Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.2 and Acme Packet Net-Net 3820 SBC with TLS and SRTP to support Cable and Wireless SIP IP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Cable and Wireless SIP IP Trunking service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Acme Packet Net-Net 3820, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server configured to use secure SIP signaling using TLS and secure voice using SRTP only in the Enterprise domain. Cable and Wireless is a member of the 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.

Table of Contents

1. Introduction 3
2. General Test Approach and Test Results 3
   2.1. Interoperability Compliance Testing 4
   2.2. Test Results 4
   2.3. Support 5
3. Reference Configuration 6
4. Equipment and Software Validated 7
5. Configure Avaya Aura® Communication Manager 8
   5.1. Confirm System Features 8
   5.2. Administer IP Node Names 10
   5.3. Administer IP Network Region 10
   5.4. Administer IP Codec Set 11
   5.5. Administer SIP Signaling Groups 12
   5.6. Administer SIP Trunk Group 13
   5.7. Administer Calling Party Number Information 15
   5.8. Administer Route Selection for Outbound Calls 15
   5.9. Administer Incoming Digit Translation 17
   5.10. EC500 Configuration 17
6. Configuring Avaya Aura® Session Manager 18
   6.1. Log in to Avaya Aura® System Manager 18
   6.2. Administer SIP Domain 19
   6.3. Administer Locations 20
   6.4. Administer Adaptations 21
   6.5. Administer SIP Entities 22
      6.5.1. Avaya Aura® Session Manager SIP Entity 23
      6.5.2. Avaya Aura® Communication Manager SIP Entity 24
      6.5.3. Acme Packet Net-Net 3820 SIP Entity 24
   6.6. Administer Entity Links 25
   6.7. Administer Routing Policies 26
   6.8. Administer Dial Patterns 28
   6.9. Administer Application for Avaya Aura® Communication Manager 30
   6.10. Administer Application Sequence for Avaya Aura® Communication Manager 31
   6.11. Administer SIP Extensions 32
7. Configure Avaya telephones for TLS and SRTP 36
8. Configure Acme Packet Net-Net 3820 SBC 37
   8.1. Create Certificate Records on Acme Packet SBC 37
   8.2. Header Manipulation Rule 38
9. Configure Cable and Wireless SIP IP Trunking 39
10. Verification Steps 39
11. Conclusion 40
12. Additional References 40

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Cable and Wireless SIP IP Trunking service and an Avaya SIP-enabled Enterprise Solution. The Avaya solution consists of Acme Packet Net-Net 3820, Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Internal voice calls within the enterprise space are secured using TLS for signaling and SRTP for media. PSTN calls are also protected up to the Acme Packet Net-Net 3820 private side interface, where they are decrypted and changed to UDP and RTP for transmission to the service provider. It is expected a Virtual Private Network will be used to secure signaling and media between the Acme Packet Net-Net 3820 public side and the service provider's equipment. Customers using this Avaya SIP-enabled enterprise solution with the Cable and Wireless SIP IP Trunking service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Acme Packet Net-Net 3820 SBC. The enterprise site was configured to use the SIP IP Trunking service provided by Cable and Wireless.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Acme Packet Net-Net 3820. The enterprise site was configured to use the SIP IP Trunking service provided by Cable and Wireless and use the Acme Packet Net-Net 3820 to secure incoming and outgoing voice calls using TLS/SRTP in the enterprise space and UDP/RTP over the service providers SIP trunks.

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DDI numbers assigned by Cable and Wireless. The calls were made to H.323, SIP and analogue telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Cable and Wireless to PSTN destinations. The calls were made from H.323, SIP and analogue telephones.
- Calls using G.711A and G.729A codec's.
- DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones, and the Avaya Desktop Video Device (ADVD) running Flare Experience.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Cable and Wireless requiring Avaya response and sent by Avaya requiring Cable and Wireless response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Cable and Wireless SIP IP Trunking service with the following observations:

- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator
- When Calling Line Identity (CLI) is restricted in the network and delivered to the enterprise, the Privacy header is not included in the INVITE
- No ringback was heard by the caller on calls from the PSTN forwarded unconditionally to another PSTN number. A workaround is required in the form of a Header Manipulation Rule on the Acme Packet SBC to provide ringback to the caller. This workaround will be required until a permanent resolution is implemented in the network.
- The conferencing of an inbound PSTN call to internal extensions is limited in that the incoming call is dropped when a fifth extension is added to the conference. This is considered to be a limitation imposed by the SIP trunk service.

- The conferencing of an outbound PSTN call to internal extensions is limited in that the outgoing call is dropped when a fifth extension is added to the conference. With the workaround in place to provide ringback for calls forwarded to the PSTN, this reduced such that the outgoing call is dropped when a fourth extension is added to the conference. This is considered to be a limitation imposed by the SIP trunk service.
- The conferencing of an outbound PSTN call to additional PSTN destinations is limited in that the outgoing call is dropped when the second additional PSTN destination is added to the conference. This occurs only with the workaround in place to provide ringback for calls forwarded to the PSTN. This is considered to be a limitation imposed by the SIP trunk service.
- T.38 Fax was not tested.
- Network Call Redirect using SIP 302 Moved Temporarily is acknowledged but the call is not routed meaning this feature can't be considered to be supported
- When Network Call Redirect was invoked using SIP REFER, Communication Manager did not react to NOTIFY message from the network indicating that the destination was busy. This is thought to be a Communication Manager configuration issue.
- When the number of members assigned to the SIP Trunk Group in the Communication Manager is exceeded, a SIP 500 "Service Unavailable" message is received in the network. The network re-attempts the call a number of times so that there is a delay before the caller gets an indication of failure
- When the signalling link between the Communication Manager and the Session Manager is unavailable, a SIP 500 "Server Link Monitor Status Down" message is received in the network. The network re-attempts the call a number of times so that there is a delay before the caller gets an indication of failure

2.3. Support

For technical support on Cable and Wireless products please use the following web link. http://www.cw.com/contact-us/.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Cable and Wireless SIP IP Trunking service. Located at the Enterprise site is an Acme Packet Net-Net 3820, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Flare Experience, Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for H.323.

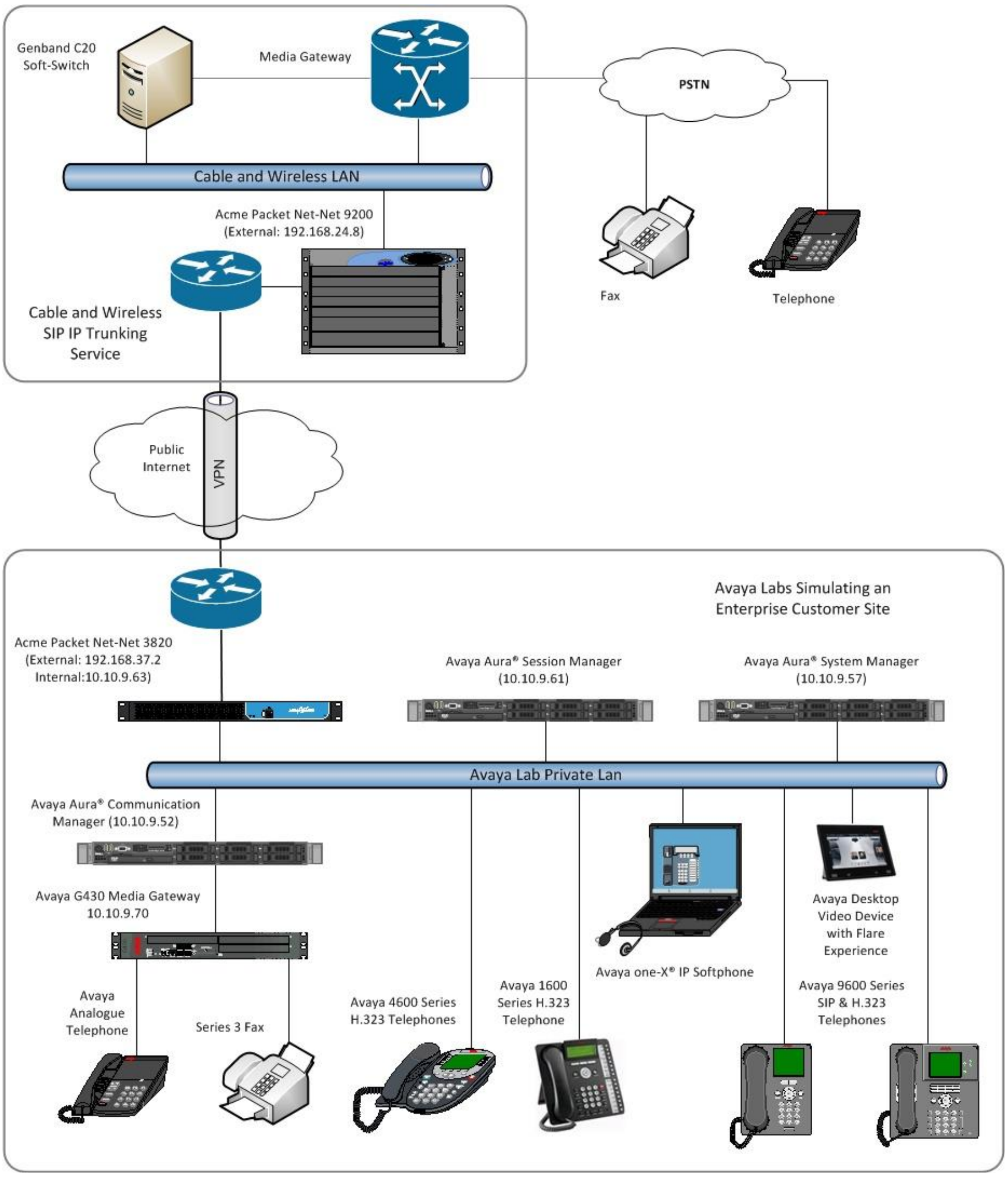


Figure 1: Test Set-up for Cable and Wireless SIP IP Trunking to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 Build R016x.02.0.823.0
Avaya G430 Media Gateway	FW 30.12.1
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 Build 6.2.0.0.620110
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 (System Platform 6.2.0.0.27, Template 6.2.12.0)
Acme Packet Net-Net 3820 SBC	SCX6.3.0 MR-2 Patch 4 (Build 419) Build Date 10/26/12
Acme Packet Quad port GiGE SFP (sub component of Acme Packet Net-Net 3820 SBC)	Part Number:002-0618-58 FunctionalRev:02.10 BoardRev:02.00
Avaya 1616 Phone (H.323)	1.301
Avaya 4621 Phone (H.323)	2.902
Avaya 9630 Phone (H.323)	3.103
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1
Avaya 9630 Phone (SIP)	R2.6 SP6
Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.3.08-SP3-Patch2-35791
Analogue Phone	N/A
Cable and Wireless	
ACME Packet Net-Net 9200 SBC	nnSD700m11
Genband C20 Soft-Switch	CVM13 (12.0.12)

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signalling associated with the Cable and Wireless SIP IP Trunking service. For incoming calls, the Session Manager receives SIP messages from the Acme Packet Net-Net 3820 SBC and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Acme Packet Net-Net 3820 at the enterprise site that then sends the SIP messages to the Cable and Wireless network. 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. The general installation of the Avaya S8800 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

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. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Cable and Wireless network, and any other SIP trunks used.

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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 20
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

On **Page 4**, verify that **IP Trunks** field is set to **y** and **Media Encryption Over IP** is set to **y**.

```
display system-parameters customer-options                          Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                          ISDN Feature Plus? n
                  Enhanced EC500? y       ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                   ISDN-PRI? y
              ESS Administration? y                 Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                       Malicious Call Trace? y
     External Device Alarm Admin? y                   Media Encryption Over IP? y
   Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                   Multifrequency Signaling? y
      Global Call Classification? y          Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                 Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
```

Use the **display system-parameters features** command and on **Page 19**, verify that the **SDP Capability Negotiation for SRTP** is set to **y**, **Direct IP-IP Audio Connections** is set to **y** and **IP Audio Hairpinning** is set to **n**.

```
display system-parameters features                                 Page  19 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
                   Direct IP-IP Audio Connections? y
                             IP Audio Hairpinning? n
                          Synchronization over IP? n
              SDP Capability Negotiation for SRTP? y
                    SIP Endpoint Managed Transfer? n

CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                   Call Pickup on Intercom Calls? y     Call Pickup Alerting? n
     Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? n
                      Extended Group Call Pickup: none
                   Enhanced Call Pickup Alerting? n


                        Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? y
                  PIN Checking for Private Calls? n
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.9.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.9.61
Sipera-SBC          10.10.9.71
default             0.0.0.0
procr               10.10.9.52
procr6              ::
```

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Acme Packet SBC.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: default
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: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        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
```

5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **Section 5.3.** Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec's supported by Cable and Wireless were configured, namely **G.729A**, and **G.711A**. Tab down to the Media Encryption settings and enter **1-srtp-aescm128-hmac80** as the chosen media encryption setting. Press **F3** to move to the next page.

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711A            n         2        20
 2: G.729A            n         2        20
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1: 1-srtp-aescm128-hmac80
 2:
 3:
```

The Cable and Wireless SIP IP Trunking service does not support T.38 for fax transmissions. To disable this capability, tab to the FAX setting and set the **Fax Mode** to **off** as shown below.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                Redundancy
    FAX             off                  0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Cable and Wireless SIP IP Trunking service. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of **5061** for security. Configure the **Signaling Group** using the **add signaling-group x** command, where **x** is an available signaling group, as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tls**
- Set **Enforce SIPS URI for SRTP** to **n**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5061** (Commonly used TLS port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

```
change signaling-group 1                                              Page   1 of   2
                                SIGNALING GROUP

Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM


   Near-end Node Name: procr                  Far-end Node Name: SM100
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain:
                                             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? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-netwrk** – required setting when using the Diversion header
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

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

Group Number: 1                  Group Type: sip           CDR Reports: y
  Group Name: Group 1                   COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Cable and Wireless to prevent unnecessary SIP messages during call setup.

```
Add trunk-group 1                                               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): 1800

 Disconnect Supervision - In? y  Out? y
```

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of CLI in E.164 format with a leading “+”.

```
add trunk-group 1                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y



                     Numbering Format: public
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
```

On **Page 4** of this form:

- Set **Send Diversion Header** to **y** to include the header in forwarded and transferred calls. This is not currently used by Cable and Wireless but is included as it was set for test.
- Set **Support Request History** to **n** as Cable and Wireless does not use History Info making it an unnecessary extension to the SIP INVITE
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Cable and Wireless
- Set **Always Use re-INVITE for Display Updates** to **y** as SIP UPDATE messages are not supported by Cable and Wireless for call forwarding

```
add trunk-group 1                                               Page   4 of  21
                              PROTOCOL VARIATIONS

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


            Convert 180 to 183 for Early Media? n
      Always Use re-INVITE for Display Updates? y
            Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                  Enable Q-SIP? N
```

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the test configuration, individual stations were mapped to send numbers allocated from the Cable and Wireless DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

```
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: 8
 4  2000           1         44149nnnnnn0    12     Maximum Entries: 9999
 4  2296           1         44149nnnnnn3    12
 4  2316           1         44149nnnnnn5    12    Note: If an entry applies to
 4  2346           1         44149nnnnnn2    12    a SIP connection to Avaya
 4  2396           1         44149nnnnnn1    12    Aura(R) Session Manager,
 4  2400           1         44149nnnnnn6    12    the resulting number must
 4  2601           1         44149nnnnnn4    12    be a complete E.164 number.
```

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Cable and Wireless SIP IP Trunking service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

```
change feature-access-codes                                     Page   1 of  10
                               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: *69
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 5
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
```

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

```
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                     8    14     1         pubu         n
    00                    13   17     1         pubu         n
    00353                 10   14     1         pubu         n
    0044                  12   14     1         pubu         n
    0800                  11   11     1         pubu         n
    118                   5    6      1         pubu         n
```

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. Numbering Plan Indictor (NPI) of the Calling Party Number is set to E.164 and Type of Numbering (TON) is set to international by using **Numbering Format** of **intl-pub**.

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

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               intl-pub  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
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Cable and Wireless can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by Cable and Wireless for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **149nnnnnn0** to **149nnnnnn8** to the 4 digit extension by deleting all (**10**) of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

```
change inc-call-handling-trmt trunk-group 1                    Page   1 of  30
                     INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 149nnnnnn0       10  2000
 public-ntwrk    10 149nnnnnn1       10  2396
 public-ntwrk    10 149nnnnnn2       10  2346
 public-ntwrk    10 149nnnnnn3       10  2296
 public-ntwrk    10 149nnnnnn4       10  2601
 public-ntwrk    10 149nnnnnn5       10  2316
 public-ntwrk    10 149nnnnnn6       10  2400
 public-ntwrk    10 149nnnnnn7       10  6103
 public-ntwrk    10 149nnnnnn8       10  2501
```

5.10. EC500 Configuration

When EC500 is enabled on a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

```
change off-pbx-telephone station-mapping 2396                  Page   1 of   3
                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number     Trunk      Config  Dual
 Extension                 Prefix                      Selection  Set     Mode
 2396             EC500         -     0035386nnnnnnn   1          1
                                -
```

Save Communication Manager changes by entering **save translation** to make them permanent.

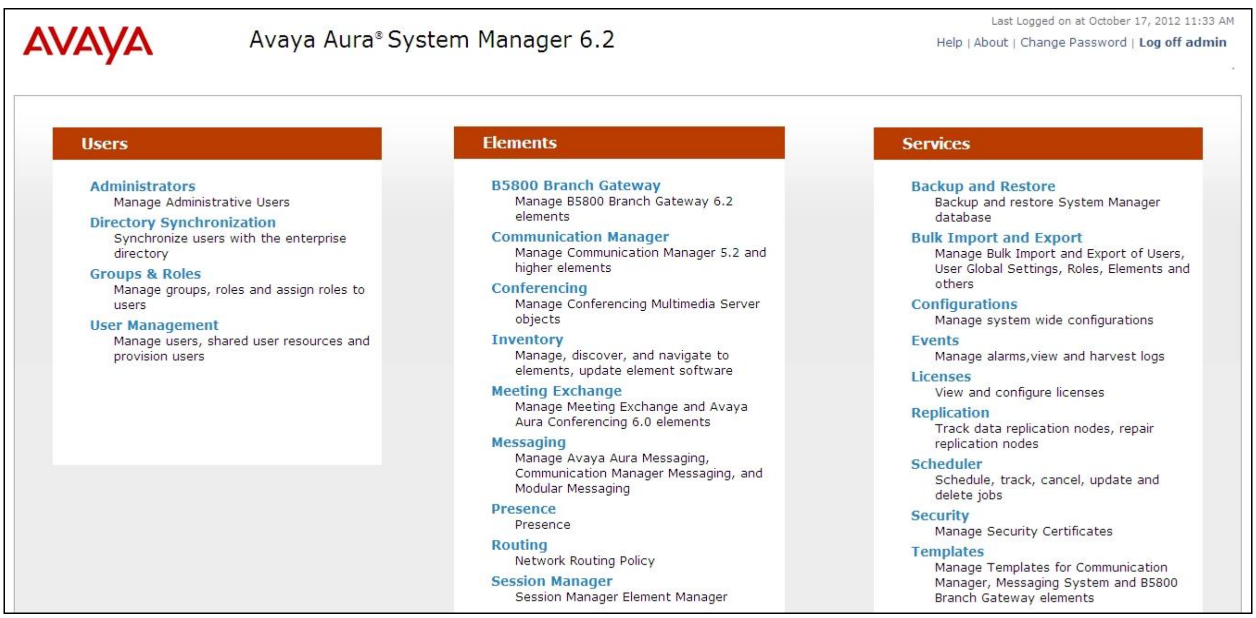
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Communication Manager
- Administer Application Sequence for Communication Manager
- Administer SIP Extensions

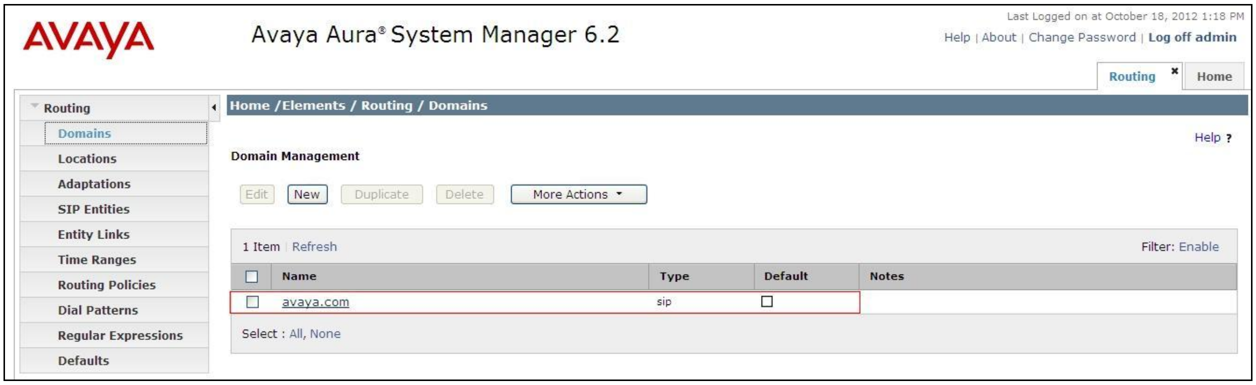
6.1. Log in to Avaya Aura® System Manager

Access System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where <**FQDN**> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.



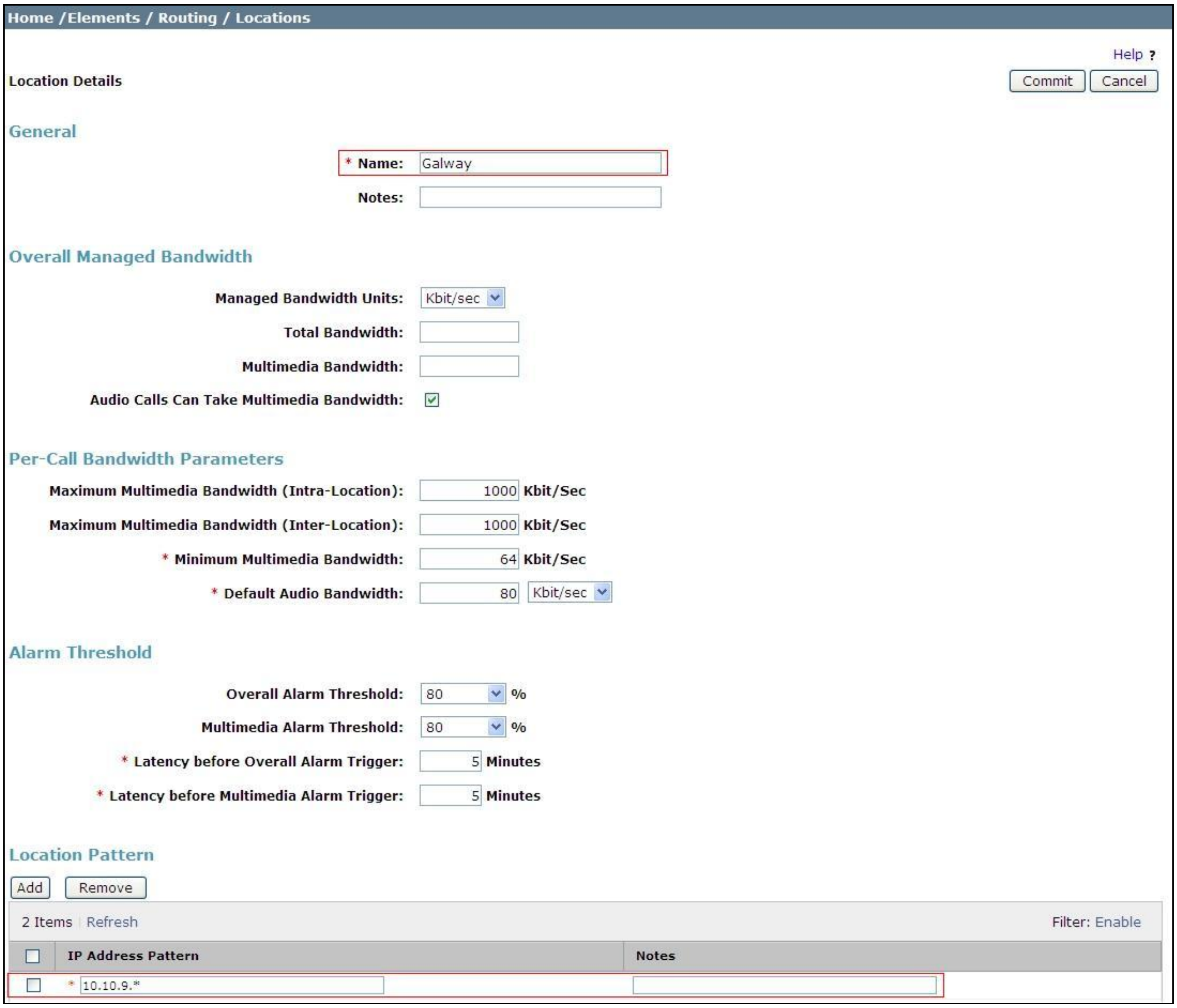
6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.



6.3. Administer Locations

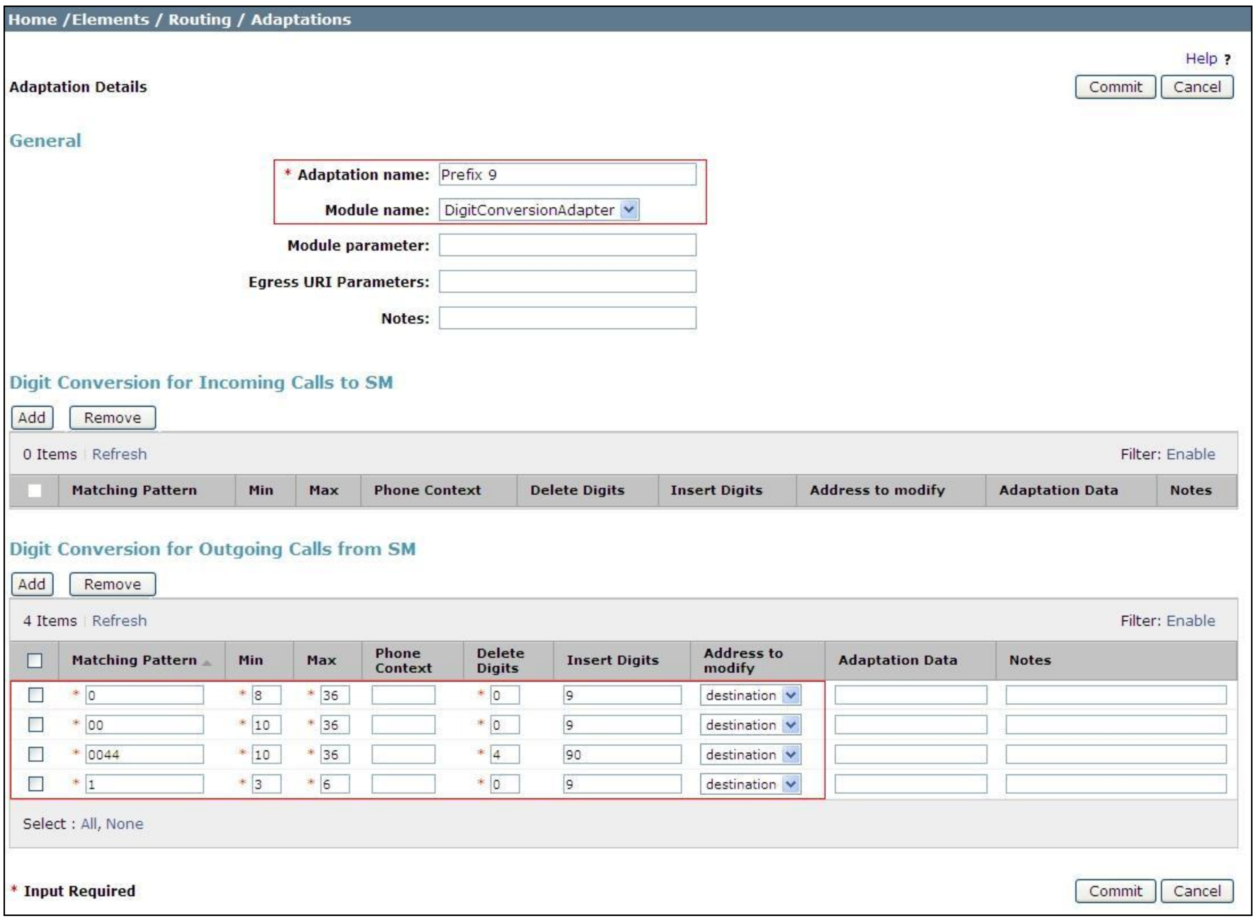
Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.



6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. The example shown was used in test to prefix the called party number with a **9** which is a requirement of Cable and Wireless. The module **DigitConversionAdaptor** is used and terminating numbers starting with a **0** for national and international calls and **1** for Operator and Directory Enquiries are analyzed and the **9** inserted. Additionally, UK numbers are converted from international to national format.

These rules are applied to the destination addresses.



6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **SIP Trunk** for the Session Border Controller SIP entity (Note that **Gateway** was used in test, there is not currently a significant difference in functionality between the two settings)
- In the Adaptation field, enter the adaptation defined in **section 6.4** where appropriate. In test this was applied to the Acme Packet SBC
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

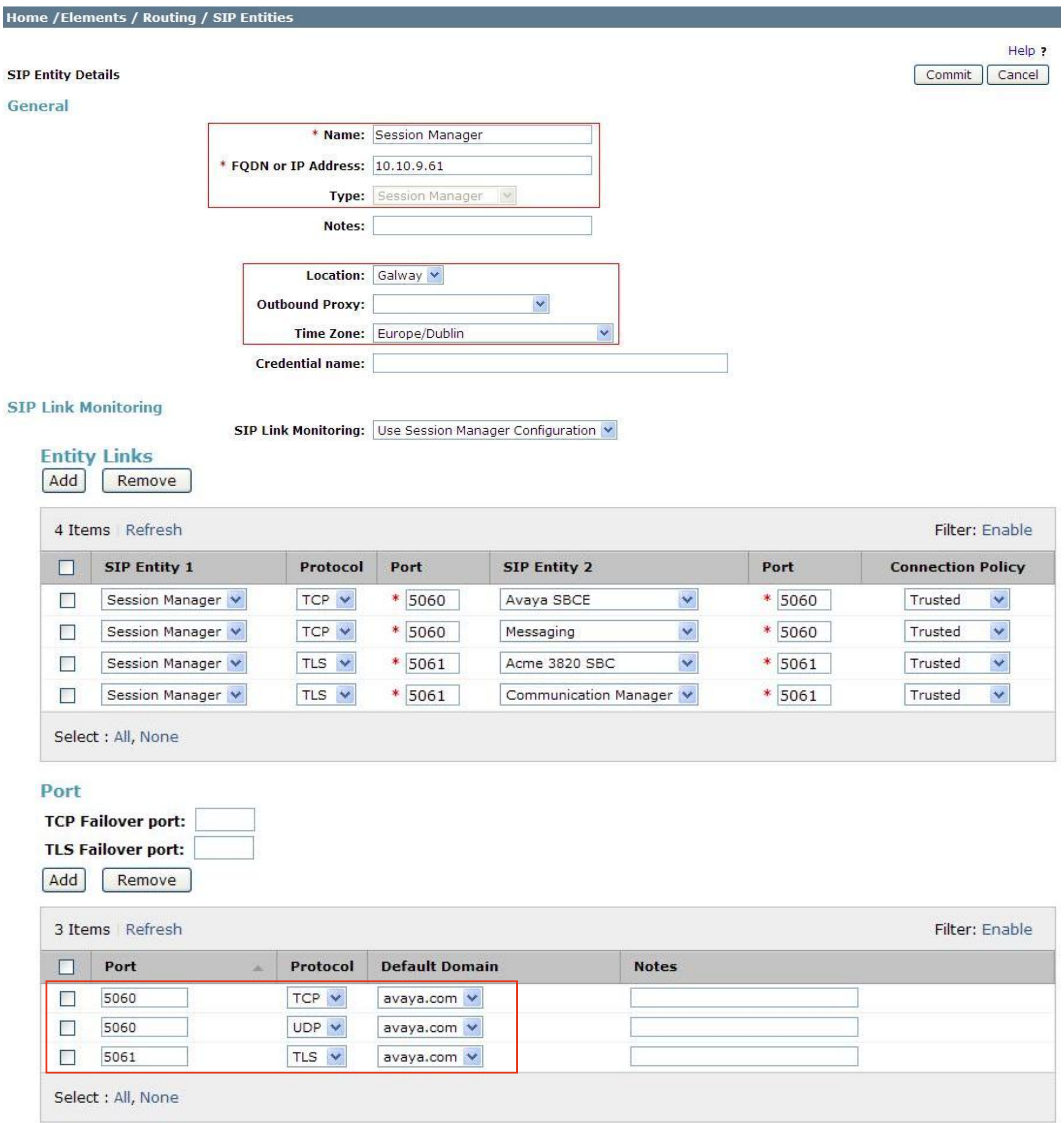
In this configuration there are three SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Acme Packet Net-Net 3820 SBC SIP Entity

6.5.1. Avaya Aura® Session Manager SIP Entity

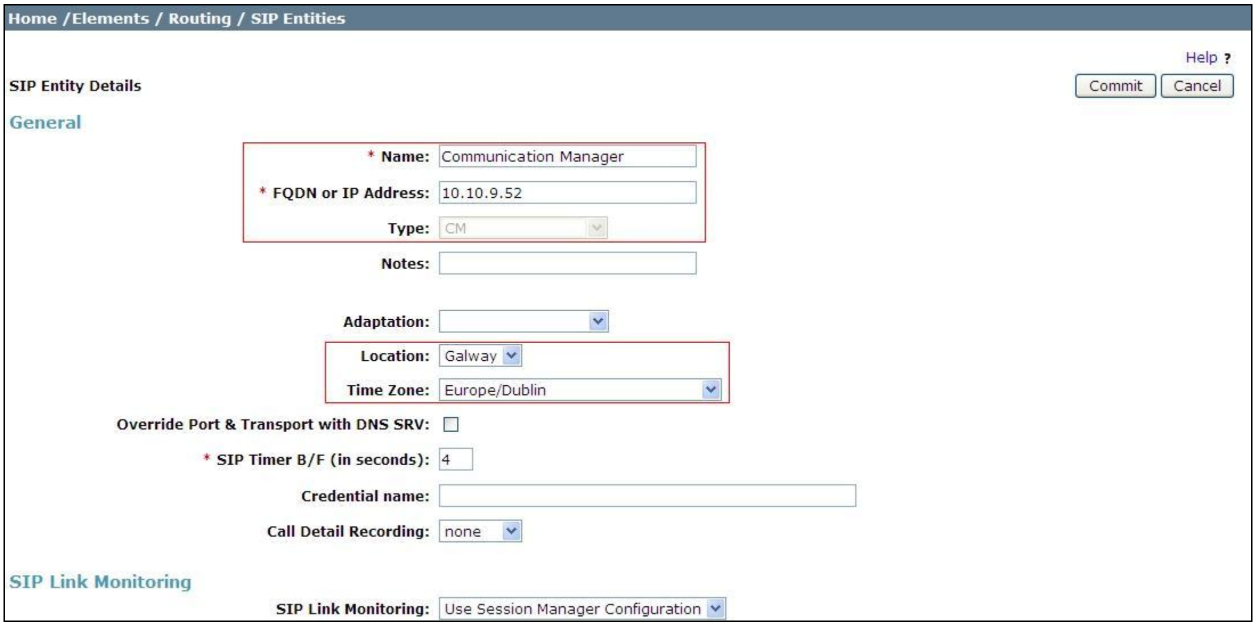
The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface. The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select **avaya.com** as the default domain



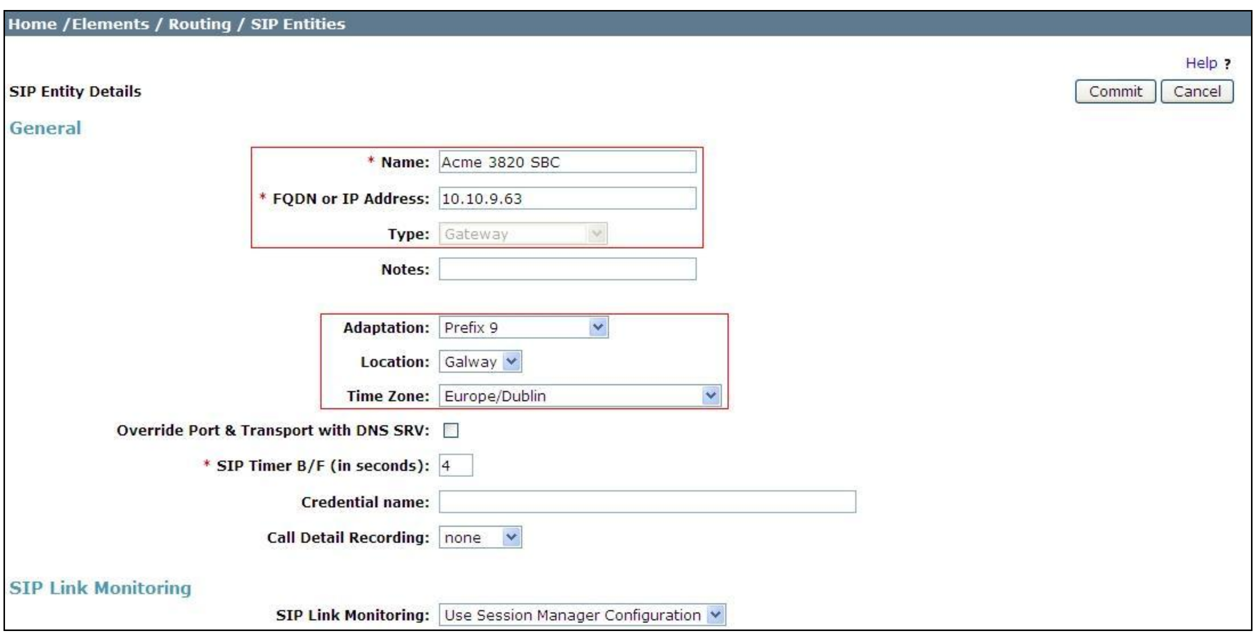
6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling.



6.5.3. Acme Packet Net-Net 3820 SIP Entity

The following screen shows the SIP Entity for the Session Border Controller. The **FQDN or IP Address** field is set to the IP address of the Acme Packet SBC enterprise network interface.

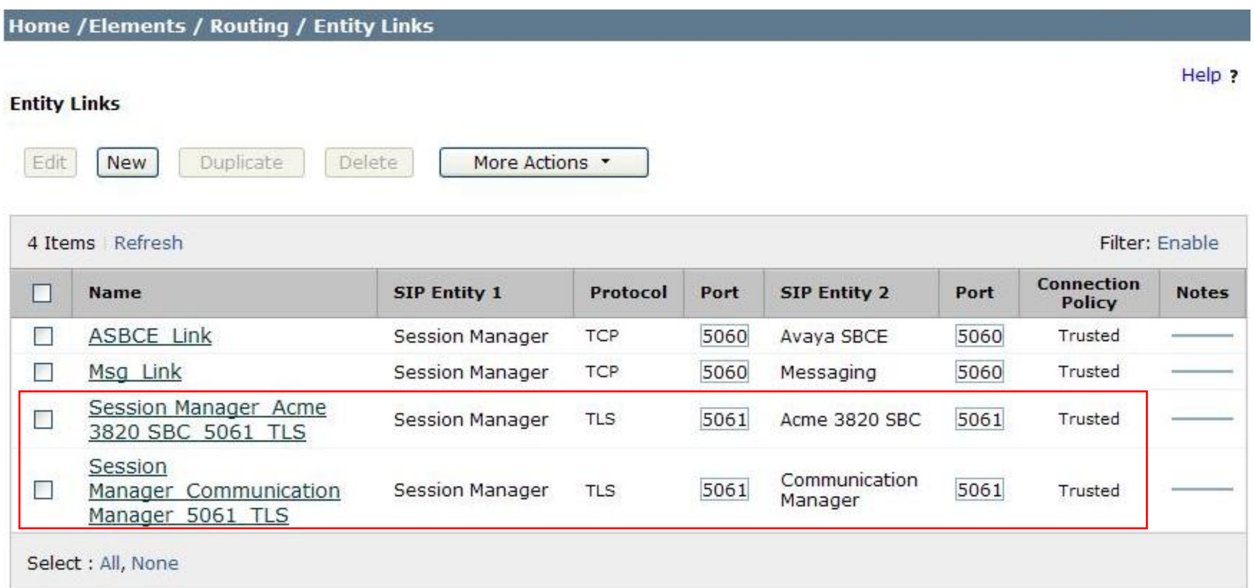


6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select the name given to the Session Manager Entity, in this case **Session Manager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.



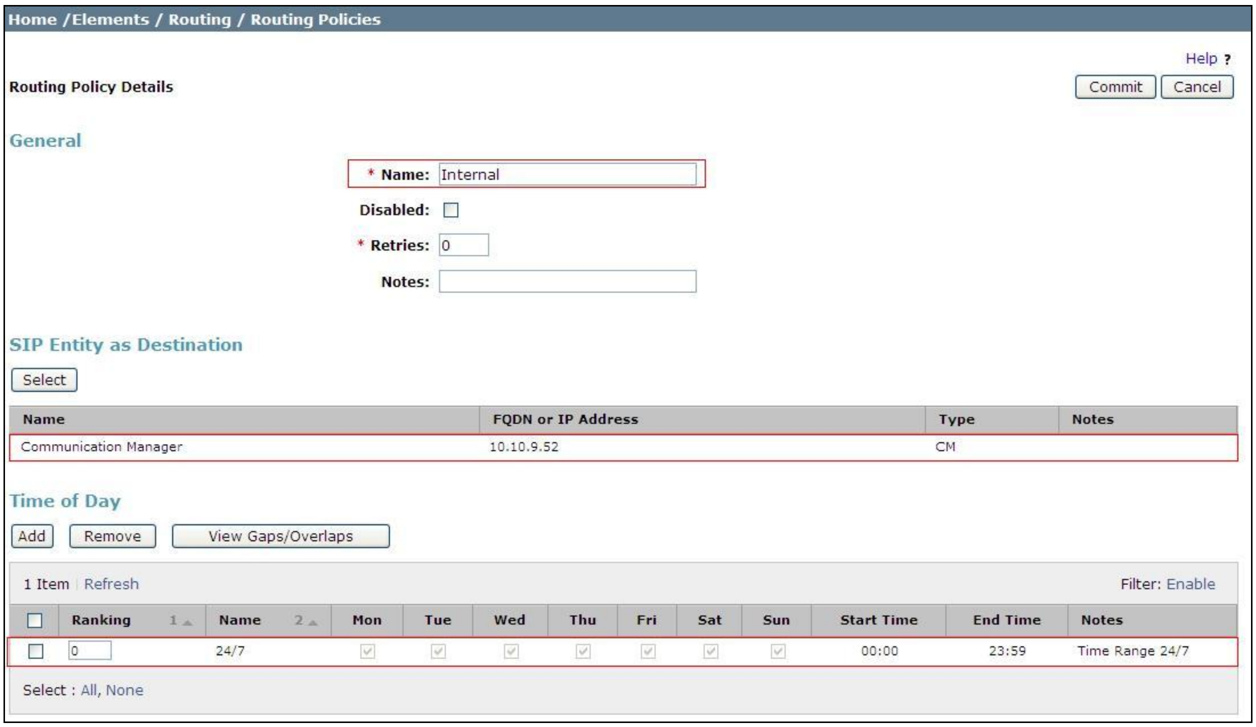
6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

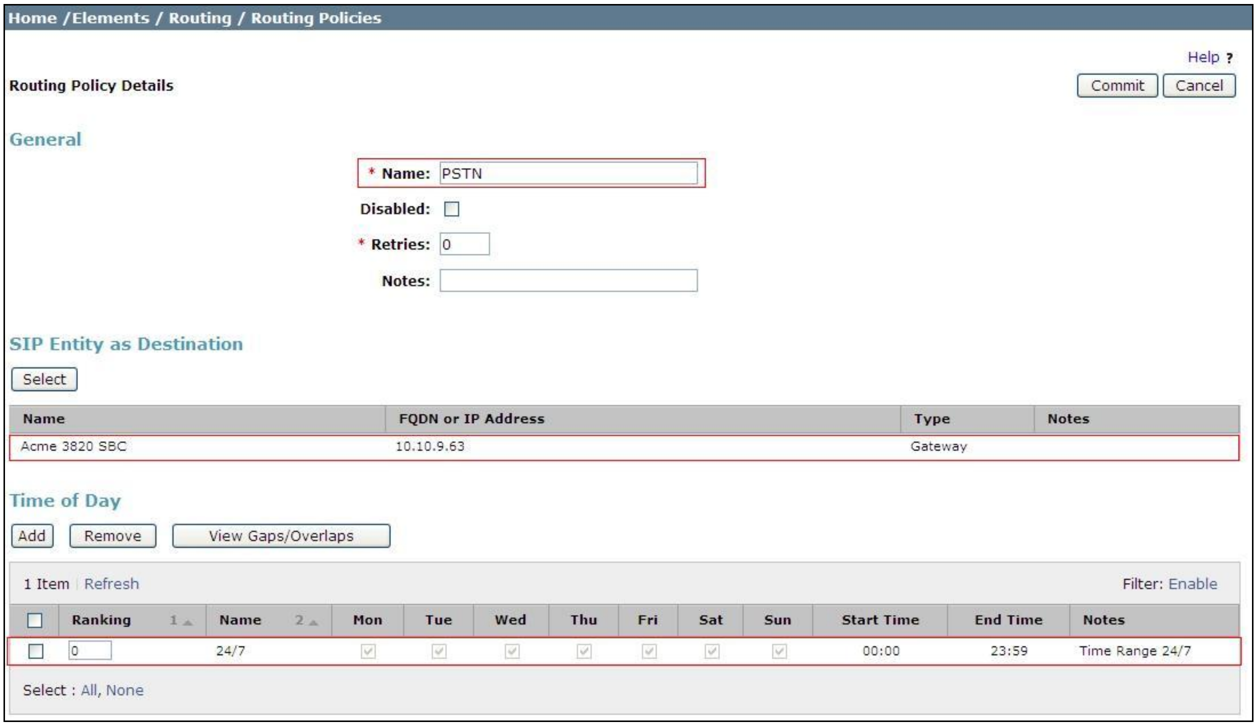
Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager.



The following screen shows the routing policy for the Acme Packet SBC.



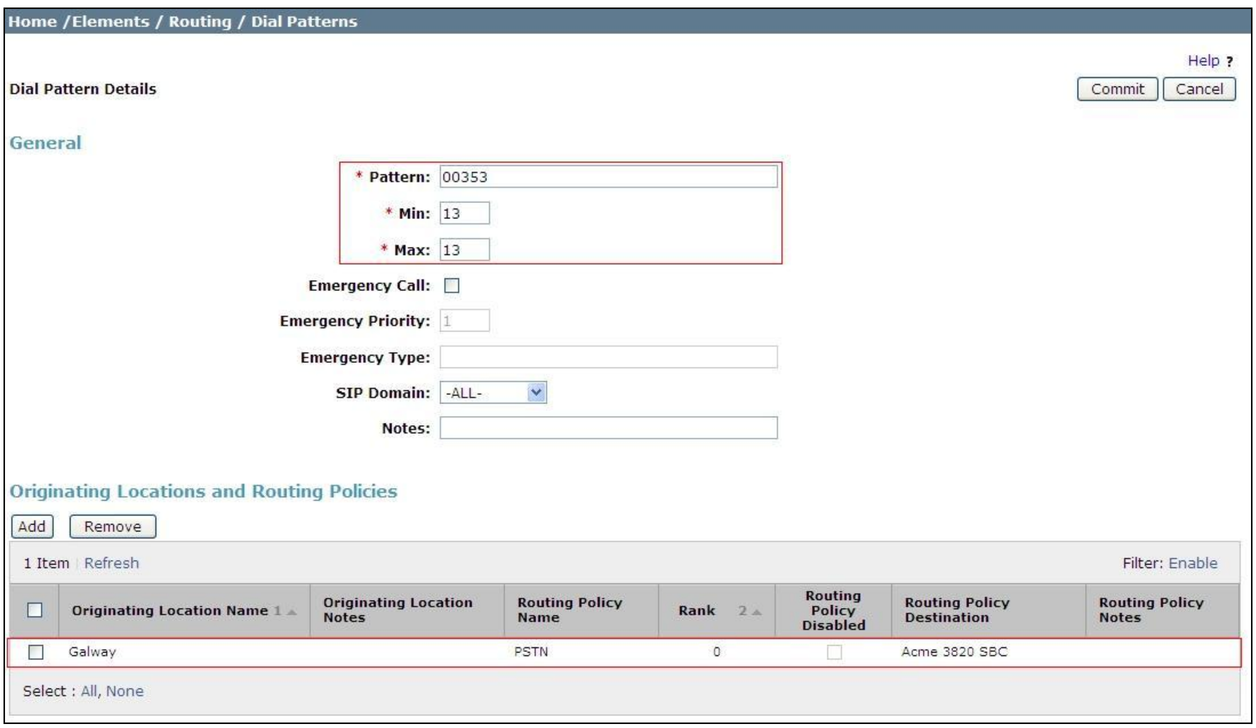
6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

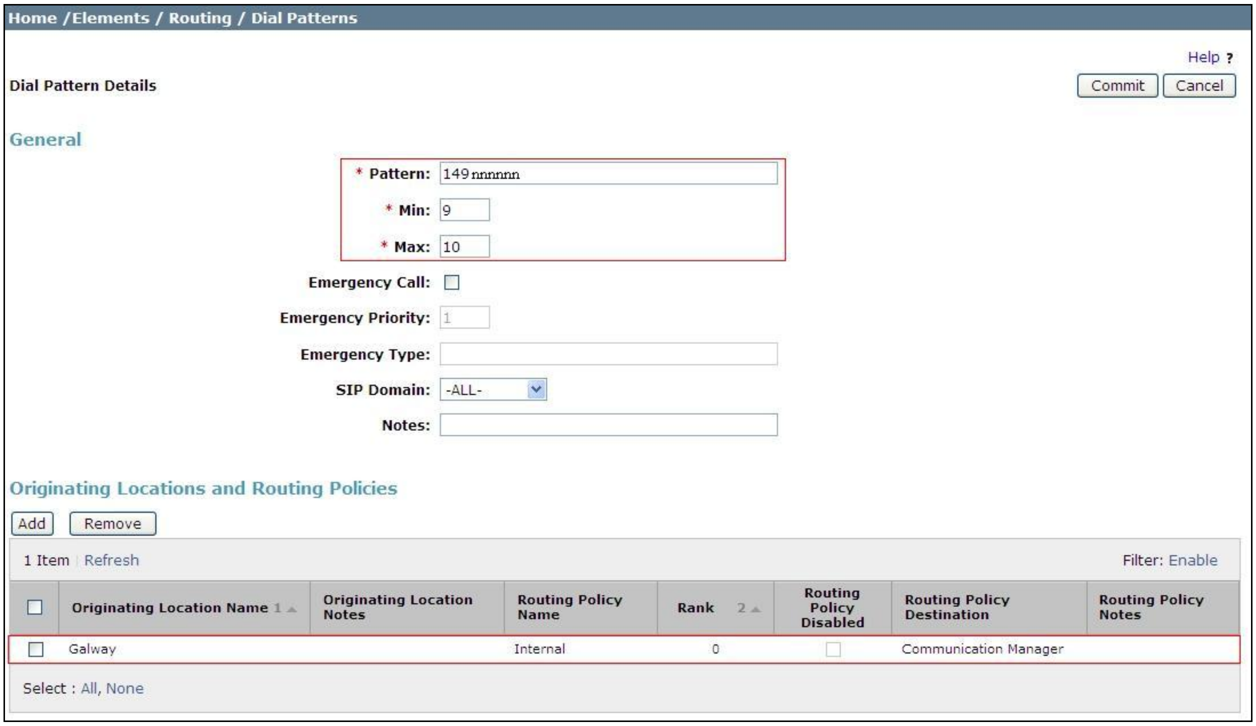
Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched
- In the **Min** field enter the minimum length of the dialled number
- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **–ALL-** or alternatively one of those configured in **Section 6.2**

Under **Originating Locations and Routing Policies**, click **Add**,. In the resulting screen (not shown), under **Originating Location** select the appropriate entry (**Galway** in this example) and under **Routing Policies** select one of the routing policies defined in **Section 6.7**, click **Select** button to save. The following screen shows an example dial pattern configured for the Acme Packet SBC which will route the calls out to the Cable and Wireless SIP IP Trunking service.



The following screen shows the test dial pattern configured for Communication Manager. Note that the number format received from Cable and Wireless was national with no leading 0.



6.9. Administer Application for Avaya Aura® Communication Manager

From the home tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New**.

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the appropriate Communication Manager element

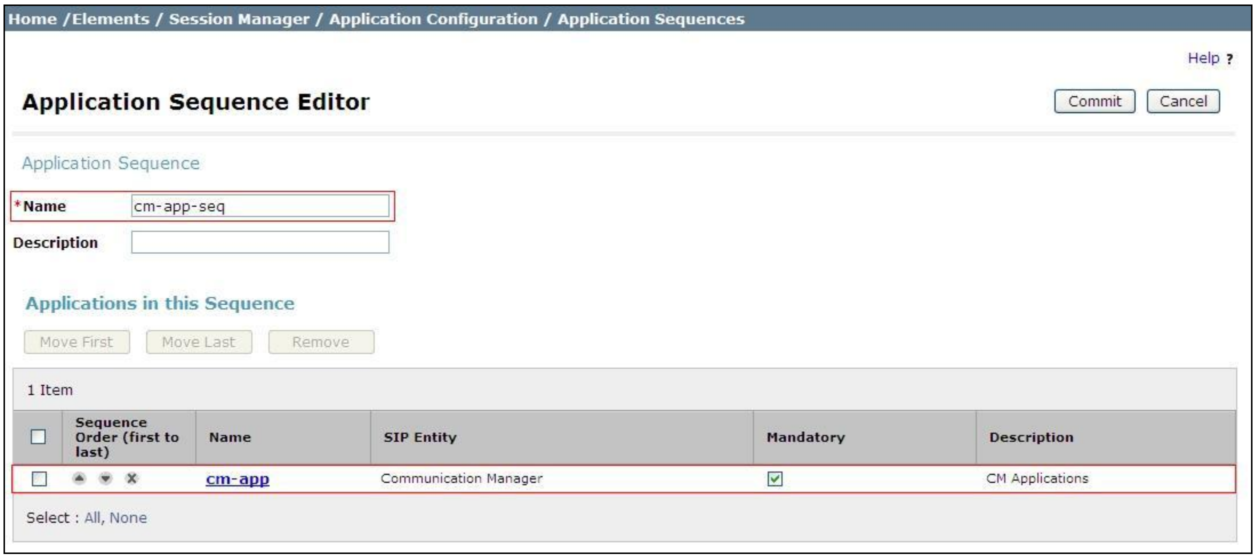
Select **Commit** to save the configuration.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New**.

- In the **Name** field enter a descriptive name
- Under **Available Applications** (not shown), click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading

Select **Commit**.

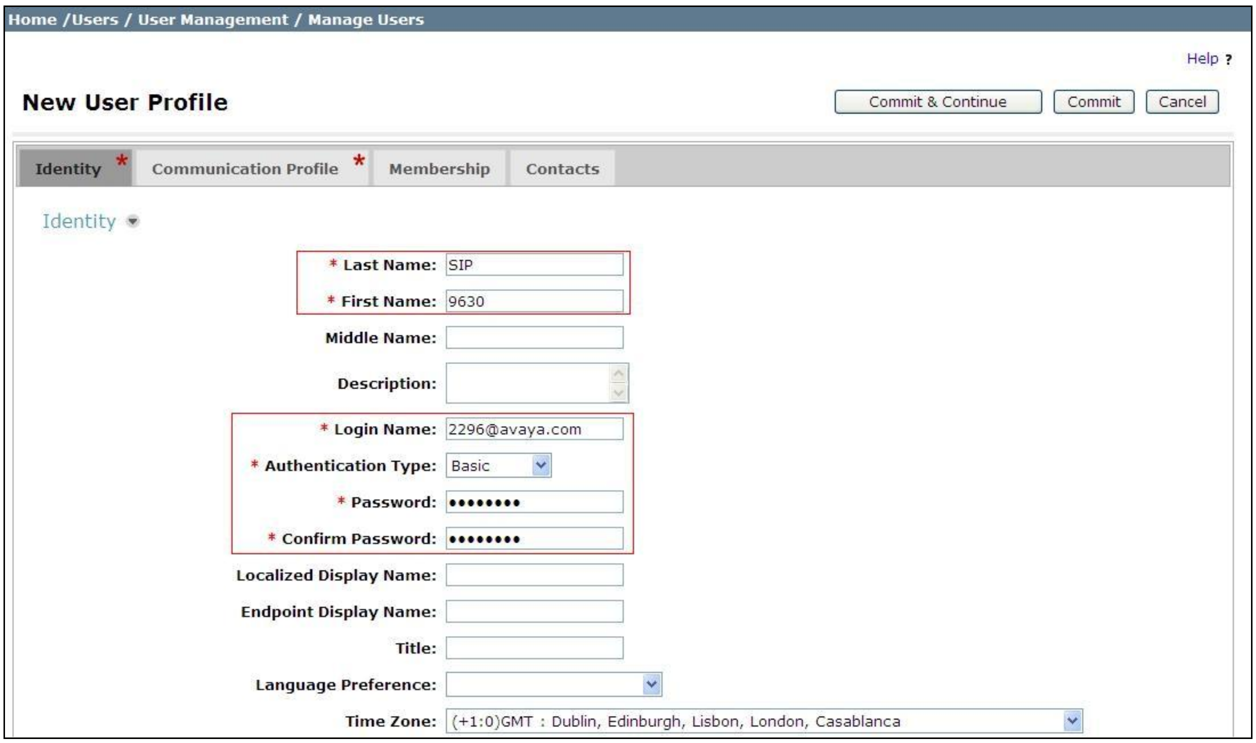


6.11. Administer SIP Extensions

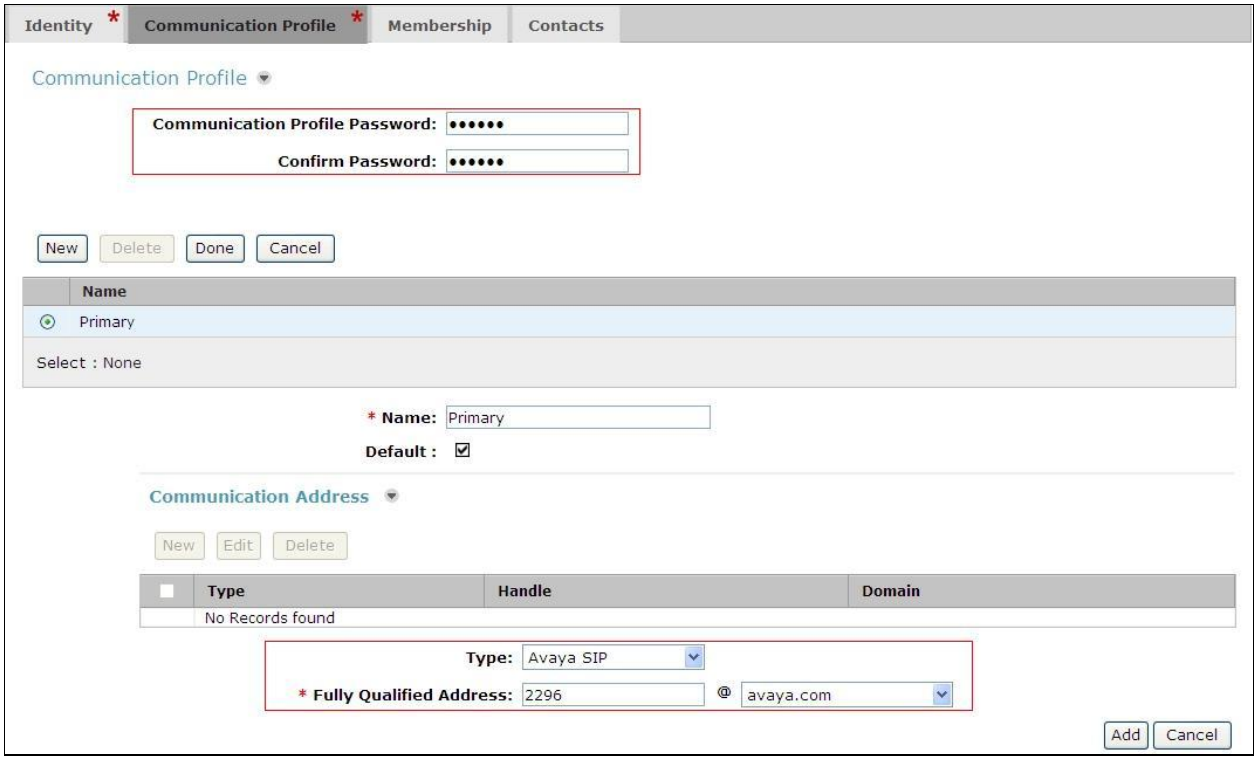
SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab, select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of **user@domain** (e.g. **2296@avaya.com**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password which will be used to login to System Manager.

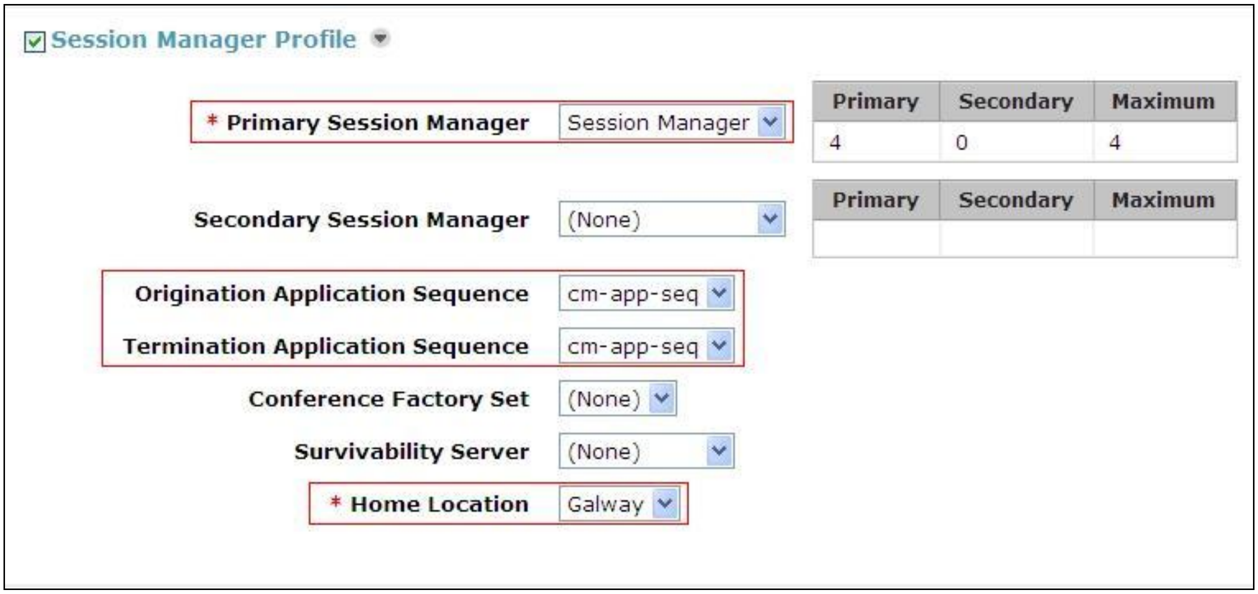


On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field, select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.



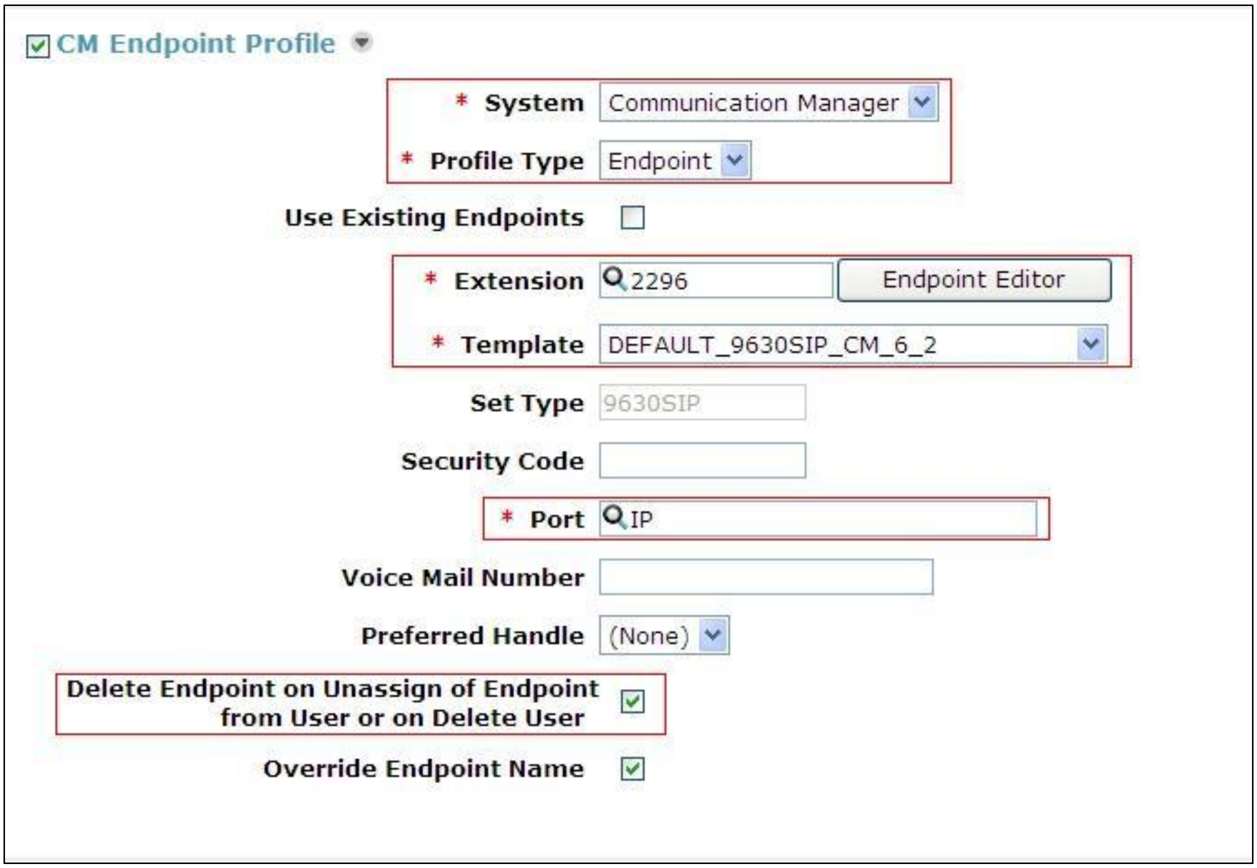
Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.10**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.10**
- Select the appropriate location from the drop-down menu in the **Home Location** field



Expand the **Endpoint Profile** section.

- Select the appropriate Communication Manager Element from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** to save changes and the System Manager will add the Communication Manager user configuration automatically



7. Configure Avaya telephones for TLS and SRTP

Avaya telephones must be configured to use SRTP for media encryption.
The media encryption algorithm and other necessary parameters are defined in a configuration file called 46xxsettings.txt. See appendix B for more information on how to activate these settings.

Configuration for TLS signaling is achieved by using the telephone menus. Only SIP telephones can be configured for TLS.

- Press the Mute button and type **CRAFT#** on the keypad.
- Scroll down to the **SIP** menu entry.
- Press the '**Select**' button.
- For **Transport Type**, select **TLS**.
- For **Port**, type **5061**.
- Select **Save**.

Exit the menu system and restart the telephone.

Avaya telephones contain a copy of the default Avaya SIP TLS certificate in firmware, negating the necessity to manually load or install certificates.

8. Configure Acme Packet Net-Net 3820 SBC

Refer to the printout of the test configuration provided in **Appendix A** for guidance on how to configure the Acme Packet Net-Net 3820 SBC. Note that the configuration is identical to that required for an Acme packet Net-Net 4500 SBC as they use the same firmware. There are two points worth mentioning:

- A built-in Header Manipulation Rule (HMR) is used for hiding the enterprise network topology. This HMR is **ACME_NAT_TO_FROM_IP** and is applied as an **out-manipulationid** in the outside session agent. It does not appear in the **sip-manipulation** as it is built-in, and can be viewed by typing **show built-in-sip-manipulation.**
- A HMR was developed as a workaround to the fault described in **Section 2.2** where no ringback was heard on calls forwarded to the PSTN.

8.1. Create Certificate Records on Acme Packet SBC

TLS permits client-server applications to encrypt data exchanges, preventing eavesdropping and alteration by unauthorized parties. The protocol requires the exchange of certificates of identity which may be signed by a CA. When Communications Manager and Session Manager are configured for SIP-TLS, the default Avaya certificates are automatically exchanged.

The Acme Packet Net-Net 3820 SBC must have an endpoint certificate generated, then signed by the CA and re-imported to the Acme Packet Net-Net 3820 SBC to facilitate SIP-TLS between it and Session Manager. The following steps must be completed to enable this.

- Use the Acme Packet Net-Net 3820 **certificate-record** element to generate a new certificate.
- Use the Acme Packet Net-Net 3820 **generate-certificate-request** command to generate a private key and an (unsigned) certificate signing request (CSR).
- Copy the screen output and paste it into the CA server (System Manager) to sign the Acme Packet Net-Net 3820 CSR.
- In the Acme Packet Net-Net 3820 **import-certificate** element, paste the newly signed CSR into the terminal window.
- In the Acme Packet Net-Net 3820 **import-certificate** element, import the Avaya default SIP-TLS certificate.

The above is a high level overview of the procedure. For more details on these requirements, please see item [**12**] in **Section 12** and see the Acme Packet Net-Net 3820 administration document from the Acme Packet Net-support Portal site at https://support.acmepacket.com.

8.2. Header Manipulation Rule

The HMR applied as a workaround to the ringback fault described in **Section 2.2** simply replaces the “Supported” header in 18x responses from the enterprise. This has the effect of removing the complete “Supported” header. Methods in this header invoke behavior in the SIP service providers’s equipment (a Genband CS2K) which result in ringback not being played to callers during call forwarding. The fault has been reproduced in the Cable and Wireless Lab and a CSR was raised with Genband. The workaround described here is required until a permanent solution is implemented in the network.

The HMR is as follows:

```
sip-manipulation
       name                            ChangeSupported
       description
       split-headers
       join-headers
       header-rule
              name                            RemoveSupported
              header-name                     Supported
              action                          delete
              comparison-type                 case-sensitive
              msg-type                        reply
              methods
              match-value
              new-value
```

It is applied in the realm-id “INSIDE” session agent as follows:

```
session-agent
       in-manipulationid               ChangeSupported
```

Refer to appendix A for Acme Packet Net-Net 3820 configuration details.

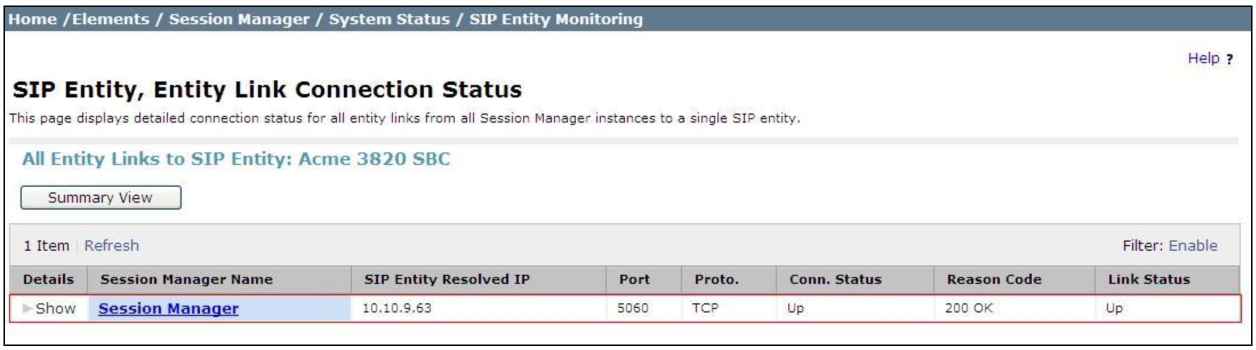
9. Configure Cable and Wireless SIP IP Trunking

The configuration of the Cable and Wireless equipment used to support the SIP IP Trunking service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Cable and Wireless equipment and system configuration please contact an authorised Cable and Wireless representative.

10. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager Home Tab click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.



Note: This is also an indication that the SIP trunk between the Acme packet SBC and the Cable and Wireless network is working effectively as OPTIONS messages are passed by the SBC from the Session Manager to the network

2. From the Communication Manager SAT interface run the command **status trunk n** where trunk **n** is previously configured in **Section 5.6**. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
```

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the calls remain active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the calls can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Acme Packet Net-Net 3820 SBC to Cable and Wireless SIP IP Trunking service. The service was successfully tested with a number of observations listed in **Section 2.2.**

12. Additional References

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

[1] *Installing and Configuring Avaya Aura® System Platform Release 6.2*, March 2012.
[2] *Administering Avaya Aura® System Platform Release 6.2*, February 2012.
[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, February 2012.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, February 2012, Document Number 555-245-205.
[5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.
[6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473
[7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.
[8] *Net-Net 4000 S-CX6.3.0 Maintenance and Troubleshooting Guide.pdf*, https://support.acmepacket.com/
[9] *Net-Net Session Director C[xz]6.3.9Final User Guide.pdf*, https://support.acmepacket.com/
[10] *Acme Packet HMR Developers Guide.pdf*, https://support.acmepacket.com/
[11] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[12] Acme Packet Net-Net 3820 Administration guide, https://support.acmepacket.com/

Appendix A

The configuration details provided here are the Acme Packet 3820 Net-Net SBC settings used during compliance testing. Publicly routable IP addresses have been obfuscated for security reasons.

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these application notes. Other parameter values may or may not match based on local configurations and are shown for illustrative purposes.

ANNOTATION: The following certificates facilitate SIP-TLS flow between the Acme Packet Net-Net 3820 and Session Manager. AcmeTLScert was signed by System Manager.

```
certificate-record
        name                                AcmeTLScert
        country                             IE
        state                               Connaught
        locality                            Galway
        organization                        lab
        unit                                testing
        common-name                         avaya.com
        key-size                            1024
        alternate-name
        trusted                             enabled
        key-usage-list
                                            digitalSignature keyEncipherment
        extended-key-usage-list
                                            serverAuth
        options

certificate-record
        name                                AvayaDefault
        country                             IE
        state                               Connaught
        locality                            Galway
        organization                        avaya
        unit                                SIP_Product_certificate_authority
        common-name                         SIP_Product_certificate_authority
        key-size                            2048
        alternate-name
        trusted                             enabled
        key-usage-list
                                            digitalSignature keyEncipherment
        extended-key-usage-list
                                            serverAuth
        options
```

ANNOTATION: The following host route is required to send/receive packets to/from the SIP trunk providers' network.

```
host-routes
        dest-network                        xxx.xxx.24.8 [IP address of SIP trunk service]
        netmask                             255.255.255.0
        gateway                             192.168.37.1 [gateway for SIP traffic]
        description                         route-to-cw
```

ANNOTATION: The local policy below controls the routing of SIP messages from the SIP trunk service provider to the session manager.

```
local-policy
       from-address
                                    *
       to-address
                                    *
       source-realm
                                    OUTSIDE [SIP trunk service provider]
       description                  Far-side-realm
       activate-time                N/A
       deactivate-time              N/A
       state                        enabled
       policy-priority              none

       policy-attribute
              next-hop                     10.10.9.61 [session manager IP address]
              realm                        INSIDE [the Enterprise realm]
              action                       none
              terminate-recursion          disabled
              carrier
              start-time                   0000
              end-time                     2400
              days-of-week                 U-S
              cost                         0
              app-protocol
              state                        enabled
              methods
              media-profiles
              lookup                       single
              next-key
              eloc-str-lkup                disabled
              eloc-str-match
```

ANNOTATION: The local policy below controls the routing of SIP messages from session manager to the C&W SIP trunk service.

```
local-policy
       from-address
                                    *
       to-address
                                    *
       source-realm
                                    INSIDE [Enterprise SIP domain]
       description
       activate-time                N/A
       deactivate-time              N/A
       state                        enabled
       policy-priority              none

       policy-attribute
              next-hop                     xxx.xxx.24.8 [SIP trunk provider address]
              realm                        OUTSIDE [SIP trunk provider realm]
              action                       none
              terminate-recursion          disabled
              carrier
              start-time                   0000
              end-time                     2400
              days-of-week                 U-S
              cost                         0
```

```
        app-protocol
        state                          enabled
        methods
        media-profiles
        lookup                         single
        next-key
        eloc-str-lkup                  disabled
        eloc-str-match

media-manager
    state                          enabled [enabled to manage voice media]
    latching                       enabled
    flow-time-limit                86400
    initial-guard-timer            300
    subsq-guard-timer              300
    tcp-flow-time-limit            86400
    tcp-initial-guard-timer        300
    tcp-subsq-guard-timer          300
    tcp-number-of-ports-per-flow   2
    hnt-rtcp                       disabled
    algd-log-level                 NOTICE
    mbcd-log-level                 NOTICE
    options                        unique-sdp-id
    red-flow-port                  1985
    red-mgcp-port                  1986
    red-max-trans                  10000
    red-sync-start-time            5000
    red-sync-comp-time             1000
    media-policing                 enabled
    max-signaling-bandwidth        10000000
    max-untrusted-signaling        100
    min-untrusted-signaling        30
    app-signaling-bandwidth        0
    tolerance-window               30
    rtcp-rate-limit                0
    trap-on-demote-to-deny         enabled
    syslog-on-demote-to-deny       disabled
    syslog-on-demote-to-untrusted  disabled
    anonymous-sdp                  disabled
    arp-msg-bandwidth              32000
    fragment-msg-bandwidth         0
    rfc2833-timestamp              disabled
    default-2833-duration          100
    rfc2833-end-pkts-only-for-non-sig enabled
    translate-non-rfc2833-event    disabled
    media-supervision-traps        disabled
    dnsalg-server-failover         disabled
```

ANNOTATION: The following media security policies define the media conversion from SRTP on the enterprise side to RTP on the SIP trunk provider side and vice versa.

```
media-sec-policy
       name                            Outside [SIP trunk provider]
       pass-through                    disabled
       inbound
              profile
              mode                            rtp [inbound calls from SIP trunk]
              protocol                        none [no encryption]
       outbound
              profile
              mode                            rtp [outbound calls to SIP trunk]
              protocol                        none [no encryption]

media-sec-policy
       name                            Inside [Enterprise domain]
       pass-through                    disabled
       inbound
              profile                         insideSRTP [a media security profile]
              mode                            srtp [inbound calls to endpoints]
              protocol                        sdes [use this encryption type]
       outbound
              profile                         insideSRTP [a media security profile]
              mode                            srtp [outbound calls from endpoints]
              protocol                        sdes [use this encryption type]
```

ANNOTATION: The following network interfaces define the IP address used on the enterprise (INSIDE) network and on the SIP trunk provider (OUTSIDE) network and the associated physical ports to which these addresses are mapped.

```
network-interface
       name                            S0P1
       sub-port-id                     0
       description                     INSIDE [the realm using this IP address]
       hostname
       ip-address                      10.10.9.63 [Acme Packet private IP address]
       pri-utility-addr
       sec-utility-addr
       netmask                         255.255.255.0
       gateway                         10.10.9.1  [private side gateway]
       sec-gateway
       gw-heartbeat
              state                           enabled
              heartbeat                       10
              retry-count                     3
              retry-timeout                   1
              health-score                    30
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                     11
        hip-ip-list                     10.10.9.63 [allow packets from session manager]
       ftp-address                     10.10.9.63 [allow packets from session manager]
        icmp-address                    10.10.9.63 [allow packets from session manager]
       snmp-address                    10.10.9.63 [allow packets from session manager]
       telnet-address                  10.10.9.63 [allow packets from session manager]
       ssh-address
```

```
      signaling-mtu                 0

network-interface
      name                          S0P0
      sub-port-id                   0
      description                   OUTSIDE [SIP trunk provider realm]
      hostname
      ip-address                    192.168.37.2 [Acme Packet public IP address]
      pri-utility-addr
      sec-utility-addr
      netmask                       255.255.255.0
      gateway                       192.168.37.1 [public side gateway (VPN router)]
      sec-gateway
      gw-heartbeat
            state                         enabled
            heartbeat                     10
            retry-count                   3
            retry-timeout                 3
            health-score                  30
      dns-ip-primary
      dns-ip-backup1

      dns-ip-backup2
      dns-domain
      dns-timeout                   11
       hip-ip-list                   192.168.37.2 [accept packets from Acme Packet]
      ftp-address
       icmp-address                  192.168.37.2 [accept packets from Acme Packet]
      snmp-address
      telnet-address
      ssh-address
      signaling-mtu                 0

phy-interface
      name                          S0P0
      operation-type                Media
      port                          0
      slot                          0
      virtual-mac
      admin-state                   enabled
      auto-negotiation              enabled
      duplex-mode                   FULL
      speed                         100
      overload-protection           disabled

phy-interface
      name                          S0P1
      operation-type                Media
      port                          1
      slot                          0
      virtual-mac
      admin-state                   enabled
      auto-negotiation              enabled
      duplex-mode                   FULL
      speed                         100
      overload-protection           disabled
```

ANNOTATION: The realm configuration "OUTSIDE" represents the external network on which the SIP trunk service resides.

```
realm-config
```

```
identifier                      OUTSIDE [SIP trunk provider realm]
description                     SIP_LAB_OUTSIDE [descriptive name]
addr-prefix                     0.0.0.0
network-interfaces
                                S0P0:0
mm-in-realm                     enabled
mm-in-network                   enabled
mm-same-ip                      enabled
mm-in-system                    enabled
bw-cac-non-mm                   disabled
msm-release                     disabled
qos-enable                      disabled
generate-UDP-checksum           disabled
max-bandwidth                   0
fallback-bandwidth              0
max-priority-bandwidth          0
max-latency                     0
max-jitter                      0
max-packet-loss                 0
observ-window-size              0
parent-realm
dns-realm
media-policy
media-sec-policy                Outside
srtp-msm-passthrough            disabled
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit              0
access-control-trust-level      none
invalid-signal-threshold        0
maximum-signal-threshold        0
untrusted-signal-threshold      0
nat-trust-threshold             0
deny-period                     30
cac-failure-threshold           0
untrust-cac-failure-threshold   0
ext-policy-svr
diam-e2-address-realm
symmetric-latching              disabled
pai-strip                       disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching             none
restriction-mask                32
accounting-enable               enabled
user-cac-mode                   none
user-cac-bandwidth              0
user-cac-sessions               0
icmp-detect-multiplier          0
icmp-advertisement-interval     0
icmp-target-ip
monthly-minutes                 0
net-management-control          disabled
delay-media-update              disabled
refer-call-transfer             disabled
```

```
refer-notify-provisional       none
dyn-refer-term                 disabled
codec-policy
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
xnq-state                      xnq-unknown
hairpin-id                     0
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp                     disabled
hide-egress-media-update       disabled
```

ANNOTATION: The realm configuration "INSIDE" represents the enterprise network where the Communication Manager and Session Manager are located.

```
realm-config
      identifier                     INSIDE [Enterprise realm]
      description                    SIP_LAB_INSIDE [descriptive name]
      addr-prefix                    0.0.0.0
      network-interfaces
                                     S0P1:0
      mm-in-realm                    enabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
      msm-release                    disabled
      qos-enable                     disabled
      generate-UDP-checksum          disabled
      max-bandwidth                  0
      fallback-bandwidth             0
      max-priority-bandwidth         0
      max-latency                    0
      max-jitter                     0
      max-packet-loss                0
      observ-window-size             0
      parent-realm
      dns-realm
      media-policy
      media-sec-policy               Inside [use this policy for secure media]
      srtp-msm-passthrough           disabled
      in-translationid
      out-translationid
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      class-profile
      average-rate-limit             0
      access-control-trust-level     none
      invalid-signal-threshold       0
      maximum-signal-threshold       0
      untrusted-signal-threshold     0
```

```
nat-trust-threshold            0
deny-period                    30
cac-failure-threshold          0
untrust-cac-failure-threshold  0
ext-policy-svr
diam-e2-address-realm
symmetric-latching             disabled
pai-strip                      disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching            none
restriction-mask               32
accounting-enable              enabled
user-cac-mode                  none
user-cac-bandwidth             0
user-cac-sessions              0
icmp-detect-multiplier         0
icmp-advertisement-interval    0
icmp-target-ip
monthly-minutes                0
net-management-control         disabled
delay-media-update             disabled
refer-call-transfer            disabled
refer-notify-provisional       none
dyn-refer-term                 disabled
codec-policy
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
xnq-state                      xnq-unknown
hairpin-id                     0
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp                     disabled
hide-egress-media-update       disabled
```

ANNOTATION: The sdes-profile defines the encryption method used between the Acme Packet 3820 and the Communication Manager media cards or H.323 or SIP endpoints for voice security. The security-policy defines when this policy is applied.

```
sdes-profile
      name                          insideSRTP [descriptive name]
      crypto-list                   AES_CM_128_HMAC_SHA1_80 [encryption algorithm]
      srtp-auth                     enabled
      srtp-encrypt                  enabled
      srtcp-encrypt                 disabled
      mki                           disabled
      egress-offer-format           same-as-ingress
      use-ingress-session-params    srtp-encrypt
      key
      salt

security-policy
      name                          insideIPSEC
      network-interface             S0P1:0
      priority                      10
      local-ip-addr-match           10.10.9.63
      remote-ip-addr-match          0.0.0.0
      local-port-match              0
      remote-port-match             0
      trans-protocol-match          UDP
      direction                     both
      local-ip-mask                 255.255.255.255
      remote-ip-mask                0.0.0.0
      action                        srtp
      ike-sainfo-name
      outbound-sa-fine-grained-mask
            local-ip-mask                 0.0.0.0
            remote-ip-mask                255.255.255.255
            local-port-mask               0
            remote-port-mask              65535
            trans-protocol-mask           255
            valid                         enabled
            vlan-mask                     0xFFF
```

ANNOTATION: The session agent below represents the Cable and Wireless SIP trunking service network border element. The Acme Packet SBC will attempt to send calls to the border element based on successful responses to the OPTIONS “ping-method”. Cable and Wireless SIP trunking service border element is also specified in the session-group section below.

```
session-agent
      hostname                      212.165.24.8
      ip-address                    212.165.24.8
      port                          5060
      state                         enabled
      app-protocol                  SIP
      app-type
      transport-method              UDP
      realm-id                      OUTSIDE
      egress-realm-id
      description                   candw
      carriers
      allow-next-hop-lp             enabled
      constraints                   disabled
```

```
max-sessions                   0
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action                Proxy
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method                    OPTIONS;hops=66
ping-interval                  120
ping-send-mode                 keep-alive
ping-all-addresses             disabled
ping-in-service-response-codes
out-service-response-codes
load-balance-dns-query         hunt
media-profiles
in-translationid
out-translationid
trust-me                       disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                    disabled
in-manipulationid
out-manipulationid             ACME_NAT_TO_FROM_IP
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
refer-notify-provisional       none
reuse-connections              NONE
tcp-keepalive                  none
tcp-reconn-interval            0
max-register-burst-rate        0
register-burst-window          0
sip-profile
sip-isup-profile
```

```
        kpml-interworking               inherit
```

ANNOTATION: The session agent below represents the Communication Manager Processor Ethernet interface used in the reference configuration.

```
session-agent
        hostname                        10.10.9.61
        ip-address                      10.10.9.61
        port                            5061
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                StaticTLS
        realm-id                        INSIDE
        egress-realm-id
        description                     session-manager
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action                 Proxy
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=66
        ping-interval                   120
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query          hunt
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid               ChangeSupported
        out-manipulationid
        manipulation-string
```

```
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        refer-notify-provisional       none
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        kpml-interworking              inherit
```

ANNOTATION: The sip-config defines global sip-parameters, including SIP timers, SIP options, and which realm to send requests to if not specified elsewhere, and enables the SD to collect statistics on requests other than REGISTERs and INVITEs.

```
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INSIDE
        egress-realm-id
        nat-mode                       None
        registrar-domain               *
        registrar-host                 *
        registrar-port                 5060
        register-service-route         always
        init-timer                     500
        max-timer                      4000
        trans-expire                   32
        invite-expire                  180
        inactive-dynamic-conn          32
        enforcement-profile
        pac-method
        pac-interval                   10
        pac-strategy                   PropDist
        pac-load-weight                1
        pac-session-weight             1
        pac-route-weight               1
        pac-callid-lifetime            600
        pac-user-lifetime              3600
        red-sip-port                   1988
        red-max-trans                  10000
        red-sync-start-time            5000
        red-sync-comp-time             1000
        add-reason-header              disabled
        sip-message-len                4096
        enum-sag-match                 disabled
        extra-method-stats             disabled
        registration-cache-limit       0
        register-use-to-for-lp         disabled
        refer-src-routing              disabled
```

```
        add-ucid-header                 disabled
        proxy-sub-events
        allow-pani-for-trusted-only     disabled
        pass-gruu-contact               disabled
        sag-lookup-on-redirect          disabled
        set-disconnect-time-on-bye      disabled
```

ANNOTATION: The SIP interface below is used to communicate with the Cable and Wireless SIP trunking service, UDP transport.

```
sip-interface
        state                           enabled
        realm-id                        OUTSIDE
        description                     candw-sip-trunk
        sip-port
                address                         192.168.37.2
                port                            5060
                transport-protocol              UDP
                tls-profile
                multi-home-addrs
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        options                         max-udp-length=0
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        subscribe-reg-event             disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
```

```
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                 0
        register-keep-alive            none
        kpml-interworking              disabled
        tunnel-name
```

ANNOTATION: The SIP interface below is used to communicate with Session Manager. SIP signaling is encrypted using TLS.

```
sip-interface
        state                          enabled
        realm-id                       INSIDE
        description                    Avaya-SBC
        sip-port
                address                        10.10.9.63
                port                           5061
                transport-protocol             TLS
                tls-profile                    CWAuth
                multi-home-addrs
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
```

```
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        subscribe-reg-event             disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode  pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
        implicit-service-route          disabled
        rfc2833-payload                 101
        rfc2833-mode                    transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                 disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles                disabled
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                  0
        register-keep-alive             none
        kpml-interworking               disabled
        tunnel-name
```

ANNOTATION: The ChangeSupported sip-manipulation below applies the RemoveSupported header rule to SIP messages between the Cable and wireless SIP trunking service and Session Manager. This rule removes the Supported header from all replies (18x messages) as these were found to cause no ringback during call transfers.

```
sip-manipulation
        name                            ChangeSupported
        description
        split-headers
        join-headers
        header-rule
                name                            RemoveSupported
                header-name                     Supported
                action                          delete
                comparison-type                 case-sensitive
                msg-type                        reply
                methods
```

```
        match-value
        new-value
```

ANNOTATION: The steering pools below define the IP Addresses and RTP port ranges on the respective realms. The "OUTSIDE" realm IP Address will be used as the media IP Address to communicate with Cable and Wireless. Likewise, the IP Address and RTP port range defined for the "INSIDE" realm steering pool will be used to communicate with the Communication Manager and endpoints.

```
steering-pool
    ip-address                      10.10.9.63
    start-port                      2048
    end-port                        3329
    realm-id                        INSIDE
    network-interface
steering-pool
    ip-address                      192.168.37.2
    start-port                      10000
    end-port                        20000
    realm-id                        OUTSIDE
    network-interface
system-config
    hostname
    description
    location
    mib-system-contact
    mib-system-name
    mib-system-location
    snmp-enabled                    enabled
    enable-snmp-auth-traps          disabled
    enable-snmp-syslog-notify       disabled
    enable-snmp-monitor-traps       disabled
    enable-env-monitor-traps        disabled
    snmp-syslog-his-table-length    1
    snmp-syslog-level               WARNING
    system-log-level                WARNING
    process-log-level               NOTICE
    process-log-ip-address          0.0.0.0
    process-log-port                0
    collect
        sample-interval                 5
        push-interval                   15
        boot-state                      disabled
        start-time                      now
        end-time                        never
        red-collect-state               disabled
        red-max-trans                   1000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        push-success-trap-state         disabled
    call-trace                      disabled
    internal-trace                  disabled
    log-filter                      all
    default-gateway                 10.10.9.1
    restart                         enabled
    exceptions
    telnet-timeout                  0
    console-timeout                 0
    remote-control                  enabled
    cli-audit-trail                 enabled
```

```
        link-redundancy-state          disabled
        source-routing                 enabled
        cli-more                       disabled
        terminal-height                24
        debug-timeout                  0
        trap-event-lifetime            0
        default-v6-gateway             ::
        ipv6-signaling-mtu             1500
        ipv4-signaling-mtu             1500
        cleanup-time-of-day            00:00
        snmp-engine-id-suffix
        snmp-agent-mode                v1v2
```

ANNOTATION: The tls-profile below lists the TLS certificates used when the Acme Packet is communicating with Session Manager.

```
tls-profile
        name                           CWAuth
        end-entity-certificate         AcmeTLScert
        trusted-ca-certificates
                                       AvayaDefault
        cipher-list
                                       all
        verify-depth                   1
        mutual-authenticate            enabled
        tls-version                    tlsv1
        cert-status-check              disabled
        cert-status-profile-list
        ignore-dead-responder          disabled
```

INFORMATION: Use the Acme 'show version' command to discover what software version is running.

```
ACME Net-Net 3820 Firmware SCX6.3.0 MR-2 Patch 4 (Build 419)
Build Date=10/26/12
```

INFORMATION: Use the Acme 'show prom-info all' command to reveal the hardware installed in the Acme Packet Net-Net 3820.

```
Contents of Main Board PROM
Assy, NetNet3820
Part Number:002-0675-50
Serial Number:151052008815
FunctionalRev:05.03
BoardRev:05.00
PCB Family Type:Main Board
ID:NetNet 3820 Main Board
Format Rev:16
Options:0
Manufacturer:Unknown manufacturer
Week/Year:52/2010
Sequence Number:008815
Number of MAC Addresses:16
Starting MAC Address:00 08 25 04 78 70
Contents of Host CPU PROM
Assy, NetNet3820
Part Number:                    MOD-0023-61
Serial Number:
FunctionalRev:
BoardRev:
PCB Family Type:
```

```
ID:
Format Rev:
Options:
Manufacturer:                    RadiSys
Week/Year:
Sequence Number:

Contents of PHY
Assy, 4 Port SFP with ETC
Part Number:002-0618-58
Serial Number:091243076589
FunctionalRev:02.10
BoardRev:02.00
PCB Family Type:Quad port GiGE SFP PHY
ID:4 Port GiGE w/QoS, Encryption & ETC
Format Rev:16
Options:16777216
Manufacturer:Benchmark Electronics
Week/Year:43/2012
Sequence Number:076589

No prom info associate of CAM
```

Appendix B

The 46xxsettings.txt configuration file is used to enable/disable optional parameters in Avaya telephones. This settings file is requested by telephones when they start up.

Changing a supported telephone parameter requires changes to be made to the 46xxsettings.txt file on an http/ftp server and the telephone must be restarted to effect the change.

The following changes were made to the 46xx settings file for Avaya H.323 and SIP endpoints to enable SRTP. Open the 46xxsettings.txt in a text editor and search the following settings:

```
SET ENFORCE_SIPS_URI
SET MEDIAENCRYPTION
SET SUBSCRIBE_SECURITY
```

Enabling or disabling a parameter requires the removal of the comment delimiters (##) at the line start and then setting the parameter value(s) as shown below.

```
## ENFORCE_SIPS_URI specifies whether a SIPS URI must be used for SRTP.
##  Value  Operation
##    0    Not enforced
##    1    Enforced (default)
##  This parameter is supported by:
##       96x1 SIP R6.0 and later
##       96x0 SIP R2.6 and later
## SET ENFORCE_SIPS_URI 1
```

SET ENFORCE_SIPS_URI 0 [disable SIPS support when SRTP enabled, feature not needed]

```
## MEDIAENCRYPTION specifies which media encryption (SRTP) options will be supported.
##  Up to 2 options may be specified in a comma-separated list.
##  Options should match those specified in CM IP-codec-set form.
##     1 = aescm128-hmac80
##     2 = aescm128-hmac32
##     3 = aescm128-hmac80-unauth
##     4 = aescm128-hmac32-unauth
##     5 = aescm128-hmac80-unenc
##     6 = aescm128-hmac32-unenc
##     7 = aescm128-hmac80-unenc-unauth
##     8 = aescm128-hmac32-unenc-unauth
##     9 = none (default)
## SET MEDIAENCRYPTION 9
```

SET MEDIAENCRYPTION 1 [enable media encryption, it must match the Acme Packet setting]

```
## SUBSCRIBE_SECURITY specifies the use of SIP or SIPS for subscriptions.
##  If SUBSCRIBE_SECURITY is 0, the phone uses SIP for both the Request URI and the
##  Contact Header regardless of whether SRTP is enabled. If SUBSCRIBE_SECURITY is 1,
##  the phone uses SIPS for both the Request URI and the Contact Header if SRTP is
enabled
##  (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite).
##  If SUBSCRIBE_SECURITY is 2, and the SES/PPM does not show a FS-DeviceData
FeatureName
##  with a FeatureVersion of 2 in the response to the getHomeCapabilities request
## SET SUBSCRIBE_SECURITY 2
```

SET SUBSCRIBE_SECURITY 0 [disable SIPS support as it is not required]

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.