Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Mobile Communication System (G350 Option) with Clear Channel Satellite XtremeSat in a Site to Site IPsec VPN Environment – Issue 1.0

Abstract

These Application Notes describes the procedures for configuring Avaya Mobile Communication System with Clear Channel Satellite XtremeSat in a site to site IPsec VPN 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. Using the Internet access provided by XtremeSat, an IPsec VPN tunnel can be established between Avaya Mobile Communication System and a main site to provide secure voice and data communication between the sites.

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

1. Introduction

These Application Notes describes the procedures for configuring Avaya Mobile Communication System with Clear Channel Satellite XtremeSat in a site to site IPsec VPN environment.

Avaya Mobile Communication System 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 [10].

For the site to site VPN application described in these Application Notes, Avaya MCS consisted of the following:

- An Avaya G350 Media Gateway with integrated VPN
  - Avaya S8300 Server running Avaya Communication Manager and Avaya IA 770 Intuity Audix
  - MM314 (24-port Ethernet media module)
- Avaya H.323 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 connectivity via a satellite link. Using the Internet access provided by XtremeSat, an IPsec VPN tunnel can be established between Avaya Mobile Communication System and a main site to provide secure voice and data communication between the sites.

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. In the case of this site to site VPN configuration, PSTN access is provided from the main site Avaya Media Gateway. Thus, the PSTN access provided by XtremeSat is not used and thus not shown in **Figure 1**. Both voice and data are transmitted to the main site using IP through the IPsec VPN tunnel.

As previously mentioned, Avaya MCS can be constructed with several platform and 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. The Avaya G350 Media Gateway will terminate the remote site side of the site to site IPsec VPN. 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. The network port of the Vmux then 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).

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. XtremeSat supports 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. Compliance testing was done with the fixed dish configuration.

Lastly, endpoints at the remote 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.

At the main site is a Juniper Networks NetScreen-50 firewall which connects to an Avaya C363T-PWR Converged Stackable Switch. The NetScreen-50 in addition to being a firewall, will also terminate the IPsec VPN at the main site. The Avaya C363T-PWR Converged Stackable Switch provides routing at the main site. Also connected to the switch is an Avaya G700 Media Gateway with Avaya S8300 Server running Avaya Communication Manager. An H.323 IP trunk is established between Avaya Communication Managers at each site to direct voice traffic through the IPsec VPN tunnel.

It should be noted that calls between the Avaya MCS and the main site will typically experience one to two seconds of delay. This is expected with the known latency of a satellite link. In addition, since the voice traffic is routed over the Internet, there is no mechanism to ensure that voice traffic is given priority over data traffic.

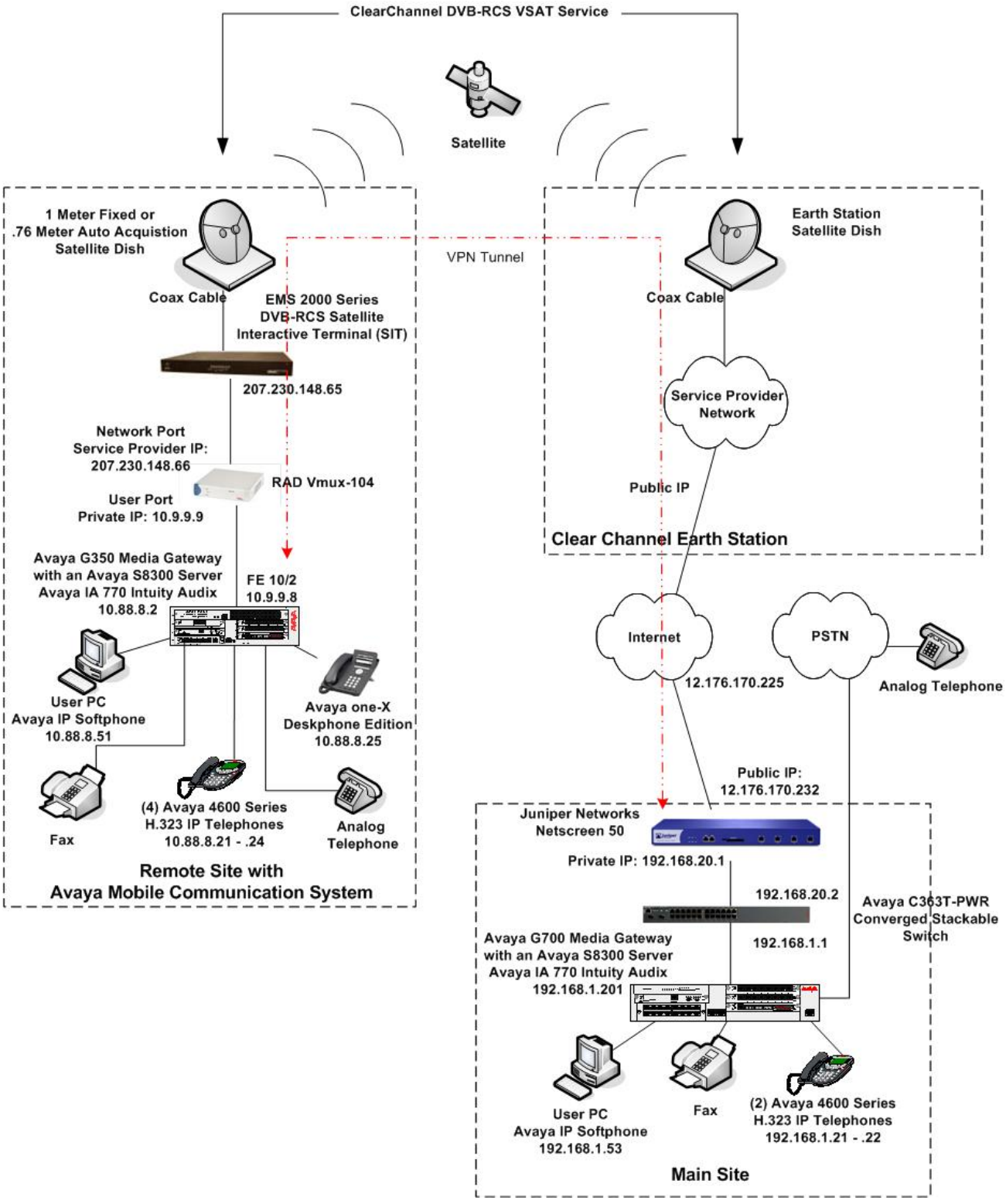


Figure 1: Avaya MCS G350 VPN Configuration

The following discussion provides an overview of the communication that takes place between each end of the VPN tunnel and the parameters used to establish the site to site VPN shown in **Figure 1**. The Internet Key Exchange (IKE) protocol is used to establish an Internet Security Association and Key Management Protocol (ISAKMP) encrypted control channel between peers. ISAKMP is used to add, modify and remove IPSec Security Associations and periodically update encryption keys in a secure manner. IKE establishes an ISAKMP Security Association (SA) by negotiating attributes in a proposal exchange known as Phase 1. An ISAKMP SA can only be established between peers if both agree to a common set of security attributes in the phase 1 proposal exchange. The following ISAKMP security attributes were administered for use in the sample configuration:

ISAKMP (Phase 1) proposal:

- Encryption Algorithm: AES
- Hash Algorithm: SHA
- Diffie-Hellman Group: 2
- Lifetime (seconds): 86400

Once an ISAKMP Security Association has been established, the peers can proceed to negotiate IPSec protection for specific traffic flows. IKE does this by establishing IPSec Security Associations (SAs) in a proposal exchange known as Phase 2. The following IPSec security attributes were administered for use in the sample configuration:

IPSec (Phase 2) proposal:

- Encryption Algorithm: AES-ESP
- Hash Algorithm: HMAC-SHA-ESP
- Security Association Lifetime (seconds): 3600
- Perfect Forward Secrecy: Enabled
- Diffie-Hellman Group: 2

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Servers	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 (with VPN License) MM314 (24-port Ethernet media module)	26.33.0 -
Avaya G700 Media Gateway	26.33.0
Avaya C363T-PWR Converged Stackable Switch	4.5.14
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 (Build 6.0.0.25) on Windows XP Professional SP2
Avaya one-X Deskphone Edition	1.5 (H.323)
Analog telephones	-
Fax machines	-
Juniper Networks NetScreen-50 Firewall / VPN	ScreenOS 5.4.0r6.0
RAD Data Communications Vmux-104	HW (2.00) FW (1.40) SW (3.04)
Clear Channel Satellite XtremeSat • EMS 2000 Series (SIT) • VSAT	- V3009.R05 -

3. Configure Avaya MCS - 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. It is also assumed the Avaya G350 Media Gateway has a VPN license installed. 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.
- Configuring one side of the IPsec VPN tunnel. The other side of the IPsec VPN tunnel configuration is done on the NetScreen-50 and shown in **Section 7**.
- Saving the configuration.

Step	Description

1.	**Interface Vlan 1**
	Configure an interface for use by Avaya Communication Manager and the Avaya IP Telephones. 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 with VLAN id of 1. This VLAN was 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 this interface.
	
	Note: The Media Gateway number will replace the question marks in the media gateway prompt once the gateway is registered to a Media Gateway Controller (MGC). This is only an indication that the H.248 signaling channel has not been established yet.
	
	`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**
	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-104. 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.
	
	`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. `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.	**ISAKMP Policy**
	Configure the ISAKMP policy (i.e., the IKE phase 1 proposal).
	
	`G350-???(super)# crypto isakmp policy 1`
	`G350-???(super-isakmp:1)# description "P1 Proposal"`
	`G350-???(super-isakmp:1)# encryption aes`
	`G350-???(super-isakmp:1)# hash sha`
	`G350-???(super-isakmp:1)# group 2`
	`G350-???(super-isakmp:1)# authentication pre-share`
	`G350-???(super-isakmp:1)# lifetime 86400`
	`G350-???(super-isakmp:1)# exit`

6.	**ISAKMP Peer**
	Configure the NetScreen-50 as the ISAKMP peer. Apply the policy of the tunnel to the NetScreen-50 peer and define the pre-shared key. The **isakmp peer address** is the IP address of the remote peer, which the G350 Media Gateway will negotiate to establish a secure ISAKMP channel.
	
	`G350-???(super)# crypto isakmp peer address 12.176.170.232`
	`G350-???(super-peer:12.170.176.232)# description "Netscreen-50"`
	`G350-???(super-peer: 12.170.176.232)# initiate mode aggressive`
	`G350-???(super-peer: 12.170.176.232)# self-identity fqdn mcs`
	`G350-???(super-peer: 12.170.176.232)# isakmp-policy 1`
	`G350-???(super-peer: 12.170.176.232)# pre-shared-key MySeCrEtKeY`
	`G350-???(super-peer: 12.170.176.232)# exit`

7.	**Transform Set**
	Configure the **transform-set** (i.e., the IKE phase 2 proposal). The **transform-set** defines security attributes, such as the protocol to employ, and the algorithm to be used.
	
	`G350-???(super)# crypto ipsec transform-set ns50 esp-aes esp-sha-hmac`
	`G350-???(super-transform:ns50)# set security-association lifetime seconds 3600`
	`G350-???(super-transform:ns50)# set pfs group2`
	`G350-???(super-transform:ns50)# exit`

Step	Description

8.	**Crypto Map**
	Configure the **crypto map**. Crypto-maps define the peers to negotiate with IPSec (IKE phase 2) protection and the transform-sets to secure the traffic flows.
	
	`G350-???(super)# crypto map 1`
	`G350-???(super-crypto:1)# description "P2 with Juniper"`
	`G350-???(super-crypto:1)# set peer 12.176.170.232`
	`G350-???(super-crypto:1)# set transform-set ns50`
	`G350-???(super-crypto:1)# exit`

9.	**Crypto List**
	Configure a **crypto-list**. A crypto-list is an ordered list of ip-rules that control which traffic requires IPSec protection and which does not, based on IP groups (source and destination IP addresses and wildcard). A crypto-list is activated per interface.
	
	To configure a crypto-list, use the **ip crypto-list** command, followed by an index number between **901** and **999**. Enter the crypto-list details as shown below.
	
	`G350-???(super)# ip crypto-list 901`
	`G350-???(super-Crypto 901)# name "Protect This Traffic"`
	`G350-???(super-Crypto 901)# local-address FastEthernet 10/2`
	`G350-???(super-Crypto 901)# ip-rule 1`
	`G350-???(super-Crypto 901/ip rule 1)# protect crypto map 1`
	`G350-???(super-Crypto 901/ip rule 1)# source-ip 10.88.8.0 0.0.0.255`
	`G350-???(super-Crypto 901/ip rule 1)# destination-ip 192.168.0.0 0.0.255.255`
	`G350-???(super-Crypto 901/ip rule 1)# exit`

10.	**Crypto Group**
	Assign **crypto-group** to Fast Ethernet interface. The **crypto-group** sub-command enables IPSec processing on a router interface by binding a **crypto-list** to it. Administrators may only bind one **crypto-list** to an interface at a time. Once IPSec is enabled, the Security Policy Database (SPD) is consulted by the interface during the processing of all inbound and outbound traffic, including non-IPSec traffic.
	
	The Avaya G350 Media Gateway Security Policy Database (SPD) includes the **crypto-list**, **ip-rules**, **crypto maps** and **transform-sets**. The **crypto-list** contains **ip-rules**, which select traffic flows requiring IPSec protection based on source and destination IP addressing. Each **ip-rule** is protected by a **crypto-map**. The **crypto-map** defines the peer to negotiate IPSec (phase 2) protection with and the transform-set to secure the traffic flow. The transform-set defines security attributes, such as the protocol to employ (e.g., AH or ESP) and the algorithm to be used (e.g., DES, 3DES, AES).
	
	`G350-???(super)# interface FastEthernet 10/2`
	`G350-???(super-if:FastEthernet 10/2)# ip crypto-group 901`
	`G350-???(super-if:FastEthernet 10/2)# exit`

Step	Description
11.	**Save Configuration** Use the **copy running-config startup-config** command to save the configuration. `G350-???(super)# copy running-config startup-config`

4. Configure Avaya MCS - 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 IP trunk and the routing of traffic to it. This includes the following components or services:

- Node names
- IP network region
- IP codec set
- Trunk group
- Signaling group
- Route pattern
- Alternate Automatic Routing (AAR)

The other side of the IP trunk configuration is performed on Avaya Communication Manager at the main site and is shown in **Section 9**.

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.	**Node Names**
	Create a node name for the main site Avaya Communication Manager. This node name is used to define the far-end of the IP trunk connecting the two sites. The example below shows the node name settings used for the compliance test.
	
	`display node-names ip`
	`IP NODE NAMES`
	`Name IP Address`
	`default 0 .0 .0 .0`
	`mainsite 192.168.1 .201`
	`myaudix 10 .88 .8 .3`
	`procr 10 .88 .8 .2`

Step	Description

2.	**IP Network Region**
	Determine which IP network region to use for the far-end of the IP trunk. The near-end of the IP trunk terminates on the Avaya S8300 Server, node name **procr**. The Avaya S8300 Server is located in the default IP network region 1. For the compliance test, a single network region (region 1) was used. Thus, both ends of the IP trunk reside in IP network region 1. Codec Set 1 was assigned to this region and Intra-region and Inter-region IP-IP Direct Audio was enabled. The example below shows the IP network region settings used for the compliance test.
	
	`display ip-network-region 1 Page 1 of 19`
	`IP NETWORK REGION`
	`Region: 1`
	`Location: Authoritative Domain:`
	`Name:`
	`MEDIA PARAMETERS` **`Intra-region IP-IP Direct Audio: yes`**
	`Codec Set: 1` **`Inter-region IP-IP Direct Audio: yes`**
	`UDP Port Min: 2048 IP Audio Hairpinning? n`
	`UDP Port Max: 3327`
	`DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y`
	`Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS`
	`Audio PHB Value: 46 Use Default Server Parameters? y`
	`Video PHB Value: 26`
	`802.1P/Q PARAMETERS`
	`Call Control 802.1p Priority: 6`
	`Audio 802.1p Priority: 6`
	`Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS`
	`H.323 IP ENDPOINTS RSVP Enabled? n`
	`H.323 Link Bounce Recovery? y`
	`Idle Traffic Interval (sec): 20`
	`Keep-Alive Interval (sec): 5`
	`Keep-Alive Count: 5`

3.	**IP Codec Set**
	Define the codecs to be used. The compliance test was performed using both G.711MU and G.729AB during different parts of the test. The example below shows the setting for G.711MU.
	
	`display ip-codec-set 1 Page 1 of 2`
	`IP Codec Set`
	`Codec Set: 1`
	`Audio Silence Frames Packet`
	`Codec Suppression Per Pkt Size(ms)`
	`1:` **`G.711MU n 2 20`**
	`2:`

Step	Description

4.	**IP Codec Set – continued**
	On **Page 2**, to support FAX calls, set the **FAX Mode** field to ***relay*** or ***t.38***. The value of ***no*** is not recommended.
	
	`display ip-codec-set 1 Page 2 of 2`
	
	`IP Codec Set`
	
	`Allow Direct-IP Multimedia? n`
	
	`Mode Redundancy`
	`FAX relay 0`
	`Modem off 0`
	`TDD/TTY US 3`
	`Clear-channel n 0`

5.	**Trunk Group**
	Create a trunk group for the IP trunk between Avaya Communication Manager running in Avaya MCS and Avaya Communication Manager at the main site. This trunk provides the access between the two sites for the voice traffic. For the purposes of the compliance test, the trunk group was created with the parameters described below.
	
	▪ **Group Type**: ***isdn***
	▪ **Group Name**: Any descriptive name can be used.
	▪ **TAC**: The TAC must be consistent with the existing dial plan.
	▪ **Carrier Medium**: ***H.323***
	▪ **Service Type: *tie*** Defines the trunk group as a tie trunk.
	▪ **Member Assignment Method: *auto*** This setting allows the trunk members to be automatically entered in the trunk group instead of being manually entered.
	▪ **Signaling Group: *3*** This field is set to the signaling group created in **Step 7**. This value can not be entered until the signaling group is created, thus the trunk group must be edited with this value after completing **Step 7**.
	▪ **Number of Members: *10*** Set this field to the number of simultaneous conversations that will be supported by this trunk group.
	
	`display trunk-group 3 Page 1 of 21`
	`TRUNK GROUP`
	
	`Group Number: 3 Group Type: isdn CDR Reports: y`
	`Group Name: mainsite COR: 1 TN: 1 TAC: 103`
	`Direction: two-way Outgoing Display? n Carrier Medium: H.323`
	`Dial Access? y Busy Threshold: 255 Night Service:`
	`Queue Length: 0`
	`Service Type: tie Auth Code? n`
	`Member Assignment Method: auto`
	`Signaling Group: 3`
	`Number of Members: 10`

Step	Description
6.	**Trunk Group – continued** On **Page 3**, set the **Send Name** and **Send Calling Number** fields to ***y***. This will allow the caller's name and number to be sent to the far-end. display trunk-group 3 Page 3 of 21 TRUNK FEATURES ACA Assignment? n Measured: none Internal Alert? n Maintenance Tests? y Data Restriction? n NCA-TSC Trunk Member: **Send Name: y** **Send Calling Number: y** Used for DCS? n Send EMU Visitor CPN? n Suppress # Outpulsing? n Format: public UUI IE Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n Send Connected Number: n Hold/Unhold Notifications? n Send UUI IE? y Modify Tandem Calling Number? n Send UCID? n Send Codeset 6/7 LAI IE? y

Step	Description
7.	**Signaling Group** Create a signaling group for the IP trunk group. For the purposes of the compliance test, the signaling group was created with the parameters described below. ▪ **Group Type**: ***h.323*** ▪ **Trunk Group for Channel Selection:** ***3*** This field is set to the trunk group created in **Step 4**. ▪ **Near-end Node Name:** ***procr*** This is the node name associated with the IP address of the Avaya S8300 Server in the Avaya MCS. ▪ **Near-end Listen Port:** ***1720*** ▪ **Far-end Node Name:** ***mainsite*** This is the node name associated with the IP address of the Avaya S8300 Server at the main site. ▪ **Far-end Listen Port:** ***1720***

```
display signaling-group 3                                    Page   1 of   5
                                SIGNALING GROUP

 Group Number: 3              Group Type: h.323
                            Remote Office? n          Max number of NCA TSC: 0
                                      SBS? n           Max number of CA TSC: 0
          IP Video? n                                Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 3
     TSC Supplementary Service Protocol: a
                         T303 Timer(sec): 10

   Near-end Node Name: procr                 Far-end Node Name: mainsite
 Near-end Listen Port: 1720                Far-end Listen Port: 1720
                                         Far-end Network Region:
         LRQ Required? n                  Calls Share IP Signaling Connection? n
         RRQ Required? n
                                              Bypass If IP Threshold Exceeded? n
                                                       H.235 Annex H Required? n
         DTMF over IP: out-of-band             Direct IP-IP Audio Connections? y
 Link Loss Delay Timer(sec): 90                          IP Audio Hairpinning? n
 Enable Layer 3 Test? n                             Interworking Message: PROGress
                                          DCP/Analog Bearer Capability: 3.1kHz
```

Step	Description
8.	**Route Pattern** Create a route pattern for use by Automatic Alternate Routing (AAR) to route calls to the trunk group defined in **Step 5** which provides voice traffic access to the main site. 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 5**. 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. Default values were used for all other fields.

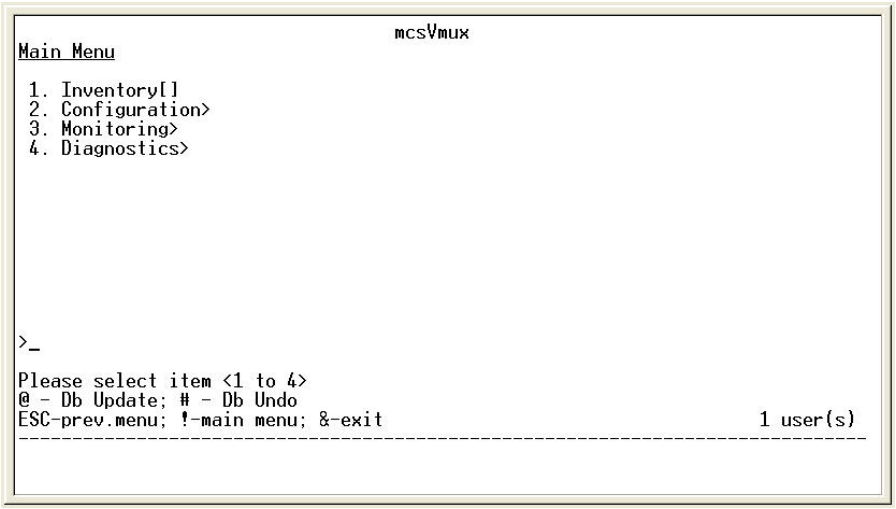
```
display route-pattern 3                                          Page   1 of   3
                   Pattern Number: 3   Pattern Name: mainsite
                                         Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                              Dgts                                    Intw
 1: 3    0                                                           n    user
 2:                                                                  n    user
 3:                                                                  n    user
 4:                                                                  n    user
 5:                                                                  n    user
 6:                                                                  n    user

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

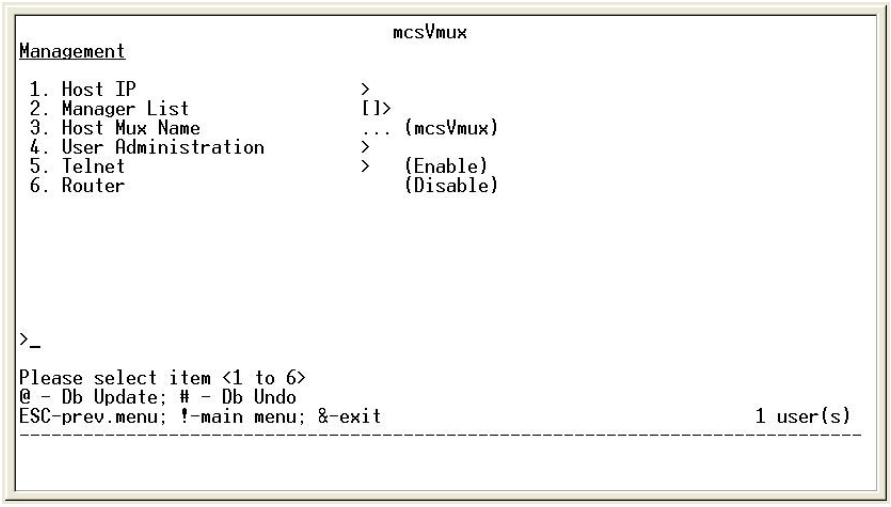
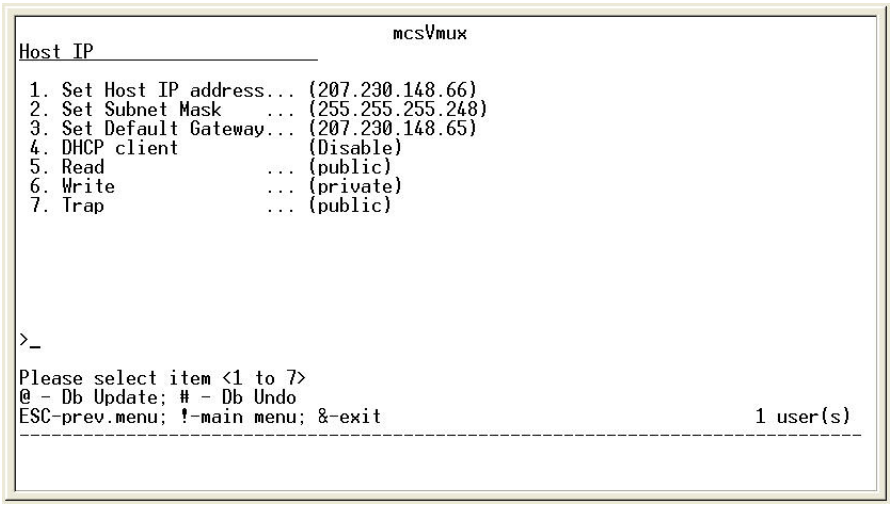
Step	Description
9.	**Automatic Alternate Routing (AAR)** AAR was used to define which dialed digits were associated with the route pattern providing access to the IP trunk group. For the purposes of the compliance test, 4xxxx extensions were assigned to the main site. Thus, dial strings of the form 4xxxx need to be routed to the IP trunk to reach the main site. The **change aar analysis *0*** command was used to add an entry in the AAR Digit Analysis Table. In the example shown, numbers that begin with 4 and are 5 digits long use route pattern 3 which was defined in the previous step.

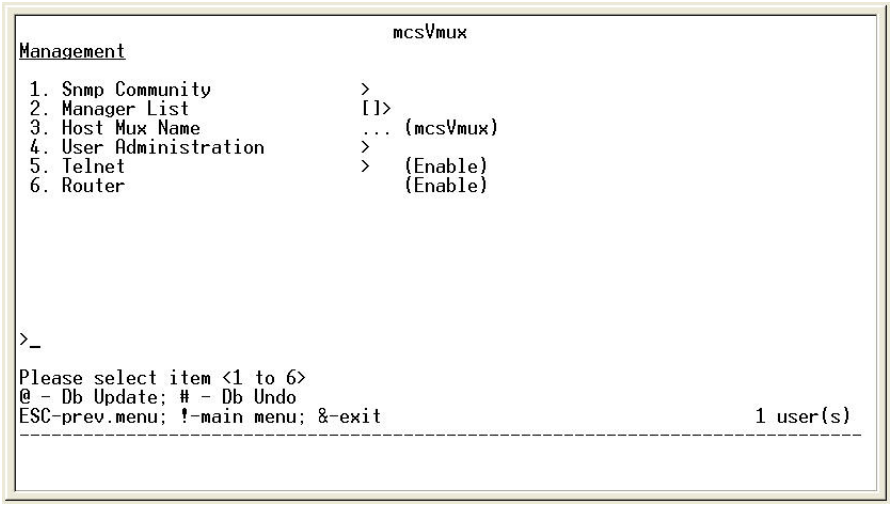
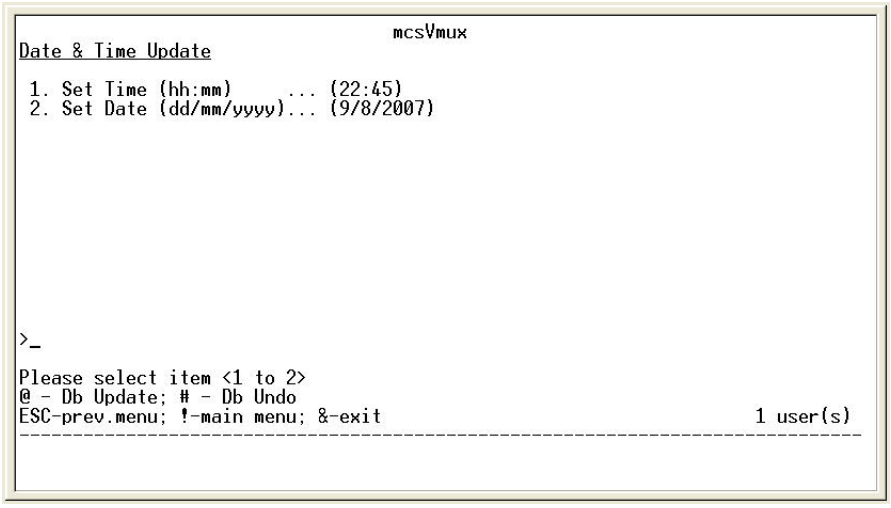
```
change aar analysis 0                                        Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                                          Percent Full:    3

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    2                     7    7     254      aar          n
    3                     7    7     254      aar          n
    39000                 5    5     99       aar          n
    4                     5    5     3        aar          n
    5                     7    7     254      aar          n
    6                     7    7     254      aar          n
    7                     7    7     254      aar          n
    8                     7    7     254      aar          n
    9                     7    7     254      aar          n
```

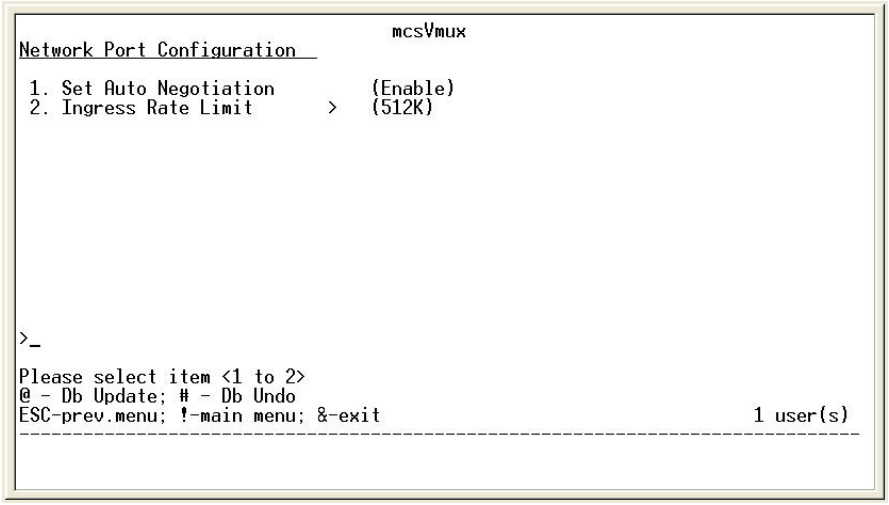
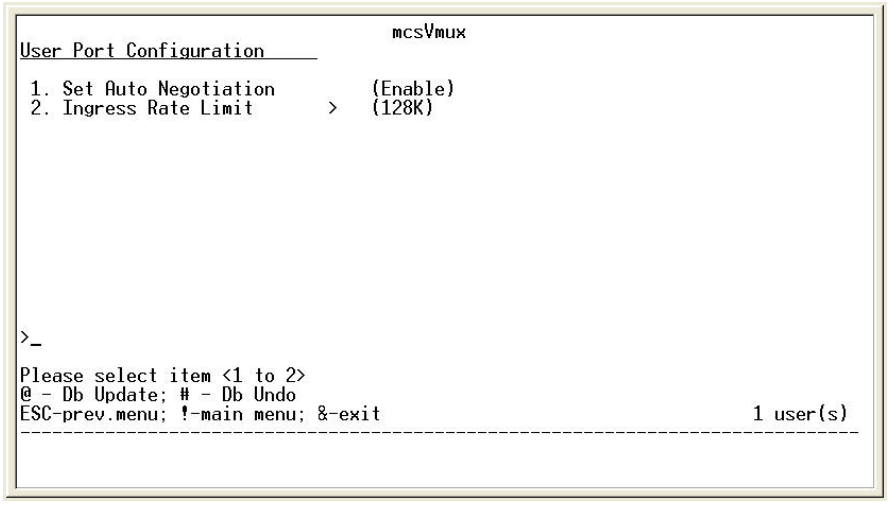
5. Configure Avaya MCS - RAD Data Communications Vmux-104

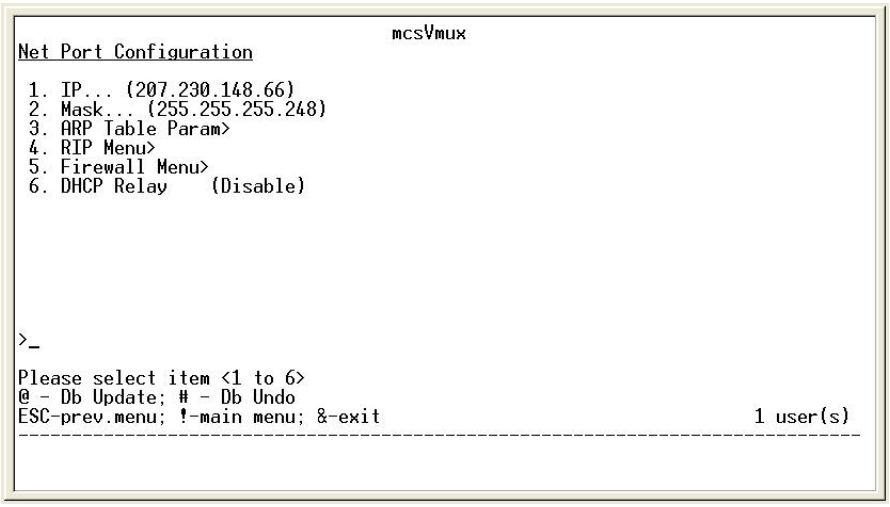
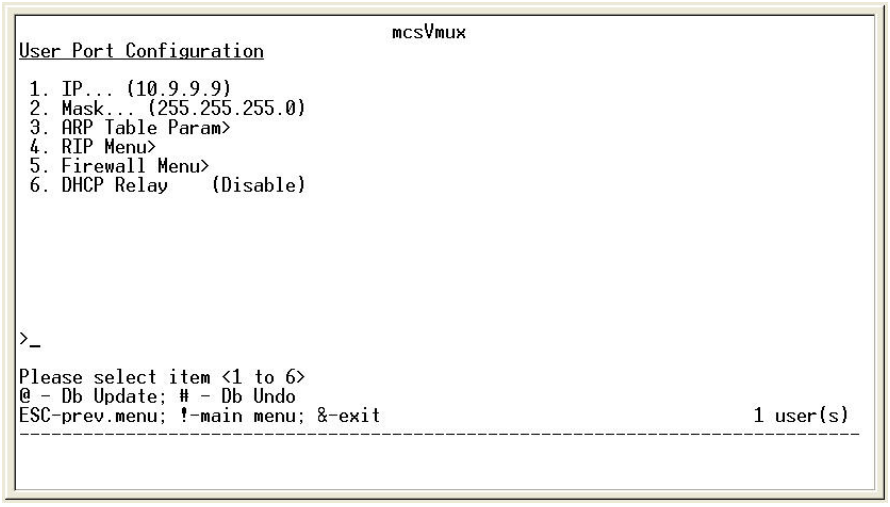
This section describes the configuration of the Vmux. This configuration was performed from a Windows PC connected to the console port of the Vmux.

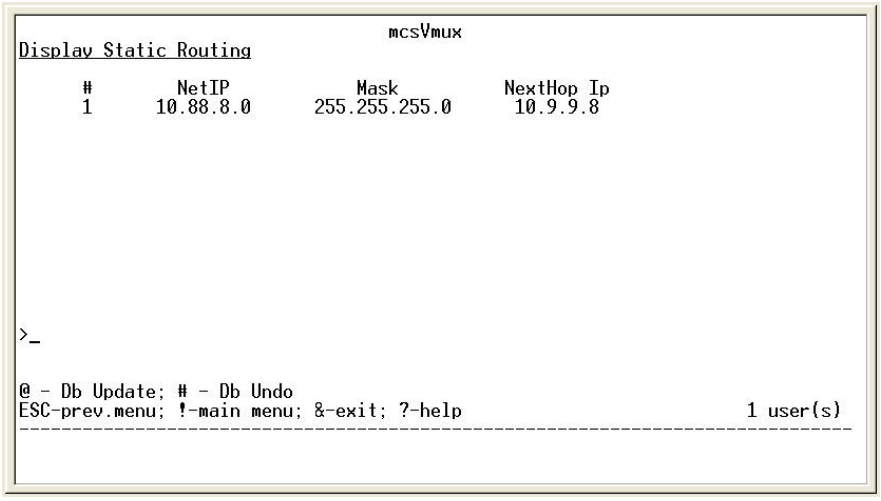
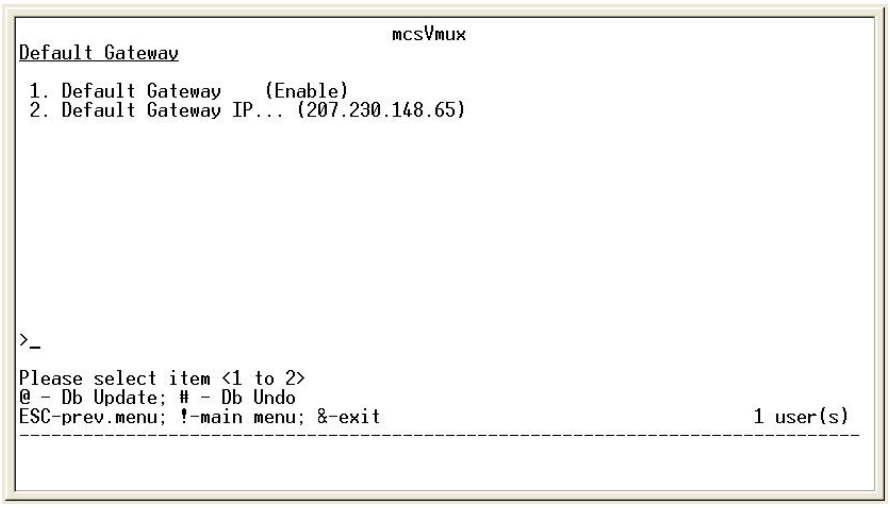
Step	Description
1.	**Main Menu** Using a terminal emulation application, connect to the console port using the following parameters: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. Log in with the appropriate user name and password. The main menu appears as shown below. Use the legend at the bottom of the screen to navigate through the menus and to save changes to the configuration database. 

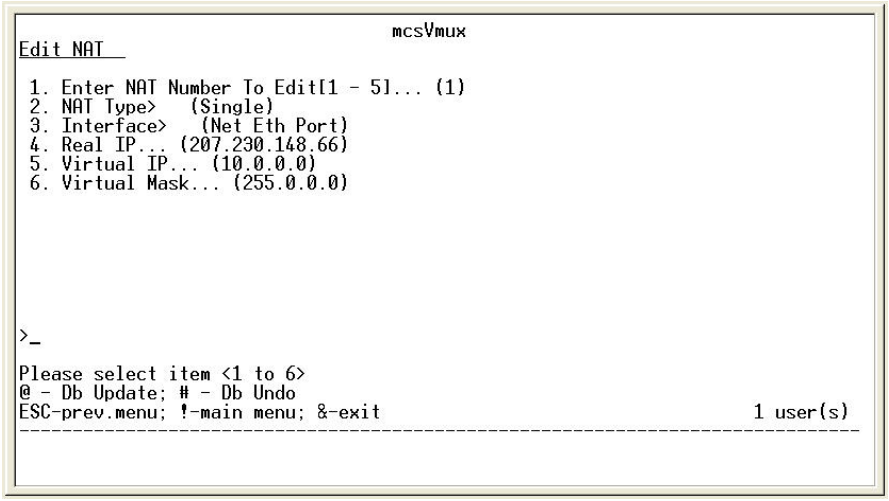
Step	Description
2.	**Host Name** Navigate to **Configuration→System→Management**. Enter a host name in the **Host Mux Name** field. Any descriptive name may be used. The example below shows the value used for the compliance test. Default values were used for all other fields shown. 
3.	**Host IP** Navigate 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. 

Step	Description
4.	**Enable Routing** 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. 
5.	**Date and Time** Navigate to **Configuration→System→Date & Time Update**. Enter the proper time and date. 

Step	Description
6.	**Network Port Configuration** 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. 
7.	**User Port Configuration** 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. 

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 2**. The example below shows the values used for the compliance test. Default values were used for all other fields. 
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. 

Step	Description
10.	**Static Route** In the case of the compliance test, Avaya Communication Manager and the Avaya IP Telephones 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[]**. 
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. 

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***. 

6. Configure XtremeSat

The configuration of 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.

7. Configure Main Site Juniper Networks NetScreen-50

This section describes the Juniper Networks NetScreen-50 configuration including in particular the other half of the IPsec VPN tunnel. This section assumes the NetScreen-50 has been installed as described in [12] and starts with the factory defaults. The complete configuration file is included in **Appendix B**.

Step	Description
1.	**Login** 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.

2.	**Trusted Zone**
	Statically administer the trusted zone Ethernet interface. The NetScreen-50 trusted zone is the protected or private side of the firewall. The IP address was also enabled to perform management.
	
	`ns50-> set interface ethernet1 zone trust`
	`ns50-> set interface ethernet1 ip 192.168.20.1/24`
	`ns50-> set interface ethernet1 manage-ip 192.168.20.1`

3.	**Untrusted Zone**
	Statically administer the untrusted zone Ethernet interface. The NetScreen-50 untrusted zone is the unprotected or public side of the firewall.
	
	`ns50-> set interface ethernet3 zone untrust`
	`ns50-> set interface ethernet3 ip 12.176.170.232/27`

4.	**Trusted Addresses** Configure an address alias for the private network at the main site. The command below adds the network addresses of the private network at the main site to the NetScreen-50 address book. The address book object **TrustedPrivateLAN** is used in **Step 11** to create security policies which define the traffic allowed to traverse the VPN. `ns50-> set address trust TrustedPrivateLAN 192.168.0.0 255.255.0.0`
5.	**Untrusted Addresses** Configure an address alias for the private network of the Avaya MCS located in the untrusted zone of the NetScreen-50. The command below adds the network addresses of the Avaya MCS to the NetScreen-50 address book. The address book object **G350** is used in **Step 11** to create security policies which define the traffic allowed to traverse the VPN. `ns50-> set address untrust G350 10.88.8.0 255.255.255.0`

Step	Description
6.	**Clear H.323 ALG** Disable the internal H.323 Application Layer Gateway provided by the NetScreen-50. This is not needed since the voice traffic is passing through a VPN tunnel which connects the two private networks at each end together. `ns50-> unset alg h323 enable`

7.	**ISAKMP Proposal**
	Configure the ISAKMP phase 1 proposal. Enter the IP address of the peer Avaya G350 Media Gateway with which to establish IKE negotiations.
	
	The Internet Key Exchange (IKE) proposal parameters must match on both peers to successfully establish a Virtual Private Network. For the compliance test, the IKE peer was defined by a peer id ***mcs*** sent from the Avaya G350 Media Gateway at the far-end (refer to **Section 3**, **Step 6**). This mechanism was used instead of using the Avaya G350 Media Gateway IP address to identify the peer. The default Juniper proposal ***pre-g2-3des-sha*** indicates that phase 1 will use a pre-shared key with Diffie-Hellman Group 2, AES-128 encryption and SHA hashing. Be sure that the preshared key value (e.g. **MySeCrEtKeY**) also matches on both sides. The IKE peer is located behind a NAT (the RAD Vmux). Thus, NAT traversal was enabled with a keep-alive interval of 5 seconds.
	
	`ns50-> set ike gateway G350gw address 0.0.0.0 id mcs main outgoing-interface ethernet3 preshare MySeCrEtKeY proposal pre-g2-aes128-sha`
	`ns50-> set ike gateway G350gw nat-traversal udp-checksum`
	`ns50-> set ike gateway G350gw nat-traversal keepalive-frequency 5`

8.	**IPSec Proposal** Configure the IPSec phase 2 proposal. The Internet Key Exchange (IKE) proposal parameters must match on both peers to successfully establish a Virtual Private Network. The default Juniper proposal **g2-esp-aes128-sha** indicates that phase 2 will use perfect forward secrecy with DH group 2, ESP payload, AES-128 encryption and SHA hashing. `ns50-> set vpn G350VPN gateway G350gw no-replay tunnel idletime 0 proposal g2-esp-aes128-sha`
9.	**Static Route** Define a static route to reach the trusted network which is not directly attached. `ns50-> set vrouter trust-vr route 192.168.1.0/24 interface ethernet1 gateway 192.168.20.2`
10.	**Default Route** Define a default static route for all traffic outbound. `ns50-> set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 12.176.170.225`

Step	Description

11.	**Security Policies**
	Configure policies to allow traffic between the Avaya MCS private network and the main site private network. Two policies are required, one for each direction.
	
	`ns50-> set policy top name toG350 from trust to untrust TrustedPrivateLAN G350 any tunnel vpn G350VPN`
	`ns50-> set policy top name fromG350 from untrust to trust G350 TrustedPrivateLAN any tunnel vpn G350VPN`

12.	**Save Configuration** Save the configuration. `ns50-> save`

8. Configure Main Site Avaya C363T-PWR Converged Stackable Switch

This section describes the Avaya C363T-PWR Converged Stackable Switch configuration. This section assumes the Avaya C363T-PWR has been installed using the procedures described in [9]. It is also assumed the Avaya C363T-PWR Converged Stackable Switch has a router license installed. The complete media gateway configuration file is included in **Appendix C**.

Step	Description

1.	**Create VLANs**
	Create a VLAN for use by Avaya Communication Manager and the Avaya IP Telephones. The compliance test created **vlan *192*** with **name *voice*** for this purpose. Create a second VLAN for the private side of the NetScreen-50. The compliance test created **vlan *2*** with **name *vlan2*** for this purpose.
	
	`G360-1(super)# set vlan 2 name V2`
	`G360-1(super)# set vlan 192 name V192`

2.	**Create VLAN Names (Layer 3)**
	For the VLANs created in **Step 1,** VLAN names must be created for these VLAN IDs at the router level so that IP addresses may be assigned to them. The names may be different than those used in Step 1. These two sets of VLAN names are tied together by the VLAN ID.
	
	`G360-1(super)# session router`
	`Router-1(super)# set vlan 2 name vlan2`
	`Router-1(super)# set vlan 192 name voice`

Step	Description

3.	**Assign IP addresses**
	For each VLAN created in **Step 1**, create a layer 3 interface and assign an IP address consistant with **Figure 1**. The example below shows how to set these parameters for the layer 3 interfaces IPI and IPI2.
	
	`G360-1(super)# session router`
	`Router-1(super)# interface IPI`
	`Router -1(super-if:IPI)# ip vlan 192`
	`Router -1(super-if:IPI)# ip address 192.168.1.1 255.255.255.0`
	`Router -1(super-if:IPI)# exit`
	`Router -1(super)# interface IPI2`
	`Router -1(super-if:IPI2)# ip vlan 2`
	`Router -1(super-if:IPI2)# ip address 192.168.20.2 255.255.255.0`
	`Router -1(super-if:IPI2)# exit`

4.	**Default Gateway** Configure a default gateway. The default gateway was set to the private side IP address of the NetScreen-50 as defined in **Figure 1**. The example below shows how to set this value. `G360-1(super)# ip default-gateway 192.168.20.1`
5.	**Save Configuration** Use the **copy run startup-config** command to save the configuration. `G360-1(super)# copy running-config startup-config`

9. Configure Main Site Avaya Communication Manager

This section describes the configuration of Avaya Communication Manager at the main site. This section assumes Avaya S8300 Server has been installed using the procedures described in [3]. As part of these procedures, the default gateway of Avaya S8300 Server was configured as the IP address of the IPI interface of the Avaya C363T-PWR Converged Stackable Switch (192.168.1.1).

This section describes the configuration of the components necessary to support the creation of an IP trunk (whose far-end was configured in **Section 4**) and the routing of traffic to it. This includes the following components or services:

- Node names
- IP network region
- IP codec set
- Trunk group
- Signaling group
- Route pattern
- Alternate Automatic Routing (AAR)

The same procedures that were described in **Section 4** were used to perform the configuration in this section.

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.	**Node Names**
	Create a node name for the Avaya S8300 Server in the Avaya MCS. This node name is used to define the far-end of the IP trunk connecting the two sites. The example below shows the node name settings used for the compliance test.
	
	`display node-names ip`
	`IP NODE NAMES`
	`Name IP Address`
	`default 0.0.0.0`
	`mobile1 10.88.8.2`
	`procr 192.168.1.201`

2.	**IP Network Region**
	Determine which IP network region to use for the far-end of the IP trunk.
	
	`display ip-network-region 1 Page 1 of 19`
	`IP NETWORK REGION`
	`Region: 1`
	`Location: Authoritative Domain:`
	`Name:`
	`MEDIA PARAMETERS` **`Intra-region IP-IP Direct Audio: yes`**
	`Codec Set: 1` **`Inter-region IP-IP Direct Audio: yes`**
	`UDP Port Min: 2048 IP Audio Hairpinning? n`
	`UDP Port Max: 3327`
	`DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y`
	`Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS`
	`Audio PHB Value: 46 Use Default Server Parameters? y`
	`Video PHB Value: 26`
	`802.1P/Q PARAMETERS`
	`Call Control 802.1p Priority: 6`
	`Audio 802.1p Priority: 6`
	`Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS`
	`H.323 IP ENDPOINTS RSVP Enabled? n`
	`H.323 Link Bounce Recovery? y`
	`Idle Traffic Interval (sec): 20`
	`Keep-Alive Interval (sec): 5`
	`Keep-Alive Count: 5`

Step	Description
3.	**IP Codec Set** Define the codecs to be used. display ip-codec-set 1 Page 1 of 2 IP Codec Set Codec Set: 1 Audio Silence Frames Packet Codec Suppression Per Pkt Size(ms) 1: **G.711MU n 2 20** 2:
4.	**IP Codec Set – continued** On **Page 2**, to support FAX calls, define the fax mode. display ip-codec-set 1 Page 2 of 2 IP Codec Set Allow Direct-IP Multimedia? n Mode Redundancy **FAX relay** 0 Modem off 0 TDD/TTY US 3 Clear-channel n 0
5.	**Trunk Group** Create a trunk group for the IP trunk. display trunk-group 3 Page 1 of 21 TRUNK GROUP Group Number: 3 **Group Type: isdn** CDR Reports: y **Group Name: mcs** COR: 1 TN: 1 **TAC: 103** Direction: two-way Outgoing Display? n **Carrier Medium: H.323** Dial Access? y Busy Threshold: 255 Night Service: Queue Length: 0 **Service Type: tie** Auth Code? n **Member Assignment Method: auto** **Signaling Group: 3** **Number of Members: 10**

Step	Description
6.	**Trunk Group – continued** display trunk-group 3 Page 3 of 21 TRUNK FEATURES ACA Assignment? n Measured: none Internal Alert? n Maintenance Tests? y Data Restriction? n NCA-TSC Trunk Member: **Send Name: y** **Send Calling Number: y** Used for DCS? n Send EMU Visitor CPN? n Suppress # Outpulsing? n Format: public UUI IE Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n Send Connected Number: n Hold/Unhold Notifications? n Send UUI IE? y Modify Tandem Calling Number? n Send UCID? n Send Codeset 6/7 LAI IE? y
7.	**Signaling Group** The **Far-end Node Name** was set to the node name created in **Step 1** for the Avaya S8300 Server in the Avaya MCS. display signaling-group 3 Page 1 of 5 SIGNALING GROUP Group Number: 3 **Group Type: h.323** Remote Office? n Max number of NCA TSC: 0 SBS? n Max number of CA TSC: 0 IP Video? n Trunk Group for NCA TSC: **Trunk Group for Channel Selection: 3** TSC Supplementary Service Protocol: a T303 Timer(sec): 10 **Near-end Node Name: procr** **Far-end Node Name: mobile1** **Near-end Listen Port: 1720** **Far-end Listen Port: 1720** **Far-end Network Region: 1** LRQ Required? n Calls Share IP Signaling Connection? n RRQ Required? n Bypass If IP Threshold Exceeded? n H.235 Annex H Required? n DTMF over IP: out-of-band Direct IP-IP Audio Connections? y Link Loss Delay Timer(sec): 90 IP Audio Hairpinning? n Enable Layer 3 Test? n Interworking Message: PROGress DCP/Analog Bearer Capability: 3.1kHz

Step	Description
8.	**Route Pattern** Create a route pattern for use by Automatic Alternate Routing (AAR) to route calls to the trunk group defined in **Step 5** which provides voice traffic access to the Avaya MCS.

```
display route-pattern 3                                          Page   1 of   3
                   Pattern Number: 3   Pattern Name: mcs
                                         Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                              Dgts                                    Intw
 1: 3    0                                                           n    user
 2:                                                                  n    user
 3:                                                                  n    user
 4:                                                                  n    user
 5:                                                                  n    user
 6:                                                                  n    user

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

9.	**Automatic Alternate Routing (AAR)** AAR was used to define which dialed digits were associated with the route pattern providing access to the IP trunk group. For the purposes of the compliance test, 30xxx extensions were assigned to the Avaya MCS. Thus, dial strings of the form 30xxx need to be routed to the IP trunk to reach the Avaya MCS.

```
display aar analysis 0                                           Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                                                 Percent Full:    3

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    2                     7    7     254      aar          n
    30                    5    5     3        aar          n
    4                     7    7     254      aar          n
    5                     7    7     254      aar          n
    6                     7    7     254      aar          n
    7                     7    7     254      aar          n
    8                     7    7     254      aar          n
    9                     7    7     254      aar          n
```

10. 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 a site to site IPsec VPN configuration. This section covers the general test approach and the test results.

10.1. 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 main site. All functionality listed below was tested using the one meter fixed dish.

10.2. 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 main site originating from each telephone type listed in **Section 2**.
- Inbound calls from the main site 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.
- Voice mail and message waiting indicators (MWI)
- Transmit and receive faxes.
- Internet access.
- Web access to main site web servers.
- Proper system recovery after a SIT restart and loss of IP connection.

The following observations were made during the compliance test.

1. A noticeable delay of one to two seconds was experienced on each call. This is expected with the known latency of a satellite link.
2. Since the voice traffic is routed over the Internet, there is no mechanism to ensure that voice traffic is given priority over data traffic.
3. Numerous fax failures were observed using G.711 in-band fax transmission (i.e., Avaya Communication Manager fax mode set to off). It is recommended that the fax mode be set to relay or T.38 on Avaya Communication Manager for reliable fax transmission.

11. 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 IP trunk group is in-service. This step can be done from both Avaya Communication Managers in the configuration.
- Verify that calls can be placed from an Avaya MCS telephone to the main site.
- Verify that calls can be placed from the main site to an Avaya MCS telephone.

12. Support

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

13. 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 a site to site IPsec VPN environment as shown in **Figure 1**.

14. 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] *Installing and Upgrading the Avaya G700 Media Gateway and Avaya S8300 Media Server*, Doc # 555-234-100, Issue 10.2, May 2007.

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

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

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

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

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

[9] *Installation and Configuration for the Avaya C360 Converged Stackable Switches Software Version 4.5*, Doc # 10-300503, Issue 2, July 2005.

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

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

[12] *Concepts & Examples Screen0S Reference Guide*, Release 5.4.0 Rev B, January 2007.

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.

```
! version 26.33.0
Config info release 26.33.0 time "14:10:35 22 SEP 2007 " serial_number 05IS35724483
!
encrypted-username CZnH3a/X9AvxehmG8bDQMg== password
1pqTQbDLUweNIAQ+VJg3wUvFKbGiPnYMJwnatqlprZU= access-type MEHm7GtOE4wOdL6qSe2tqw==
set logging file enable
set logging file condition all Error
set logging file condition BOOT Debug
!
encrypted-snmp-server community read-only E+0Mlq5UoHhj32KuWJkZaA== read-write
g2zV8BQpfVVIrYxPK8ontw==
!
ip crypto-list 901
 name "Protect This Traffic"
 local-address FastEthernet 10/2.0
!
 ip-rule 1
  protect crypto map 1
  source-ip 10.88.8.0 0.0.0.255
  destination-ip 192.168.0.0 0.0.255.255
 exit
!
exit
!
ds-mode t1
!
crypto ipsec transform-set ns50 esp-aes esp-sha-hmac
 set pfs group2
 exit
!
crypto isakmp policy 1
 description "P1 Proposal"
 encryption aes
 hash sha
 group 2
 authentication pre-share
 exit
!
crypto isakmp peer address "12.176.170.232"
 description "Netscreen-50"
 encrypted-pre-shared-key +PjLmkruezQhyoR42AipaEYFw0RmkGojddwVYECv6LA=
 isakmp-policy 1
 self-identity fqdn "mcs"
 initiate mode aggressive
 exit
!
crypto map 1
 description "P2 with Juniper"
 set peer "12.176.170.232"
 set transform-set ns50
 exit
!
interface Vlan 1
 icc-vlan
 ip address 10.88.8.4       255.255.255.0
 pmi
 exit
!
```

```
interface Vlan 2
 exit
!
interface FastEthernet 10/2
 ip crypto-group 901
 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.
```

Appendix B: NetScreen-50 Configuration File

Included below is the Juniper Networks NetScreen-50 configuration file used during the compliance testing. It can be displayed on the NetScreen-50 by using the **get configuration** command.

```
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
unset alg sip enable
unset alg mgcp enable
unset alg sccp enable
unset alg h323 enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
unset zone "Untrust" screen tear-drop
unset zone "Untrust" screen syn-flood
unset zone "Untrust" screen ping-death
unset zone "Untrust" screen ip-filter-src
unset zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
unset interface vlan1 ip
set interface ethernet1 ip 192.168.20.1/24
set interface ethernet1 nat
set interface ethernet3 ip 12.176.170.232/27
set interface ethernet3 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet3 manage ping
set interface ethernet3 manage telnet
```

```
set interface ethernet3 manage web
unset flow no-tcp-seq-check
set flow tcp-syn-check
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "TrustedPrivateLAN" 192.168.0.0 255.255.0.0
set address "Untrust" "G350" 10.88.8.0 255.255.255.0
set ike gateway "G350gw" address 0.0.0.0 id "mcs" Main outgoing-interface "ethernet3"
preshare "0hd7qca/NiYlCAsN9KCkWP2RECnSz6elUA==" proposal "pre-g2-aes128-sha"
set ike gateway "G350gw" nat-traversal udp-checksum
set ike gateway "G350gw" nat-traversal keepalive-frequency 5
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vpn "G350VPN" gateway "G350gw" no-replay tunnel idletime 0 proposal "g2-esp-aes128-
sha"
set url protocol websense
exit
set policy id 5 from "Untrust" to "Trust"  "G350" "TrustedPrivateLAN" "ANY" tunnel vpn
"G350VPN" id 1 pair-policy 4 log
set policy id 5
exit
set policy id 4 from "Trust" to "Untrust"  "TrustedPrivateLAN" "G350" "ANY" tunnel vpn
"G350VPN" id 1 pair-policy 5 log
set policy id 4
exit
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 192.168.1.0/24 interface ethernet1 gateway 192.168.20.2
set route 0.0.0.0/0 interface ethernet3 gateway 12.176.170.225
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

Appendix C: Avaya C363 Configuration File

Included below is the Avaya C363-PWR Converged Stackable Switch configuration file used during the compliance testing. It can be displayed on the Avaya C363 by using the **show run** command.

```
!#$@ DO NOT REMOVE THIS LINE - Avaya Inc. C360 Switch - Router configuration

! Avaya Inc. C360 Switch - Router configuration
! version 4.5.14
set vlan       2 name "vlan2"
set vlan     192 name "voice"
!
interface "IPI"
 ip vlan name "voice"
 ip address 192.168.1.1     255.255.255.0
!
interface "IPI2"
 ip vlan name "vlan2"
 ip address 192.168.20.2    255.255.255.0
!
ip default-gateway 192.168.20.1    1 low
!#
!# End of Configuration File
```

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