AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Mobile Communication System (G350 Option) with Clear Channel Satellite XtremeSat in a PSTN Hop-off Environment – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Avaya Mobile Communication System with Clear Channel Satellite XtremeSat in a PSTN hop-off environment.

Avaya Mobile Communication System (MCS) is a compact highly mobile full featured communication system designed for rapid deployment in disaster stricken or remote areas where other systems may have been damaged or do not exist. Avaya MCS can be connected to traditional and non-traditional networking facilities in a variety of ways. These Application Notes focus on the interoperability of Avaya MCS with the Clear Channel Satellite XtremeSat service to provide Internet and PSTN connectivity via a satellite link.

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

CTM; Reviewed:
SPOC 3/26/2008

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

1 of 30
clearMcsG350

1. Introduction

These Application Notes describe the procedures for configuring Avaya Mobile Communication System with Clear Channel Satellite XtremeSat in a PSTN hop-off environment.

Avaya Mobile Communication System (MCS) is a compact highly mobile full featured communication system designed for rapid deployment in disaster stricken or remote areas where other systems may have been damaged or do not exist. Avaya MCS can be connected to traditional and non-traditional networking facilities in a variety of ways.

Depending on the application and deployment environment, Avaya MCS can be constructed using different Avaya system platforms and various equipment and networking options which are mounted in a rugged rack case and powered by an Uninterruptable Power Supply (UPS). For more details on the various options available with Avaya MCS, refer to [8].

For the PSTN hop-off application described in these Application Notes, Avaya MCS consisted of the following:
- Avaya G350 Media Gateway
  - S8300 Server running Avaya Communication Manager and Avaya IA 770 Intuity Audix
  - MM314 (24-port Ethernet media module)
- Avaya H.323 IP endpoints
- Optionally, other media modules and endpoints to support other interfaces (e.g., analog)
- RAD Communications voice multiplexer (Vmux) (required for satellite option)
- EMS 2000 Series satellite interactive terminal (SIT) (required for satellite option)
- Very Small Aperture Terminal (VSAT) (required for satellite option)

These Application Notes focus on the interoperability of Avaya MCS with the Clear Channel Satellite XtremeSat service to provide Internet and PSTN connectivity via a satellite link.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows Avaya MCS at a remote site connected through XtremeSat to the Clear Channel Satellite earth station. The Clear Channel Satellite earth station provides connectivity to the Internet and the PSTN for the users of the XtremeSat service.

As previously mentioned, Avaya MCS can be constructed with several equipment options. **Figure 1** shows Avaya MCS with the G350 option which consists of an Avaya G350 Media Gateway with a S8300 Server running Avaya Communication Manager and Avaya IA 770 Intuity Audix. Avaya IA 770 Intuity Audix provides voice mail for the endpoints located at the remote site. Typically, the components of Avaya MCS, except the satellite dish and telephones, are mounted in a compact rugged rack case. For the purposes of clarity, the components are shown separately in **Figure 1**.

The Avaya G350 Media Gateway is connected to a RAD Data Communications Vmux-104 voice multiplexer (Vmux) by an IP connection. This connection spans from the FastEthernet 10/2 port on

the Avaya G350 Media Gateway to the user port of the Vmux. In addition, the Avaya G350 Media Gateway is connected to the Vmux using two of a possible four FXS analog connections. The purpose of the Vmux is to multiplex data traffic on the user port IP connection with voice traffic on the analog connections into a single data stream on the network port of the Vmux which connects to the EMS 2000 Series satellite interactive terminal (SIT). Both the network port of the Vmux and the SIT are assigned public IP addresses from the service provider (Clear Channel Satellite). For reasons of security, all public IP addresses referenced in these Application Notes have been replaced with IP addresses in the range of 192.168.100.0 to 192.168.110.254.

The SIT is connected directly via coax cable to the satellite dish. XtremeSat uses a small dish at the remote site known as a Very Small Aperture Terminal (VSAT) to communicate to the earth station at the other end using the Digital Video Broadcast Return Channel via Satellite (DVB-RCS) standard. Compliance testing was conducted with two types of VSATs: a one meter fixed dish and a .76 meter auto-acquisition dish. The auto-acquisition dish is designed to automatically locate and lock on the satellite signal when powered up and deployed.

Lastly, endpoints at the site include four Avaya 4600 Series IP Telephones (with H.323 firmware), an Avaya one-X Deskphone Edition (H.323), an Avaya IP Softphone (H.323), an analog phone and fax machine.

In the PSTN hop-off configuration shown in **Figure 1**, all calls between the remote site and the earth station utilize the analog trunks. All data traffic between the remote site and the earth station use the IP connection. The Vmux multiplexes the traffic on the user port IP connection with the traffic on the analog trunks prior to sending the media stream to the network port IP connection. At the earth station, the media stream is received from the satellite connection and demultiplexed by a Vmux located in the service provider network (not shown). The data traffic is sent to the Internet and the voice traffic is sent to the PSTN. A similar procedure happens in the reverse direction for incoming calls to the remote site.

It should be noted that calls between the Avaya MCS and the main site will experience one to two seconds of delay. This is expected with the known latency of a satellite link.
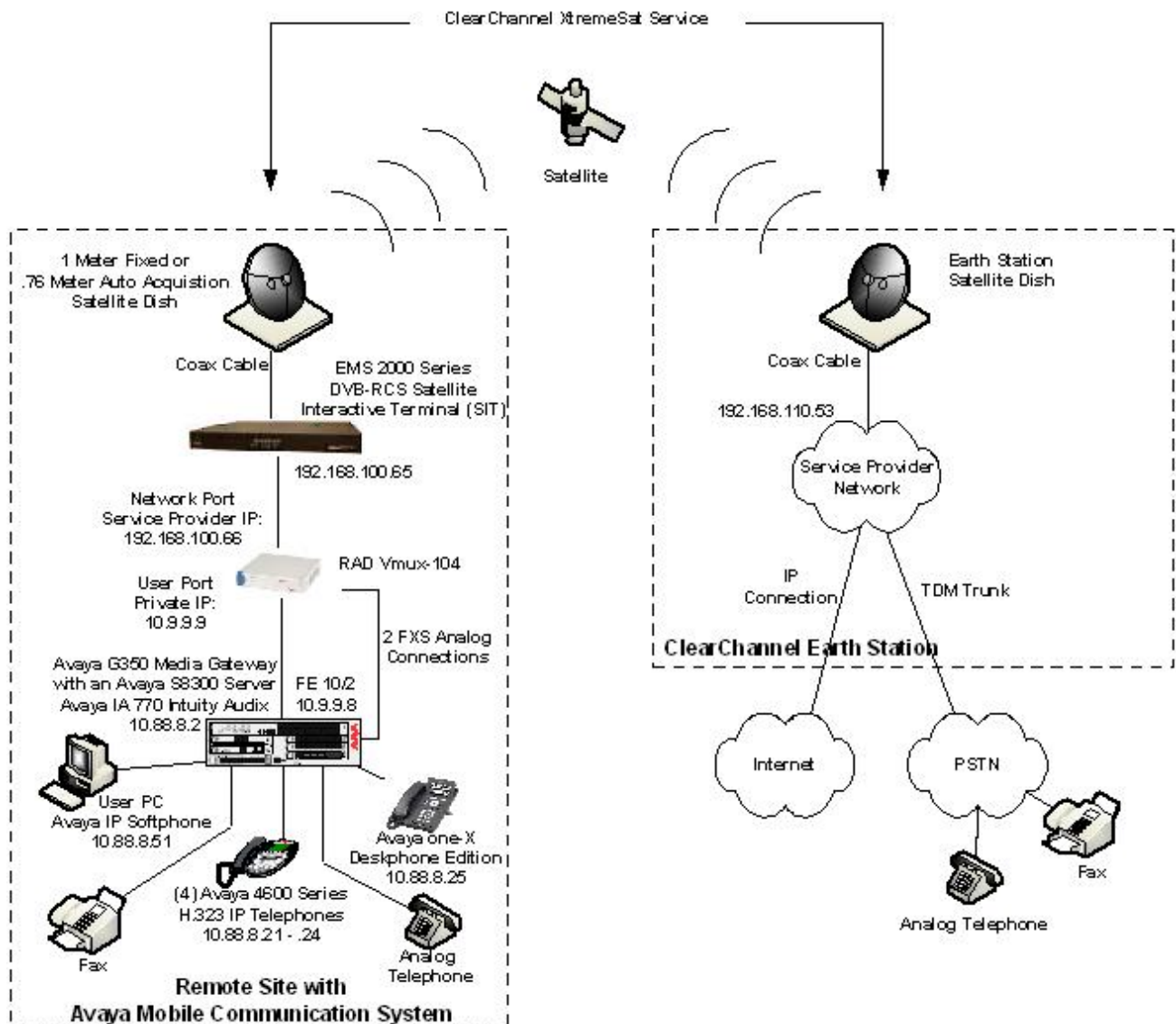
Figure 1: Avaya MCS PSTN Hop-off Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server	Avaya Communication Manager 4.0.1 (with Avaya IA 770 Intuity Audix) (R014x.00.1.731.2) Service Pack 00.1.731.2-14330

Avaya G350 Media Gateway
    MM314   (24-port Ethernet media module)
    MM711AP (8-port Analog media module)
	26.33.0
	 -
	 HW 5 FW 17

Avaya 4602SW IP Telephone	H.323 version 2.3
Avaya 4620SW IP Telephone Avaya 4621SW IP Telephone Avaya 4625SW IP Telephone	H.323 version 2.8
Avaya IP Softphone	6.0 (H.323) (Build 6.0.0.25) on Windows XP Professional SP2
Avaya one-X Deskphone Edition	1.5 (H.323)
Analog telephones	-
Fax machines	-
RAD Data Communications Vmux-104	HW (2.00) FW (1.40) SW (3.04CW)

Clear Channel Satellite XtremeSat
    • EMS 2000 Series (SIT)
    • VSAT
	-
	 V3009.R05
	 -

3. Configure Avaya G350 Media Gateway

This section describes the Avaya G350 Media Gateway configuration. This section assumes the media gateway has been installed using the procedures described in [1] and [2] and contains a MM314 Ethernet media module and a MM711 Analog media module for connecting to the Vmux. The complete media gateway configuration file is included in **Appendix A**.

This section covers the following topics:
- Configuring interfaces.
- Creating the media gateway controller (mgc) list.
- Defining a default gateway.
- Saving the configuration.

Step	Description
| 1. | **Interface VLAN 1**<br>Create a VLAN for use by Avaya Communication Manager and the Avaya H.323 endpoints. The compliance test used the default VLAN configuration for the Avaya G350 Media Gateway. In the default configuration, all 24 ports of the MM314 are assigned to a single VLAN named V1 with VLAN id of 1. This VLAN was also configured to be the primary management interface (**pmi**) and the VLAN where the Avaya S8300 Server was connected (**icc-vlan**). In addition, an IP address and subnet mask (layer 3 routing interface) was assigned to this VLAN. The example below shows how to set these parameters for VLAN 1.<br><br>```
G350-???(super)# interface Vlan 1
G350-???(super-if:Vlan 1)# pmi
G350-???(super-if:Vlan 1)# icc-vlan
G350-???(super-if:Vlan 1)# ip address 10.88.8.4 255.255.255.0
G350-???(super-if:Vlan 1)# exit
``` |
| 2. | **Interface FastEthernet 10/2**<br>Configure an interface for connection to XtremeSat. The compliance test used the **FastEthernet 10/2** port on the Avaya G350 Media Gateway chassis as the WAN connection to XtremeSat. This port on the media gateway was connected to the **User** port on the Vmux. In addition, an IP address and subnet mask (layer 3 routing interface) was assigned. The example below shows how to configure the **FastEthernet 10/2** interface.<br><br>```
G350-???(super)# interface FastEthernet 10/2
G350-???(super-if:FastEthernet 10/2)# ip address 10.9.9.8 255.255.255.0
G350-???(super-if:FastEthernet 10/2)# exit
``` |

Step	Description
3.	**Media Gateway Controller List** Create the list of controllers with which the media gateway will attempt to register. For the compliance test, a single controller was used which was the Avaya S8300 Server in the Avaya MCS with IP address 10.88.8.2. `G350-???(super)# `**`set mgc list 10.88.8.2`**
4.	**Default Gateway** Configure a default gateway. The default gateway was set to the private side IP address (**User** port) of the Vmux as defined in **Figure 1**. The example below shows how to set this value. `G350-???(super)# `**`ip default-gateway 10.9.9.9`**
5.	**Save Configuration** Use the **copy running-config startup-config** command to save the configuration. `G350-???(super)# `**`copy running-config startup-config`**

4. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration. This section assumes the Avaya S8300 Server has been installed using the procedures described in [2]. As part of these procedures, the default gateway of the Avaya S8300 Server was configured as the IP address of the Vlan 1 interface of the Avaya G350 Media Gateway (10.88.8.4).

This section describes the configuration of the components necessary to support the creation of an analog trunk and the routing of traffic to it. This includes the following components or services:
- Trunk group
- Route pattern
- Automatic Route Selection (ARS)

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

Step	Description

1.	**Trunk Group**
	Create a trunk group for the analog trunks between the MM711 media module and the FXS ports of the Vmux. These trunks provide the physical access to XtremeSat for the voice traffic. The Vmux can support up to four trunks. For the purposes of the compliance test, two trunks were used. The trunk group was created with the parameters described below.
	
	• **Group Type**: *co* Defines the trunk group as analog central office trunks.
	• **Group Name**: Any descriptive name can be used.
	• **TAC**: The TAC must be consistent with the existing dial plan.
	• **Incoming Destination**: This extension will ring when an incoming call seizes a trunk in this group. In a customer configuration, this would normally be the extension of an attendant.
	• **Trunk Type:** *loop-start* Defines the trunk group to use loop-start signaling.
	
	<pre>display trunk-group 1 Page 1 of 21
	                         TRUNK GROUP
	
	Group Number: 1 Group Type: co CDR Reports: y
	  Group Name: PSTN COR: 1 TN: 1 TAC: 101
	    Direction: two-way Outgoing Display? n
	 Dial Access? y Busy Threshold: 255 Night Service:
	Queue Length: 0 Country: 1 Incoming Destination: 30103
	   Comm Type: voice Auth Code? n Digit Absorption List:
	    Prefix-1? y Trunk Flash? n Toll Restricted? y
	
	        Trunk Type: loop-start
	</pre>

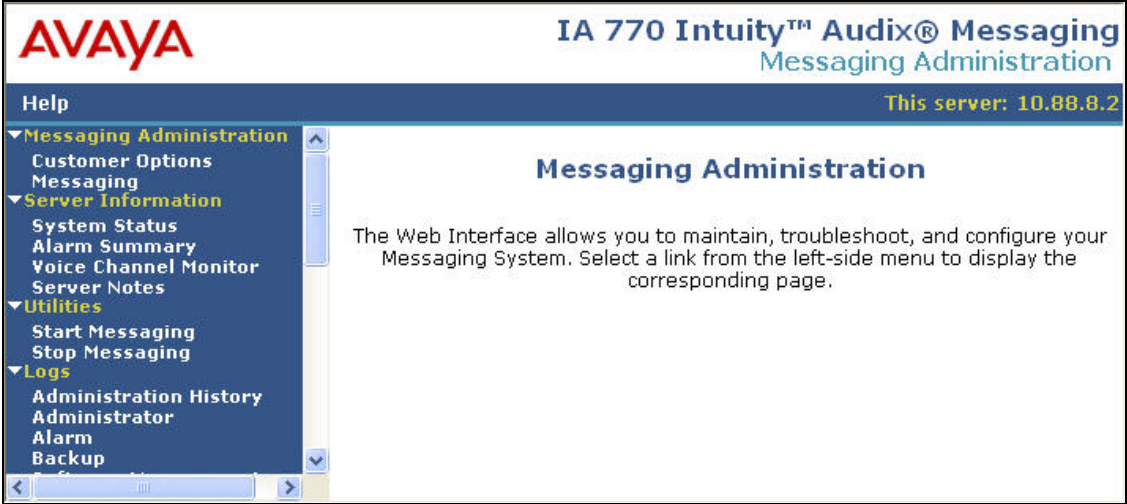| Step	Description

2.	**Trunk Group – continued**
	Navigate to **Page 3**, set the **Receive Analog Incoming Call ID** field to the Caller ID format that the trunk is expecting to receive. In the case of the compliance test, the value of *Bellcore* was used.
	
	Please note that this parameter will not appear on the trunk group form if analog Caller ID has not been enabled. Use the **display system-parameters customer-options** command to verify that the **Analog Trunk Incoming Call ID** field is set to *y*.
	
	<pre>display trunk-group 1 Page 3 of 21
	TRUNK FEATURES
	         ACA Assignment? n Measured: none
	                                                 Maintenance Tests? y
	                              Data Restriction? n
	
	   Abandoned Call Search? n
	   Suppress # Outpulsing? n
	
	      Charge Conversion: 1
	         Decimal Point: none Replace Restricted Numbers? n
	        Currency Symbol: Replace Unavailable Numbers? n
	            Charge Type: units **Receive Analog Incoming Call ID: Bellcore**
	                                             Per Call CPN Blocking Code:
	                                           Per Call CPN Unblocking Code:
	
	             Outgoing ANI: Ds1 Echo Cancellation? n</pre>

3.	**Trunk Group – continued**
	Enter each individual trunk to the trunk group. On **Page 5**, enter the port designation of the trunk in the **Port** column. In the compliance test, the MM711 was in slot 4 of the Avaya G350 Media Gateway. The first two ports of the MM711 were connected to the Vmux. Thus, the example below shows ports *001V401* and *001V402* in the trunk group.
	
	<pre>display trunk-group 1 Page 5 of 21
	                             TRUNK GROUP
	                               Administered Members (min/max): 1/2
	GROUP MEMBER ASSIGNMENTS Total Administered Members: 2
	
	       Port Code Sfx Name Night Mode Type Ans Delay
	  1: **001V401** MM711
	  2: **001V402** MM711
	  3:
	  4:</pre>

Step	Description

4.	**Route Pattern**
	
	Create a route pattern for use by Automatic Route Selection (ARS) to route calls to the trunk group defined in **Step 1** which provides the voice access to XtremeSat.
	
	The example below shows the route pattern created for the compliance test. The **Pattern Name** can be set to any descriptive name. The **Grp No** field was set to the trunk group number defined in **Step 1**. The Facility Restriction Level (**FRL**) field was set to a level that allows access to this trunk for all users that require it. The value of *0* is the least restrictive level. The Prefix Mark (**Pfx Mrk**) field was set to *1*. This will add a 1 to all user-dialed 10 digit calls and will not alter $1 + 10$ digit dialed calls. Default values were used for all other fields.
	
	<pre>display route-pattern 1 Page 1 of 3
	              Pattern Number: 1 Pattern Name: PSTN
	                           Secure SIP? n
	    Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC
	    No Mrk Lmt List Del Digits QSIG
	                        Dgts Intw
	  1: 1 0 1 n user
	  2: n user
	  3: n user
	  4: n user
	  5: n user
	  6: n user
	
	     BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR
	     0 1 2 3 4 W Request Dgts Format
	                                                            Subaddress
	  1: y y y y y n n rest none
	  2: y y y y y n n rest none
	  3: y y y y y n n rest none
	  4: y y y y y n n rest none
	  5: y y y y y n n rest none
	  6: y y y y y n n rest none</pre>

Step	Description

5.	**Automatic Route Selection (ARS)**
	ARS was used to define which dialed digits are associated with the route pattern providing access to XtremeSat. In a customer installation, all PSTN dialed numbers would be routed to XtremeSat and the ARS table would reflect this fact. For the purposes of the compliance test, only PSTN numbers that begin with 1732 were used for testing.
	
	The **display ars analysis _n_** command shows the entry in the ARS Digit Analysis Table for the dialed string beginning with **_n_**. In the example shown, PSTN numbers that begin with 1732 and 11 digits long use route pattern 1 which was defined in the previous step.
	
	<pre>display ars analysis 1732 Page 1 of 2
	                        ARS DIGIT ANALYSIS TABLE
	                           Location: all Percent Full: 3
	
	            Dialed Total Route Call Node ANI
	            String Min Max Pattern Type Num Reqd
	       1732 11 11 1 fnpa n
	       174 11 11 deny fnpa n
	       175 11 11 deny fnpa n
	       176 11 11 deny fnpa n
	       177 11 11 deny fnpa n</pre>

5. Configure Avaya IA 770 Intuity Audix

The section describes how to configure the disconnect options on Audix so that Audix disconnects on silence. This is necessary since the Vmux does not send far-end disconnect/disconnect supervision to the Avaya G350 Media Gateway when the caller at the far-end hangs up. For all other information relating to Audix configuration, refer to [4].
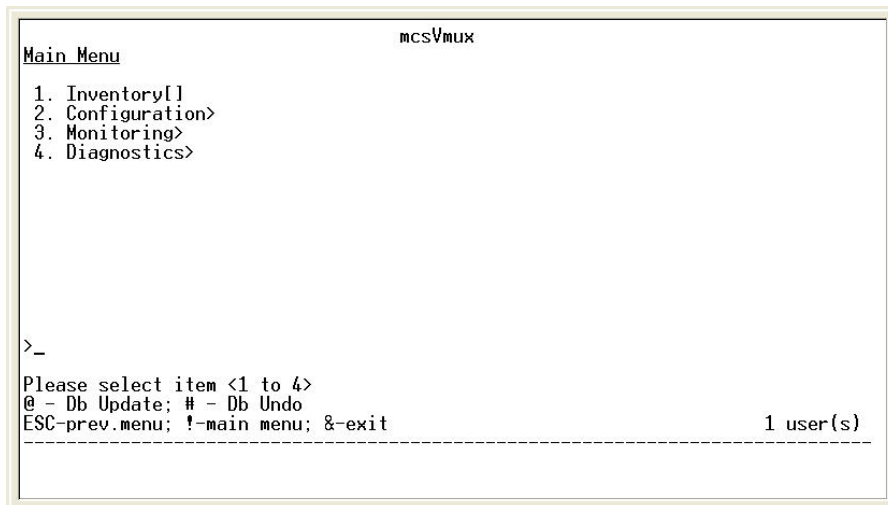
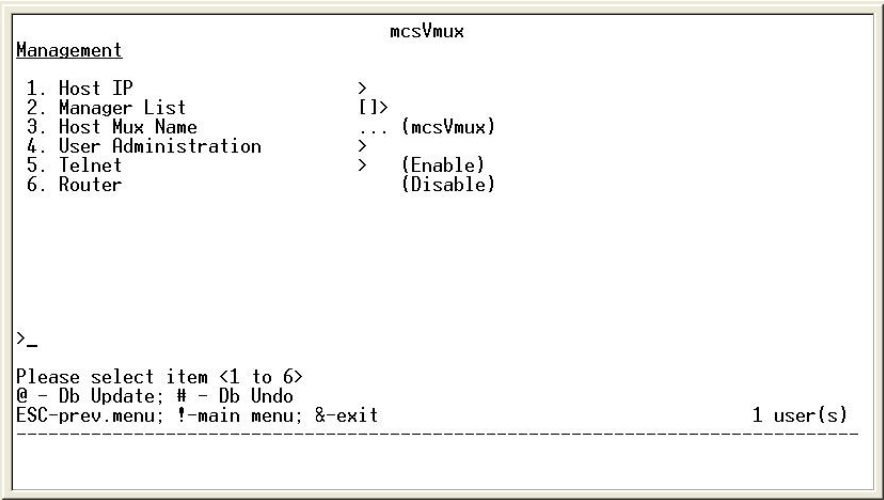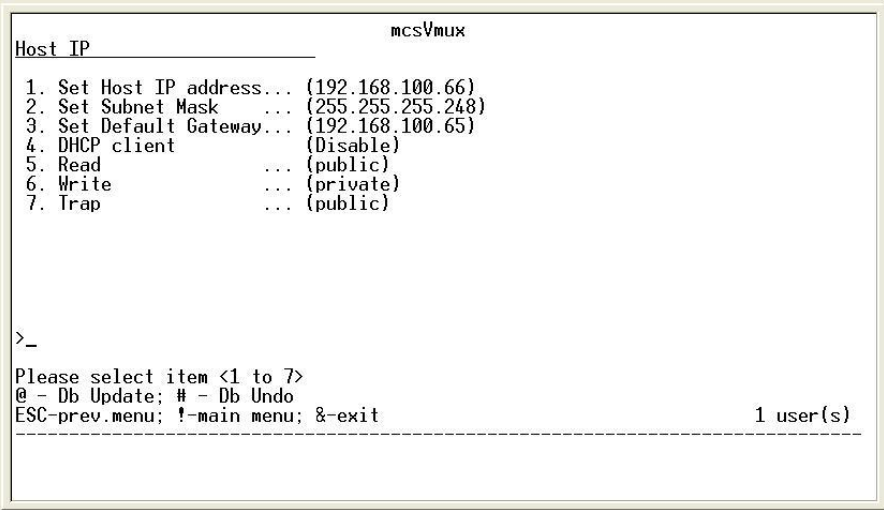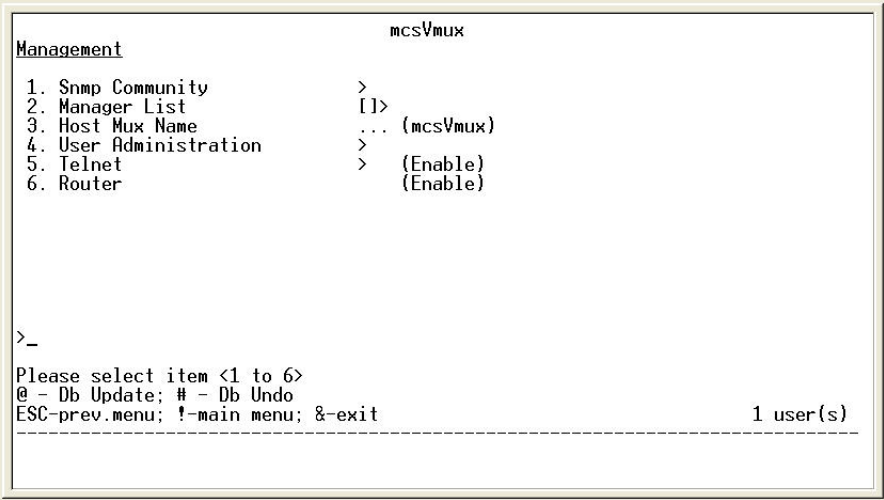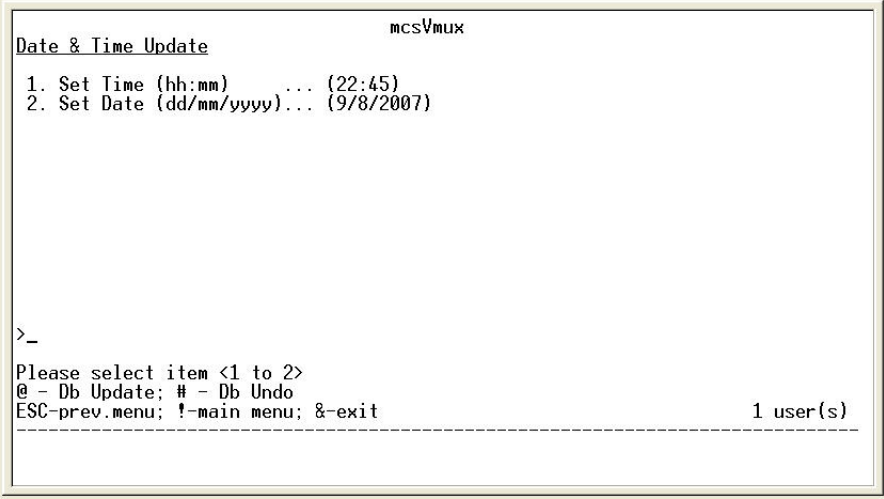| Step	Description
1.	**Main Menu** The Audix main menu is accessed from the Avaya Communication Manager web interface. Launch a web browser and enter the IP address of the Avaya Communication Manager in the URL field. On the resulting page, Click the **Launch Maintenance Web Interface** link. On the resulting page, navigate to **Miscellaneous→Messaging Administration** in the left pane. The Audix main menu will appear as shown below.

Step	Description
2.	**Disconnect Options** Navigate to **Messaging Administration→Messaging** in the left pane. A new window will open similar to the Avaya Communication Manager SAT. Enter the **change system-parameters features** command and set the **Quick Silence Disconnect** field to *y* and the **Silence Limit** to *5*. Click the **F3** function key to submit the form. ```
change system-parameters features   Page 1 of 4
                       SYSTEM-PARAMETERS FEATURES

LOG-IN PARAMETERS
            Login Retries: 3   Consecutive Invalid Attempts: 18
 System Guest Password: _____   Minimum Password Length: 0

SUBSCRIBER PASSWORD AGING LIMITS (DAYS)
    Password Expiration Interval: 0   (0 for no password aging)
       Minimum Age Before Changes: 0
                Expiration Warning: 0   (0 for no warning)

INPUT TIME LIMITS (SECONDS)
         Normal: 60   Full Mailbox Timeout: 5   Wait (*W): 180
         Between Digits at Auto-attendant or Standalone Menu: 3 (3-12)

DISCONNECT OPTIONS
         Quick Silence Disconnect? y   Silence Limit? 5 (5-30 seconds)
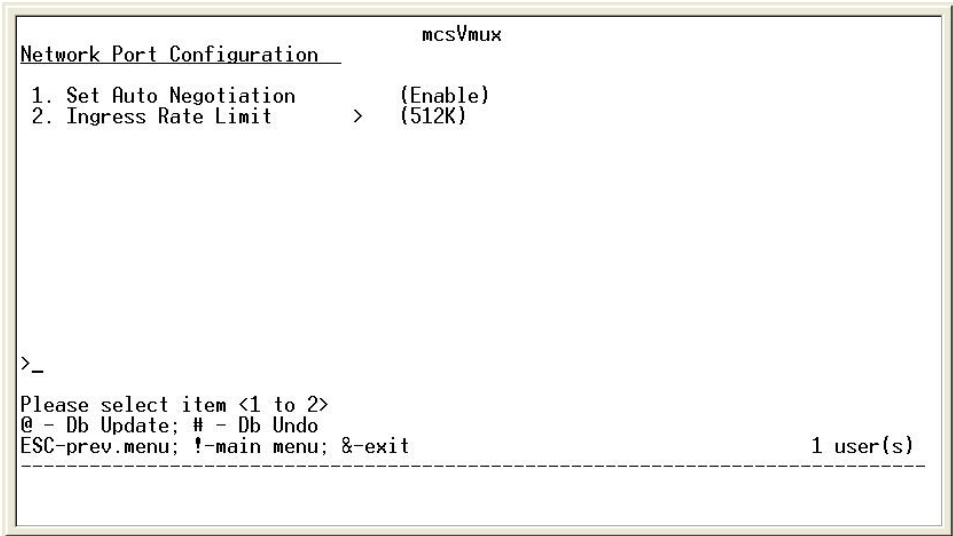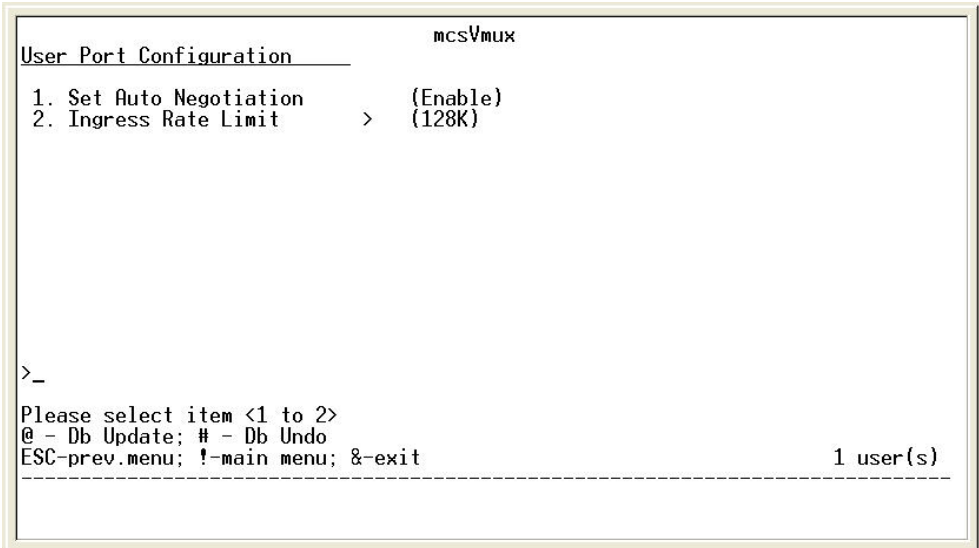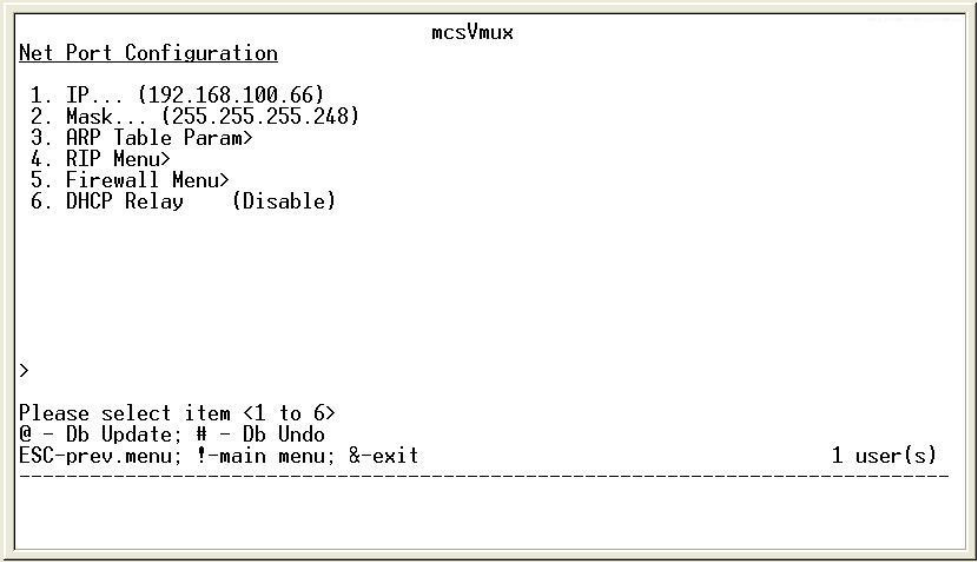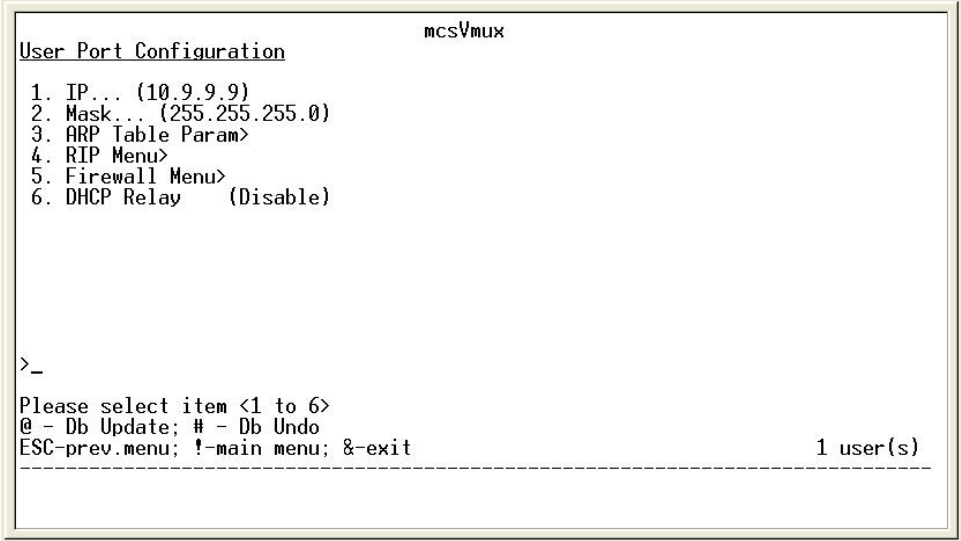``` |

6. Configure RAD Data Communications Vmux-104

This section describes the configuration of the Vmux. This configuration was performed from a Windows PC connected to the console port of the Vmux.

Step	Description
1.	**Main Menu** Using a terminal emulation application, connect to the console port using the following parameters: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. Log in with the appropriate user name and password. The main menu appears as shown below. Use the legend at the bottom of the screen to navigate through the menus and to save changes to the configuration database. ``` mcsVmux Main Menu 1. Inventory[] 2. Configuration> 3. Monitoring> 4. Diagnostics> >_ Please select item <1 to 4> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) -- ```

Step	Description
2.	**Host Name** Navigate to **Configuration→System→Management**. Enter a host name in the **Host Mux Name** field. Any descriptive name may be used. The example below shows the value used for the compliance test. Default values were used for all other fields shown. If the **Router** field is set to *Enable*, the menu list will not show the Host IP option configured in the next step. If this is the case, then the Host IP address has already been configured. Thus, skip **Steps 3 - 4** and proceed to **Step 5**. <pre> mcsVmux Management 1. Host IP > 2. Manager List []> 3. Host Mux Name ... (mcsVmux) 4. User Administration > 5. Telnet > (Enable) 6. Router (Disable) >_ Please select item <1 to 6> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) --</pre>
3.	**Host IP** Navigate to **Configuration→System→Management→Host IP**. Enter a host IP address, subnet mask and default gateway for the Vmux that is consistent with the network. These values correspond to the public side IP address of the Vmux. The example below shows the values used for the compliance test. Default values were used for all other fields. Save the changes to the database, exit the console interface and cycle power on the Vmux for these values to take effect. <pre> mcsVmux Host IP 1. Set Host IP address... (192.168.100.66) 2. Set Subnet Mask ... (255.255.255.248) 3. Set Default Gateway... (192.168.100.65) 4. DHCP client (Disable) 5. Read ... (public) 6. Write ... (private) 7. Trap ... (public) >_ Please select item <1 to 7> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) --</pre>

Step	Description
| 4. | **Enable Routing**<br>Once the Vmux has rebooted, log into the console interface as described in **Step 1**. Return to **Configuration→System→Management** as shown in **Step 2**. Enable the router function as shown below.<br><br>```
                                          mcsVmux
Management

  1. Snmp Community            >
  2. Manager List              []>
  3. Host Mux Name             ... (mcsVmux)
  4. User Administration       >
  5. Telnet                    >    (Enable)
  6. Router                         (Enable)




>_

Please select item <1 to 6>
@ - Db Update; # - Db Undo
ESC-prev.menu; !-main menu; &-exit                              1 user(s)
--------------------------------------------------------------------------------
``` |
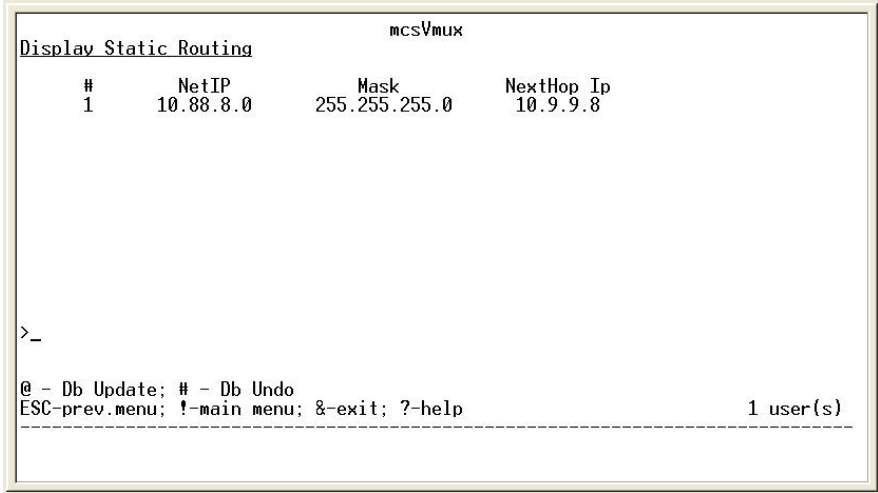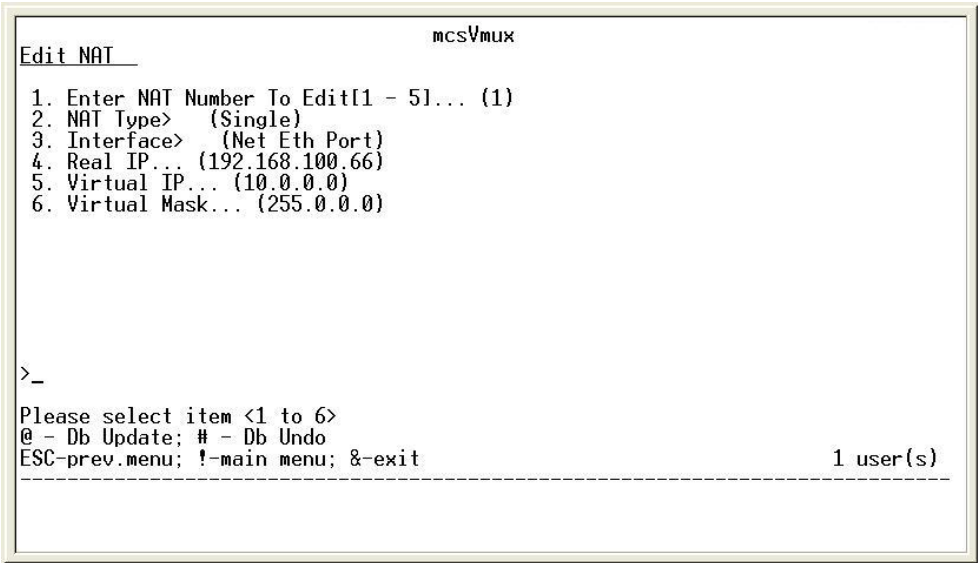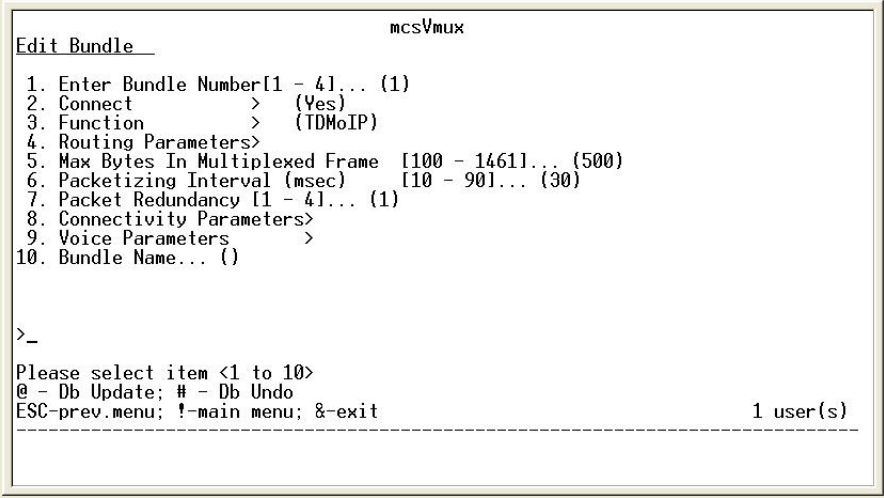| 5. | **Date and Time**<br>Navigate to **Configuration→System→Date & Time Update**. Enter the proper time and date.<br><br>```
                                          mcsVmux
Date & Time Update

  1. Set Time (hh:mm)     ... (22:45)
  2. Set Date (dd/mm/yyyy)... (9/8/2007)






>_

Please select item <1 to 2>
@ - Db Update; # - Db Undo
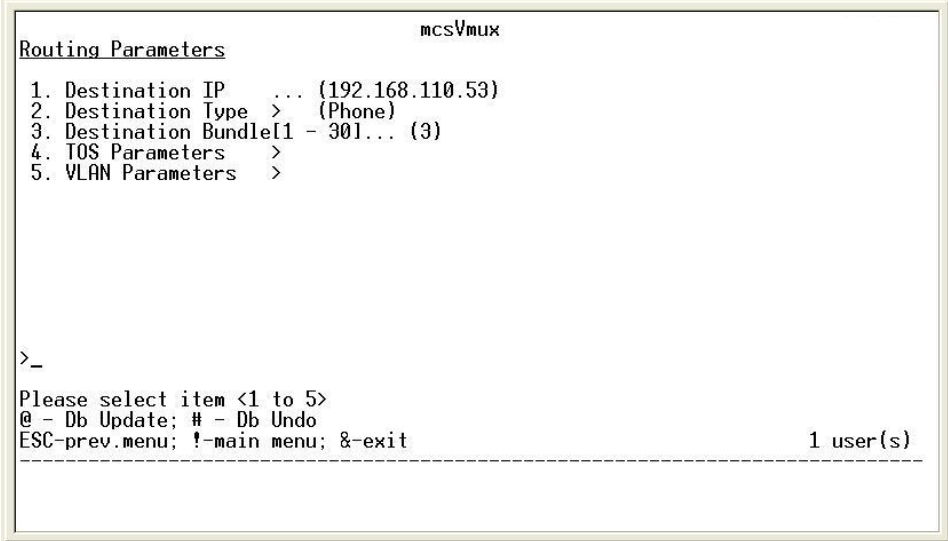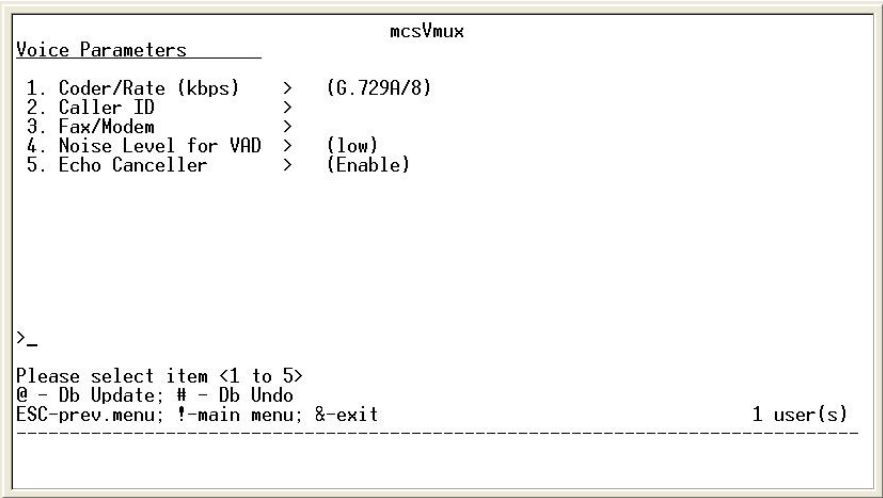ESC-prev.menu; !-main menu; &-exit                              1 user(s)
--------------------------------------------------------------------------------
``` |

Step	Description
| 6. | **Network Port Configuration**<br>Navigate to **Configuration→Switch LAN Configuration→Network Port Configuration**. Enable auto-negotiation. Set the **Ingress Rate Limit** to the value provided by Clear Channel Satellite based on the level of service which was purchased. The network port ingress rate limit is the limit of the downlink data rate from the satellite link. For the purposes of the compliance test, the value was set to 512K.<br><br>```
                                    mcsVmux
Network Port Configuration

 1. Set Auto Negotiation        (Enable)
 2. Ingress Rate Limit      >    (512K)




>_

Please select item <1 to 2>
@ - Db Update; # - Db Undo
ESC-prev.menu; !-main menu; &-exit                        1 user(s)
------------------------------------------------------------------------
``` |
| 7. | **User Port Configuration**<br>Navigate to **Configuration→Switch LAN Configuration→User Port Configuration**. Enable auto-negotiation. Set the **Ingress Rate Limit** to the value provided by Clear Channel Satellite based on the level of service which was purchased. The user port ingress rate limit is the limit of the uplink data rate to the satellite link. For the purposes of the compliance test, the value was set to 128K.<br><br>```
                                    mcsVmux
User Port Configuration

 1. Set Auto Negotiation        (Enable)
 2. Ingress Rate Limit      >    (128K)




>_

Please select item <1 to 2>
@ - Db Update; # - Db Undo
ESC-prev.menu; !-main menu; &-exit                        1 user(s)
------------------------------------------------------------------------
``` |

Step	Description
8.	**Router – Network Port** Navigate to **Configuration→Router Configuration→Interfaces Menu→Net Port Configuration**. Enter the IP address and subnet mask for the public side of the Vmux. This must match the values entered in **Step 3**. The example below shows the values used for the compliance test. Default values were used for all other fields. <pre> mcsVmux Net Port Configuration 1. IP... (192.168.100.66) 2. Mask... (255.255.255.248) 3. ARP Table Param> 4. RIP Menu> 5. Firewall Menu> 6. DHCP Relay (Disable) > Please select item <1 to 6> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) ---</pre>
9.	**Router – User Port** Navigate to **Configuration→Router Configuration→Interfaces Menu→User Port Configuration**. Enter the IP address and subnet mask for the private side of the Vmux. The example below shows the values used for the compliance test. Default values were used for all other fields. <pre> mcsVmux User Port Configuration 1. IP... (10.9.9.9) 2. Mask... (255.255.255.0) 3. ARP Table Param> 4. RIP Menu> 5. Firewall Menu> 6. DHCP Relay (Disable) >_ Please select item <1 to 6> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) ---</pre>

Step	Description
10.	**Static Route** In the case of the compliance test, Avaya Communication Manager and the Avaya H.323 endpoints were located on a different network (10.88.8.0) than the private side of the Vmux (10.9.9.0). A static route was required on the Vmux to define what next hop IP address should be used to reach the 10.88.8.0 network. The example below shows the static route used for the compliance test. The next hop IP address is the IP address of the Avaya G350 Media Gateway FastEthernet 10/2 interface. To add or view a static route, navigate to **Configuration→Router Configuration→Static Routing** and select either **Add Route** or **Display Static Routing[]**. ``` mcsVmux Display Static Routing # NetIP Mask NextHop Ip 1 10.88.8.0 255.255.255.0 10.9.9.8 >_ @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit; ?-help 1 user(s) --- ```
11.	**Default Gateway** Navigate to **Configuration→Router Configuration→Default Gateway**. Enable the default gateway function. Enter the IP address of the SIT as the default gateway. The SIT has a fixed public IP address provided by Clear Channel Satellite. The example below shows the value used for the compliance test. ``` mcsVmux Default Gateway 1. Default Gateway (Enable) 2. Default Gateway IP... (192.168.100.65) >_ Please select item <1 to 2> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) --- ```

Step	Description
12.	**Network Address Translation (NAT)** The Vmux performs network address translation between its public side and private side. To set or view the NAT parameters, navigate to **Configuration→Router Configuration→NAT** and select **Add NAT** or **Edit NAT**. The example below shows the values used for the compliance test. The **Real IP** field must be set to the IP address of the Vmux. The **Virtual IP** and **Virtual Mask** fields are set based on the range of addresses that are required to be translated behind the public address. In the case of the compliance test, all addresses on the 10.88.8.0 and 10.9.9.0 networks needed to be translated. Thus, the **Virtual IP** was chosen as *10.0.0.0* with a **Virtual Mask** of *255.0.0.0*.

```
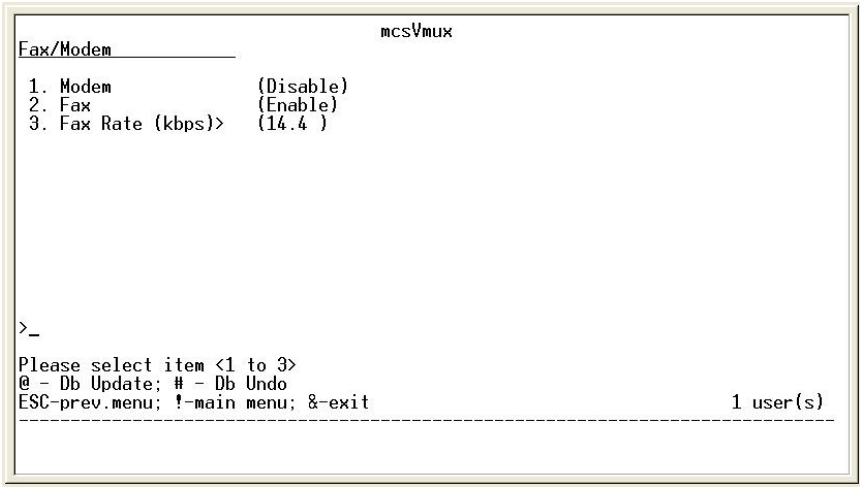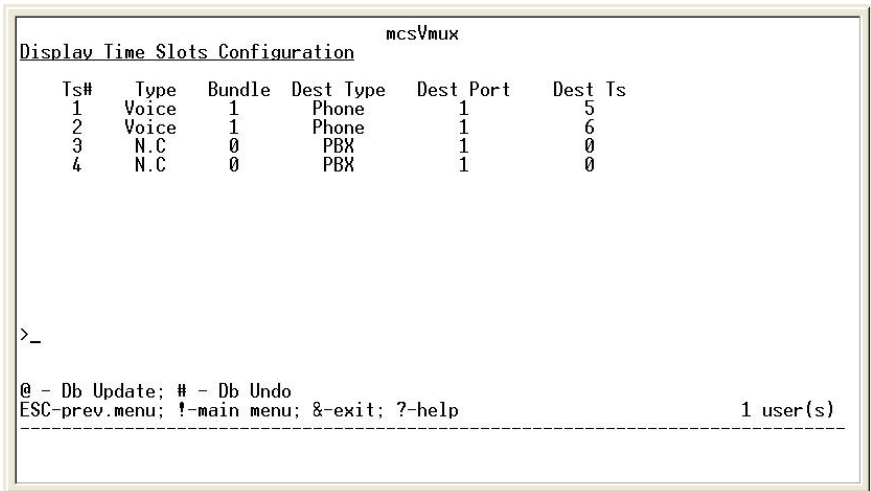                                          mcsVmux
Edit NAT

  1. Enter NAT Number To Edit[1 - 5]... (1)
  2. NAT Type>    (Single)
  3. Interface>   (Net Eth Port)
  4. Real IP... (192.168.100.66)
  5. Virtual IP... (10.0.0.0)
  6. Virtual Mask... (255.0.0.0)




>_

Please select item <1 to 6>
@ - Db Update; # - Db Undo
ESC-prev.menu; !-main menu; &-exit                          1 user(s)
----------------------------------------------------------------------
```
|

Step	Description
| 13.  | **Bundles**<br>A bundle describes a collection of voice traffic that will be transmitted to/from the far-end. To create or view a bundle, navigate to **Configuration→Analog Voice Configuration→Bundle Parameters→Bundle Configuration** and select either **Add Bundle** or **Edit Bundle**.  The example below shows the values used for the compliance test.  The **Connect** field must be set to *Yes*.  The **Function** field must be set to *TDMoIP*.  Default values were used for all other fields.<br><br>```
                               mcsVmux
Edit Bundle

  1. Enter Bundle Number[1 - 4]... (1)
  2. Connect           >   (Yes)
  3. Function          >   (TDMoIP)
  4. Routing Parameters>
  5. Max Bytes In Multiplexed Frame  [100 - 1461]... (500)
  6. Packetizing Interval (msec)     [10 - 90]... (30)
  7. Packet Redundancy [1 - 4]... (1)
  8. Connectivity Parameters>
  9. Voice Parameters       >
 10. Bundle Name... ()



>_

Please select item <1 to 10>
@ - Db Update; # - Db Undo
ESC-prev.menu; !-main menu; &-exit                          1 user(s)
-------------------------------------------------------------------------
``` |

Step	Description
14.	**Bundle Routing Parameters** Navigate to **Configuration→Analog Voice Configuration→Bundle Parameters→Bundle Configuration→Edit Bundle→Routing Parameters**. The **Destination IP**, **Destination Type** and **Destination Bundle** must match values configured at the far-end in the Clear Channel Satellite earth station. Thus, these values will be provided by Clear Channel Satellite. The example below shows the values used for the compliance test. ``` mcsVmux Routing Parameters 1. Destination IP ... (192.168.110.53) 2. Destination Type > (Phone) 3. Destination Bundle[1 - 30]... (3) 4. TOS Parameters > 5. VLAN Parameters > >_ Please select item <1 to 5> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) -- ```
15.	**Bundle Voice Parameters** Navigate to **Configuration→Analog Voice Configuration→Bundle Parameters→Bundle Configuration→Edit Bundle→Voice Parameters**. The compliance test used the G.729A codec as shown below. Default values were used for all other fields. ``` mcsVmux Voice Parameters 1. Coder/Rate (kbps) > (G.729A/8) 2. Caller ID > 3. Fax/Modem > 4. Noise Level for VAD > (low) 5. Echo Canceller > (Enable) >_ Please select item <1 to 5> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) -- ```

Step	Description
16.	**Fax** To enable fax support, navigate to **Configuration→Analog Voice Configuration→Bundle Parameters→Bundle Configuration→Edit Bundle→Voice Parameters→Fax/Modem**. Set the **Fax** field to *Enable*. The example below shows the values used for the compliance test. Default values were used for all other fields shown. ``` mcsVmux Fax/Modem 1. Modem (Disable) 2. Fax (Enable) 3. Fax Rate (kbps)> (14.4) >_ Please select item <1 to 3> @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit 1 user(s) -- ```

Step	Description
17.	**Time Slots** A time slot represents an individual voice channel coming to/from the voice ports of the Vmux. In the case of analog trunks, there is a one-to-one mapping of time slots 1 - 4 to FXS ports 1 – 4. To view the time slot configuration, navigate to **Configuration→Analog Voice Configuration→Ports Distribution→Display Time Slots Configuration[]**. The example below shows the values used for the compliance test. The compliance test used ports 1 and 2 for testing, so only time slots 1 and 2 are configured below. The configuration must match values configured at the far-end in the Clear Channel Satellite earth station. Thus, the values of destination type, port and time slot will be provided by Clear Channel Satellite. ``` mcsVmux Display Time Slots Configuration Ts# Type Bundle Dest Type Dest Port Dest Ts 1 Voice 1 Phone 1 5 2 Voice 1 Phone 1 6 3 N.C 0 PBX 1 0 4 N.C 0 PBX 1 0 >_ @ - Db Update; # - Db Undo ESC-prev.menu; !-main menu; &-exit; ?-help 1 user(s) --- ```

7. Configure XtremeSat

The configuration of the XtremeSat is done by Clear Channel Satellite and is not expected to be done by the end user or a third party technician. This includes configuration of the SIT and dish alignment if using a fixed dish. The auto-acquisition dish does not require manual alignment. The auto-acquisition dish will automatically align with the satellite signal once it is powered up and deployed.

8. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Clear Channel Satellite XtremeSat with Avaya Mobile Communication System with the G350 option to support PSTN hop-off. This section covers the general test approach and the test results.

8.1. General Test Approach

The general test approach was to make varying types of calls through XtremeSat and exercise common PBX features. Calls were made between Avaya MCS and the PSTN. All functionality listed below was tested using the one meter fixed dish. A subset of the functionality was repeated using the .76 meter auto-acquisition dish.

8.2. Test Results

XtremeSat passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.
- Outbound calls from Avaya MCS to the PSTN originating from each telephone type listed in **Section 2**.
- Inbound calls from the PSTN to Avaya MCS terminating on each telephone type listed in **Section 2**.
- Intra-site calls from each telephone type listed in **Section 2** to any other Avaya MCS endpoint.
- PBX features including Hold, Transfer, Call Forwarding and Conference.
- Proper DTMF tone detection.
- Voicemail and message waiting indicators (MWI).
- Transmit and receive faxes.
- Internet access.
- Proper system recovery after a SIT restart and loss of IP connection.

The following observations were made during the compliance test.
1. On outbound calls, a series of scratches/clicks can be heard after dialing is complete and before ringback is heard.
2. On inbound calls, after the call has been completed and hung up, the Avaya MCS telephone which just received the previous call will ring twice. If the user answers the phone at this time, dial tone is heard.
3. A noticeable delay of one to two seconds was experienced on each call. This is expected with the known latency of a satellite link.

4. Initially, the audio volume was noticeably low in one direction. This was corrected by adjusting the gain values on the Vmux. Directions on how to adjust the Vmux gain parameters are included in Appendix B.
5. The Vmux does not support far-end disconnect/disconnect supervision to the Avaya Media Gateway connected to the FXS port. Thus, external inbound calls that get forwarded to voicemail or an auto-attendant do not get disconnected when the caller hangs up. Conference calls are also affected if an external party drops off the conference before the call is complete. The trunk is not released and CO announcements are heard by the other parties on the conference. The impact to voicemail can be reduced by setting Audix to disconnect on silence but the interval has to be set very small to work reliably (~ 5 sec).
6. On inbound calls, the Vmux does not send Caller ID information to the FXS port.

9. Verification Steps

The following steps may be used to verify the configuration:
- From a PC on the Internet, ping the public IP addresses of the SIT and Vmux to verify data connectivity inward to the Vmux.
- From a PC connected to the Avaya G350 Media Gateway, ping the public IP addresses of the SIT and Vmux to verify data connectivity outward to the Vmux.
- From a PC connected to the Avaya G350 Media Gateway, verify that a web browser can be used to access a public Internet website.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the analog trunk group is in-service.
- Verify that calls can be placed from an Avaya MCS telephone to the PSTN.
- Verify that calls can be placed from the PSTN to an Avaya MCS telephone.

10. Support

For technical support on XtremeSat, contact Clear Channel Satellite via the support link at www.clearchannelsatellite.net.

11. Conclusion

Clear Channel Satellite XtremeSat passed compliance testing. These Application Notes describe the procedures required to configure Avaya Mobile Communication System to interoperate with Clear Channel Satellite XtremeSat to support PSTN hop-off as shown in **Figure 1**.

12. Additional References

[1] *Installing and Upgrading the Avaya G350 Media Gateway*, Doc # 03-300394, Issue 4, February 2007.

[2] *Administration for the Avaya G250 and Avaya G350 Media Gateways,* Doc # 03-300436, Issue 3, February 2007.

[3] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007.

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

[5] *4600 Series IP Telephone Release 2.8 LAN Administrator Guide*, Doc # 555-233-507, Issue 6, February 2007.

[6] *Avaya IP Softphone Release 6.0 User Reference,* Issue 1, May 2007.

[7] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 1.5*, Doc # 16-300698, Issue 4, May 2007.

[8] *Avaya Mobile Communication Overview*, http://www.avaya.com/gcm/master-usa/en-us/solutions/offers/mobile_communication_system.htm.

[9] *RAD Data Communications Vmux-104 User's Manual,* Publication No. 407-300-02/06, 2006.

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

Product documentation for Vmux-104 can be obtained from RAD Data Communications.

Product documentation for XtremeSat can be obtained from Clear Channel Satellite.

Appendix A: Avaya G350 Media Gateway Configuration File

Included below is the Avaya G350 Media Gateway configuration file used during the compliance testing. It can be displayed on the Avaya G350 Media Gateway by using the **show run** command.

```
G350-001(super)# show run
G350-001(super)#
! version 25.28.0
!
ds-mode t1
!
interface Vlan 1
 icc-vlan
 ip address 10.88.8.4       255.255.255.0
 pmi
 exit
!
interface FastEthernet 10/2
ip address 10.9.9.8        255.255.255.0
 exit
!
interface Console
 exit
!
interface USB-Modem
 shutdown
 exit
!
ip default-gateway 10.9.9.9        1 low
!
set mgc list 10.88.8.2
set mediaserver 10.88.8.2 10.88.8.2 23 telnet
set mediaserver 10.88.8.2 10.88.8.2 5023 sat
rtp-stat qos-trap
no rtp-stat fault
!#
!# End of configuration file. Press Enter to continue.
```

Appendix B: RAD Data Communications Vmux Gain Adjustments

Tx Gain (db) Gain level

This gain level is from the PBX or handset towards the Vmux-104 analog port. This is the analog input signal level applied to the FXS/FXO port. The Vmux-104 automatically adjusts according to this gain level. For example, if the PBX amplifies by 4 dB, set the Tx Gain to +4 dB, and the Vmux-104 will reduce the input signal level by 4 dB in order to get 0dBm at the digital end. The Default value is 0.

Rx Gain (db) Gain level

This gain level is applied by the Vmux-104 towards the PBX or handset. This is actually the analog output signal level from the Vmux port. For example, to get -1 dBm set the gain level to -1.