Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking Using MTS Allstream SIP Trunk Service and Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the MTS Allstream SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and various Avaya endpoints. However, use of the Avaya one-X Communicator in telecommuter mode is limited to basic inbound and outbound calling.

MTS Allstream is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the MTS Allstream SIP Trunk service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and various Avaya H.323, digital and analog endpoints. Avaya SIP phones were not used since Session Manager does not currently support direct registration of SIP endpoints.

Customers using this Avaya SIP-enabled enterprise solution with the MTS Allstream SIP Trunk service are able to place and receive PSTN calls via a dedicated broadband Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

1.1. Interoperability Compliance Testing

A simulated enterprise site using Communication Manager and Session Manager was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to connect to the MTS Allstream SIP Trunk Service.

To verify SIP trunking interoperability the following features and functionality were covered during the interoperability compliance test:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by MTS Allstream. Incoming PSTN calls were made to H.323, digital, and analog endpoints at the enterprise.
- Outgoing calls from the enterprise site were completed via MTS Allstream to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, digital, and analog endpoints.
- Various call types were tested including: inbound, outbound, international, outbound toll-free, operator, and directory assistance.
- Inbound toll-free and 911 emergency calls are both supported but were not tested as part of the compliance test.
- Calls using G.729A, G.711MU, and G.711A codecs.
- DTMF transmission using RFC 2833 with successful vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and extension to cellular, when the call arrived from the SIP trunk from MTS Allstream, or when the call forwarding destination and extension to cellular mobile number routed out the SIP trunk to MTS Allstream, or both.
- Caller ID Presentation and Caller ID Restriction.
- T.38 fax is not supported by MTS Allstream.
- Avaya one-X Communicator in both “Road Warrior” and “Telecommuter” modes, where incoming PSTN calls arrived from MTS Allstream, or the telecommute number routed out the SIP Trunk to MTS Allstream, or both.

- Direct IP-to-IP media (also known as "shuffling") with H.323 telephones. This allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

Interoperability testing of the MTS Allstream SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Use of Avaya one-X Communicator (H.323 soft client)**: When placing outbound calls from an Avaya H.323 one-X Communicator in telecommuter mode, if the call is placed on hold and retrieved from hold, the call no longer has audio and the call is disconnected after several seconds. This behavior also impacts the use of transfer and conference of PSTN calls. Thus, the Avaya one-X Communicator can only be used for basic inbound and outbound calls in telecommuter mode without the use of hold, transfer or conference.
- **Inbound Calling Party Number Block**: When an inbound call from a PSTN phone with Calling Party Number Block enabled terminates to a H.323 phone, the calling party number is blocked during ringing but is displayed after the call is answered. This is expected to be fixed in a future release of Session Manager.

1.2. Support

For technical support on the MTS Allstream SIP Trunk service, contact MTS Allstream Customer Care by calling 866-282-0111 or by sending email to ABC3@mtsallstream.com.

2. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the MTS Allstream SIP Trunk Service. This is the configuration used for compliance testing.

The Avaya components used to create the simulated customer site included:

- Avaya S8720 Servers running Communication Manager
- Avaya G650 Media Gateway
- Avaya S8510 Server running Session Manager
- Avaya S8510 Server running System Manager
- Avaya 9600-Series IP telephones (H.323)
- Avaya 4600-Series IP telephones (H.323)
- Avaya 1600-Series IP telephones (H.323)
- Avaya one-X Communicator (H.323)
- Avaya digital and analog telephones

Located at the edge of the enterprise is an Acme Packet Net-Net 4250 Session Director Session Border Controller (SBC). It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC provides network address translation at both the IP and SIP layers. In the compliance test, the SBC configuration was designed to be as "neutral" as possible to the

SIP call flows between the service provider and Session Manager – providing only the network address translation mentioned previously. The SBC was not configured with any SIP protocol manipulations to force interoperability between the service provider and the Avaya equipment. Thus, the solution presented in these Application Notes should also work if the SBC is not present at the enterprise. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.

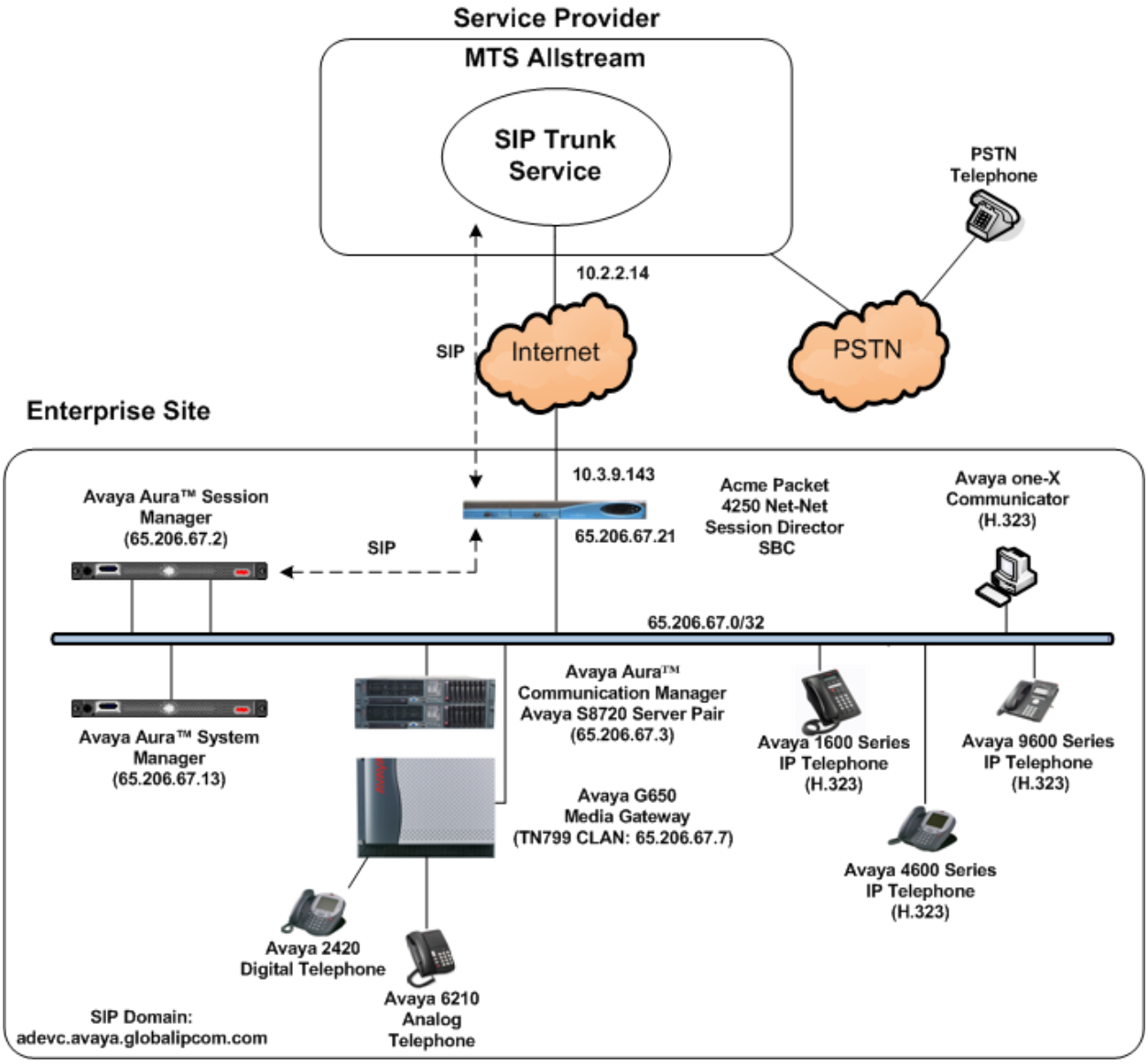


Figure 1: Avaya IP Telephony Network using the MTS Allstream SIP Trunk Service

For inbound calls, the calls flow from the service provider to the SBC then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case the Communication Manager) and on which link to send

the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the SBC. From the SBC, the call is sent to the MTS Allstream network.

The MTS Allstream SIP Trunk service supports 10 digit dialing for local calling and 1+10 digit dialing for domestic long distance to North American Numbering Plan (NANP) numbers. The dial plan and routing shown in these Application Notes require the user to properly dial the necessary digits for local and long distance calling.

3. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura™ Communication Manager running on an Avaya S8720 Server Pair	5.2.1 with patch 02.1.016.4-17959
Avaya G650 Media Gateway	TN2312AP(IPSI): HW03 FW45 TN799DP (CLAN): HW13 FW32 TN2602AP (MedPro):HW02 FW47
Avaya Aura™ Session Manager running on an Avaya S8510 Server	5.2
Avaya Aura™ System Manager running on an Avaya S8510 Server	5.2
Avaya 1608 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.2.2
Avaya 4621SW IP Telephone (H.323)	2.9.1
Avaya 9640 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.1
Avaya one-X Communicator (H.323)	R1.030-SP3-16918
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Acme Packet Net-Net 4250 Session Director Session Border Controller	SC6.1.0 MR-2 Patch 5 (Build 471)
MTS Allstream SIP Trunk Service Solution Components	
Component	Release
Genband S3 Session Border Controller	4.3m7
Nortel MG15000 and IWSPM Media Gateways	SN09U

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

4. Configure Communication Manager

This section describes the procedure for configuring Communication Manager for SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from MTS Allstream. It is assumed the general installation of Communication Manager, Avaya G650 Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

4.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. Each non-SIP telephone (i.e., analog, digital, H.323) on a 2-party call with the SIP service provider uses one SIP trunk. The example shows that 300 licenses are available and 103 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                   Maximum Video Capable H.323 Stations: 0     0
                    Maximum Video Capable IP Softphones: 0     0
                        Maximum Administered SIP Trunks: 300   103
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                              Maximum TN2501 VAL Boards: 10    1
                      Maximum Media Gateway VAL Sources: 10    1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

4.2. System Features

Use the **change system-parameters feature** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to ***none***.

```
change system-parameters features                               Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
                 Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                         Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                  AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: music Type: ext   21021
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n


             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of ***AV-Restricted*** and ***AV-Unavailable*** respectively.

```
change system-parameters features                               Page   9 of  18
                         FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: AV-Restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: AV-Unavailable

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code:
          International Access Code:

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

4.3. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and

the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 5 was chosen for the service provider trunk. Use the **change ip-network-region 5** command to configure region 5 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***adevc.avaya.globalipcom.com***. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to ***yes*.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 5 was selected.
- Default values can be used for all other fields.

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

On **Page 2**, define the IP codec set to be used for traffic between region 5 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 5                                    Page   3 of  19

 Source Region: 5     Inter Network Region Connection Management     I       M
                                                                    G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    5     y    NoLimit                                          n
 2
 3
 4
 5    5
```

4.4. Codecs

Use the **change ip-codec-set 5** command to define the codec(s) contained in this set which is used for calls between the enterprise and the service provider as defined in the previous section. The MTS Allstream SIP Trunk Service supports G.729A, G.711A, and G.711MU. Thus, these codecs were included in this set in order of preference. The order of preference is defined by the end customer. Enter ***G.729A***, ***G.711A, and G.711MU*** in the **Audio Codec** column of the table. Default values can be used for all other fields.

```
change ip-codec-set 5                                         Page   1 of   2

                         IP Codec Set

    Codec Set: 5

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

On **Page 2**, set the **Fax Mode** field to ***none***. The MTS Allstream SIP Trunk Service does not support T.38 fax.

```
change ip-codec-set 5                                         Page   2 of   2

                         IP Codec Set

                             Allow Direct-IP Multimedia? n



                    Mode               Redundancy
    FAX             none                0
    Modem           off                 0
    TDD/TTY         US                  3
    Clear-channel   n                   0
```

4.5. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 30 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.***
- Set the **Near-end Node Name** to ***GW1-CLAN1***. This node name maps to the IP address of the CLAN circuit pack in the Avaya G650 Media Gateway that terminates the SIP trunk. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to ***ASM***. This node name maps to the IP address of Session Manager as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 4.3**.
- Set the **Far-end Domain** to the domain of the service provider. This may be a fully qualified domain name or an IP address but it must match the domain that the service provider expects to see in the SIP URI and the "To" header. If a fully qualified domain name is used, then a DNS server must be present in the network that can resolve the name to the appropriate IP address. In the case of the compliance test, this field was set to the IP address of the Genband SBC at the edge of the MTS Allstream SIP Trunk service.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **15**. This timer determines how many seconds to wait for a response other than "100 Trying" after sending an INVITE. If no response other than 100 Trying is received before this time, then the call will be terminated. The default value of 6 was not always long enough for the MTS Allstream network.
- Default values may be used for all other fields.

```
add signaling-group 30                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 30              Group Type: sip
                         Transport Method: tls
  IMS Enabled? n



   Near-end Node Name: GW1-CLAN1             Far-end Node Name: ASM
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 5
Far-end Domain:10.2.2.14

                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? n                    Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 15
```

4.6. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 4.5**. For the compliance test, trunk group 30 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- The default values were used for all other fields.

```
add trunk-group 30                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 30                  Group Type: sip           CDR Reports: y
  Group Name: Allstream Trk              COR: 1        TN: 1        TAC: 130
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                      Signaling Group: 30
                                                    Number of Members: 6
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the MTS Allstream Trunk Service the value of ***600*** seconds was used.

```
add trunk-group 30                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                        Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                    Preferred Minimum Session Refresh Interval(sec): 600
```

On **Page 3**, set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number (CPN) sent to the far-end. Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 4.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end

destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 30                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y

                      Numbering Format: public
                                                  UUI Treatment: service-provider

                                                   Replace Restricted Numbers? y
                                                  Replace Unavailable Numbers? y

 Show ANSWERED BY on Display? y
```

On **Page 4**, set the **Send Diversion Header** field to ***y***. This field provides additional information to the destination party if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Telephone Event Payload Type** to ***101***, the value preferred by MTS Allstream.

```
add trunk-group 30                                              Page   4 of  21
                              PROTOCOL VARIATIONS

                       Mark Users as Phone? n
             Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? y
                  Support Request History? y
             Telephone Event Payload Type: 101
```

4.7. Calling Party Information

Public unknown numbering defines the calling party number to be sent to the far-end. This calling party number is sent in the SIP "From" header. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 30011, 30012 and 30013. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                              Total
Ext Ext           Trk       CPN               CPN
Len Code          Grp(s)    Prefix            Len
                                                      Total Administered: 3
 5  30011         30        6475551111        10         Maximum Entries: 9999
 5  30012         30        6475552222        10
 5  30013         30        6475553333        10
```

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single public unknown numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 3 will send the calling party number as the **CPN Prefix** plus the extension number.

```
change public-unknown-numbering 0                              Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk        CPN           CPN
Len Code          Grp(s)     Prefix        Len
                                                  Total Administered: 1
 5  3             30         64755         10          Maximum Entries: 9999
```

4.8. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).

```
change dialplan analysis                                       Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                 Location:  all           Percent Full:    2

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     1            3    dac
     2            5    ext
     3            5    ext
     4            5    ext
     6            3    fac
     7            5    ext
     8            1    fac
     9            1    fac
```

Use the **change feature-access-codes** command to configure ***9*** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                    Page   1 of   8
                                FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: 666
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                  Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: 600    All: 601    Deactivation: 602
   Call Forwarding Enhanced Status:        Act: 607    Deactivation: 608
                         Call Park Access Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 30 which contains the SIP trunk to the service provider (as defined below). Note that **Dialed String *647*** has **Call Type** of ***hnpa*** (Home Numbering Plan Area - HNPA) since it is a local number and will be dialed with 10 digits. All dialed strings that begin with a 1 have a **Call Type** of ***fnpa*** (Foreign Numbering Plan Area - FNPA) and are long distance calls and will be dialed with 1 + 10 digits.

```
change ars analysis 0                                          Page   1 of   2
                           ARS DIGIT ANALYSIS TABLE
                                 Location:  all           Percent Full:    0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern  Type   Num   Reqd
    0                     1    1    30       op           n
    0                     11   11   30       op           n
    00                    2    2    30       iop          n
    011                   10   18   30       intl         n
    647                   10   10   30       hnpa         n
    1732                  11   11   30       fnpa         n
    1800                  11   11   30       fnpa         n
    1877                  11   11   30       fnpa         n
    1908                  11   11   30       fnpa         n
    411                   3    3    30       svcl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 30 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 30 was connected to MTS Allstream.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: ***1*** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

```
change route-pattern 30                                          Page   1 of   3
                     Pattern Number: 30  Pattern Name: SP Route
                                SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                                Dgts                                    Intw
 1: 30   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 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
```

5. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to Communication Manager, the SBC and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Regular Expressions, which also can be used to route calls
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

5.1. System Manager Login and Navigation

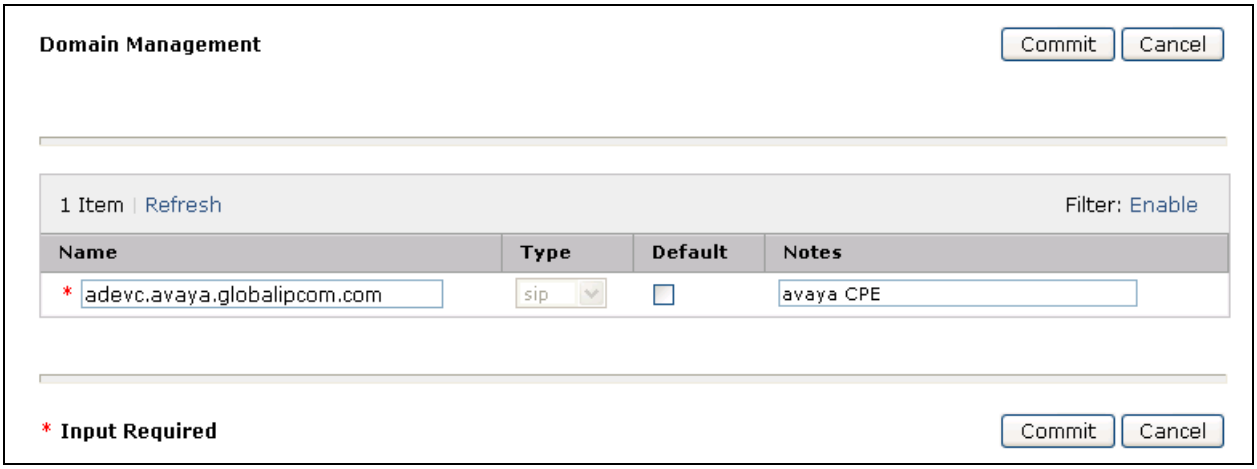
Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **OK** in the subsequent confirmation screen. The menu shown below is then displayed. Expand the **Network Routing Policy** link on the left side as shown. The sub-menus displayed in the left column below will be used to configure all but the last one of the above items (**Sections 5.2** through **5.9**).

5.2. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Navigate to **Network Routing Policy → SIP Domains** in the left-hand navigation pane (**Section 5.1**) and click the **New** button (not shown) on the right. In the new right pane that appears (shown below), fill in the following:

- **Name:** The authoritative domain name (e.g., "adevc.avaya.globalipcom.com").
- **Notes:** Descriptive text (optional).

Click **Commit**.



5.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Network Routing Policy →Locations** in the left-hand navigation pane (**Section 5.1**) and click the **New** button (not shown) on the right.

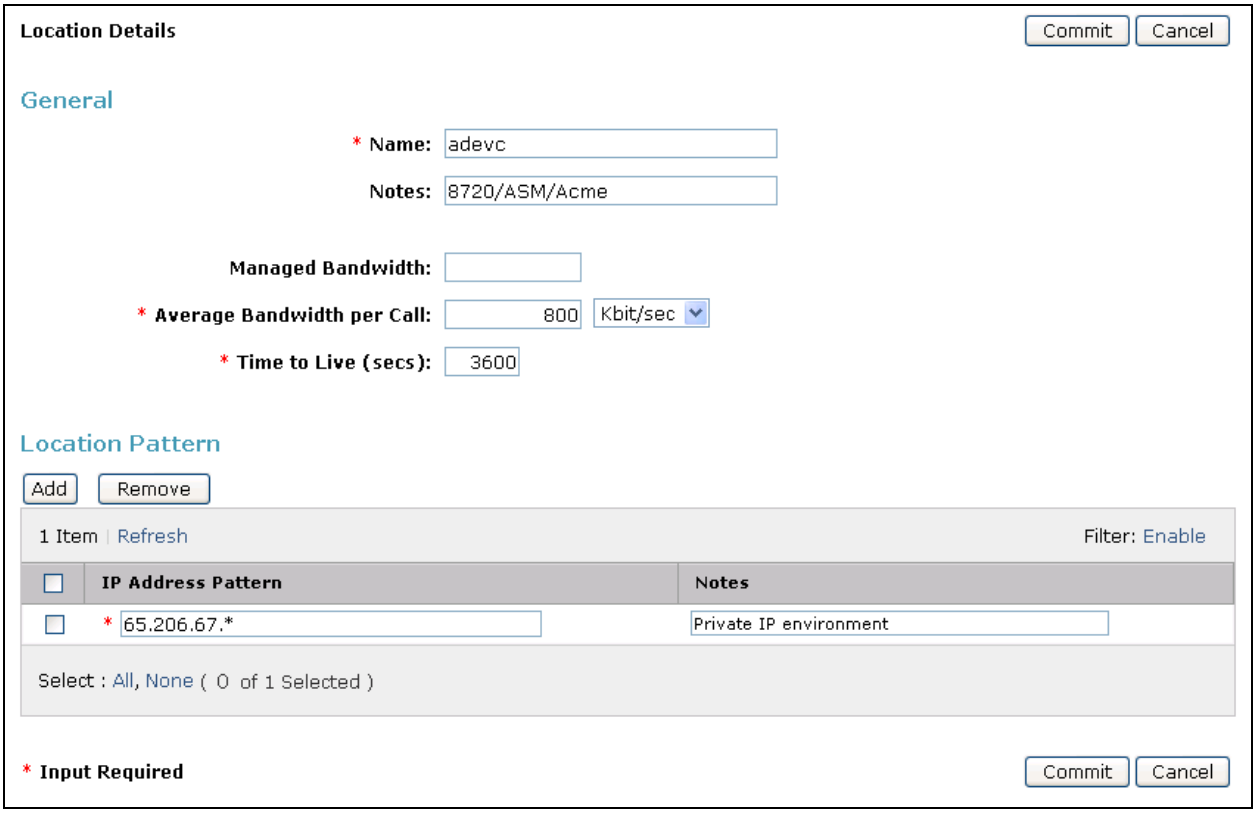
Under *General*, enter:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows the addition of the ***adevc*** location, which includes all equipment on the 65.206.67.x subnet including Communication Manager, Session Manager, and the Acme Packet SBC. Click **Commit** to save the Location definition.



The fields under *General* can be filled in to specify bandwidth management parameters between Session Manager and this location. These were not used in the sample configuration, and reflect

default values. Note also that although not implemented in the sample configuration, routing policies can be defined based on location.

5.4. Add Adaptation Module

Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products. In the sample configuration, inbound DID numbers from MTS Allstream are converted to local Communication Manager extensions.

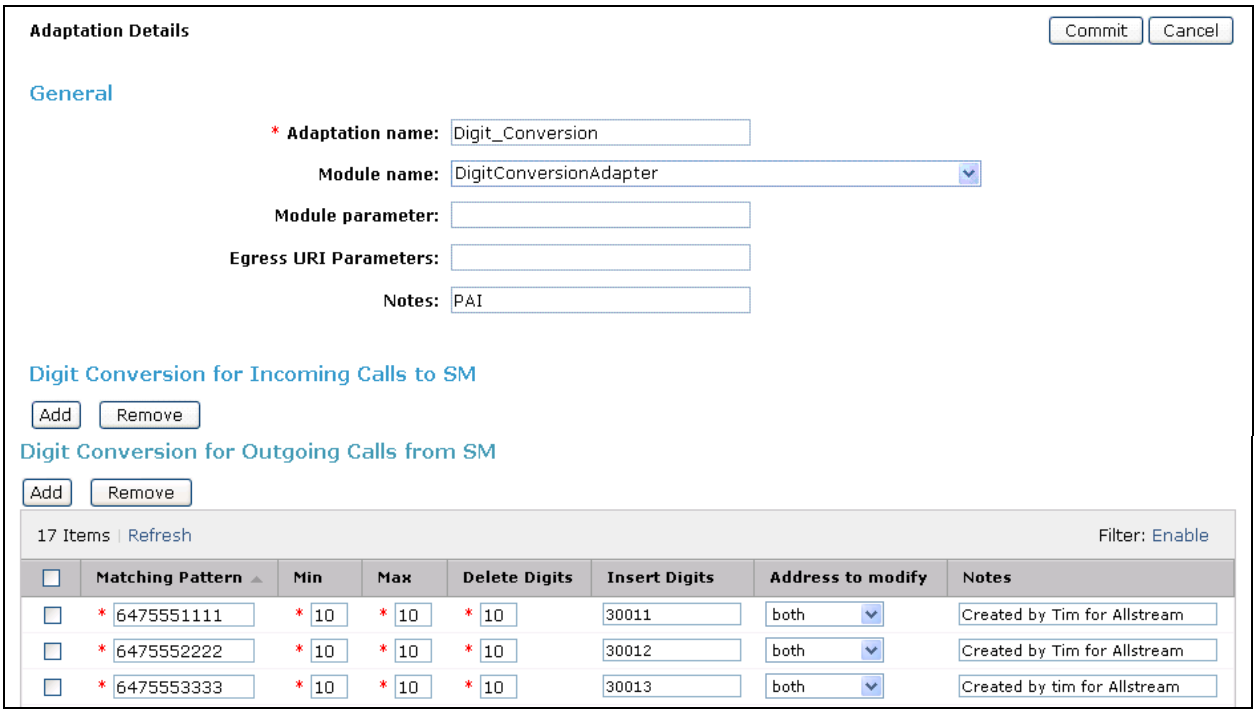
To add the generic adaptation module, select **Adaptations** on the left and click on the **New** button (not shown) on the right. Under *General*, fill in:

- **Adaptation Name:** A descriptive name.
- **Module Name:** Adaptation Module name and parameters (case sensitive)

The remaining fields can be left blank. Under *Digit Conversion for Incoming Calls to SM* and *Digit Conversion for Outgoing Calls from SM*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Matching Pattern:** A digit string used to match the dialed number
- **Min:** Minimum dialed number length
- **Max:** Maximum dialed number length
- **Delete Digits:** Number of digits to delete from the beginning
- **Insert Digits:** Number of digits to insert at the beginning
- **Address to modify:** Choose between "origination," "destination," or "both"

Click **Commit** to save the Adaptation Module definition. The screen below specifies the **DigitConversionAdapter** is to be used when modifying the SIP messages. No conversions are defined for calls from Communication Manager to MTS Allstream (*Digit Conversion For Incoming calls to SM*). For calls from MTS Allstream to Communication Manager (*Digit Conversion For Outgoing Calls*), each of 3 DID numbers are converted to a 5 digit Communication Manager extension. Session Manager will route the call based on the resulting 5 digit extension.

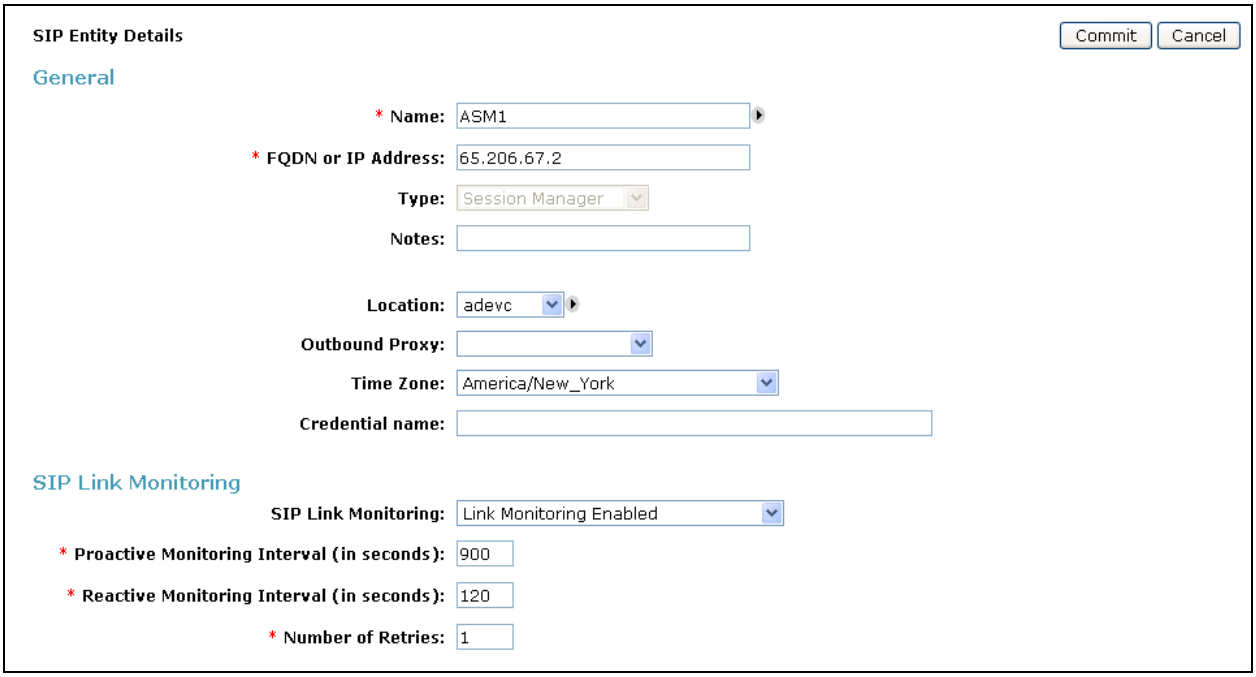


5.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system supported by it using SIP trunks: the C-LAN board in the Avaya G650 Media Gateway and the Acme Packet SBC. Navigate to **Network Routing Policy → SIP Entities** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button (not shown) on the right. Under *General*, fill in:

- **Name:** A descriptive name.
- **FQDN or IP Address:** FQDN or IP address of the Session Manager or the signaling interface on the telephony system.
- **Type:** "Session Manager" for Session Manager or "CM" for Communication Manager.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

The following screen shows the addition of Session Manager. The IP address of the SM-100 Security Module is entered for **FQDN or IP Address**.



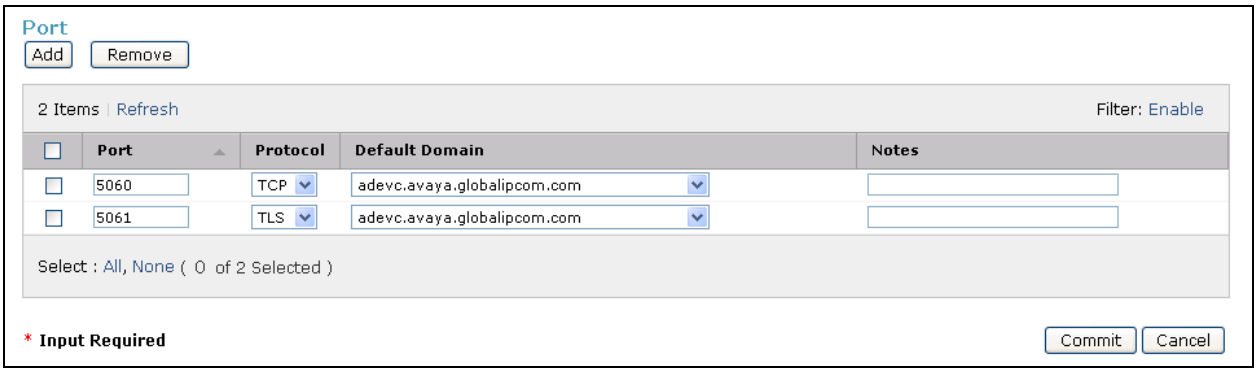
To define the ports used by Session Manager, scroll down to the *Port* section of the *SIP Entity Details* screen.

Under *Port*, click **Add**, and then edit the fields in the resulting new row as shown below:

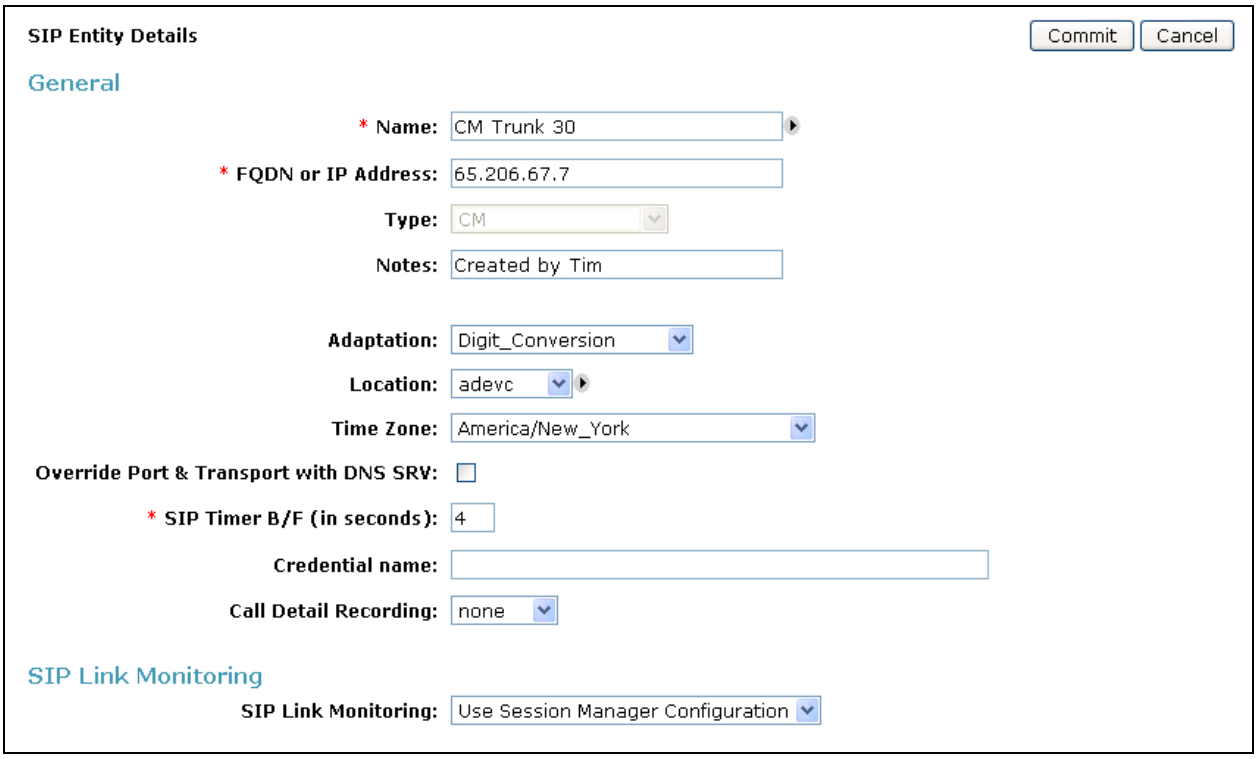
- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise (e.g., "adevc.avaya.globalipcom.com").

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

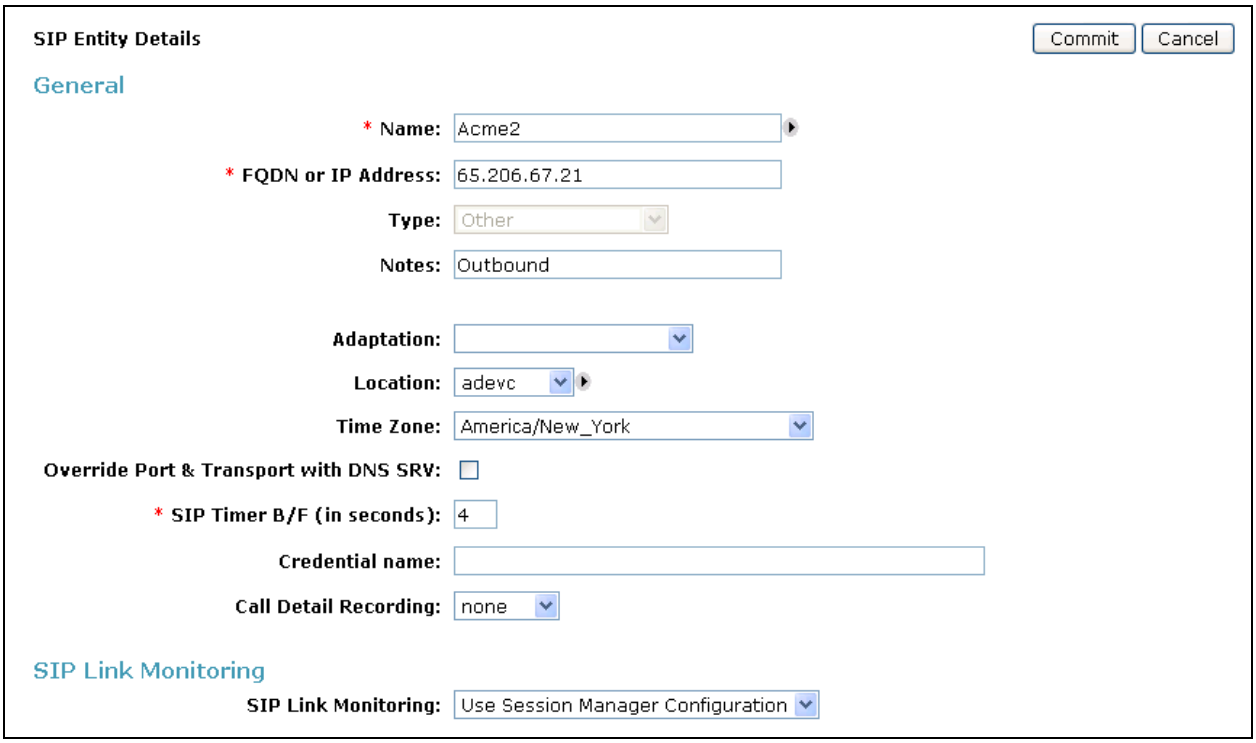
For the compliance test, two *Port* entries were added. TCP port 5060 was used for communicating with the Acme Packet SBC and TLS port 5061 was used for communication with Communication Manager.



The following screen shows the addition of Communication Manager. In this case, **FQDN or IP Address** is the IP address of the C-LAN board in the Avaya G650 Media Gateway. For **Adaptation**, select the adaptation module previously defined for dial plan digit manipulation in **Section 5.4**.



The following screen shows the addition of the Acme Packet SBC. **FQDN or IP Address** is the IP address of its network interface (see **Figure 1**).

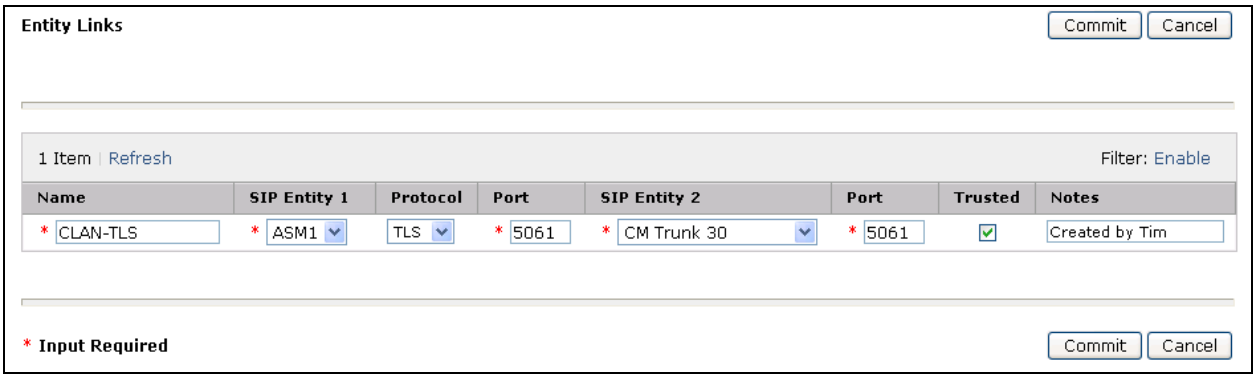


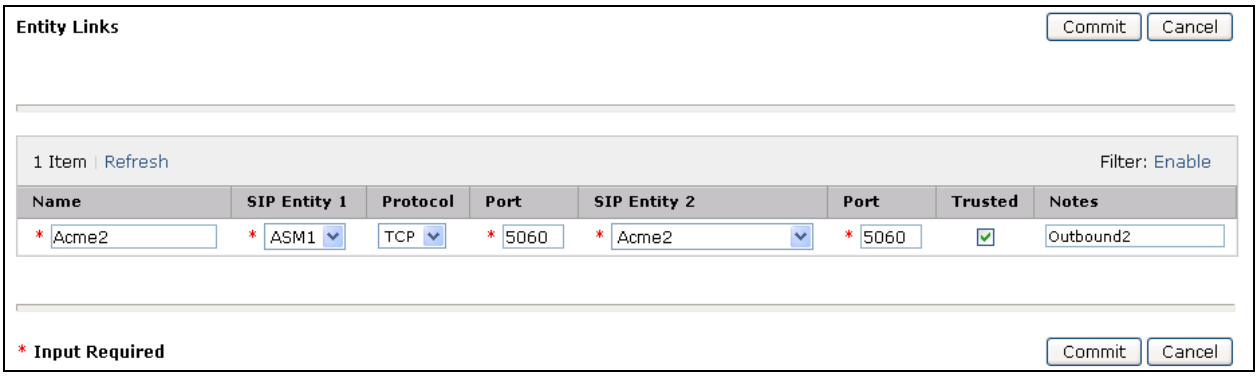
5.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. To add an Entity Link, navigate to **Network Routing Policy → Entity Links** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 5.5** will be denied.*

Click **Commit** to save each Entity Link definition. The following screens illustrate adding the Entity Links for Communication Manager and the Acme Packet SBC. TLS (well-known port 5061) is used for Communication Manager. TCP (well-known port 5060) was used for the Acme Packet SBC.





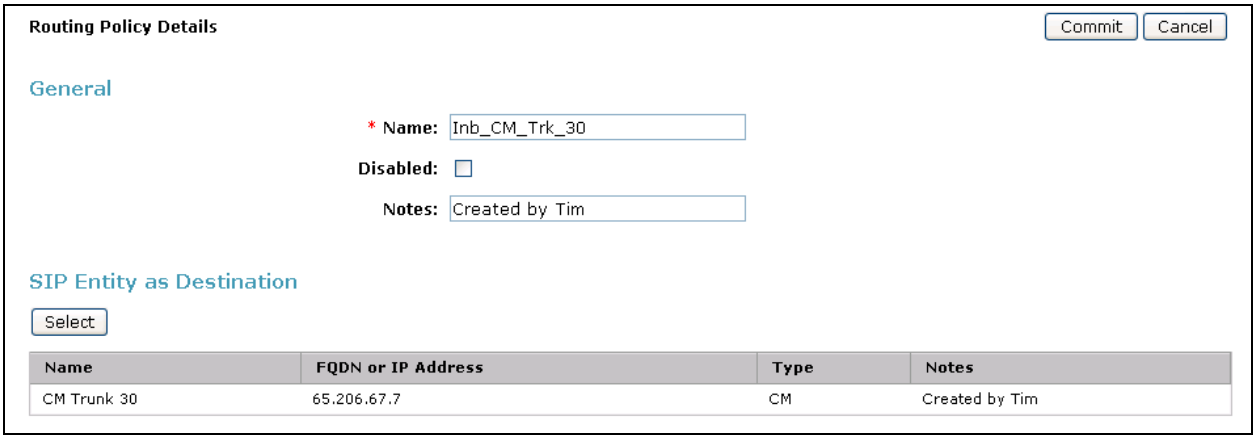
5.7. Add Routing Policies

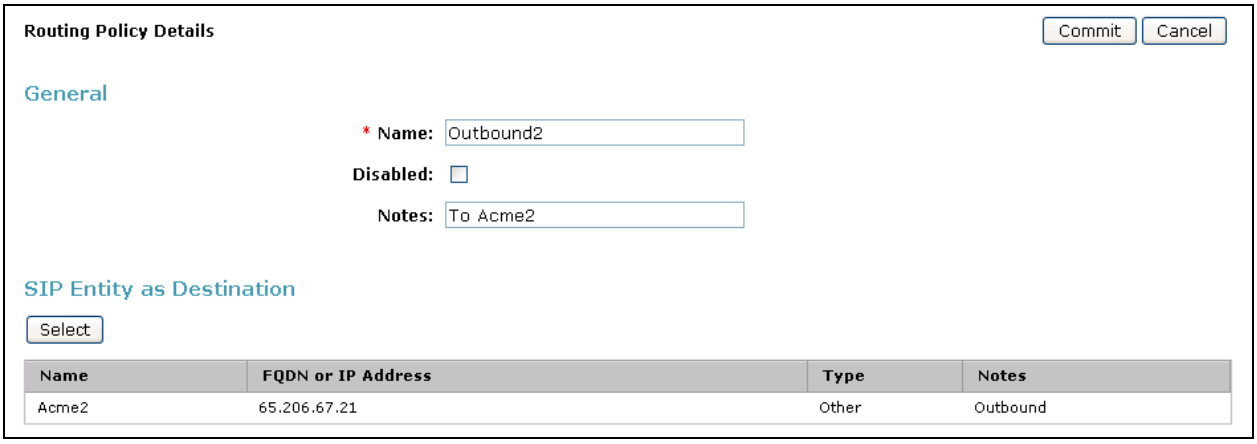
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5.5**. Two routing policies must be added for Communication Manager and the Acme Packet SBC. To add a routing policy, navigate to **Network Routing Policy → Routing Policies** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:
Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screens show the Routing Policies for Communication Manager and the SBC.





5.8. Add Dial Patterns

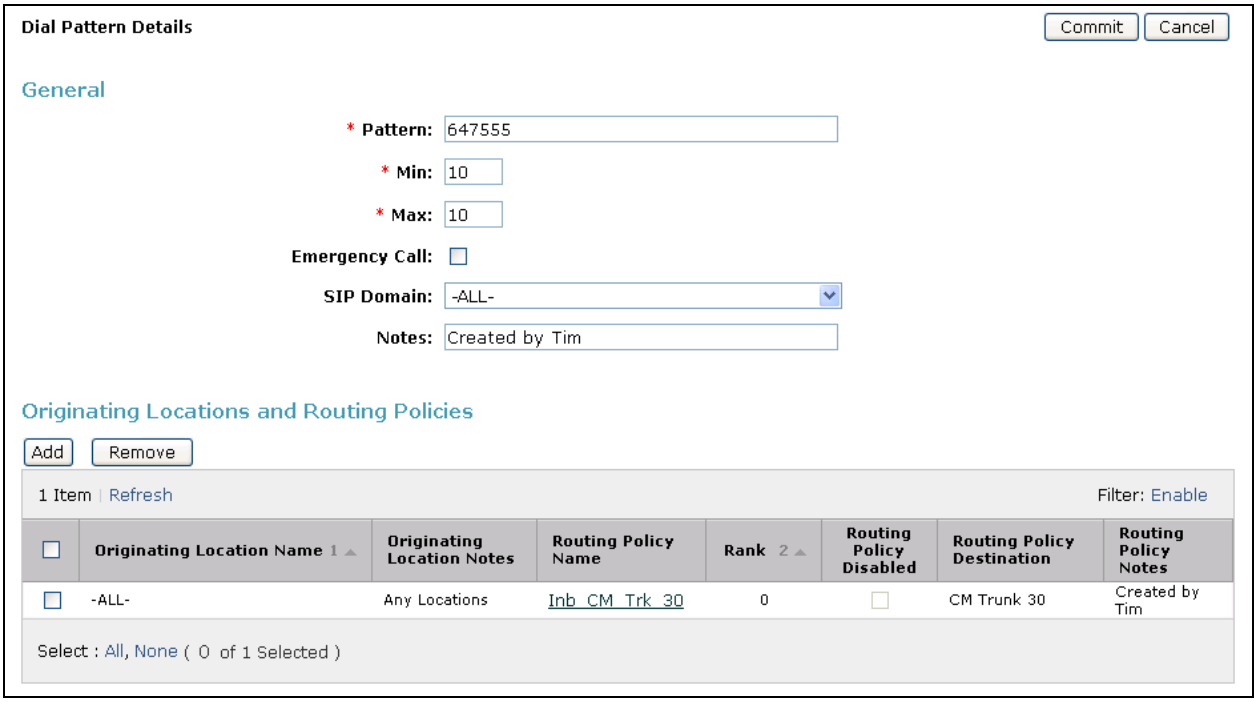
For calls from MTS Allstream to Communication Manager, dial patterns were defined to direct the calls. Calls to 10 digit numbers beginning with 647555 and originating from any domain should be routed to Communication Manager. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** The SIP domain from which the dial pattern may originate. In the case of the compliance test, enter ***–All-***.
- **Notes:** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate originating location (***-ALL-***) and routing policy (***Inb_CM_TRK_30***) from the list.

Default values can be used for the remaining fields. Click **Commit** to the dial pattern. The following screens show the resulting dial pattern definition. Note that similar to Communication Manager, the dial pattern selected will correspond to the longest match of a **Pattern** with the dialed number.



5.9. Add Regular Expressions

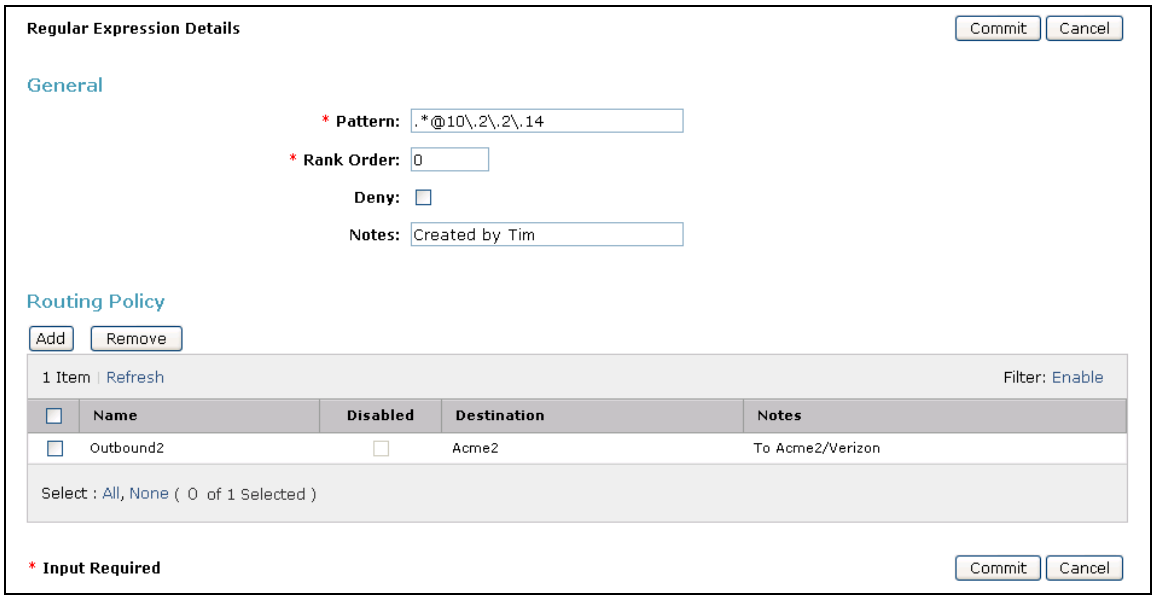
For calls from Communication Manager to MTS Allstream, a regular expression was defined to route the call. The MTS Allstream network expects the IP address of the MTS Allstream SIP proxy to appear in the SIP URI of outbound INVITE messages. Thus, this value is entered in the Far-end Domain field of the Communication Manager signaling group (**Section 4.5**). A regular expression was created to match on this string in the SIP URI to use for routing the call through the Session Manager. To add a regular expression, navigate to **Network Routing Policy → Regular Expressions** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under *General*:

- **Pattern:** Regular expression to match.
- **Notes:** Comment on purpose of regular expression.

Under *Routing Policies*:
Click **Add**, and then select the routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save the regular expression. The following screen shows the resulting regular expression definition. Note that some characters with special meaning in the pattern (such as a period) will need to be preceded with a \ to negate the special meaning and to provide a literal match. The example below will match on any SIP URI containing ***@10.2.2.14*** and will use routing policy ***Outbound2*** to complete the call.



Dial Patterns could also have been used as another approach to route these calls. Dial Patterns match on dialed digits and the destination domain. However, the destination domain must be a domain defined within Session Manager or defined as ***–All-***. Session Manager requires that SIP Domains be defined as fully qualified domain names and not IP addresses. So, it is not possible

to define the IP address of the MTS Allstream SIP proxy as a Session Manager SIP Domain. As a result, the dial pattern would have to use a destination domain of ***–All-***. Thus, the same dial pattern would match for all calls with the same dialed string, regardless of the destination domain.

5.10. Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

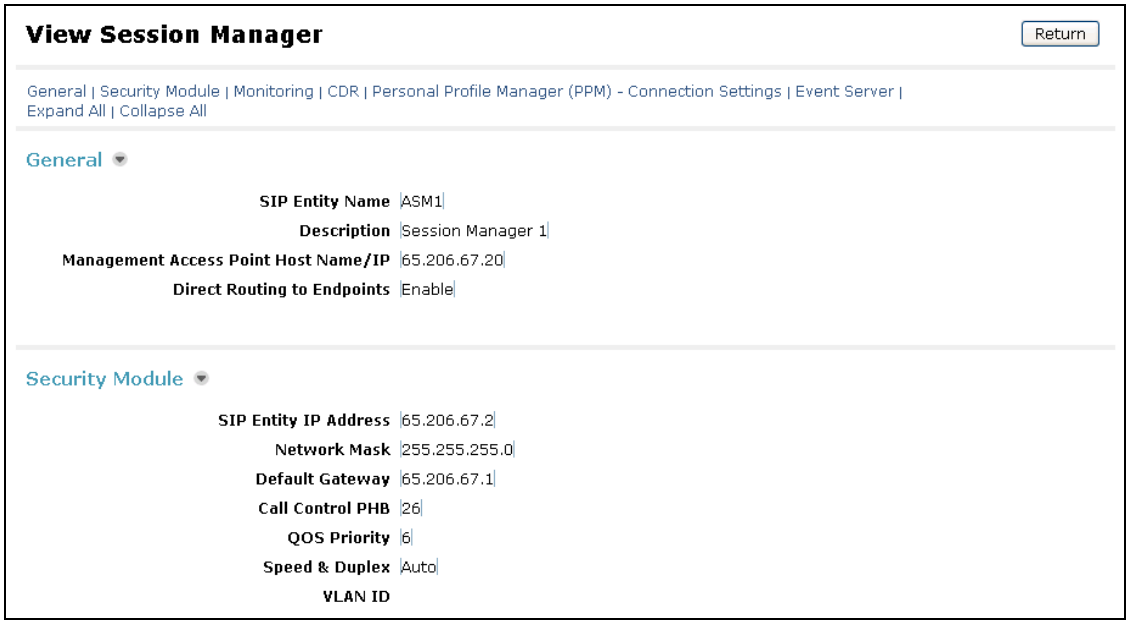
Under *General*:

- **SIP Entity Name:** Select the SIP Entity added for Session Manager.
- **Description**: Descriptive comment (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under *Security Module*:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the resulting Session Manager definition.



6. Configure Acme Packet 4250 Net-Net Session Director

The following Sections describe the provisioning of the Acme Packet SBC. Only the Acme Packet provisioning required for the reference configuration is described in these Application Notes. For more information on Acme Packet configuration see **[13 & 14]**.

The Acme Packet SBC was configured using the Acme Packet CLI via a serial console port connection. An IP remote connection to a management port is also supported. The following are the generic steps for configuring various elements.

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** command and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to (*configure)#.*
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4-8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until returned to the Superuser prompt.
10. Type **save-configuration** to save the configuration.
11. Type **activate-configuration** to activate the configuration.

Once the provisioning is complete, the configuration may be verified by entering the ***show running-config*** command.

6.1. Local Policies

Allows any SIP requests from the **INSIDE** realm to be routed to the **ALLSTREAM** Session Agent Group (SAG) in the **OUTSIDE2** realm (and vice-versa).

6.1.1. INSIDE to OUTSIDE2

From the *configure* prompt (steps 1 thru 3 in **Section 6**):

1. Create a local-policy for the **INSIDE** realm.
   a. Enter **session-router → local-policy**
   b. Enter **from-address → ***
   c. Enter **to-address → ***
   d. Enter **source-realm → INSIDE**
   e. Enter **state → enabled**
   f. Enter **policy-attributes**
   g. Enter **next-hop → SAG:ALLSTREAM**
   h. Enter **realm → OUTSIDE2**

i. Enter **terminate-recursion → enabled**
j. Enter **start-time → 0000**
k. Enter **end-time → 2400**
l. Enter **days-of-week → U-S**
m. Enter **app-protocol → SIP**
n. Enter **state → enabled**
o. Enter **exit**
p. Enter **done**

6.1.2. OUTSIDE2 to INSIDE

1. Create a local-policy for the **OUTSIDE2** realm. Procedures are the same as for the **INSIDE** local-policy except:
   a. Enter **source-realm → OUTSIDE**
   b. Enter **policy-attributes**
   c. Enter **next-hop → SAG:ENTERPRISE**
   d. Enter **realm → INSIDE**

6.2. Network Interfaces

This section defines the network interfaces to the private (Avaya CPE) and public (MTS Allstream) IP networks.

6.2.1. Public Interface

1. Create a network-interface to the public (MTS Allstream) side of the Acme.
   a. Enter **system → network-interface**
   b. Enter **name → M01**
   c. Enter **ip-address → 10.3.9.143**
   d. Enter **netmask → 255.255.255.128**
   e. Enter **gateway → 10.3.9.129**
   f. Enter **exit**
   g. Enter **done**

6.2.2. Private Interface

1. Create a network-interface to the private (Avaya CPE) side of the Acme. Procedures are the same as for the public network-interface except:
   a. Enter **system → network-interface**
   b. Enter **name → M10**
   c. Enter **ip-address → 65.206.67.21**
   d. Enter **netmask → 255.255.255.0**
   e. Enter **gateway → 65.206.67.100**
   f. Enter **exit**
   g. Enter **done**

6.3. Physical Interfaces

This section defines the physical interfaces to the private (Avaya CPE) and public (MTS Allstream) networks.

6.3.1. Public Interface

1. Create a network-interface to the public (MTS Allstream) side of the Acme.
   a. Enter **system → phy-interface**
   b. Enter **name → M01**
   c. Enter **operation-type → media**
   d. Enter **port → 1**
   e. Enter **slot → 0**
   f. **virtual-mac → 00:08:25:01:b5:69**
      i. Virtual MAC addresses are assigned based on the MAC address assigned to the Acme. This MAC address is found by entering the command → *show prom-info mainboard* (e.g. **00 08 25 01 b5 60**). To define a virtual MAC address, replace the last digit with **8** thru **f**.
   g. Enter **duplex-mode → full**
   h. Enter **speed → 100**
   i. Enter **exit**
   j. Enter **done**

6.3.2. Private Interface

1. Create a phy-interface to the private (Avaya CPE) side of the Acme. Procedures are the same as for the public phy-interface except:
   a. Enter **system → phy-interface**
   b. Enter **name → M10**
   c. Enter **port → 0**
   d. Enter **slot → 1**
   e. **virtual-mac → 00:08:25:01:be:6e**
   a. Enter **exit**
   b. Enter **done**

6.4. Realms

Realms are used as a basis for determining egress and ingress associations between physical and network interfaces as well as applying header manipulation such as NAT.

6.4.1. Outside2 Realm

1. Create a realm for the outside network.
   a. Enter **media-manager → realm-config**
   b. Enter **identifier → OUTSIDE2**
   c. Enter **addr-prefix → 0.0.0.0**
   d. Enter **network-interfaces → M01:0**
   e. Enter **out-manipulationid → NAT_IP**
   f. Enter **mm-in-realm → enabled**

g. Enter **mm-in-network → enabled**
h. Enter **mm-same-ip → enabled**
i. Enter **mm-in-system → enabled**
j. Enter **access-control-trust-level → medium**
k. Enter **invalid-signal-threshold → 1**
l. Enter **maximum-signal-threshold → 1**
m. Enter **untrusted-signal-threshold → 1**
n. Enter **exit**
o. Enter **done**

6.4.2. Inside Realm

1. Create a realm for the inside network. Procedures are the same as for the outside realm except:
   a. Enter **media-manager → realm-config**
   b. Enter **identifier → INSIDE**
   c. Enter **addr-prefix → 0.0.0.0**
   d. Enter **network-interfaces → M10:0**
   e. Enter **access-control-trust-level → high**
   f. Enter **invalid-signal-threshold → 0**
   g. Enter **maximum-signal-threshold → 0**
   h. Enter **untrusted-signal-threshold → 0**
   i. Enter **exit**
   j. Enter **done**

6.5. Steering-Pools

Steering pools define sets of ports that are used for steering media flows thru the Acme.

6.5.1. Outside Steering-Pool

1. Create a steering-pool for the outside network.
   a. Enter **media-manager → steering-pool**
   b. Enter **ip-address → 10.3.9.143**
   c. Enter **start-port → 49152**
   d. Enter **end-port → 65535**
   e. Enter **realm-id → OUTSIDE2**
   f. Enter **exit**
   g. Enter **done**

6.5.2. Inside Steering-Pool

1. Create a steering-pool for the inside network. Procedures are the same as for the outside steering-pool except:
   a. Enter **media-manager → steering-pool**
   b. Enter **ip-address → 65.206.67.21**
   c. Enter **start-port → 49152**
   d. Enter **end-port → 65535**
   e. Enter **realm-id → INSIDE**

f. Enter **exit**
g. Enter **done**

6.6. Session-Agents

A session-agent defines an internal "next hop" signaling entity for the SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent is defined for MTS Allstream (outside) and Session Manager (inside).

6.6.1. Outside Session-Agent

1. Create a session-agent for the outside network.
   a. Enter **session-router → session-agent**
   b. Enter **hostname → 10.2.2.14**
   c. Enter **ip-address → 10.2.2.14**
   d. Enter **port → 5060**
   e. Enter **state → enabled**
   f. Enter **app-protocol → SIP**
   g. Enter **transport-method → UDP**
   h. Enter **realm-id → OUTSIDE2**
   i. Enter **description → Allstream**
   j. Enter **ping-method → Options;hops=0**
   k. Enter **ping-interval → 60**
   l. Enter **ping-send-mode → keep-alive**
   m. Enter **exit**
   n. Enter **done**

6.6.2. Inside Session-Agent

1. Create a session-agent for the inside network. Procedures are the same as for the outside session-agent except:
   a. Enter **session-router → session-agent**
   b. Enter **hostname → 65.206.67.2**
   c. Enter **ip-address → 65.206.67.2**
   d. Enter **port → 5060**
   e. Enter **transport-method → staticTCP**
   f. Enter **realm-id → INSIDE**
   g. Enter **description → Enterprise Session Manager**
   h. Enter **options → trans-timeout=1**
   i. Enter **reuse-connections → TCP**
   j. Enter **tcp-keepalive → enabled**
   k. Enter **tcp-reconn-interval → 10**
   a. Enter **exit**
   b. Enter **done**

6.7. Session Groups

Session-groups (SAG) define single or multiple destinations that are referenced in provisioning session-agents.

6.7.1. MTS Allstream Session-group

1. Create a session-group for the MTS Allstream network.
   a. Enter **session-router → session-group**
   b. Enter **groupname → ALLSTREAM**
   c. Enter **state → enabled**
   d. Enter **app-protocol → SIP**
   e. Enter **strategy → hunt**
   f. Enter **dest → 10.2.2.14**
   g. Enter **stop-sag-recurse → 401,407**
   h. Enter **exit**
   i. Enter **done**

6.7.2. Avaya CPE Session-group

1. Create a session-group for the Avaya CPE network. Procedures are the same as for the Verizon session-group except:
   a. Enter **session-router → session-group**
   b. Enter **groupname → ENTERPRISE**
   c. Enter **dest → 65.206.67.2**
   c. Enter **exit**
   d. Enter **done**

6.8. SIP Configuration

This command sets the values for the Acme Packet SIP operating parameters. The home-realm defines the SIP daemon location, and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere.

1. Enter **session-router → sip-config**
2. Enter **state → enabled**
3. Enter **operation-mode → dialog**
4. Enter **home-realm-id → INSIDE**
5. Enter **egress-realm-id → INSIDE**
6. Enter **exit**
7. Enter **done**

6.9. SIP Interfaces

The SIP interface defines the signaling interface (IP address and port) to which the Acme Packet sends and receives SIP messages.

6.9.1. Outside SIP- interface

1. Create a sip-interface for the outside network.
   a. Enter **session-router → sip-interface**
   b. Enter **state → enabled**
   c. Enter **realm-id → OUTSIDE2**
   d. Enter **sip-port →**
      1. Enter **address → 10.3.9.143**

2. Enter **port → 5060**
3. Enter **transport-protocol → UDP**

e. Enter **stop-recurse → 401,407,486,488**
f. Enter **exit**
g. Enter **exit**
h. Enter **done**

6.9.2. Inside SIP- interface

1. Create a sip-interface for the inside network. Procedures are the same as for the outside sip-interface except:
   a. Enter **session-router → sip-interface**
   b. Enter **realm-id → INSIDE**
   c. Enter **sip-port →**
      1. Enter **address → 65.206.67.21**
      2. Enter **port → 5060**
      3. Enter **transport-protocol → TCP**
   d. Enter **exit**
   e. Enter **exit**
   f. Enter **done**

6.10. SIP Manipulation

SIP manipulation specifies rules for manipulating the contents of specified SIP headers. In the reference configuration the following header manipulations are performed:

- NAT IP addresses in the From header of SIP requests.
- NAT IP addresses in the To header of SIP requests.
- NAT IP addresses in the Remote-Party-ID header of SIP requests.
- NAT IP addresses in the History-Info header of SIP requests.
- NAT IP addresses in the Alert-Info header of SIP requests. This is different from other rules because it will NAT CID (caller ID) URIs in addition to SIP URIs.

1. Enter **session-router → sip-manipulation**
2. Enter **name → NAT_IP**
3. Enter **description → Topology hiding SIP headers**
4. Enter **session-router → sip-manipulation → header-rule**
5. Proceed to the following sections

6.10.1. From Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipFrom**
3. Enter **action → manipulate**
4. Enter **comparison-type → case-sensitive**
5. Enter **msg-type → request**
6. Enter **element-rule →**
   a. Enter **name → FROM**

b. Enter **type → uri-host**
c. Enter **action → replace**
d. Enter **match-val-type → ip**
e. Enter **comparison-type → uri-host**
f. Enter **new-value → $LOCAL_IP**

7. Enter **exit**
8. Enter **done**

6.10.2. To Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipTo**
3. Enter **action → manipulate**
4. Enter **comparison-type → case-sensitive**
5. Enter **msg-type → request**
6. Enter **element-rule →**
   a. Enter **name → TO**
   b. Enter **type → uri-host**
   c. Enter **action → replace**
   d. Enter **match-val-type → ip**
   e. Enter **comparison-type → case-sensitive**
   f. Enter **new-value → $REMOTE_IP**
7. Enter **exit**
8. Enter **done**

6.10.3. Remote Party ID Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipRpid**
3. Enter **header-name → Remote-Party-ID**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule →**
   a. Enter **name → RPID**
   b. Enter **type → uri-host**
   c. Enter **action → replace**
   d. Enter **match-val-type → ip**
   e. Enter **comparison-type → case-sensitive**
   f. Enter **new-value → $LOCAL_IP**
8. Enter **exit**
9. Enter **done**

6.10.4. History Info Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → manipHistInfo**
3. Enter **header-name → History-Info**

4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule →**
    a. Enter **name → HISTORYINFO**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → ip**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $REMOTE_IP**
8. Enter **exit**
9. Enter **done**

6.10.5. Alert-info Header

1. Enter **session-router → sip-manipulation → header-rule**
2. Enter **name → storeAlertInfo**
3. Enter **header-name → Alert-Info**
4. Enter **action → store**
5. Enter **comparison-type → pattern-rule**
6. Enter **match-value → (.+@) ([0-9.]+) (.+)**
7. Enter **msg-type → request**
8. Enter **exit**
9. Enter **header-rule**
10. Enter **name → manipAlertInfo**
11. Enter **header-name → Alert-Info**
12. Enter **action → manipulate**
13. Enter **comparison-type → boolean**
14. Enter **match-value → $storeAlertInfo**
15. Enter **msg-type → request**
16. Enter **new-value → $storeAlertInfo.$1+$REMOTE_IP+$storeAlertInfo.$3**
17. Enter **exit**
18. Enter **done**

6.11. Other Acme Packet provisioning

6.11.1. Access-control

This is a static Access Control List that is used to limit SIP access to only known devices.

1. Enter **session-router → access-control**
2. Enter **realm-id → OUTSIDE2**
3. Enter **source-address → 10.2.2.14:5060**
4. Enter **application-protocol → SIP**
5. Enter **transport-protocol → UDP**
6. Enter **access → permit**
7. Enter **exit**
8. Enter **done**

6.11.2. Media-Manager

Verify that the media-manager process is enabled.

1. Enter **media-manager → media-manager**
2. Enter **select → show →** Verify that the media-manager state is enabled. If not, perform steps 3 -5.
3. Enter **state → enabled**
4. Enter **exit**
5. Enter **done**

7. MTS Allstream Services Configuration

To use the MTS Allstream SIP Trunk Service, a customer must request service from MTS Allstream using their sales processes. The process can be started by contacting MTS Allstream via the corporate web site at www.allstream.com and requesting information via the online sales links or telephone numbers.

During the signup process, MTS Allstream will require that the customer provide the public IP address used to reach the SBC at the edge of the enterprise or the public IP address of the Session Manager server if a SBC is not used. MTS Allstream will provide the IP address of the MTS Allstream SIP proxy/SBC, and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager and Session Manager configuration discussed in the previous sections.

8. General Test Approach and Test Results

A simulated enterprise site using Communication Manager and Session Manager was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to connect to the MTS Allstream SIP Trunk Service.

To verify SIP trunking interoperability the following features and functionality were covered during the interoperability compliance test:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by MTS Allstream. Incoming PSTN calls were made to H.323, digital, and analog endpoints at the enterprise.
- Outgoing calls from the enterprise site were completed via MTS Allstream to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, digital, and analog endpoints.
- Various call types were tested including: inbound, outbound, international, outbound toll-free, operator, and directory assistance.
- Inbound toll-free and 911 emergency calls are both supported but were not tested as part of the compliance test.
- Calls using G.729A, G.711MU, and G.711A codecs.

- DTMF transmission using RFC 2833 with successful vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and extension to cellular, when the call arrived from the SIP trunk from MTS Allstream, or when the call forwarding destination and extension to cellular mobile number routed out the SIP trunk to MTS Allstream, or both.
- Caller ID Presentation and Caller ID Restriction.
- T.38 fax is not supported by MTS Allstream.
- Avaya one-X Communicator in both "Road Warrior" and "Telecommuter" modes, where incoming PSTN calls arrived from MTS Allstream, or the telecommute number routed out the SIP Trunk to MTS Allstream, or both.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones. This allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

Interoperability testing of the MTS Allstream SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Use of Avaya one-X Communicator (H.323 soft client)**: When placing outbound calls from an Avaya H.323 one-X Communicator in telecommuter mode, if the call is placed on hold and retrieved from hold, the call no longer has audio and the call is disconnected after several seconds. This behavior also impacts the use of transfer and conference of PSTN calls. Thus, the Avaya one-X Communicator can only be used for basic inbound and outbound calls in telecommuter mode without the use of hold, transfer or conference.
- **Inbound Calling Party Number Block**: When an inbound call from a PSTN phone with Calling Party Number Block enabled terminates to a H.323 phone, the calling party number is blocked during ringing but is displayed after the call is answered. This is expected to be fixed in a future release of Session Manager.

9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

10. Conclusion

These Application Notes describe the configuration necessary to connect Communication Manager and Session Manager to the MTS Allstream SIP Trunk Service. The MTS Allstream

SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The MTS Allstream SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunk lines.

11. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.
Acme Packet documentation is available from Acme Packet.

[1] *Administering Avaya Aura™ Communication Manager*, May 2009, Document Number 03-300509.
[2] *Avaya Aura™ Communication Manager Feature Description and Implementation,* May 2009, *D*ocument Number 555-245-205.
[3] *Installing and Upgrading Avaya Aura™ System Manager 5.2 GA Version*, January 2010.
[4] *Installing Avaya Aura™ Session Manager*, January 2010.
[5] *Administering Avaya Aura™ Session Manager,* March 2010, Document Number 03-603324.
[6] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x,* February 2010, Document Number 16-601443.
[7] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.
[8] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.
[9] *Avaya one-X Communicator Getting Started, November 2009.*
[10] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/
[11] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/
[12] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/
[13] *Net-Net® 4000, ACLI Reference Guide, Release Version S-C6.1.0*
[14] *Net-Net® 4000 ACLI, Configuration Guide, Release Version S-C6.1.0*

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.