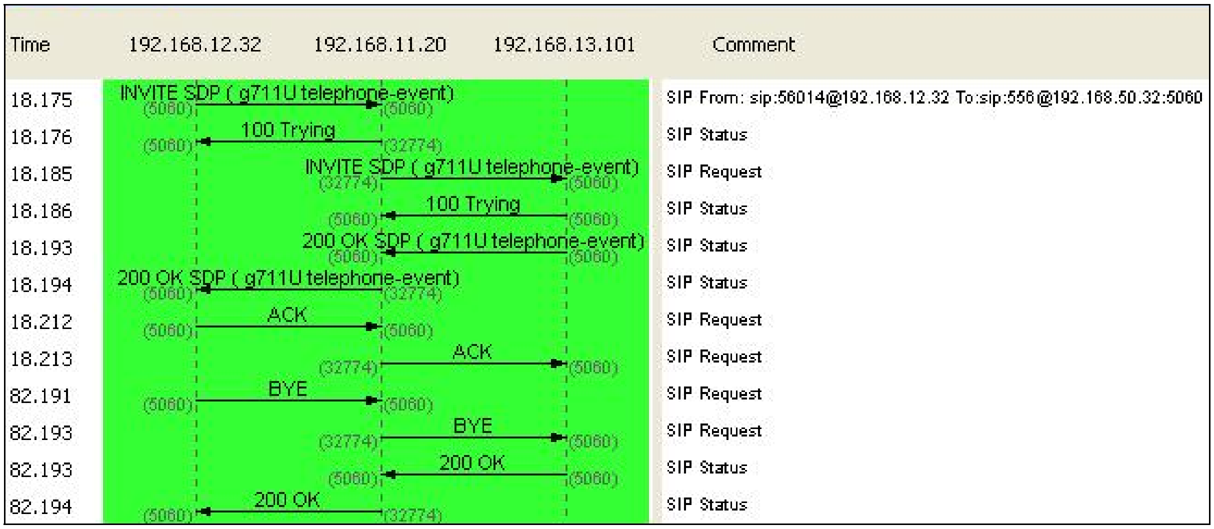
- From an endpoint registered to the public network, Dial **556** to enter a conference as **Moderator** (without passcode) while simultaneously invoking the associated Auto Blast dial feature for this conference (see **Step 3.37**).
- If not already logged on, log in to the Avaya Bridge Talk application with the appropriate credentials.
- **Double-Click on the** highlighted **Conf #** to open a **Conference Room** window.
- Verify conference participants are added/removed from conferences by observing the Conference Navigator and/or Conference Room windows.

  ***Note**: The ANI extracted via the procedures in **Step 3.3** is displayed in the **Caller ID** field for the participant Dialing-In to this conference.*

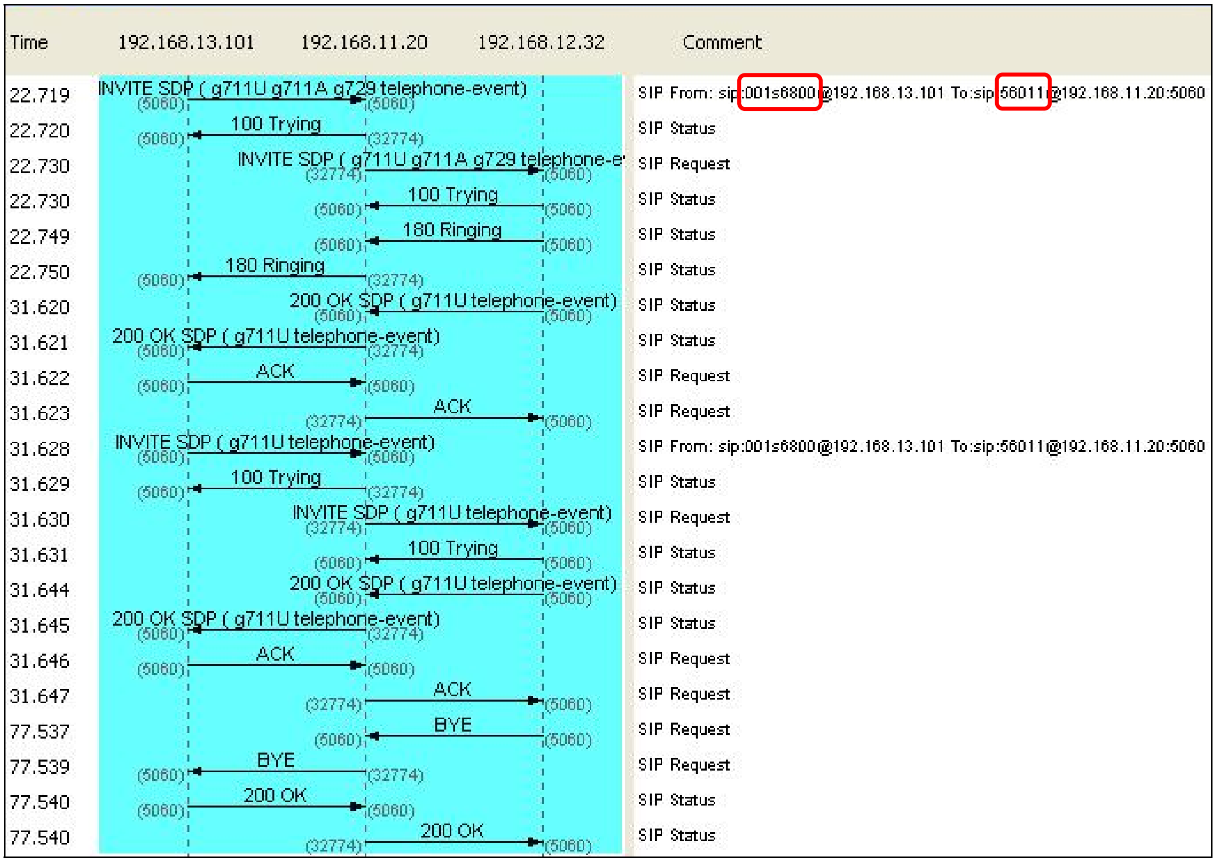


Conf #	Conf Name	TP	Conf ID
1	Blast Dial	3	000000000... 00
2		0	
3		0	
4		0	
5		0	
6		0	
7		0	
8		0	
9		0	
10		0	
11		0	
12		0	
13		0	
14		0	
15		0	
16		0	
17		0	
18		0	
19		0	
20		0	
21		0	
22		0	
23		0	

Talk	Line	Name	Conf	Company	Phone	Caller ID	PIN	Network	Current	Base
	1	Public56011	C1		56011			VOIP	Normal	Normal
	2	Public56012	C1		56012			VOIP	Normal	Normal
	3	556	C1			56014		VOIP	Moderator	Moderator

Step	Description
7.10	The following SIP call flow displays the moderator Dial-In to the Avaya Meeting Exchange S6800 Conferencing Server from an endpoint (**56014**) on the public network invoked in **Step 7.9**. The call flow was captured from a mirrored port of Avaya SIP Enablement Services' Ethernet interface, utilizing a network protocol analyzer and shows SIP signaling between: • The private signaling interface on the NexTone MSX iServer (**192.168.12.32**). • Avaya SIP Enablement Services (**192.168.11.20**). • The Avaya Meeting Exchange S6200 Application Server (**192.168.13.101**). 

Time	192.168.12.32	192.168.11.20	192.168.13.101	Comment
18.175	INVITE SDP (g711U telephone-event) (5060)	(5060)		SIP From: sip:56014@192.168.12.32 To:sip:556@192.168.50.32:5060
18.176	(5060)	100 Trying (32774)		SIP Status
18.185		INVITE SDP (g711U telephone-event) (32774)	(5060)	SIP Request
18.186		(5060)	100 Trying (5060)	SIP Status
18.193		(5060)	200 OK SDP (g711U telephone-event) (5060)	SIP Status
18.194	(5060)	200 OK SDP (g711U telephone-event) (32774)		SIP Status
18.212	ACK (5060)	(5060)		SIP Request
18.213		ACK (32774)	(5060)	SIP Request
82.191	BYE (5060)	(5060)		SIP Request
82.193		BYE (32774)	(5060)	SIP Request
82.193		(5060)	200 OK (5060)	SIP Status
82.194	(5060)	200 OK (32774)		SIP Status

Step	Description
7.11	The following SIP call flow displays the Dial-Out from the Avaya Meeting Exchange S6800 Conferencing Server to an endpoint (**56011**) on the public network invoked in **Step 7.9**. The call flow was captured from a mirrored port of Avaya SIP Enablement Services' Ethernet interface, utilizing a network protocol analyzer and shows SIP signaling between: • The Avaya Meeting Exchange S6200 Application Server (**192.168.13.101**). • Avaya SIP Enablement Services (**192.168.11.20**). • The private signaling interface on the NexTone MSX iServer (**192.168.12.32**). ***Note****: For brevity, the Blast dial to only one of the endpoints in the Dial List provisioned in* ***Step 3.34*** *is displayed****.*** *The user field* ***001s6800*** *provisioned in* ***Step 3.2*** *present in the* ***From*** *header field in the call flow displayed below. The dialed number* ***56011*** *is present in the* ***To*** *header field (see* ***Step 3.4****).* 

Time	192.168.13.101 192.168.11.20 192.168.12.32	Comment
22.719	INVITE SDP (g711U g711A g729 telephone-event)	SIP From: sip:001s6800@192.168.13.101 To:sip:56011@192.168.11.20:5060
22.720	100 Trying	SIP Status
22.730	INVITE SDP (g711U g711A g729 telephone-e	SIP Request
22.730	100 Trying	SIP Status
22.749	180 Ringing	SIP Status
22.750	180 Ringing	SIP Status
31.620	200 OK SDP (g711U telephone-event)	SIP Status
31.621	200 OK SDP (g711U telephone-event)	SIP Status
31.622	ACK	SIP Request
31.623	ACK	SIP Request
31.628	INVITE SDP (g711U telephone-event)	SIP From: sip:001s6800@192.168.13.101 To:sip:56011@192.168.11.20:5060
31.629	100 Trying	SIP Status
31.630	INVITE SDP (g711U telephone-event)	SIP Request
31.631	100 Trying	SIP Status
31.644	200 OK SDP (g711U telephone-event)	SIP Status
31.645	200 OK SDP (g711U telephone-event)	SIP Status
31.646	ACK	SIP Request
31.647	ACK	SIP Request
77.537	BYE	SIP Request
77.539	BYE	SIP Request
77.540	200 OK	SIP Status
77.540	200 OK	SIP Status

Step	Description
7.12	Verify port utilization on the Convedia CMS-6000 Media Server MPC in slot 2 following the scenario invoked in **Step 7.9** as follows: - From the **Show Real-Time Statistics** screen (opened via procedures in **Step 7.7**), click **Execute**. - Note that the number of **Ports Created** for the MPC in slot 2 is greater that the number of ports created prior to the scenario invoked in **Step 7.9**. ***Note**: This step (in conjunction with **Step 7.7** and **Step 7.8**) validates that the Convedia CMS-6000 Media Server is functioning as a media server. The Avaya Meeting Exchange S6200 Application Server has the capability to function as a stand-alone media server. Validating that ports were created on the Convedia CMS-6000 Media Server following a call scenario verifies the Avaya Meeting Exchange S6800 Conferencing Server configuration.*

Alarms: Critical:0 Major:0 Minor:1 SCC-1 [Online-Active]

Show Real-Time Statistics

Slot number for the card: 2

Output Messages:

```
Card Statistics
---------------

Max CPU Utilization                        8%
Avg CPU Utilization                        0%
Current CPU Utilization                    0%
Ports Created                              4
Max Announcements                          4
Max Conference Bridges                     1
Max Recordings                             0
Max DTMF Detectors                         3
Port 1 TX Average Bandwidth Utilization    0%
Port 1 RX Average Bandwidth Utilization    0%
Port 1 TX Max Bandwidth Utilization        2%
Port 1 RX Max Bandwidth Utilization        1%
Port 2 TX Average Bandwidth Utilization    0%
```

8. Conclusion

These Application Notes provide administrators with the procedures to configure connectivity between the Avaya Meeting Exchange S6800 Conferencing Server and a public network via Avaya SIP Enablement Services and the NexTone MSX iServer. These procedures were validated according to the general test approach as defined in **Section 5.1**.

9. Additional References

Avaya references, available at http://support.avaya.com

1. *Meeting Exchange 4.1 Administration and Maintenance S6200/S6800 Media Server*, Issue 1, Doc ID 04-601168, July 2006.
2. *Meeting Exchange 4.1 Configuring S6200, S6500, and S6800 Conferencing Servers*, Issue 1, Doc ID 04-601338, July 2006.
3. *Avaya Meeting Exchange Groupware Edition Version 4.1 User's Guide for Bridge Talk*, Doc ID 04-600878, Issue 2, July 2006.

NexTone references, available at http://www.nextone.com

4. *NexTone iServer (MSC and MSW) Installation and Operation Guide Release 4.0,* BN-MSX4.0-IOG-5, Issue 5, February 2, 2006.
5. *iView Management System (iVMS) Installation and Operations Guide Release 4.0,* BN-IVMS4.0-IOG-1, Issue 2 August 31, 2005.

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.