AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R8.1 as an Evolution Server, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.0 to support Virgin Media SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Virgin Media SIP Trunk Service and an Avaya SIP enabled enterprise solution.

The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Virgin Media is a member of the DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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.

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

1 of 68
VMBCMSM81SBC80

Table of Contents

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Virgin Media's SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Customers using this Avaya SIP-enabled enterprise solution with Virgin Media SIP Trunk 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 Avaya SBCE. The enterprise site was configured to use the SIP Trunking service provided by Virgin Media.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

No encryption was used during this compliance test as requested by the Service Provider.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming PSTN calls to various phone types including H.323, SIP, digital and analogue telephones at the enterprise. Calls were routed to the enterprise across the SIP trunk from Virgin Media Business.
- Outgoing PSTN calls from various phone types including H.323, SIP and analogue telephones at the enterprise. Calls were routed from the enterprise across the SIP trunk to Virgin Media Business.
- Direct IP-to-IP media with SIP and H.323 telephones
- Calls using the G.711A and G.711MU codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38 and G.711 pass-through fax transmissions.
- Outgoing calls from the enterprise site completed via Virgin Media's SIP Trunk to UK Emergency Call handling 999, 112 and 18000 Text Direct
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, conference, do not disturb, call park and call pickup.
- Off-net call forwarding and mobile twinning.
- Transmission and response of SIP OPTIONS messages sent by Virgin Media's SIP Trunk requiring Avaya response and sent by Avaya requiring Virgin Media response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Virgin Media's SIP Trunk Service with the following observations:

- The Virgin Media SIP Trunk was unable to handle outbound SIP INVITEs/messages with an Avaya proprietary parameter in the Contact header. The parameter "+avaya-cm-keep-mpro" is present with a value of "no" when Initial IP-IP Direct Media is enabled on Communication Manager SIP Trunk. A SigMa script on the Avaya SBCE was required to remove the parameter "+avaya-cm-keep-mpro". The details of the Sigma Script and how to configure the script on the Avaya SBCE are outlined in **Section 7.5**.

- When attempting to execute a Blind Transfer to a PSTN phone for both inbound and outbound calls, Virgin Media were responding with "415 Unsupported Media Type" as Communication Manager uses the UPDATE method to execute the Blind Transfer successfully. In order for Blind Transfers to execute successfully for inbound and outbound calls, set "Always Use re-INVITE for Display Updates" to "y" within the trunk groups settings in **Section 5.6**.

- It was observed during testing that reINVITEs from the Avaya Enterprise to Virgin Media contained the Avaya proprietary header P-Location even though an Adaptation was enabled on Session Manager to remove Avaya proprietary headers as per **Section 6.4**. The Session Manager Adaptation was removing P-Location from the originating INVITE but not from reINVITEs sent from the Avaya Enterprise to Virgin Media. In order to remove the P-Location Header successfully from all reINVITEs sent from the Avaya Enterprise to Virgin Media, a Signalling Rule and End Point Policy Group were created as per **Section 7.9**.

- At the time of testing, the Virgin Media SIP trunk was not configured to support the G.729 codec.

- Inbound and Outbound fax was tested successfully using T.38 and G.711 pass-through protocols however T.38 is the preferred fax protocol supported by Avaya.

- The conferencing of outbound calls from Avaya Communicator for Windows was not tested. The softphone requires the use of a conferencing server that was not available at the time of testing.

- Inbound Toll-Free calls were not tested as no Toll-Free access was available for test.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on Virgin Media Business products please contact the following website: http://www.virginmediabusiness.co.uk/help/s/

3. Reference Configuration

The following equipment in **Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Virgin Media's SIP Trunk Service. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration were Avaya One-X® Communicator and Avaya Equinox™ for Windows soft phones running on a laptop PC.
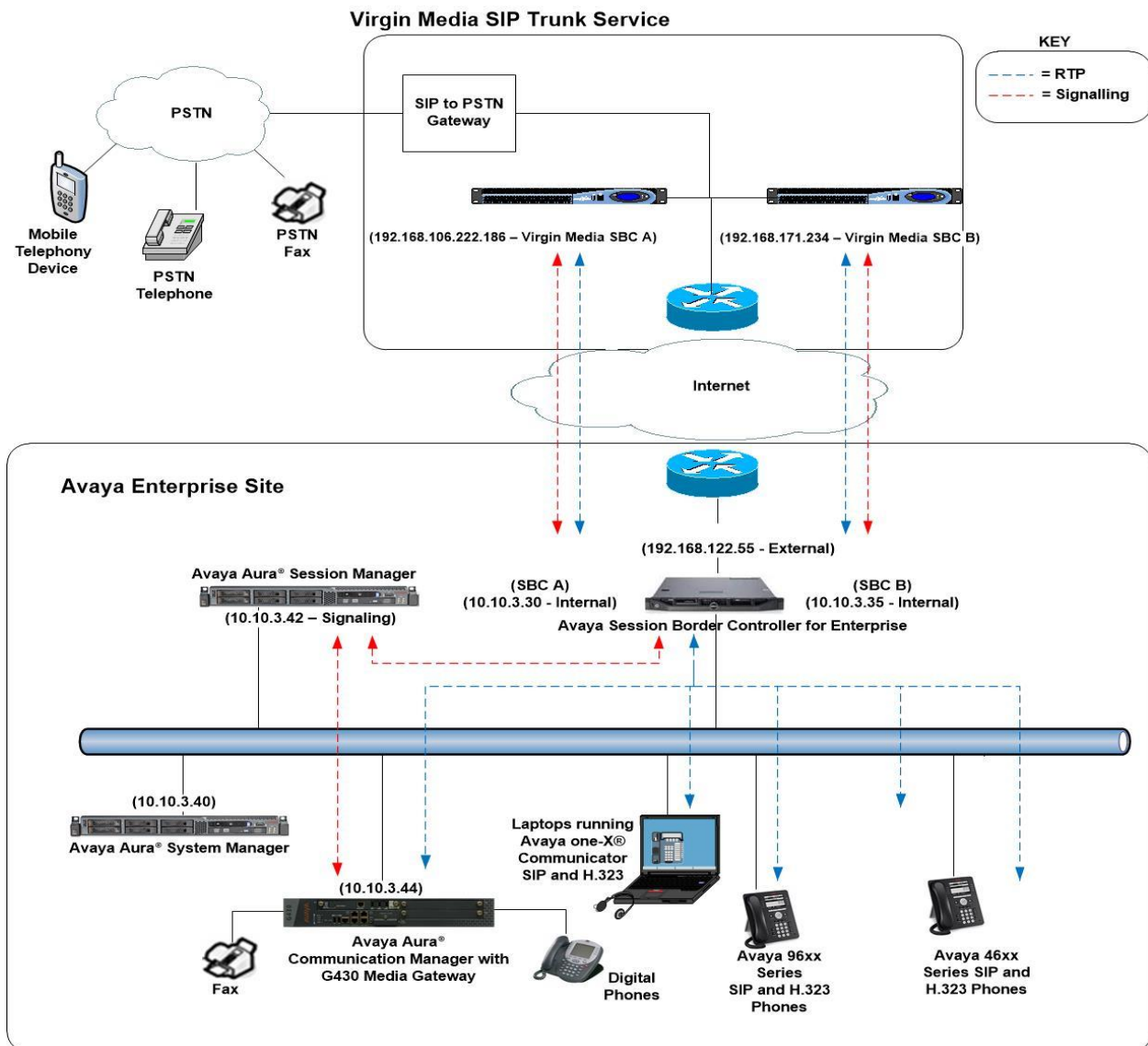

Figure 1: Test Setup Virgin Media SIP Trunk to Avaya Enterprise

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

7 of 68
VMBCMSM81SBC80

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® System Manager	8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.0.079814
Avaya Aura® Session Manager	8.1.0.0.801007
Avaya Aura® Communication Manager	8.1.0.2 – SP2
Avaya Session Border Controller for Enterprise	8.0.1.0-10-175555
Avaya G430 Media Gateway	41.9.0
Avaya Aura® Media Server	v.8.0.0.205
Avaya 1600 IP DeskPhone (H.323)	1.3.12
Avaya 96x0 IP DeskPhone (H.323)	3.2.4
Avaya 96x1 IP DeskPhone (H.323)	6.8.2
Avaya 9611 IP DeskPhone (SIP)	7.1.6.0
Avaya 9608 IP DeskPhone (SIP)	7.1.6.0
Avaya one–X® Communicator (H.323 & SIP)	6.2.14.1 -SP14
Avaya Equinox™ for Windows	3.6.4.31.2
Analogue Handset	N/A
Analogue Fax	N/A
Virgin Media	
Soft Switch C20	CVM18
Genband Q20 SBC	V9.3.18

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 Virgin Media SIP Trunk. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC for Enterprise (Avaya SBCE) 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 Avaya SBCE at the enterprise site that then sends the SIP messages to the Virgin Media 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

CMN; Reviewed:
SPOC 1/21/2020
Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
8 of 68
VMBCMSM81SBC80

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 Virgin Media SIP Trunk network, and any other SIP trunks used.

```
display system-parameters customer-options              Page   2 of  12
                            OPTIONAL FEATURES

IP PORT CAPACITIES                                         USED
                    Maximum Administered H.323 Trunks: 4000  0
          Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                      Maximum Video Capable Stations: 2400  0
                 Maximum Video Capable IP Softphones: 2400  0
                    Maximum Administered SIP Trunks: 4000  10
   Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
    Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

On **Page 5**, verify that **IP Trunks** field is set to **y.**

```
display system-parameters customer-options                      Page   5 of  12
                             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? n
  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
```

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 Session Manager. In this case, **SM100** and **10.10.3.42** 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             10.10.3.42
default           0.0.0.0
procr             10.10.3.44
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 Avaya SBCE.
- 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.
- The rest of the fields can be left at default values.

```
change ip-network-region 1                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name: default                  Stub Network Region: n
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 supported by Virgin Media was configured, namely **G.711A** and **G.711MU**.

```
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.711MU           n          2         20


```

Virgin Media's SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define T.38 fax as follows:
- Set the **FAX - Mode** to **t.38-standard**.
- Leave **ECM** at default value of **y**.

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

                          IP CODEC SET

                       Allow Direct-IP Multimedia? n


                                                                 Packet
                        Mode               Redundancy            Size(ms)
    FAX                 t.38-standard          0        ECM: y
    Modem               off                    0
    TDD/TTY             US                     3
    H.323 Clear-channel n                      0
    SIP 64K Data        n                      0                  20
```

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Virgin Media SIP Trunk network. During test, this was configured to use TCP and port 5060 to facilitate tracing and fault analysis. 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 as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tcp**.
- 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 **5060** (Commonly used TCP 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).
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set **Initial IP-IP Direct Media** to **y**.
- Set **H.323 Station Outgoing Direct Media** to **y**.

The default values for the other fields may be used.

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

 Group Number: 1                      Group Type: sip
  IMS Enabled? n              Transport Method: tcp
        Q-SIP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y   Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                   Far-end Node Name: SM
 Near-end Listen Port: 5060                  Far-end Listen Port: 5060
                                           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? y
H.323 Station Outgoing Direct Media? y          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**.
- 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: OUTSIDE CALL                   COR: 1      TN: 1       TAC: 101
   Direction: two-way          Outgoing Display? n
 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 Virgin Media to prevent unnecessary SIP messages during call setup. During the compliance testing, **Preferred Minimum Session Refresh Interval (sec)** was set to **1800** to configure the Min-SE timer to 3600 as requested by Virgin Media.

```
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


          XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of CLI in format of E.164 with leading "+". Also, set the **Hold/Unhold Notifications** to **y**.

```
TRUNK FEATURES
         ACA Assignment? n           Measured: none
                                                     Maintenance Tests? y


  Suppress # Outpulsing? n  Numbering Format: public
                                          UUI Treatment: service-provider

                                           Replace Restricted Numbers? n
                                         Replace Unavailable Numbers? n

                                          Hold/Unhold Notifications? y
                              Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

On **Page 4** of this form:
- Set **Mark Users as Phone** to **y**.
- Set **Send Transferring Party Information** to **n**.
- Set **Network Call Direction** to **n**.
- Set **Send Diversion Header** to **y**.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Virgin Media.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- Set the **Identity for Calling Party Display** to **P-Asserted-Identity**.

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

                                        Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                   Send Transferring Party Information? n
                             Network Call Redirection? n

                                 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
             Accept Redirect to Blank User Destination? n
                                         Enable Q-SIP? n

       Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                         Request URI Contents: may-have-extra-digits
```

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 format required. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

```
change private-numbering 0                                    Page   1 of   2
                        NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk       CPN           CPN
Len Code          Grp(s)    Prefix        Len
                                                  Total Administered: 4
  4  6102          1         441xxxxxxx40  12        Maximum Entries: 240
  4  6010          1         441xxxxxxx41  12
  4  6020          1         441xxxxxxx42  12     Note: If an entry applies to
  4  6104          1         441xxxxxxx43  12     a SIP connection to Avaya
                                                  Aura(R) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.


                                                  Communication Manager
                                                  automatically inserts
                                                  a '+' digit in this case.
```

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 Virgin Media's SIP Trunk. 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**. As Call Park was included in the testing remit by Virgin Media, the feature access codes configured for **Call Park Access Code *72** and **Answer Back Access Code *74** were used to test Call Park successfully.

```
change feature-access-codes                                   Page   1 of  11
                           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: *74
                         Attendant Access Code:
        Auto Alternate Routing (AAR) Access Code:
     Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
                   Automatic Callback Activation:       Deactivation:
Call Forwarding Activation Busy/DA:        All:         Deactivation:
   Call Forwarding Enhanced Status:        Act:         Deactivation:
                    Call Park Access Code: *72
                    Call Pickup Access Code: *73
CAS Remote Hold/Answer Hold-Unhold Access Code:
```

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. 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               11   14    1        pubu         n
    00              13   15    1        pubu         n
    0035391         13   13    1        pubu         n
    030             10   10    1        pubu         n
    0800            8    10    1        pubu         n
    0900            8    8     1        pubu         n
    118             3    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 Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **unk-unk**.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1     Pattern Name:
                            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                                 unk-unk   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 Virgin Media can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DDI numbers provided by Virgin Media correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DDI numbers have been masked for security purposes.

```
change inc-call-handling-trmt trunk-group 1                  Page   1 of   3
INCOMING CALL HANDLING TREATMENT
 Service/       Number   Number       Del Insert
 Feature        Len       Digits
 public-ntwrk    13 +441xxxxxx40      all 6102
 public-ntwrk    13 +441xxxxxx41      all 6010
 public-ntwrk    13 +441xxxxxx42      all 6020
 public-ntwrk    13 +441xxxxxx43      all 6104
```

5.10. EC500 Configuration

When EC500 is enabled on the 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 6102. 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. **0035391xxxxxx**).
- 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 6102               Page   1 of   3
                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station          Application Dial   CC  Phone Number    Trunk        Config  Dual
 Extension                    Prefix                     Selection    Set     Mode
 6102             EC500        -      0035391xxxxxx  1            1
-
```

Note: The phone number shown is for a mobile phone used for testing at Avaya Labs and is in international format with international dialling prefix 00. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

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. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP Domain.
- Administer SIP Location.
- Administer Adaptations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Routing Policies.
- Administer Dial Patterns.

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Log in to Avaya Aura® System Manager

Access the 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.
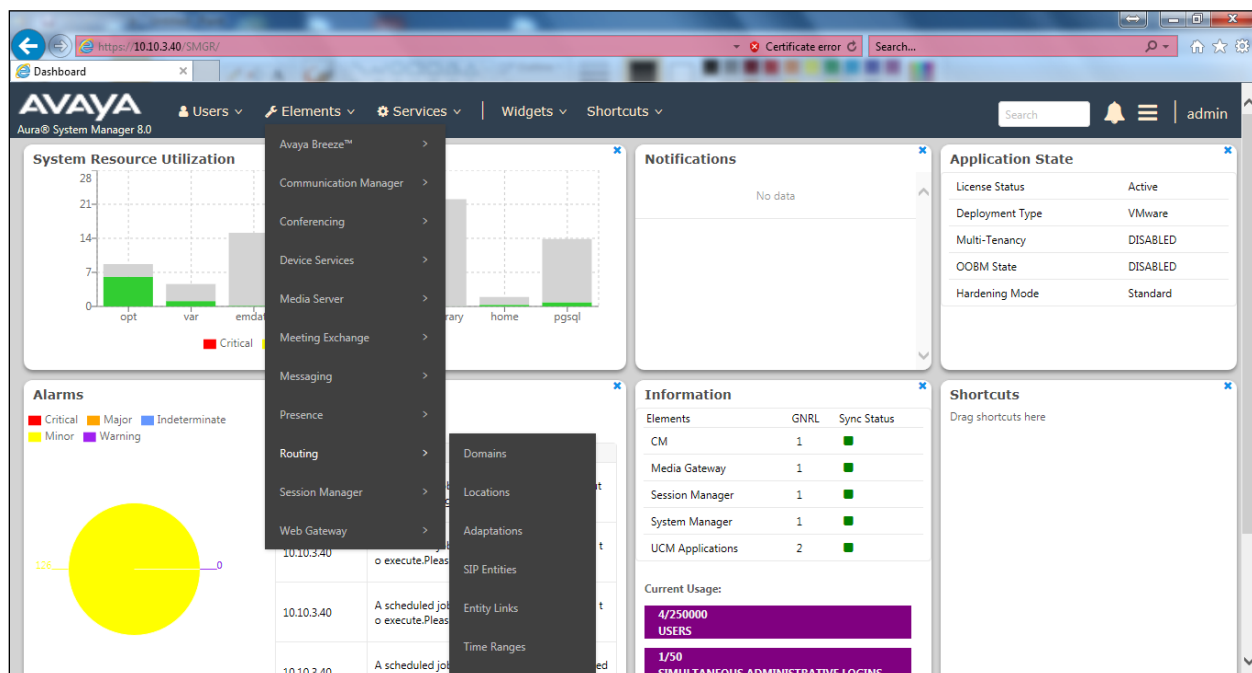
Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.
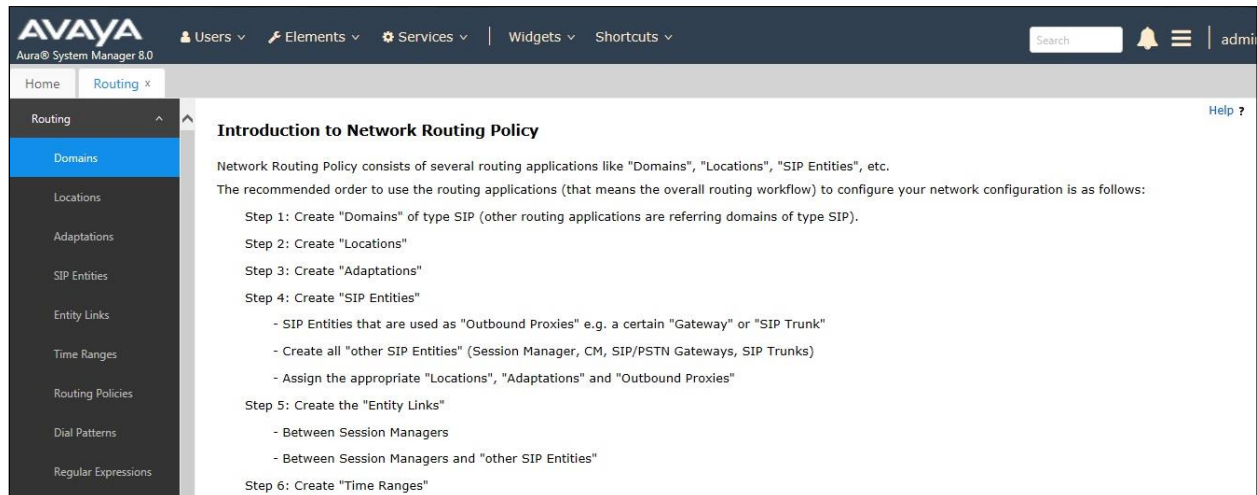
6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements → Routing** and select **Domains** from the left navigation menu, click **New** (not shown)**.** Enter the following values and use default values for remaining fields.

- **Name**   Enter a Domain Name**.** In the sample configuration, **avaya.com** was used.
- **Type**   Verify **SIP** is selected.
- **Notes**   Add a brief description [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.
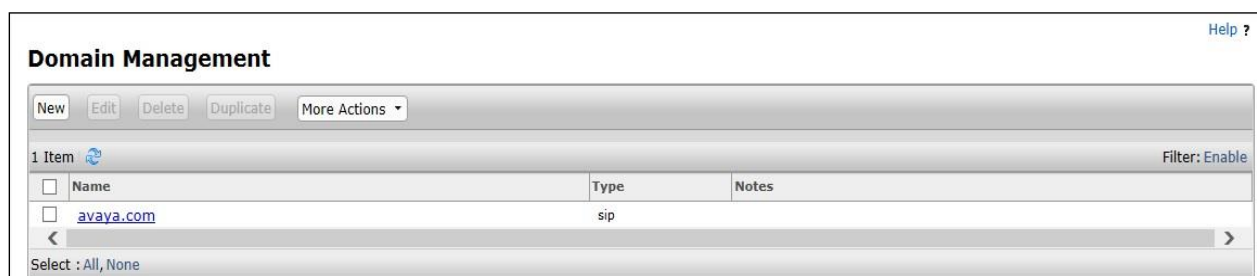
6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing→Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:**   Enter a descriptive name for the location.
- **Notes:**   Add a brief description (optional).

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity.

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **SMGR_8** defined for the compliance testing.

6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers. An Adaptation was used during testing to remove Avaya proprietary headers from messages sent 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. In order to improve interoperability with third party elements, Session Manager R8.1 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary or unnecessary for non-Avaya elements. For the compliance test, an Adaptation named "**VMB**" was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. These headers contain private information from the enterprise and also add unnecessary size to outbound messages, while they have no significance to the service provider.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown). Under **Adaptation Details →General**:

- **Adaption Name**:   Enter an appropriate name such as **VMB**.
- **Module Name**:   Select **DigitConversionAdapter**.
- **Modular Parameter Type**: Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

- **Name**:   Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value**:   Enter **AV-Global-Session-ID**, **AV-Correlation-ID**, **Alert-Info**, **Endpoint-View**, **P-AV-Message-ID**, **P-Charging-Vector**, **P-Location**.
- **Name**:   Enter **fromto**. Modifies From and To header of a message.
- **Value**:   Enter **true**.
- **Name**:   Enter **MIME**. Remove MIME message bodies from Session Manager.
- **Value**:   Enter **no**.

Scroll down the page and under **Digit Conversion for Outgoing Calls from SM**, click the **Add**

CMN; Reviewed:
SPOC 1/21/2020
Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
22 of 68
VMBCMSM81SBC80

button and specify the digit manipulation to be performed as follows:
- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so **both** have been selected.

Digit Conversion for Outgoing Calls from SM

Add	Remove								
1 Item									Filter: Enable
☐	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
☐	* 00	* 2	* 15		* 2	+	both ▼		

Select : All, None

Commit | Cancel

This will ensure any outgoing numbers matching 00 will be deleted and have + inserted being converted to E.164 format before being forwarded to the Avaya SBCE.

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 signaling 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 Avaya SBCE SIP Entity.
- 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 four SIP Entities.
- Session Manager SIP Entity.
- Communication Manager SIP Entity.
- Avaya SBCE SIP Entity x 2.

CMN; Reviewed:
SPOC 1/21/2020
Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
23 of 68
VMBCMSM81SBC80

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 and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

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 the domain added in **Section 6.2** 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 and **Type** is **CM**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows one of the SIP Entities for the Avaya SBCE. Two SIP Entities were used for the two interfaces established so that routing could take place to both the Virgin Media SBCs. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interfaces (see **Figure 1**). Set **Type** to **SIP Trunk** and **Adaptation** to that defined in **Section 6.4**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

The following screenshot shows the SIP Entity for Virgin SBC B.

General

* Name:	VMB_SBC_B
* FQDN or IP Address:	10.10.3.35
Type:	SIP Trunk
Notes:	
Adaptation:	VMB
Location:	SMGR_8
Time Zone:	Europe/Dublin
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	☐
Call Detail Recording:	egress

Loop Detection

Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200
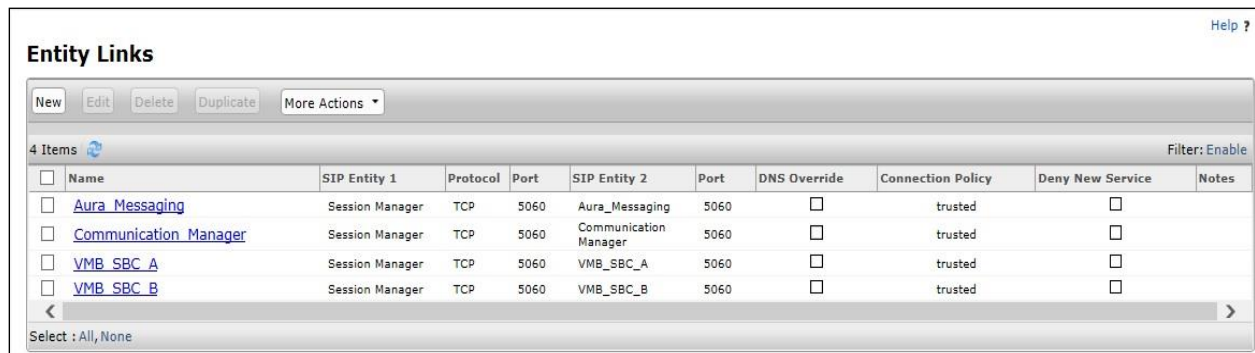
6.6. Administer Entity Links

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 **Session Manager**.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- 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.

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

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
☐	Aura_Messaging	Session Manager	TCP	5060	Aura_Messaging	5060	☐	trusted	☐	
☐	Communication_Manager	Session Manager	TCP	5060	Communication Manager	5060	☐	trusted	☐	
☐	VMB_SBC_A	Session Manager	TCP	5060	VMB_SBC_A	5060	☐	trusted	☐	
☐	VMB_SBC_B	Session Manager	TCP	5060	VMB_SBC_B	5060	☐	trusted	☐	

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

28 of 68
VMBCMSM81SBC80

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.

In the Virgin Media network, two network SBCs are provided as the interface to the enterprise equipment. These are Sandbox SBCs and for the purposes of this document have been designated as A and B. The routing and fallback for these two SBCs is configured on the Session Manager, with two server flows configured on the Avaya SBCE for routing to each network SBC. There is an interface configured on the Avaya SBCE for each of these server flows, and a corresponding SIP Entity, Entity Link and Routing Policy is required on the Session Manager for each of these interfaces.

A full description of the configuration of the interfaces and server flows on the Avaya SBCE is provided in **Section 7**.

CMN; Reviewed:
SPOC 1/21/2020
Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
29 of 68
VMBCMSM81SBC80

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed on to Virgin Media via SBC A.

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed on to Virgin Media via SBC B.

Note: Ranking value has been set to **1** for VMB_SBC_A and set to **2** for VMB_SBC_B. Lower ranking values indicate higher priority for call routing so all calls will route to VMB_SBC_A. Should VMB_SBC_A encounter routing difficulties, then all call routing will automatically failover to VMB_SBC_B.

As part of the Virgin Media test requirements, round robin call routing was also required to be tested. In order to configure round robin call routing if required, the ranking value for both VMB_SBC_A and VMB_SBC_B is set to **1** so all calls are distributed evenly across both VMB_SBC_A and VMB_SBC_B.

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 location defined in **Section 6.3** or **ALL**.
- 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 Avaya SBCE which will route the calls out to the Virgin Media network via network VMB_SBC_A with fallback via network VMB_SBC_B.

CMN; Reviewed:
SPOC 1/21/2020
Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
31 of 68
VMBCMSM81SBC80

The following screen shows the test dial pattern configured for Communication Manager.

Dial Pattern Details			Commit Cancel	Help ?

General

* **Pattern:**	+44118
* **Min:**	6
* **Max:**	16
Emergency Call:	☐
SIP Domain:	avaya.com ▼
Notes:	

Originating Locations and Routing Policies

Add   Remove

1 Item 🔁   Filter: Enable

	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	SMGR_8		to_Communication_Manager	0	☐	Communication Manager	

Select : All, None

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.
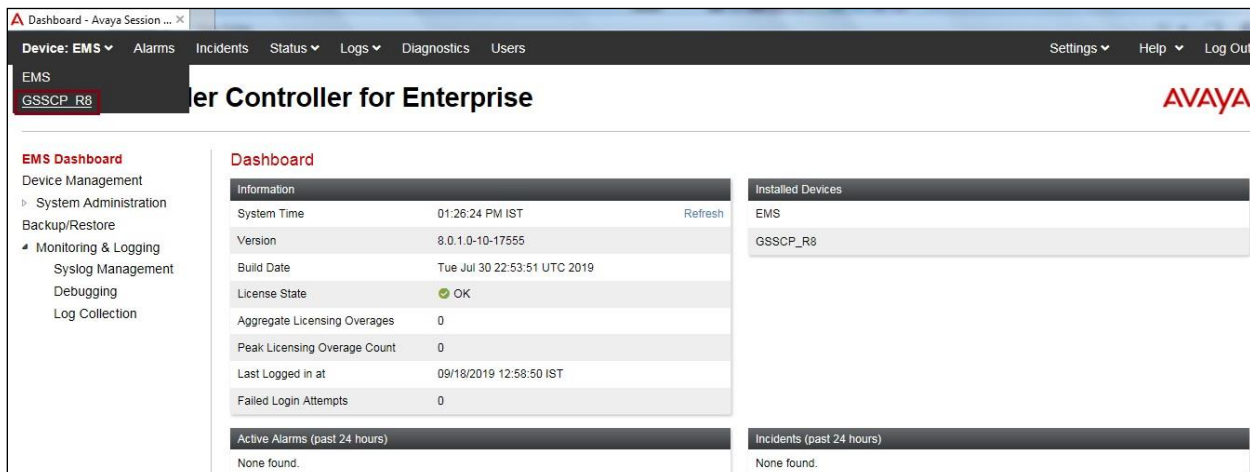
7.1. Access Avaya Session Border Controller for Enterprise

Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.

Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu. with a menu on the left-hand side. In this case, **GSSCP_R8** is used as a starting point for all configuration of the Avaya SBCE.

To view system information that was configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_R8** is shown. To view the configuration of this device, click **View** (the third option from the right).
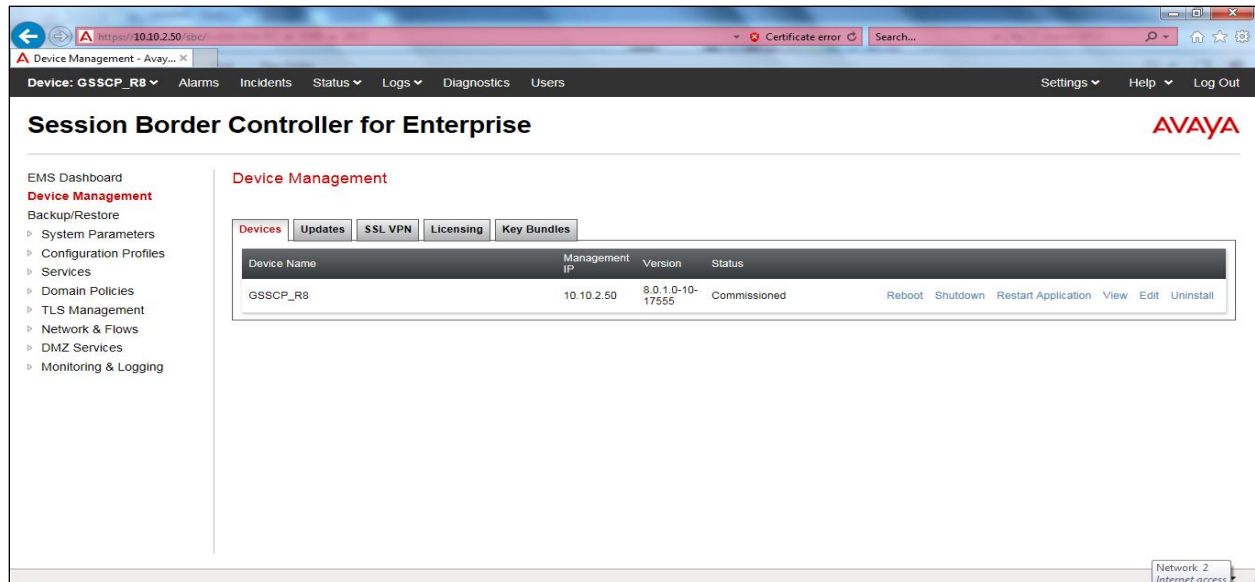
The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.

7.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external.

In the test configuration, two IP addresses were used on the internal interface so that different server flows could be assigned depending on which interface address the SIP messages were received on. These server flows were used to direct traffic to the two Virgin Media SBCs separately.

To define the network information, navigate to **Network & Flows → Network Management** in the main menu on the left-hand side and click on **Add**. Enter details for the external interfaces in the dialogue box:
- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBCE. Enter details in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address of the Avaya SBCE used for VMB_SBC_A on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Add** again.
- Enter the internal IP address of the Avaya SBCE used for VMB_SBC_B on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:

Select the **Interfaces** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **Device Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Network & Flows → Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface to be used in the server flow for Virgin SBC A:
- Select **Add** and enter details of the first internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select one of the **A1_Internal** signalling interface IP addresses defined in **Section 7.2**.
- Select **TCP** port number, **5060** is used for the Session Manager.

To enter details of transport protocol and ports for the SIP signalling on internal interface to be used in the server flow for Virgin SBC B:
- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for interface.
- For **Signaling IP**, select the other **A1_internal** signalling interface IP address defined in **Section 7.2**.
- Select **TCP** port number, **5060** is used for the Session Manager.

To enter details of transport protocol and ports for the SIP signalling on the external interface:
- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **B1_external** signalling interface IP address defined in **Section 7.2**.
- Select **UDP** port number, **5060** is used for the Virgin Media SIP Trunk.
- Click **Finish**.

Signaling Interface

Signaling Interface

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig_Ext	192.168.122.55 B1_External (B1, VLAN 0)	5060	5060	---	None	Edit	Delete
Sig_Int_B	10.10.3.35 A1_Internal (A1, VLAN 0)	5060	---	5061	GSSCP_Server	Edit	Delete
Sig_Int_A	10.10.3.30 A1_Internal (A1, VLAN 0)	5060	---	5061	GSSCP_Server	Edit	Delete

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

39 of 68
VMBCMSM81SBC80

7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Network & Flows → Media Interface** from the menu on the left-hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow for Virgin SBC A:
- Select **Add** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **A1_Internal** media interface IP address for VMB_SBC_A defined in **Section 7.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow for Virgin SBC B:
- Select **Add** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **A1_Internal** media interface IP address for VMB_SBC_B defined in **Section 7.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.
- Select **Add** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **B1_External** media interface IP address defined in **Section 7.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.

Media Interface

Name	Media IP Network	Port Range		
Med_Ext	192.168.122.55 B1_External (B1, VLAN 0)	35000 - 40000	Edit	Delete
Med_Int_A	10.10.3.30 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
Med_Int_B	10.10.3.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete

CMN; Reviewed:
SPOC 1/21/2020
Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
40 of 68
VMBCMSM81SBC80

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Virgin Media SIP platform is connected as the Trunk Server and the Session Manager is connected as the Call Server.

7.4.1. Server Interworking Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Configuration Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

41 of 68
VMBCMSM81SBC80

On the **Advanced** Tab:

- Check **Record Routes** = **Both Sides**.
- Ensure **Extensions** = **Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

7.4.2. Server Interworking – Virgin Media

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Configuration Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as **VMB** and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **Delayed SDP Handling** as Virgin Media require all INVITEs to be populated with SDP.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	☐
URI Group	None ▾
Send Hold	☐
Delayed Offer	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☑
Re-Invite Handling	☐
Prack Handling	☐
Allow 18X SDP	☐
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

On the **Advanced** Tab:
- Check **Record Routes** = **Both Sides**.
- Ensure **Extensions** = **None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

7.5. Signalling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa. The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE

During compliance testing, an issue was also found with the handling of an Avaya specific parameter in the Contact Header. The Avaya proprietary parameter "+avaya-cm-keep-mpro=no" is present when Initial IP-IP Direct Media is enabled on Communication Manager SIP Trunk. A script was required to remove the proprietary parameter "+avaya-cm-keep-mpro" from the Contact Header.

To define the signalling manipulation to delete the Avaya proprietary parameter from the Contact Header, navigate to **Configuration Profiles → Signaling Manipulation** and click on **Add** (not shown)and enter a title. A new blank SigMa Editor window will pop up. The script text is as follows:

```
/*Script to remove attribute (+avaya-cm-keep-mpro) from Contact Header */

within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
       if (exists(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"])) then
        {
            remove(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"]);
          }
        }
    }
```

Once entered and saved, the script appears as shown in the following screenshot:

7.6. Define Servers

Servers are defined for each server connected to the Avaya SBCE. In this case, Virgin Media's SBC A and SBC B are connected as the Trunk Servers and Session Manager is connected as the Call Server.

7.6.1. Server Configuration – Avaya

From the left-hand menu select **Services → SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profiles** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5060**.
- For **Transport,** select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

Server Configuration Profile - General		X
Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.		

Server Type	Call Server
SIP Domain	
DNS Query Type	NONE/A
TLS Client Profile	None
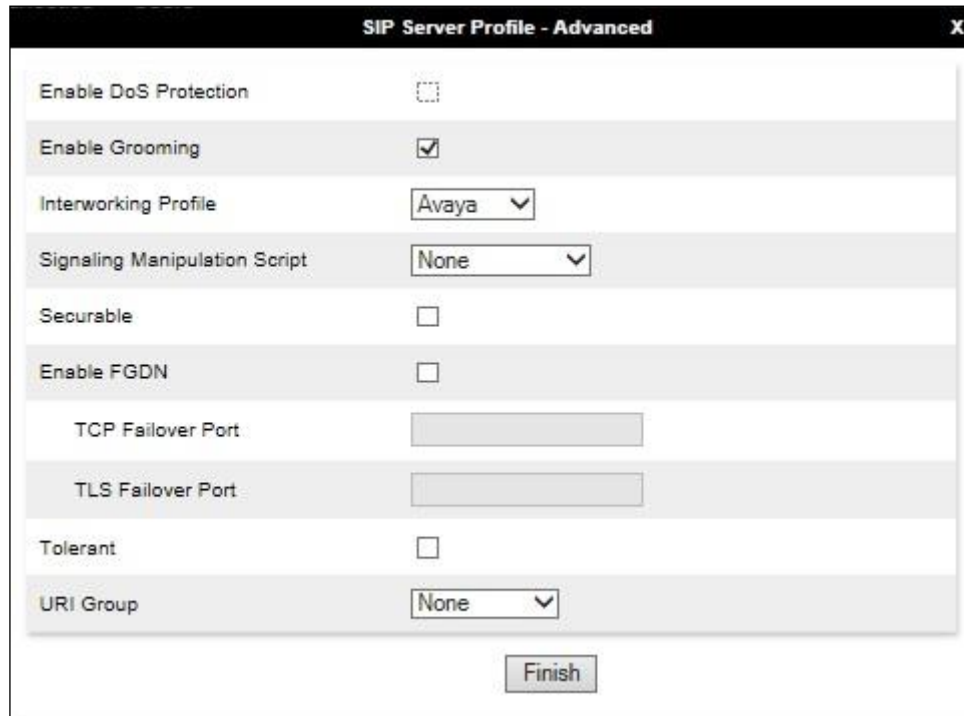
Add

IP Address / FQDN	Port	Transport	
10.10.3.42	5060	TCP	Delete

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

46 of 68
VMBCMSM81SBC80

On the **Advanced** tab:
- Check **Enable Grooming**.
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.

7.6.2. Server Configuration – Virgin Media

To define Virgin Media SBC A as a Trunk Server, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **192.168.222.186** (Virgin SBC A address).
- For **Port**, enter **5060**.
- For **Transport,** select **UDP**.
- Click on **Next** (not shown).

In the new window that appears, enter the following values as Virgin Media require authentication to connect to their network:
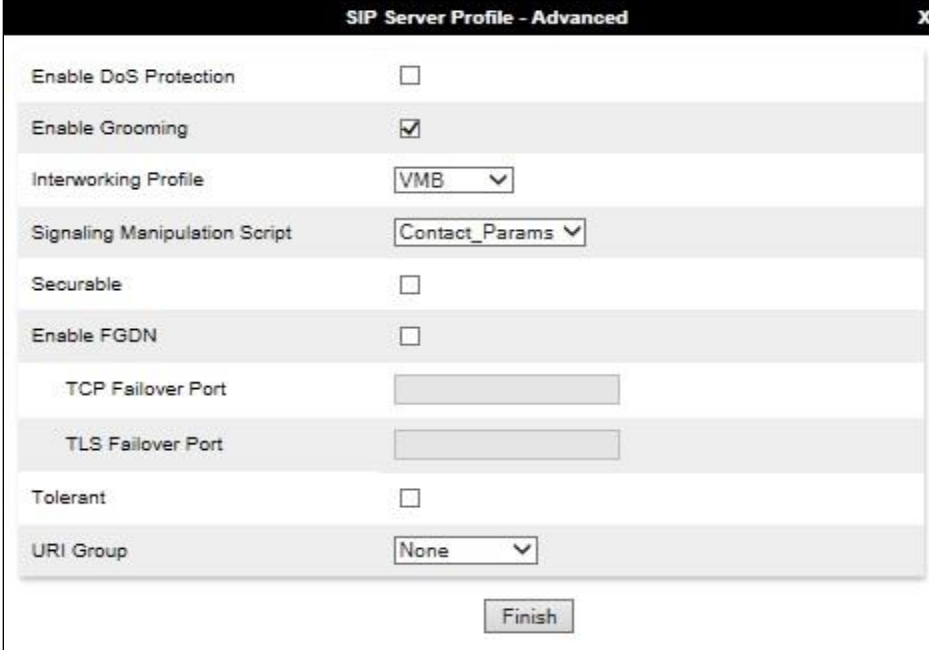
- **Enabled Authentication:**   Checked.
- **User Name:**   Enter username provided by the Service Provider.
- **Realm:**   Enter realm details provided by the Service Provider.
- **Password**   Enter password provided by the Service Provider.
- **Confirm Password**   Re-enter password provided by the Service Provider.

Click on **Next** (not shown) to use default entries on the **Heartbeat**, **Registration** and **Ping** tabs as registration to the Virgin Media SIP trunk was not required during testing.

On the Advanced tab:
- Select **VMB** for Interworking Profile.
- Check **Enable Grooming**.
- Select **Contact_Params** for **Signaling Manipulation Script** (**Section 7.5**).
- Click **Finish**.

Repeat the process to define a Server Configuration for Virgin SBC B.

7.7. Routing

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Routing information is required for routing to Session Manager on the internal side and Virgin Media address on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

7.7.1. Routing – Avaya

Create a Routing Profile for Session Manager.
* Navigate to **Configuration Profiles → Routing** and select **Add Profile**.
* Enter a **Profile Name** and click **Next**.

The Routing Profile window will open. Use the default values displayed and click **Add**.

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

On the **Next Hop Address** window, set the following:
- **Priority/Weight** = **1**.
- **SIP Server Profile** = **Avaya** (**Section 7.6.1**) from drop down menu.
- **Next Hop Address** = Select **10.10.3.42:5060(TCP)** from drop down menu.
- Click **Finish**.

7.7.2. Routing – Virgin Media

Create a Routing Profile for Virgin Media SIP network.
- Navigate to **Configuration Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

51 of 68
VMBCMSM81SBC80

The Routing Profile window will open. Use the default values displayed and click **Add**.

On the **Next Hop Address** window, set the following:
- **Priority/Weight** = **1**.
- **SIP Server Profile** = **VMB_SBC_A** (**Section 7.6.2**) from drop down menu.
- **Next Hop Address** = Select **192.168.222.186:5060 (UDP)** from drop down menu.
- Click **Finish**.

Repeat the process to define a Routing Profile for Virgin SBC B.

7.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for Session Manager, navigate to **Configuration Profiles →
Topology Hiding** from menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Avaya

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya.com
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Overwrite	avaya.com
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya.com

Topology Hiding Profiles: default, cisco_th_profile, **Avaya**, VMB

To define Topology Hiding for Virgin Media, navigate to **Configuration Profiles → Topology Hiding** from the menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Virgin Media and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).

Topology Hiding Profiles: VMB

Add	Rename Clone Delete

Topology Hiding Profiles				
default	Click here to add a description.			
cisco_th_profile	**Topology Hiding**			
Avaya				
VMB	Header	Criteria	Replace Action	Overwrite Value
	SDP	IP/Domain	Auto	---
	Request-Line	IP/Domain	Auto	---
	Record-Route	IP/Domain	Auto	---
	Via	IP/Domain	Auto	---
	Referred-By	IP/Domain	Auto	---
	From	IP/Domain	Auto	---
	Refer-To	IP/Domain	Auto	---
	To	IP/Domain	Auto	---
		Edit		

7.9. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.10**. Virgin Media was tested with a signalling rule to remove unnecessary and Avaya proprietary SIP headers that couldn't be removed with a Session Manager Adaptation (see **Section 6.4**). This was not necessary for the effective functioning of the SIP Trunk but was used to reduce the SIP message size.

7.9.1. Signalling Rules

Signalling rules are used to handle any non-standard signalling that may be encountered on a SIP Trunk, in this case the transmission of Avaya proprietary and unnecessary SIP message headers from the Avaya equipment. Signalling rules were created Virgin Media to remove unwanted Avaya proprietary Headers such as P-Location. The Virgin Media signalling rule was named **VMB**.

To define the Virgin Media signalling rule, navigate to **Domain Policies →Signaling Rules** in the main menu on the left hand side. Highlight the default signalling rule and click on **Clone**.

Enter a **Rule Name** in the **Clone Rule** dialogue box and click on **Finish**.

In the test environment, the P-Location Header was removed from the SIP reINVITE message from Communication Manager. This parameter is the only one of the identified unnecessary parameters that could not be removed using the Session Manager Adaptation described in **Section 6.4**.

To remove the P-Location Header, highlight the recently created Signalling Rule click on the **Request Headers** tab and click on **Add Out Header Control** (not shown).

- Check the **Proprietary Request Header** box.
- Type **P-Location** in the **Header Name** field.
- Leave **Method Name** at the default value of **ALL**.
- Check the **Forbidden** radio button in the **Header Criteria field**.
- Leave the **Presence Action** at the default value of **Remove Header**.
- Click on **Finish**.

Note: The above is an example of removal of P-Location proprietary header. When finished, all the Request Headers defined will be shown under the Request Headers tab as shown in the screenshot below.

CMN; Reviewed:
SPOC 1/21/2020
Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
56 of 68
VMBCMSM81SBC80

7.9.2. End Point Policy Group

An End Point Policy Group is required to implement the signalling rule. To define one for use in the Virgin Media server flows, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side.

Select an appropriate pre-defined Policy Group, in the test environment this was **default-low**, and click on **Clone**.

Enter an appropriate name in the pop-up box.

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.
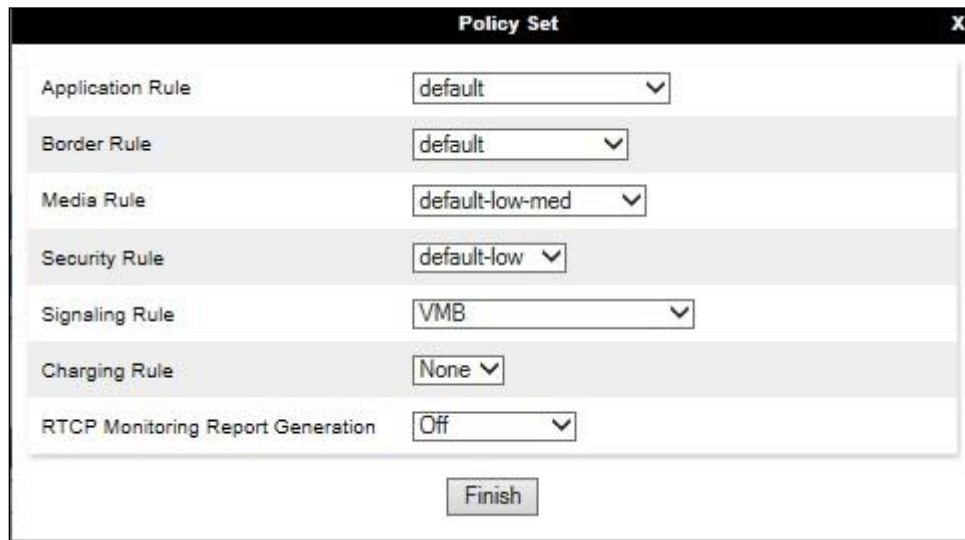
Highlight the resulting Policy Group and click on **Edit**. Enter details as follows:

- Leave the **Application Rule**, **Border Rule**, **Media Rule**, **Security Rule**, **Charging Rule** and **RTCP Monitoring Report Generation** at their default values.
- Select the **Signaling Rule** created in the previous section in the drop down menu.
- Click on **Finish**.

The completed Virgin Media Policy Group is shown in the screenshot below:

7.10. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Virgin Media's SIP Trunk and incoming flows from Virgin Media's SIP Trunk to Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from the Session Manager to the PSTN via the Virgin Media network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.
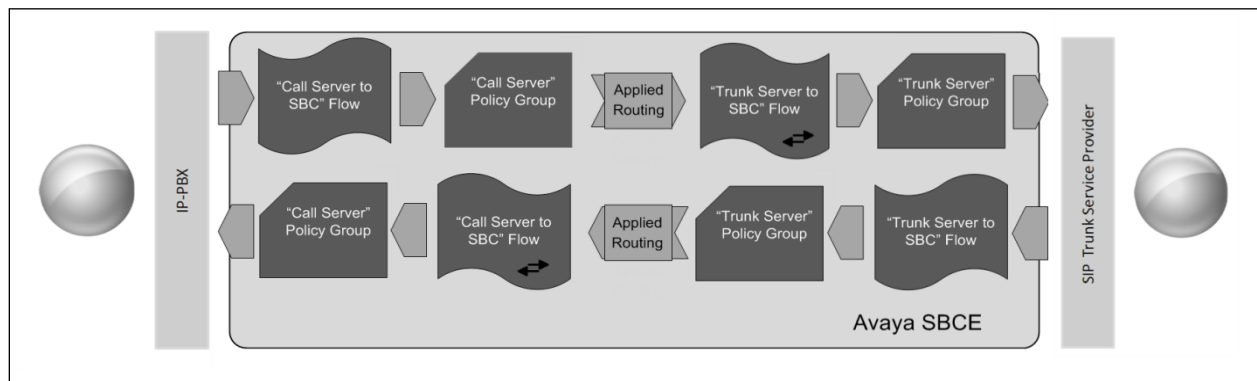
Two server flows are required for outgoing traffic and two are required for incoming. This is so that traffic can be routed to both the network SBCs and can also be received from both network SBCs. As mentioned previously, the network SBCs have been designated as Virgin SBC A and Virgin SBC B for the purposes of the testing and documentation.

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

59 of 68
VMBCMSM81SBC80

To define a Server Flow for Session Manager to each of the network SBCs, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for the Session Manager, in this case **Call_Server_A** was used.
- In the **Server Configuration** drop-down menu, select the Session Manager server configuration defined in **Section 7.6.1**.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3.1**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3.1**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3.2**. This is the interface that media bound for Session Manager is sent
- Set the **End Point Policy Group** to the endpoint policy group **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of Virgin SBC A defined in **Section 7.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.8** and click **Finish**.

Flow: Call_Server_A			X
Criteria		**Profile**	
Flow Name	Call_Server_A	Signaling Interface	Sig_Int_A
Server Configuration	Avaya	Media Interface	Med_Int_A
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	default-low
Remote Subnet	*	Routing Profile	VMB_SBC_A
Received Interface	Sig_Ext	Topology Hiding Profile	Avaya
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	☐

Repeat the above process for Call Server B, selecting the specific Call Server B entries for server flow configuration.

To define Server Flows for the Virgin Media network SBCs (Virgin SBC A and Virgin SBC B),
navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for Virgin SBC A
  SIP Trunk, in the test environment **Trunk_Server_A** was used.
- In the **Server Configuration** drop-down menu, select the Virgin SBC A server
  configuration defined in **Section 7.6.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface
  defined in **Section 7.3.1**. This is the interface that signalling bound for Virgin SBC A SIP
  Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface
  defined in **Section 7.3.1**. This is the interface that signalling bound for Virgin SBC A SIP
  Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in
  Section 7.3.2. This is the interface that media bound for Virgin SBC A SIP Trunk is sent
  on.
- Set the **End Point Policy Group** to the endpoint policy group **VMB** defined in **Section
  7.9.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager
  defined in **Section 7.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of
  Virgin SBC A SIP Trunk defined in **Section 7.8** and click **Finish**.

Flow: Trunk_Server_A			X
Criteria		**Profile**	
Flow Name	Trunk_Server_A	Signaling Interface	Sig_Ext
Server Configuration	VMB_SBC_A	Media Interface	Med_Ext
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	VMB
Remote Subnet	*	Routing Profile	Avaya
Received Interface	Sig_Int_A	Topology Hiding Profile	VMB
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	☐

Repeat the above process for Virgin SBC B, selecting the specific Virgin SBC B entries for
server flow configuration.

8. Configure Virgin Media SIP Trunk Equipment

The configuration of the Virgin Media equipment used to support Virgin Media's SIP Trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Virgin Media equipment and system configuration please contact an authorised Virgin Media representative.

9. 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 Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Help

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: Session Manager

Status Details for the selected Session Manager:

Summary View

5 Items | Refresh

Filter: Enable

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○ Virgin_SBC_A	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
○ Communication_Manager	10.10.3.44	5060	TCP	FALSE	UP	200 OK	UP
○ Aura_Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP
○ CS1K_7.6	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP
○ Virgin_SBC_B	10.10.3.35	5060	TCP	FALSE	UP	200 OK	UP

2. From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. 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 T00010    in-service/idle     no
```

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call 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.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from the Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

To define the trace, navigate to **Monitoring & Logging → Trace** in the main menu on the left-hand side and select the **Packet Capture** tab.
- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a ***** to capture all traffic.
- Specify the protocol type from the **Protocol** field.
- Specify the **Maximum Number of Packets to Capture**, **1000** is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
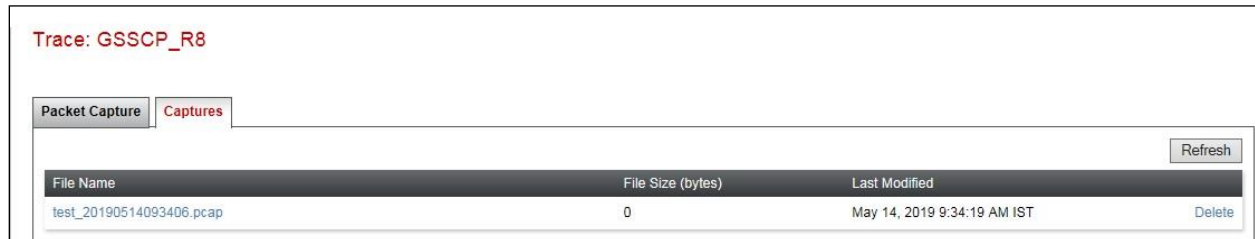- Click on **Start Capture**.

Trace: GSSCP_R8

Packet Capture	Captures

Packet Capture Configuration

Status	Ready
Interface	B1
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	UDP
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	test.pcap

Start Capture   Clear

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

Trace: GSSCP_R8

File Name	File Size (bytes)	Last Modified	
test_20190514093406.pcap	0	May 14, 2019 9:34:19 AM IST	Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Virgin Media network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R8.1 as an Evolution Server, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.0 to Virgin Media's SIP Trunk Service. Virgin Media's SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.
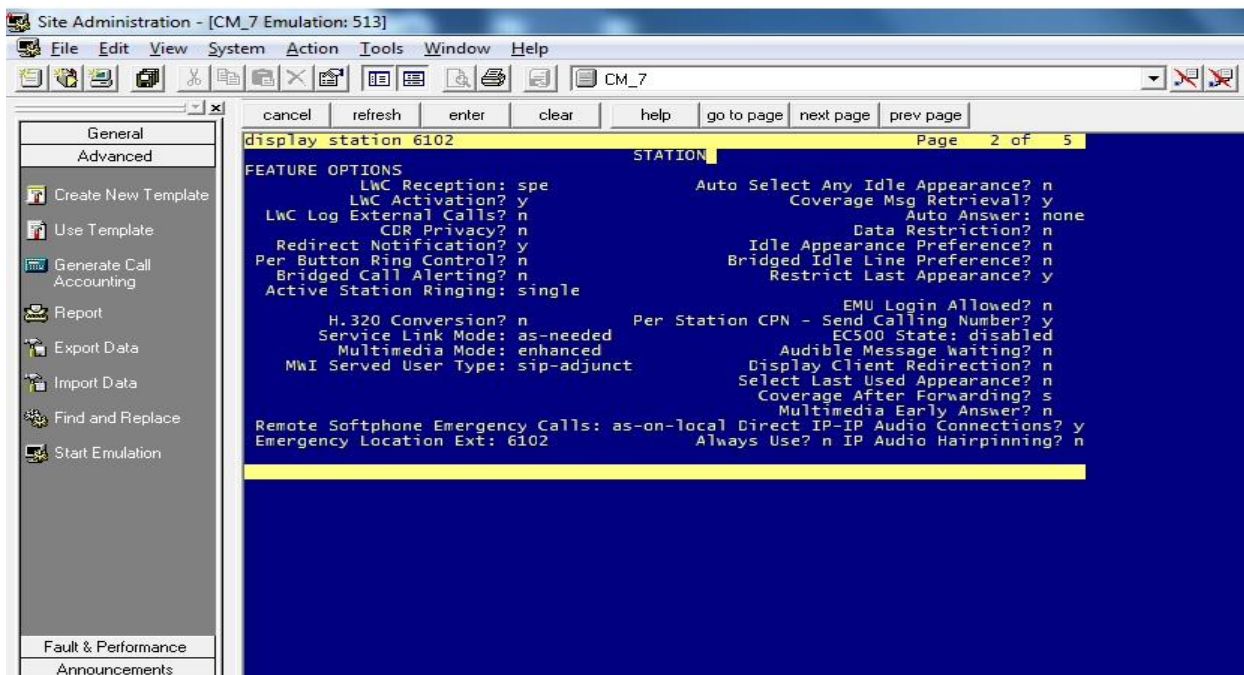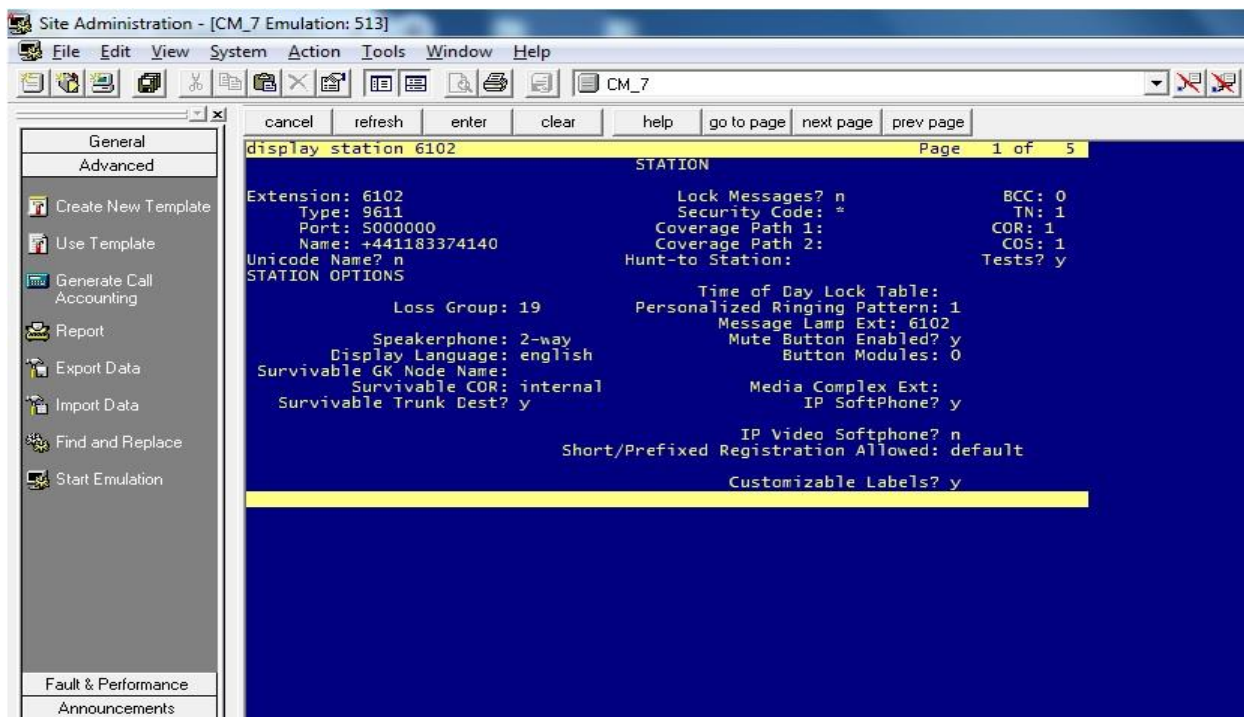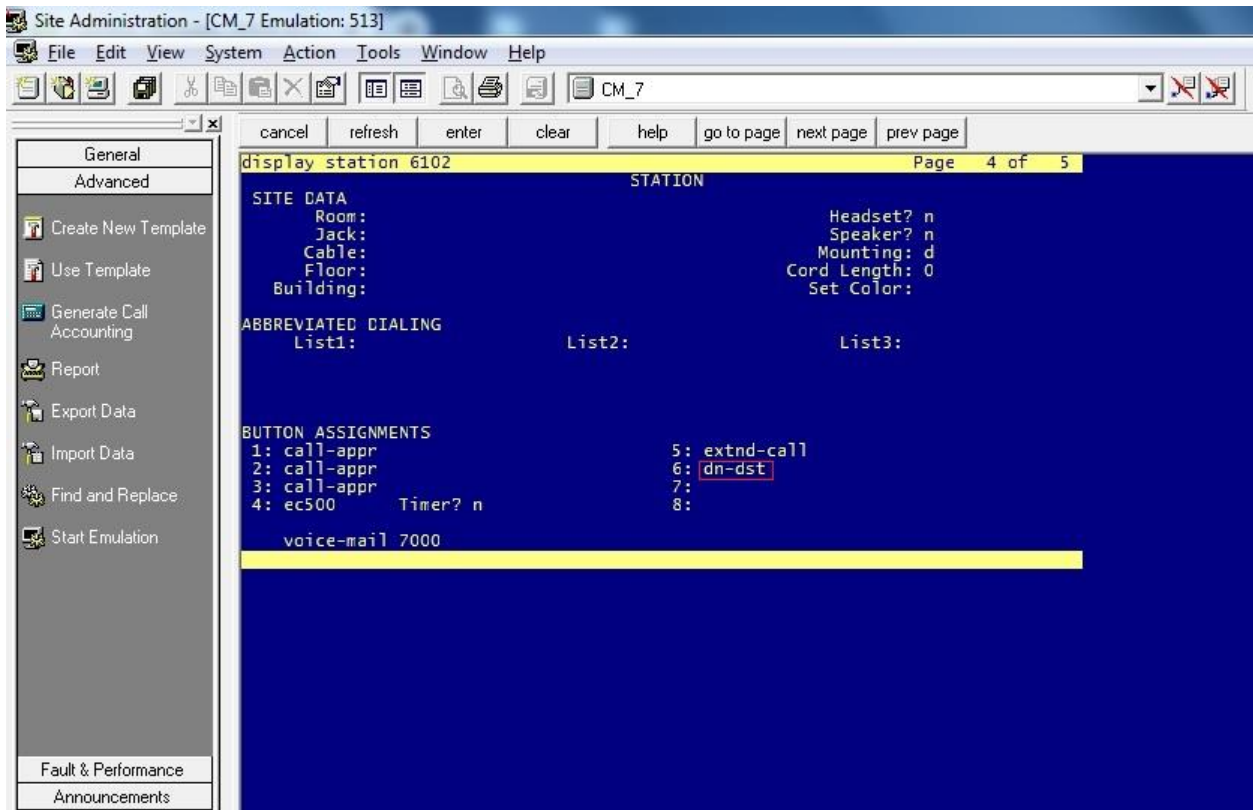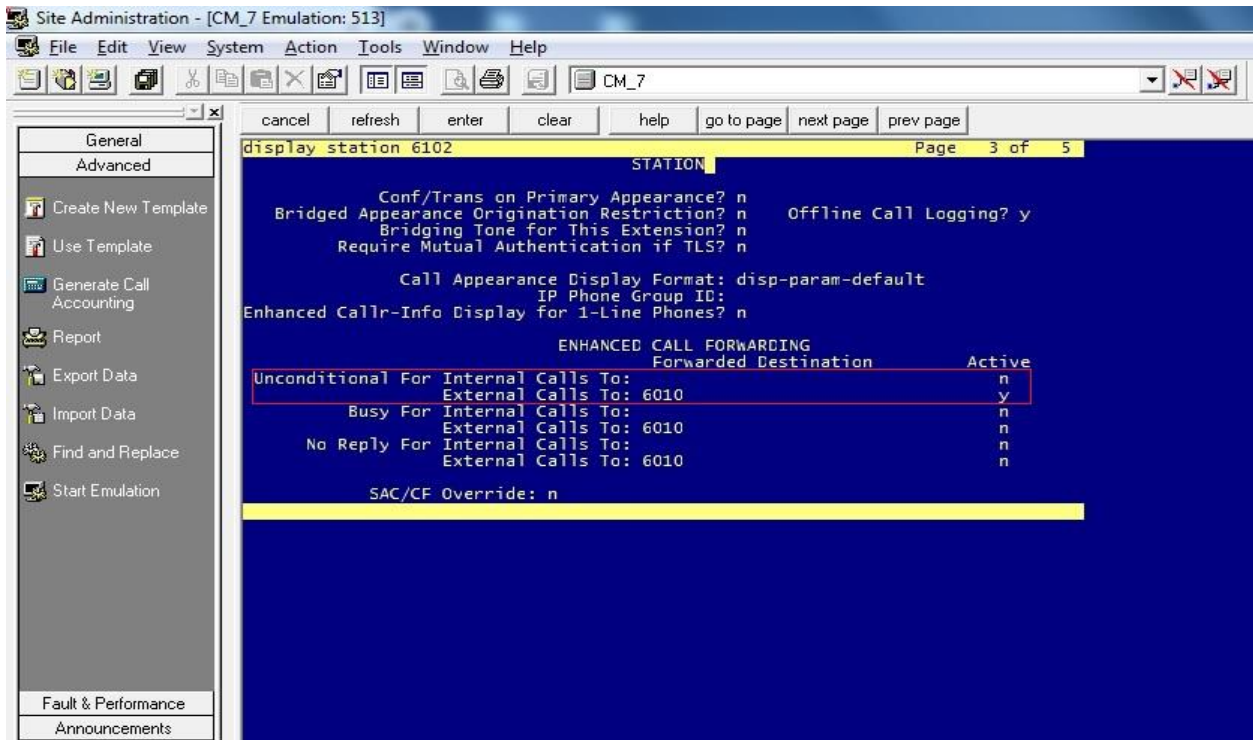
11. Additional References

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

[1] *Deploying Avaya Appliance Virtualization Platform*, Release 8.1, Jun 2019.
[2] *Upgrading Avaya Aura® applications*, Release 8.1, Jun 2019.
[3] *Deploying Avaya Aura® applications from System Manager,* Release 8.1, Jun 2019
[4] *Deploying Avaya Aura® Communication Manager*, Release 8.1, Jul 2019
[5] *Administering Avaya Aura® Communication Manager,* Release 8.1, Jul 2019
[6] *Upgrading Avaya Aura® Communication Manager,* Release 8.1, Jun 2019
[7] *Deploying Avaya Aura® System Manager Release 8.1,* Jul 2019
[8] *Upgrading Avaya Aura® System Manager to Release 8.1*, Jul 2019.
[9] *Administering Avaya Aura® System Manager for Release 8.1,* Jul 2019
[10] *Deploying Avaya Aura® Session Manager,* Release 8.1 Jun 2019
[11] *Upgrading Avaya Aura® Session Manager* Release 8.1, Jun 2019
[12] *Administering Avaya Aura® Session Manager* Release 8.1, Jun 2019
[13] *Deploying Avaya Session Border Controller for Enterprise Release 8.0*, Jul 2019
[14] *Upgrading Avaya Session Border Controller for Enterprise Release 8.0,* Jul 2019
[15] *Administering Avaya Session Border Controller for Enterprise Release 8.0,* Jul 2019
[16] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

Appendix A – Communication Manager H.323 Station Example Configuration

Configuration highlights unconditional call forwarding and button feature assignment such as Do Not Disturb in RED.

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

67 of 68
VMBCMSM81SBC80

CMN; Reviewed:
SPOC 1/21/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

68 of 68
VMBCMSM81SBC80