Avaya Solution & Interoperability Test Lab

Application Notes for Configuring CenturyLink SIP Trunking with Avaya Aura® Communication Manager 5.2.1 and Avaya Aura® Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager, Avaya Aura® Session Border Controller and various Avaya endpoints.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager, Avaya Aura® Session Border Controller and various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the CenturyLink SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager and the Avaya Aura® Session Border Controller. Throughout the remainder of this document, the Avaya Aura® Session Border Controller may simply be referred to as the SBC.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test. Please note that SIP endpoints were not tested since SIP endpoints are not supported in a configuration without an Avaya Aura® Session Manager.

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various phone types including H.323, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Only the H.323 version of Communicator was tested.
- Various call types including: local, long distance, international, outbound toll-free, and operator (0).
- Codec G.711MU
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and mobility (extension to cellular)

- Network call redirection using the REFER method and/or a 302 response.

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested.
- Operator assisted calls (0 + 10 digits) and local directory assistance are supported but were not tested due to limitations in the test environment.
- T.38 Fax is not supported.
- Only codec G.711MU is supported in the CenturyLink production environment.

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Off-net call forwarding and EC500 require use of the Diversion header and disabling of the History-Info header**: Both of these features may redirect an inbound call back to the PSTN. If the outbound INVITE from the enterprise to CenturyLink contains both the Diversion and History-Info headers, CenturyLink returns a "604 Does not exist anywhere" response and the redirected call fails. This failure can be addressed by disabling use of the History-Info header on the Communication Manager trunk group (**Section 5.7**). Calls succeed when using only the Diversion header.
- **EC500 Extend function results in the call being dropped:** The EC500 Extend function allows a user with EC500 enabled on their enterprise phone to extend an active call from the enterprise phone to a remote device (typically a cell phone). The active call may then continue on the remote device. If the active call is between the PSTN and the enterprise phone and is extended to another PSTN endpoint, then the call will drop soon after being connected. The problem is caused by the fact that the resulting SIP connection has negotiated a DTMF payload header value that is different in each direction of the call which is not supported by CenturyLink. As a result, CenturyLink and Communication Manager will attempt to re-negotiate the DTMF payload header to a value that is acceptable to both. These attempts are unsuccessful and eventually the call drops. Communication Manager avoids this scenario in release 6.0 SP2 (or later) by adjusting the DTMF payload header value it offers when extending the call to the EC500 device. However, for Communication Manager 5.2.1 SP6, it is recommended that the EC500 Extend function is not used with CenturyLink.
- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. (See related item below.)
- **Incorrect Contact header sent by Avaya Aura® Session Border Controller**: After the transfer of an inbound PSTN call to a 2nd PSTN phone is completed, Communication Manager sends an UPDATE message to the Avaya Aura® Session Border Controller with updated Contact header information to reflect the actual connected party. It was observed that the UPDATE message sent to the Avaya Aura® Session Border Controller correctly contained the originating PSTN phone number (the actual connected party) in

the Contact header. However, in the UPDATE message sent from the Avaya Aura® Session Border Controller to CenturyLink, the Contact header was altered to contain the number of the transferring party. This problem was addressed via configuration in a previous release of the Avaya Aura® Session Border Controller. However, this same configuration failed to work in the Avaya Aura® Session Border Controller release used for this compliance test. This issue was reported to development and will be addressed in a later release of the Avaya Aura® Session Border Controller software.

- **Network Call Redirection**: If a Communication Manager vector is programmed to redirect an inbound call to a PSTN number before answering, Communication Manager will send a "302 Moved Temporarily" response to CenturyLink. CenturyLink will send an ACK in response to this message but will not redirect the call to the new party in the Contact header of the 302 message. The inbound caller hears fast busy. Network call redirection works successfully when the Communication Manager vector is programmed to redirect the inbound call to a PSTN number after answering the call first. This scenario uses the SIP REFER message for network call redirection instead of the 302 message. Using REFER for transferring inbound calls to the PSTN from an enterprise phone also works properly.
- **No error indication when all trunks are busy**: This occurs when calling the enterprise from a PSTN POTS line when all SIP trunks are busy at the enterprise. The PSTN caller does not get any error indication but instead hears ringback until the caller decides to hang-up. If the same call is made from a PSTN PBX phone, the PSTN caller hears fast busy. In each case, the enterprise returns a "404 Not Found" to the CenturyLink network.

2.3. Support

For technical support on CenturyLink SIP Trunking, contact CenturyLink using the **Support→Contact Us** links at www.centurylink.com or by calling business customer support at 1-800-201-4102.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Selecting the **Support Contact Options** link followed by **Maintenance Support** provides the worldwide support directory for Avaya Global Services. Specific numbers are provided for both customers and partners based on the specific type of support or consultation services needed. Some services may require specific Avaya service support agreements. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to CenturyLink SIP Trunking. This is the configuration used for compliance testing.

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

- Duplex Avaya S8720 Servers running Communication Manager
- Avaya G650 Media Gateway
- Avaya S8800 Server running Avaya Aura® Session Border Controller
- Avaya 9600-Series IP telephones (H.323)
- Avaya 4600-Series IP telephones (H.323)
- Avaya 1600-Series IP telephones (H.323)
- Avaya one-X® Communicator (H.323)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the SBC. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.

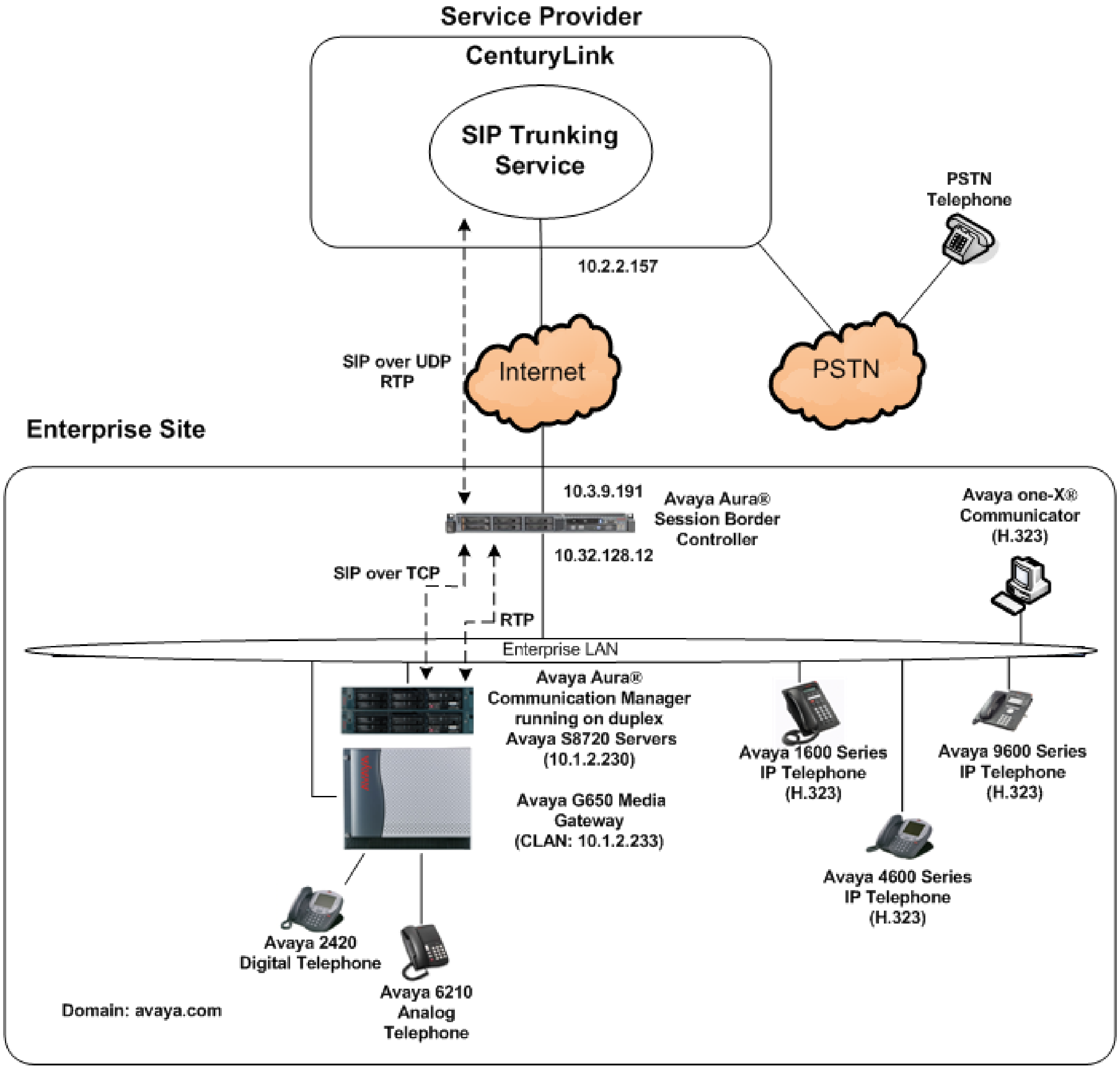

Service Provider
CenturyLink
SIP Trunking Service
PSTN Telephone
10.2.2.157
SIP over UDP
RTP
Internet
PSTN
Enterprise Site
10.3.9.191
Avaya Aura® Session Border Controller
10.32.128.12
Avaya one-X® Communicator (H.323)
SIP over TCP
RTP
Enterprise LAN
Avaya Aura® Communication Manager running on duplex Avaya S8720 Servers (10.1.2.230)
Avaya G650 Media Gateway (CLAN: 10.1.2.233)
Avaya 1600 Series IP Telephone (H.323)
Avaya 9600 Series IP Telephone (H.323)
Avaya 4600 Series IP Telephone (H.323)
Avaya 2420 Digital Telephone
Avaya 6210 Analog Telephone
Domain: avaya.com

Figure 1: Avaya IP Telephony Network using CenturyLink SIP Trunking

A separate trunk was created between Communication Manager and the SBC to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and not affect other traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the SBC then to Communication Manager. Once the call arrives at Communication Manager, incoming call treatment such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to the SBC. From the SBC, the call is sent to CenturyLink SIP Trunking.

For the compliance test, the enterprise sent 11 digits in the destination headers (e.g., Request-URI and To) and sent 10 digits in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). CenturyLink sent 10 digits in both the source and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on duplex Avaya S8720 Servers	5.2.1 SP6 (R015x.02.1.016.4-18576)
Avaya G650 Media Gateway • IP Server Interface (IPSI) TN2312BP • Control LAN (CLAN) TN799DP • IP Media Processor (MEDPRO) TN2602AP	HW15 FW046 HW01 FW032 HW02 FW047
Avaya 1608 IP Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.2.2
Avaya 4621SW IP Telephone (H.323)	2.9.1
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya one-X® Communicator (H.323)	6.0.0.26
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura® Session Border Controller	6.0 (Build SBCT_6.0.0.1.5) (System Platform 6.0.1.0.5)
CenturyLink SIP Trunking Solution Components	
Component	Release
Acme Packet Net-Net Session Border Controller	6.1
BroadSoft Softswitch	R16 sp1
Sonus Media Gateway	V07.02.07 R001

Table 1: Equipment and Software Tested

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

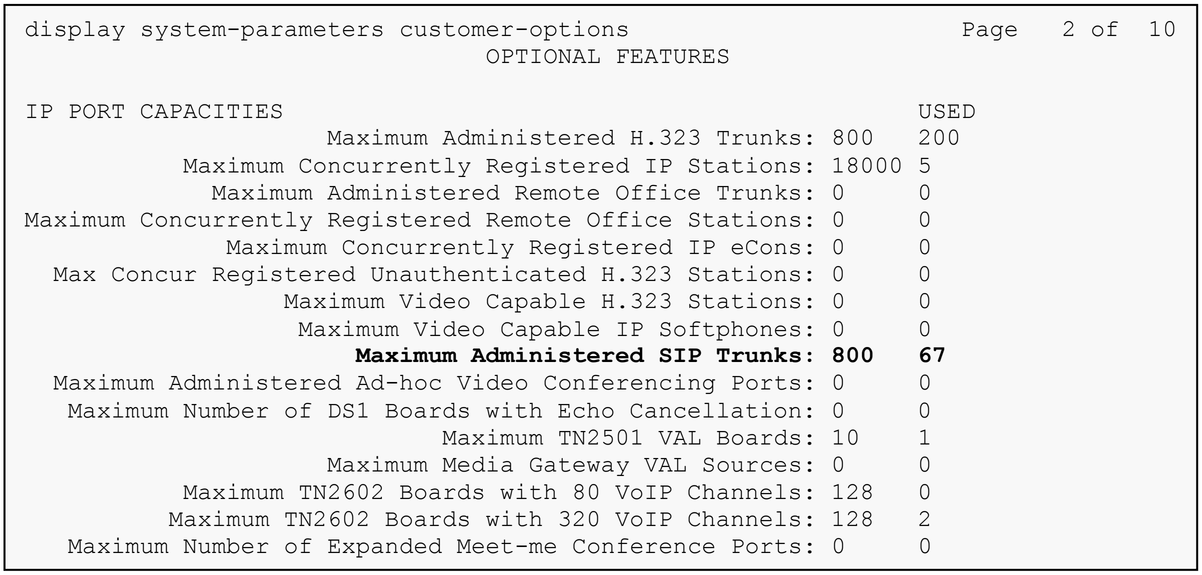
5. Configure Avaya Aura® Communication Manager

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

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 800 SIP trunks are available and 67 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.



```
display system-parameters customer-options                      Page   2 of  10
                                   OPTIONAL FEATURES

IP PORT CAPACITIES                                                   USED
                     Maximum Administered H.323 Trunks: 800   200
           Maximum Concurrently Registered IP Stations: 18000 5
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 800   67
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

5.2. System Features

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

```
change system-parameters features                              Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

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

```
change system-parameters features                               Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: UNKNOWN
  CPN/ANI/ICLID Replacement for Unavailable Calls: UNKNOWN

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

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

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the CLAN circuit pack ***(clan1***) and for the SBC (***SP-AuraSBC1***). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SP-AuraSBC1         10.32.128.12
clan1               10.1.2.233
default             0.0.0.0
medpro1             10.1.2.235
procr                 .  .  .
procr1              10.1.2.11
procr2              10.1.2.21
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, G.711mu was tested using ip-codec-set 4. To this codec, enter ***G.711MU*** in the **Audio Codec** column of the table. Default values can be used for all other fields.

```
change ip-codec-set 4                                             Page   1 of   2

                          IP Codec Set

    Codec Set: 4

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

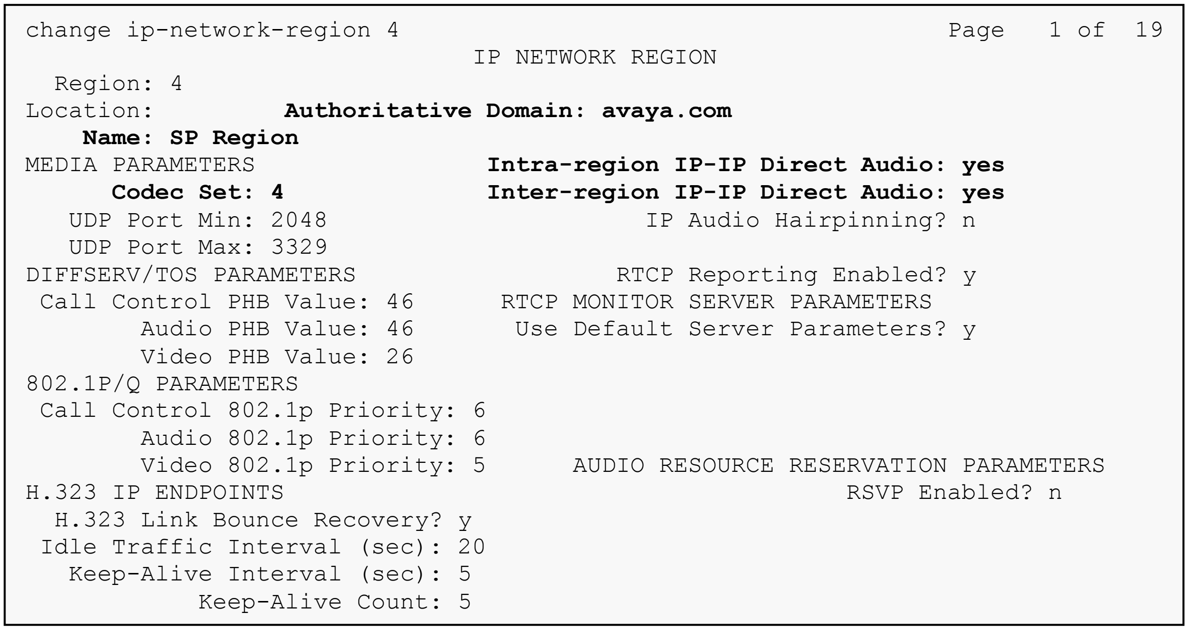
On **Page 2**, set the **Fax Mode** to ***off*** since T.38 fax is not supported.

```
change ip-codec-set 4                                             Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                    Mode                Redundancy
    FAX             off                  0
    Modem           off                  0
    TDD/TTY         US                   3
```

5.5. IP Network Region

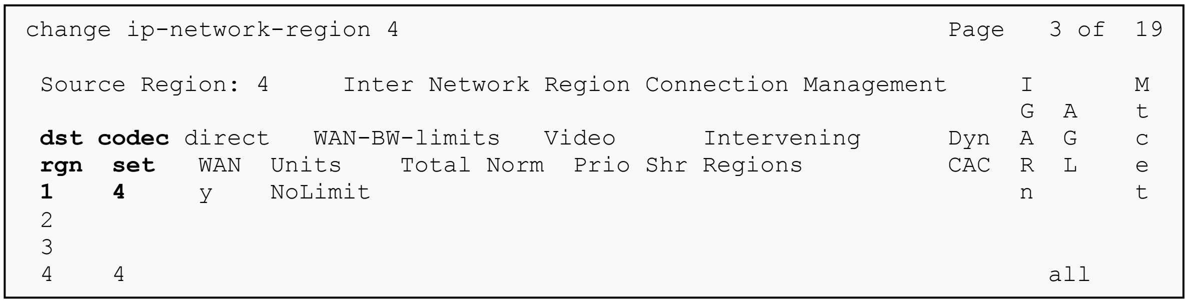
Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 4 was chosen for the service provider trunk. Use the **change ip-network-region 4** command to configure region 4 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***avaya.com***. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to ***yes*.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.



```
change ip-network-region 4                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 4
Location:         Authoritative Domain: avaya.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 4              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                  RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 3**, define the IP codec set to be used for traffic between region 4 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 4 will be used for calls between region 4 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for ip network region 4 will automatically create a complementary table entry on the ip network region 1 form for destination region 4. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).



```
change ip-network-region 4                                     Page   3 of  19

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the SBC for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 35 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tcp***.
- Set the **IMS Enabled** field to ***n***.
- Set the **Near-end Node Name** to ***clan1***. This node name maps to the IP address of the CLAN circuit pack as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***SP-AuraSBC1***. This node name maps to the IP address of the SBC as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to ***5060***. This is the standard TCP port for SIP traffic.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the IP address of the CenturyLink SIP proxy.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.

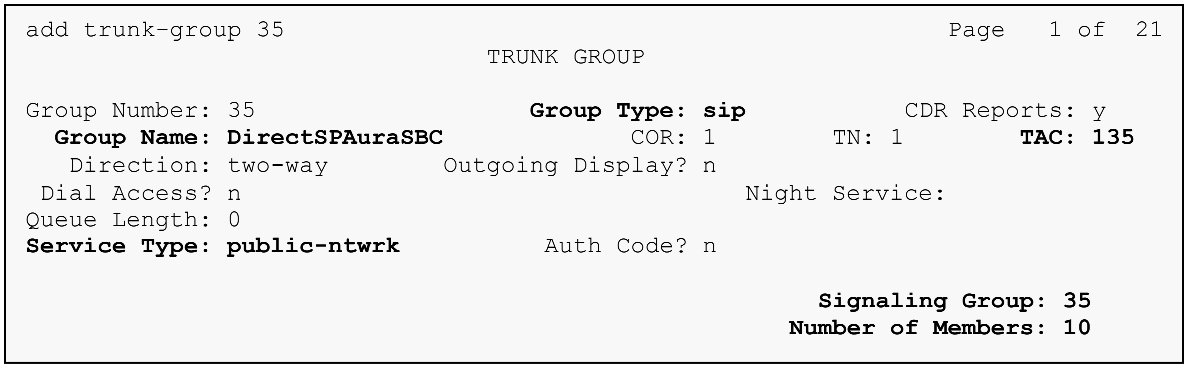
- Set the **Alternate Route Timer** to ***15***. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

```
add signaling-group 35                                            Page   1 of   1
                                SIGNALING GROUP

 Group Number: 35             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n




   Near-end Node Name: clan1                Far-end Node Name: SP-AuraSBC1
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 4
Far-end Domain: 10.2.2.157

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

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 35 was configured using the parameters highlighted below.

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



```
add trunk-group 35                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 35                   Group Type: sip           CDR Reports: y
  Group Name: DirectSPAuraSBC             COR: 1        TN: 1        TAC: 135
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                      Signaling Group: 35
                                                    Number of Members: 10
```

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.6**.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of ***600*** seconds was used.

```
add trunk-group 35                                             Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 15000

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

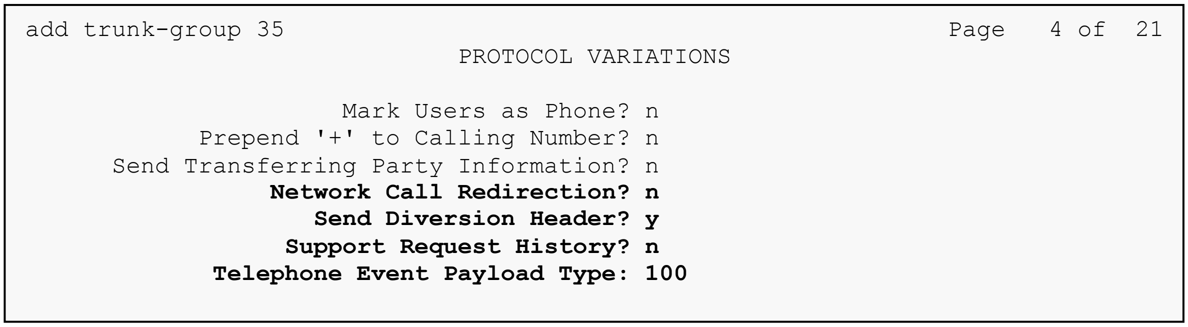
On **Page 3**, set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number (CPN) sent to the far-end.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 35                                             Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y


 Show ANSWERED BY on Display? y
```

On **Page 4**, the **Network Call Redirection** field may be set to ***n*** or ***y***. If set to ***n***, Communication Manager will not attempt to use the SIP REFER method to redirect inbound calls back to the PSTN. If set to ***y***, Communication Manager will use the SIP REFER method to redirect inbound calls back to the PSTN. Set the **Send Diversion Header** field to ***y*** and the **Support Request History** field to ***n***. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to ***100***, the value preferred by CenturyLink.

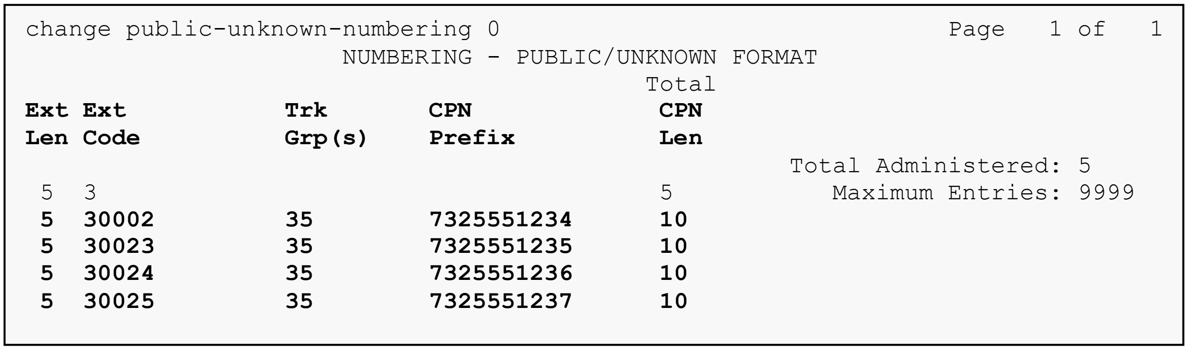


```
add trunk-group 35                                              Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? y
                  Support Request History? n
              Telephone Event Payload Type: 100
```

5.8. Calling Party Information

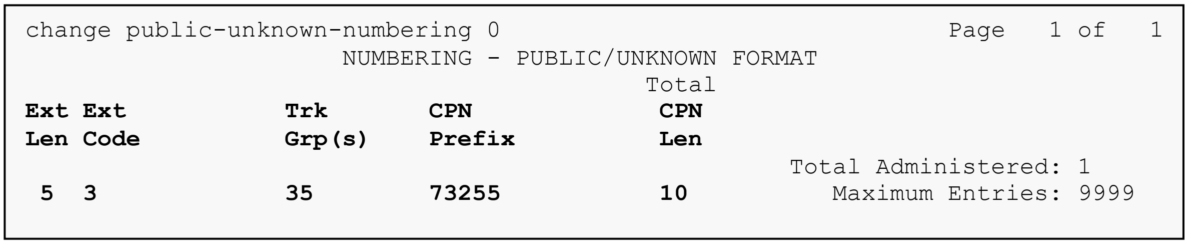
The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, four DID numbers were assigned for testing. These four numbers were assigned to the four extensions 30002, 30023, 30024 and 30025. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these four extensions.



```
change public-unknown-numbering 0                               Page   1 of   1
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 5
 5  3                                       5           Maximum Entries: 9999
 5  30002         35        7325551234      10
 5  30023         35        7325551235      10
 5  30024         35        7325551236      10
 5  30025         35        7325551237      10
```

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



```
change public-unknown-numbering 0                               Page   1 of   1
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 1
 5  3             35        73255           10          Maximum Entries: 9999
```

5.9. Outbound Routing

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

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

       Dialed   Total  Call    Dialed   Total  Call      Dialed   Total  Call
       String   Length Type    String   Length Type      String   Length Type
     1            3    dac
     2            5    ext
     222          5    aar
     3            5    ext
     3234         7    ext
     4            5    ext
     5            5    ext
     6            5    ext
     7            7    ext
     8            1    fac
     9            1    fac
     *            3    fac
     #            3    fac
```

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

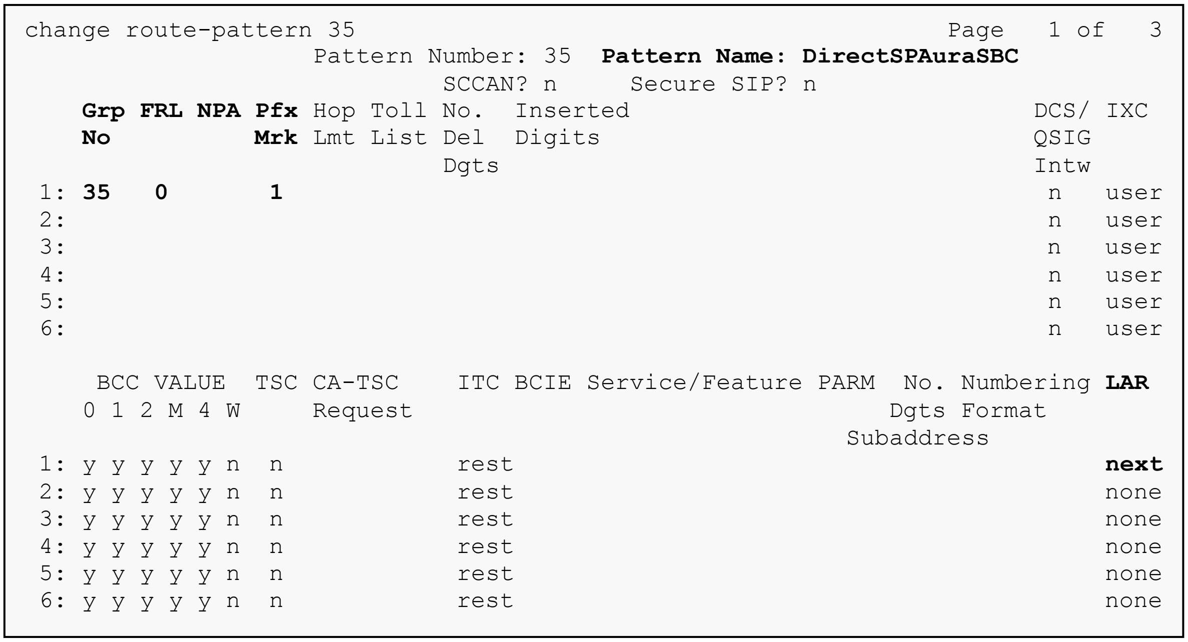
```
change feature-access-codes                                     Page   1 of   8
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *01
         Abbreviated Dialing List2 Access Code: *02
         Abbreviated Dialing List3 Access Code: *03
Abbreviated Dial - Prgm Group List Access Code: *04
                      Announcement Access Code: *05
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *13    All: *11    Deactivation: *12
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 35 which contains the SIP trunk to the service provider (as defined next).

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

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    0                     1    1      35       op           n
    0                     11   11     35       op           n
    00                    2    2      35       op           n
    011                   10   18     35       intl         n
    1800                  11   11     35       fpna         n
    1877                  11   11     35       fpna         n
    1908                  11   11     35       fpna         n
    411                   3    3      35       svcl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 35 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 35 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: ***1*** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers.
- **LAR**: ***next***



```
change route-pattern 35                                         Page   1 of   3
                    Pattern Number: 35  Pattern Name: DirectSPAuraSBC
                             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: 35   0       1                                                     n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

5.10. Inbound Routing

Inbound routing is accomplished by performing incoming call handling treatment on the SIP trunk. Use the **change inc-call-handling-trmt trunk-group 35** command to map an incoming DID number on trunk 35 to an internal extension.

- Set the **Service/Feature** field to ***public-ntwrk***.
- Set **Number Len** to the length of the incoming DID number.
- Set **Number Digits** to the DID number to be mapped.
- Set the **Del** field to the number of digits to be deleted from the incoming number. In the case of the compliance test, all 10 digits are deleted to be replaced with an internal extension.
- Set the **Insert** field to the digits to be inserted. In the case of the compliance test, this is the internal extension to which the incoming DID number is being mapped.
- Repeat for each DID number provided by the service provider.

```
change inc-call-handling-trmt trunk-group 35                        Page   1 of  30
                          INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 7325551234       10  30000
 public-ntwrk    10 7325551235       10  30023
 public-ntwrk    10 7325551236       10  30024
 public-ntwrk    10 7325551237       10  30025
```

6. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® Session Border Controller. This configuration is done in two parts. The first part is done during the SBC installation via the installation wizard. These Application Notes will not cover the SBC installation in its entirety but will include the use of the installation wizard. For information on installing the Avaya Aura® System Platform and the loading of the SBC template see [1] and [5].

The second part of the configuration is done after the installation is complete using the SBC web interface. The resulting SBC configuration file is shown in **Appendix A**.

6.1. Installation Wizard

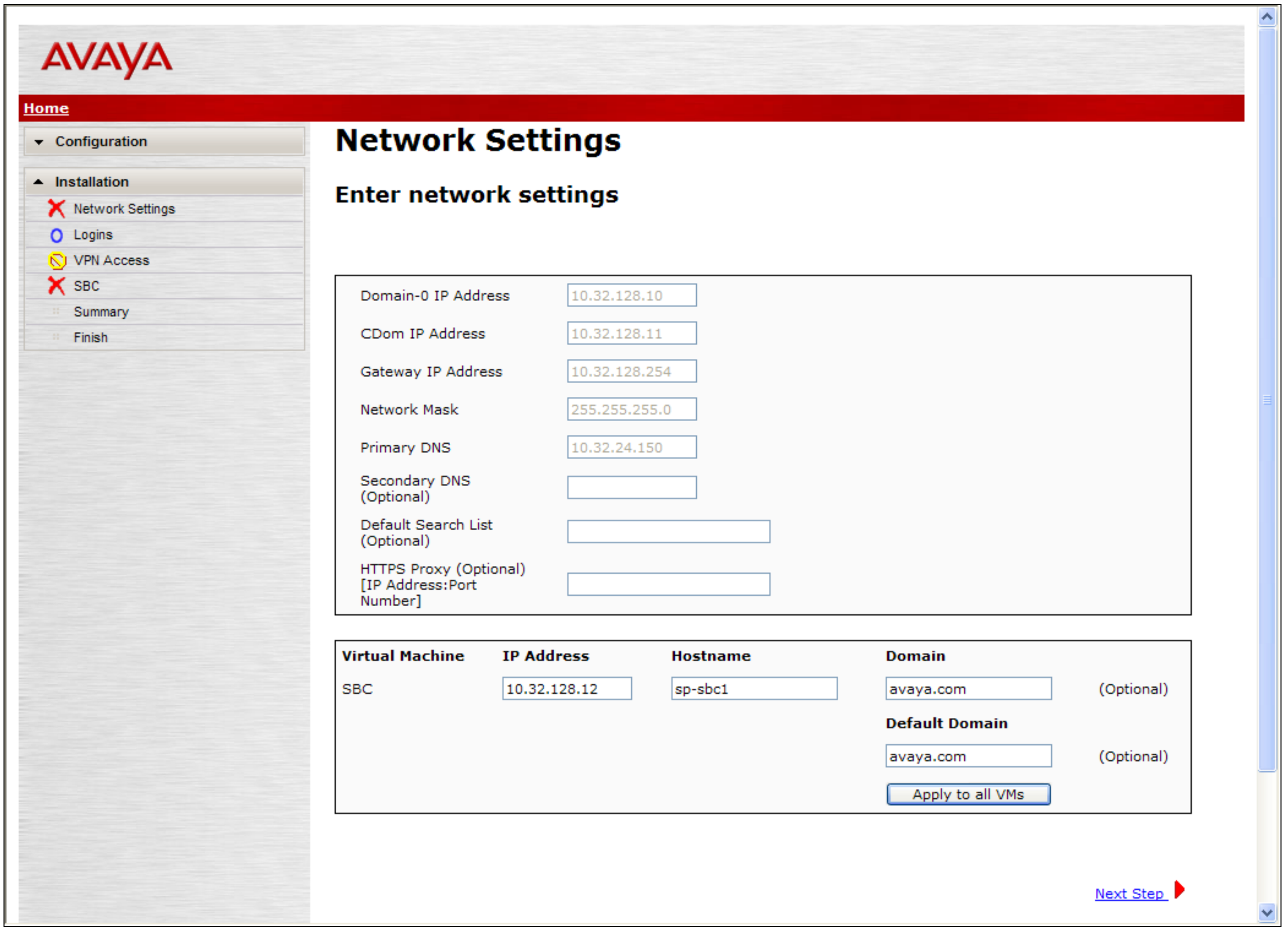
During the installation of the SBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the SBC.

6.1.1. Network Settings

The first screen of the installation wizard is the **Network Settings** screen. Fill in the fields as described below and shown in the following screen:

- **IP Address**: Enter the IP address of the private side of the SBC.
- **Hostname**: Enter the host name of the SBC.
- **Domain**: Enter the domain of the host name provided.
- **Default Domain**: Enter the domain of the host name provided.

Click the **Apply to all VMs** button. Click **Next Step** to continue.



Network Settings

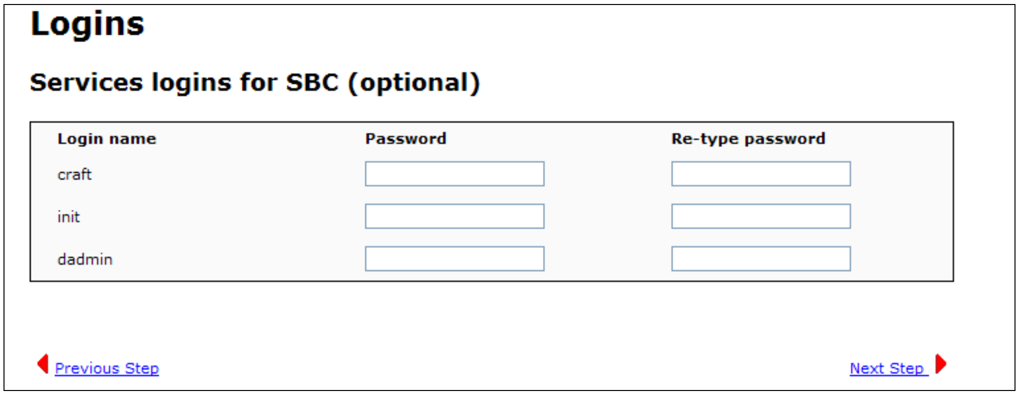
Enter network settings

Domain-0 IP Address	10.32.128.10
CDom IP Address	10.32.128.11
Gateway IP Address	10.32.128.254
Network Mask	255.255.255.0
Primary DNS	10.32.24.150
Secondary DNS (Optional)	
Default Search List (Optional)	
HTTPS Proxy (Optional) [IP Address:Port Number]	

Virtual Machine	IP Address	Hostname	Domain	
SBC	10.32.128.12	sp-sbc1	avaya.com	(Optional)
			Default Domain	
			avaya.com	(Optional)

6.1.2. Service Logins

Optionally, logins can be created for the following login names ***craft***, ***init***, and ***dadmin***. To create the login, simply enter and re-enter a password for the login to be created in the screen below. The creation of a service login was not required for the compliance test. Click **Next Step** to continue.



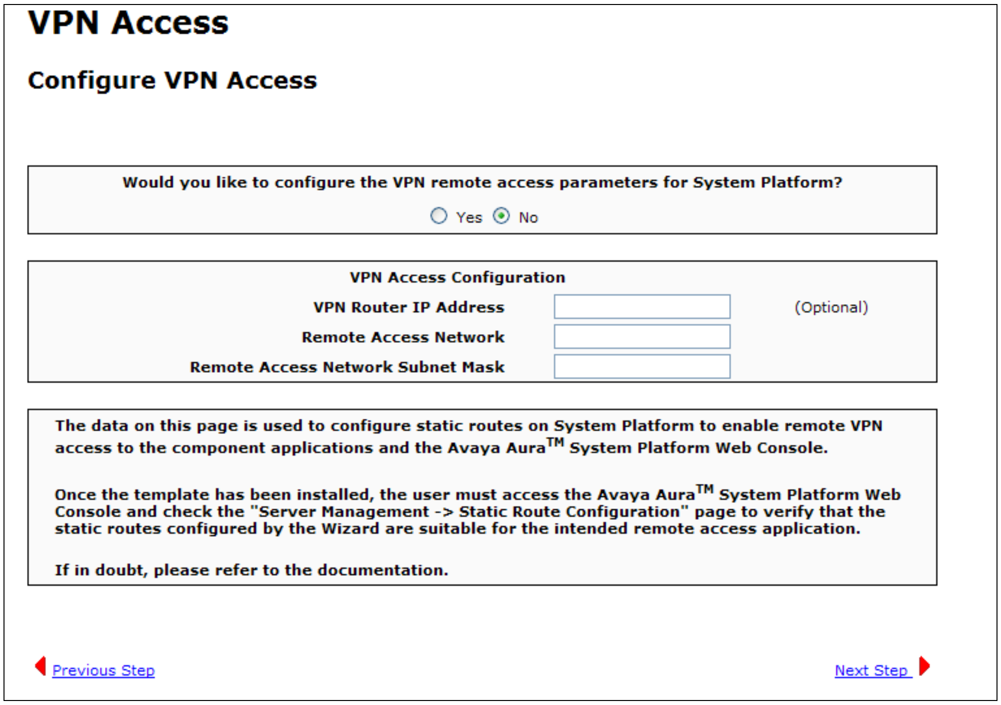
Logins

Services logins for SBC (optional)

Login name	Password	Re-type password
craft		
init		
dadmin		

6.1.3. VPN Access

VPN remote access to the SBC was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?** Click **Next Step** to continue.



VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

○ Yes ● No

VPN Access Configuration

VPN Router IP Address		(Optional)
Remote Access Network		
Remote Access Network Subnet Mask		

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

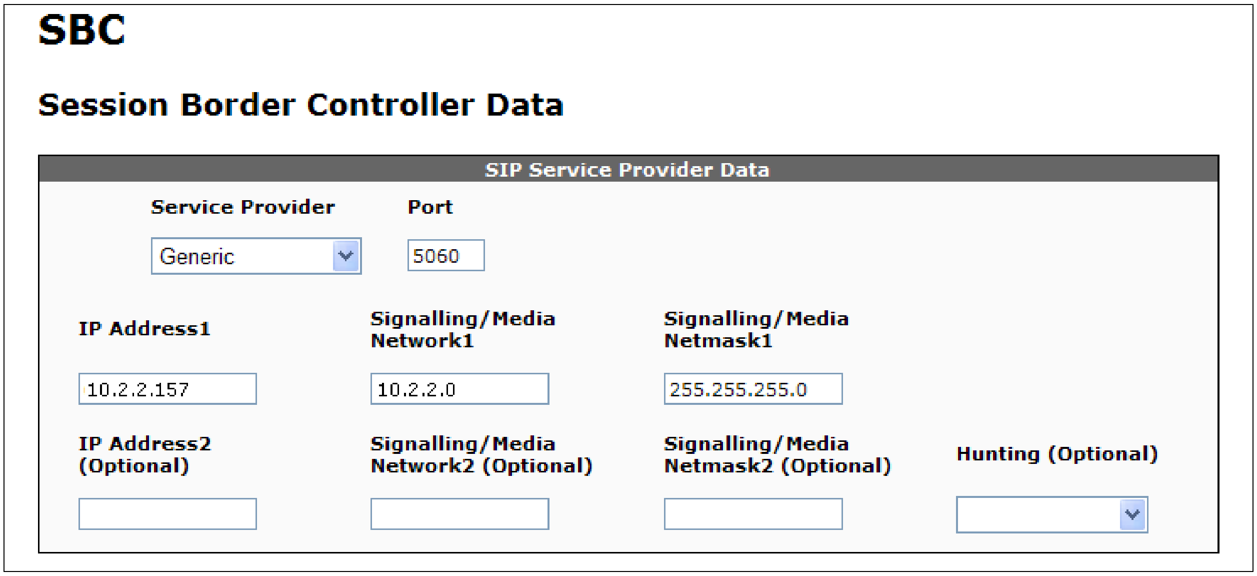
6.1.4. SBC

On the **SBC** screen, fill in the fields as described below and shown in the following screen:

In the **SIP Service Provider Data** section:

- **Service Provider**: From the pull-down menu, select the name of the service provider to which the SBC will connect. This will allow the wizard to create a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for CenturyLink. Thus, **Generic** was chosen instead and further customization was done manually after the wizard was complete.
- **Port**: Enter the port number that the service provider uses to listen for SIP traffic.
- **IP Address1**: Enter the IP address of the SIP proxy of the service provider.
- **Signalling/Media Network1**: Enter the network address of the network where media traffic will originate from the service provider.
- **Signalling/Media Netmask1**: Enter the netmask corresponding to the **Media Network**.

Default values may be used for all other fields. Scroll down to continue.



SBC

Session Border Controller Data

SIP Service Provider Data

Service Provider: Generic

Port: 5060

IP Address1: 10.2.2.157

Signalling/Media Network1: 10.2.2.0

Signalling/Media Netmask1: 255.255.255.0

IP Address2 (Optional):

Signalling/Media Network2 (Optional):

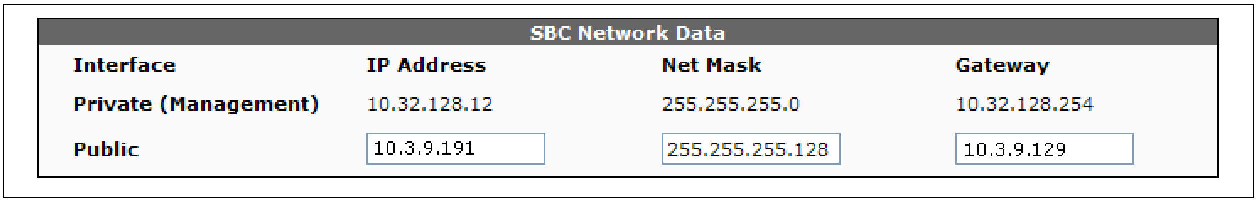
Signalling/Media Netmask2 (Optional):

Hunting (Optional):

Further down on the same **SBC** screen, fill in the fields as described below:

In the **SBC Network Data** section:

- **Public IP Address**: Enter the IP address of the public side of the SBC.
- **Public Net Mask**: Enter the netmask associated with the public network to which the SBC connects.
- **Public Gateway**: Enter the default gateway of the public network.



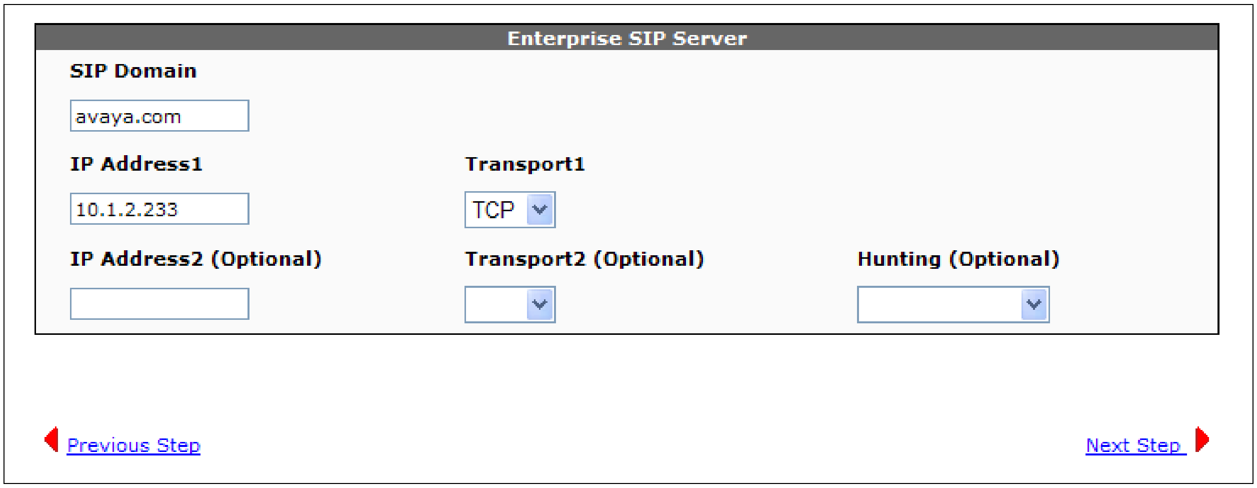
SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	10.32.128.12	255.255.255.0	10.32.128.254
Public	10.3.9.191	255.255.255.128	10.3.9.129

In the **Enterprise SIP Server** section:

- **SIP Domain** Enter the enterprise SIP domain.
- **IP Address1**: Enter the IP address of the Enterprise SIP Server to which the SBC will connect. In the case of the compliance test, this is the IP address of the Communication Manager CLAN board.
- **Transport1**: From the pull-down menu, select the transport protocol to be used for SIP traffic between the SBC and Communication Manager.

Default values may be used for all other fields. Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to continue to the final step.



Enterprise SIP Server

SIP Domain: avaya.com

IP Address1: 10.1.2.233

Transport1: TCP

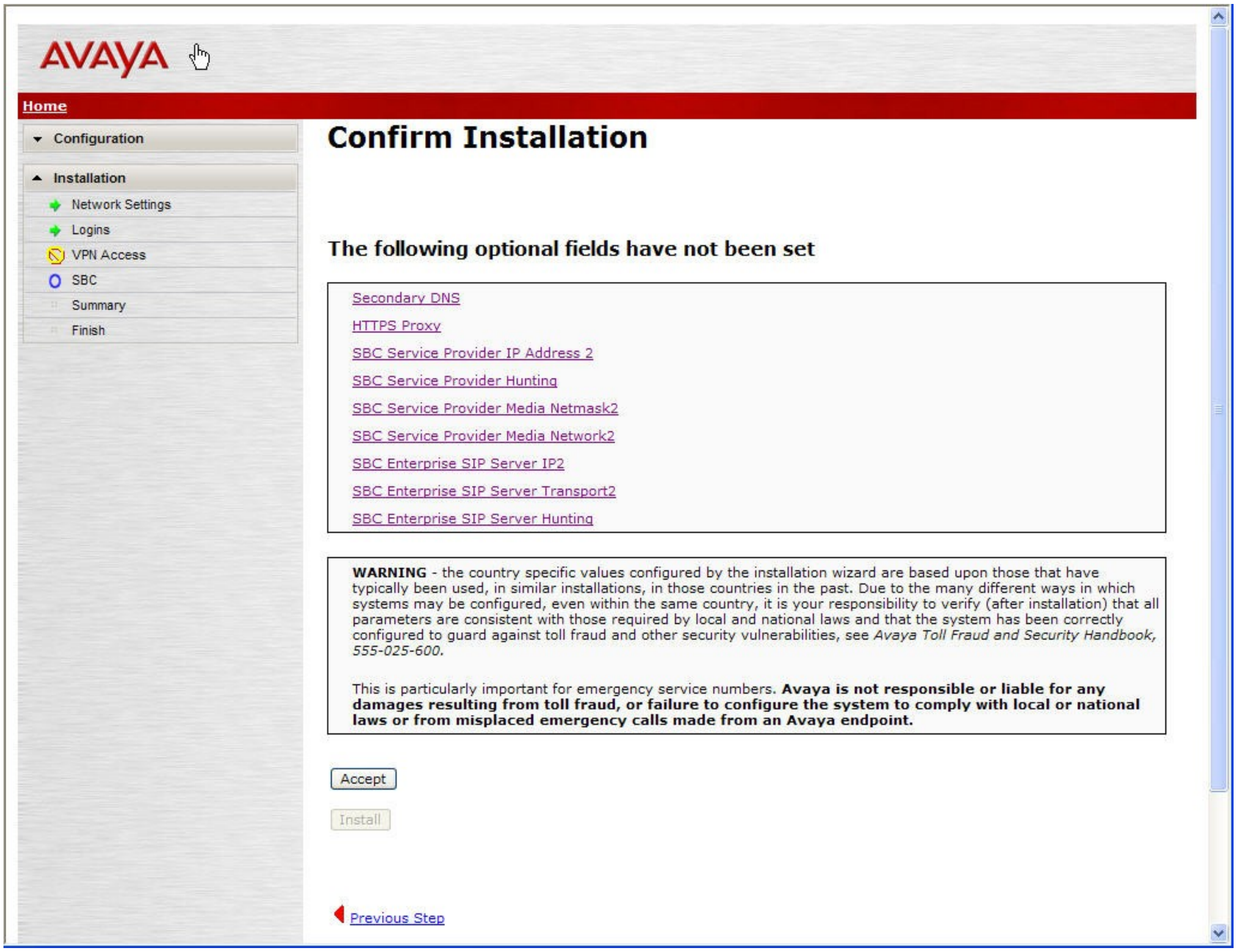
IP Address2 (Optional):

Transport2 (Optional):

Hunting (Optional):

6.1.5. Confirm Installation

The **Confirm Installation** screen will indicate if any required or optional fields have not been set. All required fields should be set. If not, click **Previous Step** to navigate to the necessary screen to set the required field. Otherwise, click **Accept**. This will change the state of the **Install** button on this same page so that it is no longer grayed-out. Click **Install** to finish the wizard and to continue the overall template installation.



Confirm Installation

The following optional fields have not been set

- Secondary DNS
- HTTPS Proxy
- SBC Service Provider IP Address 2
- SBC Service Provider Hunting
- SBC Service Provider Media Netmask2
- SBC Service Provider Media Network2
- SBC Enterprise SIP Server IP2
- SBC Enterprise SIP Server Transport2
- SBC Enterprise SIP Server Hunting

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook, 555-025-600.*

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

7. CenturyLink SIP Trunking Configuration

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

During the signup process, CenturyLink will require that the customer provide the public IP address used to reach the SBC at the edge of the enterprise. CenturyLink will provide the IP address of the CenturyLink SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager, and the SBC configuration discussed in the previous sections.

8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

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

Troubleshooting:

Communication Manager:

- **list trace station** <extension number> - Traces calls to and from a specific station.
- **list trace tac** <trunk access code number> - Traces calls over a specific trunk group.
- **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
- **status trunk** <trunk access code number> - Displays trunk group information.
- **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, and Avaya Aura® Session Border Controller to CenturyLink SIP Trunking. CenturyLink SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. CenturyLink SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. CenturyLink SIP Trunking passed compliance testing. Please refer to **Section 2.2** for any exceptions or workarounds.

10. 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, June 2010.

[2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.

[3] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* May 2009, *D*ocument Number 555-245-205.

[5] *Avaya Aura® Session Border Controller – Installation Guide,* November 2010.

[6] *Avaya Aura® Session Border Controller System Administration,* September 2010.

[7] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.

[8] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.

[9] *Avaya one-X® Communicator Getting Started, August 2010.*

[10] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/

[11] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

11. Appendix A: Avaya Aura® Session Border Controller Configuration File

```
#
#  Copyright (c) 2004-2010  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 16:09:33 Thu 2011-03-17
#
config cluster
 config box 1
  set hostname sp-sbc1.avaya.com
  set timezone America/New_York
  set name sp-sbc1.avaya.com
  set identifier 00:ca:fe:46:46:93
  config interface eth0
   config ip inside
    set ip-address static 10.32.128.12/24
    config ssh
    return
    config snmp
     set trap-target 10.32.128.11 162
     set trap-filter generic
     set trap-filter dos
     set trap-filter sip
     set trap-filter system
    return
    config web
    return
    config web-service
     set protocol https 8443
     set authentication certificate "vsp\tls\certificate ws-cert"
    return
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
    return
    config icmp
    return
    config media-ports
    return
    config routing
     config route Default
      set gateway 10.32.128.254
     return
     config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.32.128.10
     return
     config route Static1
      set admin disabled
     return
   config route Static2
    set admin disabled
   return
   config route Static3
    set admin disabled
   return
   config route Static4
    set admin disabled
   return
   config route Static5
    set admin disabled
   return
   config route Static6
    set admin disabled
   return
   config route Static7
    set admin disabled
   return
  return
 return
return
config interface eth2
 config ip outside
  set ip-address static 10.3.9.191/25
  config ssh
  return
  config web
  return
  config sip
   set udp-port 5060 "" "" any 0
  return
  config icmp
  return
  config media-ports
  return
  config routing
   config route Default
    set admin disabled
   return
   config route external-sip-media-1
    set destination network 10.2.2.0/24
    set gateway 10.3.9.129
   return
  return
  config kernel-filter
   config allow-rule allow-sip-udp-from-peer-1
    set destination-port 5060
    set source-address/mask 10.2.2.0/24
    set protocol udp
   return
   config deny-rule deny-all-sip
    set destination-port 5060
   return
  return
 return
return
```

```
  config cli
   set prompt sp-sbc1.avaya.com
  return
 return
return

config services
 config event-log
  config file access
   set filter access info
   set count 3
  return
  config file system
   set filter system info
   set count 3
  return
  config file errorlog
   set filter all error
   set count 3
  return
  config file db
   set filter db debug
   set filter dosDatabase info
   set count 3
  return
  config file management
   set filter management info
   set count 3
  return
  config file peer
   set filter sipSvr info
   set count 3
  return
  config file dos
   set filter dos alert
   set filter dosSip alert
   set filter dosTransport alert
   set filter dosUrl alert
   set count 3
  return
  config file krnlsys
   set filter krnlsys debug
   set count 3
  return
 return
return

config master-services
 config database
  set media enabled
 return
return

config vsp
 set admin enabled
 config default-session-config
 config media
  set anchor enabled
  set rtp-stats enabled
 return
 config sip-directive
  set directive allow
 return
 config log-alert
  set apply-to-methods-for-filtered-logs
 return
 config third-party-call-control
  set admin enabled
  set handle-refer-locally disabled
 return
return
config tls
 config default-ca
  set ca-file /cxc/certs/sipca.pem
 return
 config certificate ws-cert
  set certificate-file /cxc/certs/ws.cert
 return
 config certificate aasbc.p12
  set certificate-file /cxc/certs/aasbc.p12
  set passphrase-tag aasbc-cert-tag
 return
return
config session-config-pool
 config entry ToTelco
  config to-uri-specification
   set host next-hop
   set user-param keep
  return
  config from-uri-specification
   set host local-ip
   set user-param keep
  return
  config request-uri-specification
   set host next-hop
   set user-param keep
  return
  config p-asserted-identity-uri-specification
   set host local-ip
   set user-param keep
  return
 return
 config entry ToPBX
  config to-uri-specification
   set host next-hop-domain
  return
  config request-uri-specification
   set host next-hop-domain
  return
 return
 config entry Discard
  config sip-directive
```

```
   return
  return
 return
 config dial-plan
  config route Default
   set priority 500
   set location-match-preferred exclusive
   set session-config vsp\session-config-pool\entry Discard
  return
  config source-route FromTelco
   set peer server "vsp\enterprise\servers\sip-gateway PBX"
   set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
   set peer server "vsp\enterprise\servers\sip-gateway Telco"
   set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
 return
 config enterprise
  config servers
   config sip-gateway PBX
    set domain avaya.com
    set failover-detection ping
    set ping-interval 30
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
     config server PBX1
      set host 10.1.2.233
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set failover-detection ping
    set ping-interval 30
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
     config server Telco1
      set host 10.2.2.157
     return
    return
   return
  return
 return
 config dns
  config resolver
   config server 10.32.24.150
   return
  return
 return
 config settings
  set read-header-max 8191
 return
return
```

```
config external-services
return

config preferences
 config gui-preferences
 return
return

config access
 config permissions superuser
  set cli advanced
 return
 config permissions read-only
  set config view
  set actions disabled
 return
 config users
  config user admin
   set password 0x008b1aa0559fa5adc1cd4c692f5a73c5dd5b2f3d1df8fd632fbf9ea981
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x00a2eeeaecdb573565634107edc9012890961d7f408f59cbbf80e5b827
   set permissions access\permissions read-only
  return
  config user craft
   set password 0x0057181e3fa2b43e7d9f2ec6ea4d7998e992868f970a2077b6e289a924
   set permissions access\permissions superuser
  return
 return
return

config features
return
```

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.