Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the PAETEC Dynamic IP SIP Trunk Service (BroadSoft Platform) with Avaya Aura® Communication Manager and Avaya Aura® Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the PAETEC Dynamic IP SIP Trunk Service and an Avaya SIP-enabled enterprise solution. PAETEC can offer the Dynamic IP SIP Trunk Service using several different platform technologies in the PAETEC network. These Application Notes correspond to the Dynamic IP SIP Trunk Service offered using a Broadsoft platform in the network. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Communication Manager and various Avaya endpoints. The Avaya Aura® Session Manager is not used in this configuration.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the PAETEC Dynamic IP SIP Trunk Service and an Avaya SIP-enabled enterprise solution. PAETEC can offer the Dynamic IP SIP Trunk Service using several different platform technologies in the PAETEC network. These Application Notes correspond to the Dynamic IP SIP Trunk Service offered using a Broadsoft platform in the network. The Avaya solution consists of Avaya Aura® Session Border Controller (SBC), Avaya Aura® Communication Manager and various Avaya endpoints. The Avaya Aura® Session Manager is not used in this configuration. As a result, SIP endpoints are not supported.

Customers using this Avaya SIP-enabled enterprise solution with the PAETEC Dynamic IP SIP Trunk Service 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.

1.1. Interoperability Compliance Testing

A simulated enterprise site using Communication Manager and the SBC was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to the Dynamic IP SIP Trunk Service.

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test. As previously noted, SIP endpoints are not supported in this configuration.

- Incoming PSTN calls to various phone types
  Phone types included 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
  Phone types included 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 one-X Communicator was tested.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls and local directory assistance (411)
- Codecs G.729A, G.711MU and G.711A.
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, transfer, and conference

- Off-net call forwarding and mobility (extension to cellular)

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- T.38 Fax not supported.
- Network Call Redirection using the SIP REFER method or a 302 response is supported but was not tested.

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

- **Inbound Calling Party Number (CPN) Block:** To accept an incoming call, Communication Manager requires the PAI header to contain a recognizable domain. In the absence of a PAI header, Communication Manager will perform the same check on the From header. PAETEC does not send a PAI header and in the case of an inbound call with CPN block enabled, the domain in the From header is purposely altered. Thus, to allow these calls to succeed, a SIP header modification was added to the SBC to overwrite the incoming From header with a value recognizable to Communication Manager (**Section 5.2.5**). This modification occurs on all incoming INVITEs, not just the ones with CPN block enabled. When using a configuration with Session Manager, this modification is not necessary. Session Manager will generate a PAI header for the INVITE sent to Communication Manager if the incoming INVITE from the service provider does not contain one.
- **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.
- **Avaya one-X® Communicator (telecommuter mode)**: If an inbound call is hung-up first by the Avaya one-X® Communicator, this results in a SIP message exchange where a "487 Request terminated" message sent by PAETEC does not receive an ACK from the enterprise. The SBC is not passing the ACK message from its private interface through to the public interface. The blocking of the ACK message in this scenario is not user impacting since it happens after the call is properly torn down.

1.2. Support

For technical support on the Dynamic IP SIP Trunk Service, contact PAETEC using the Customer Care links at www.paetec.com.

2. Reference Configuration

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

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

- Avaya S8300D Server running Communication Manager
- Avaya G450 Media Gateway
- 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.

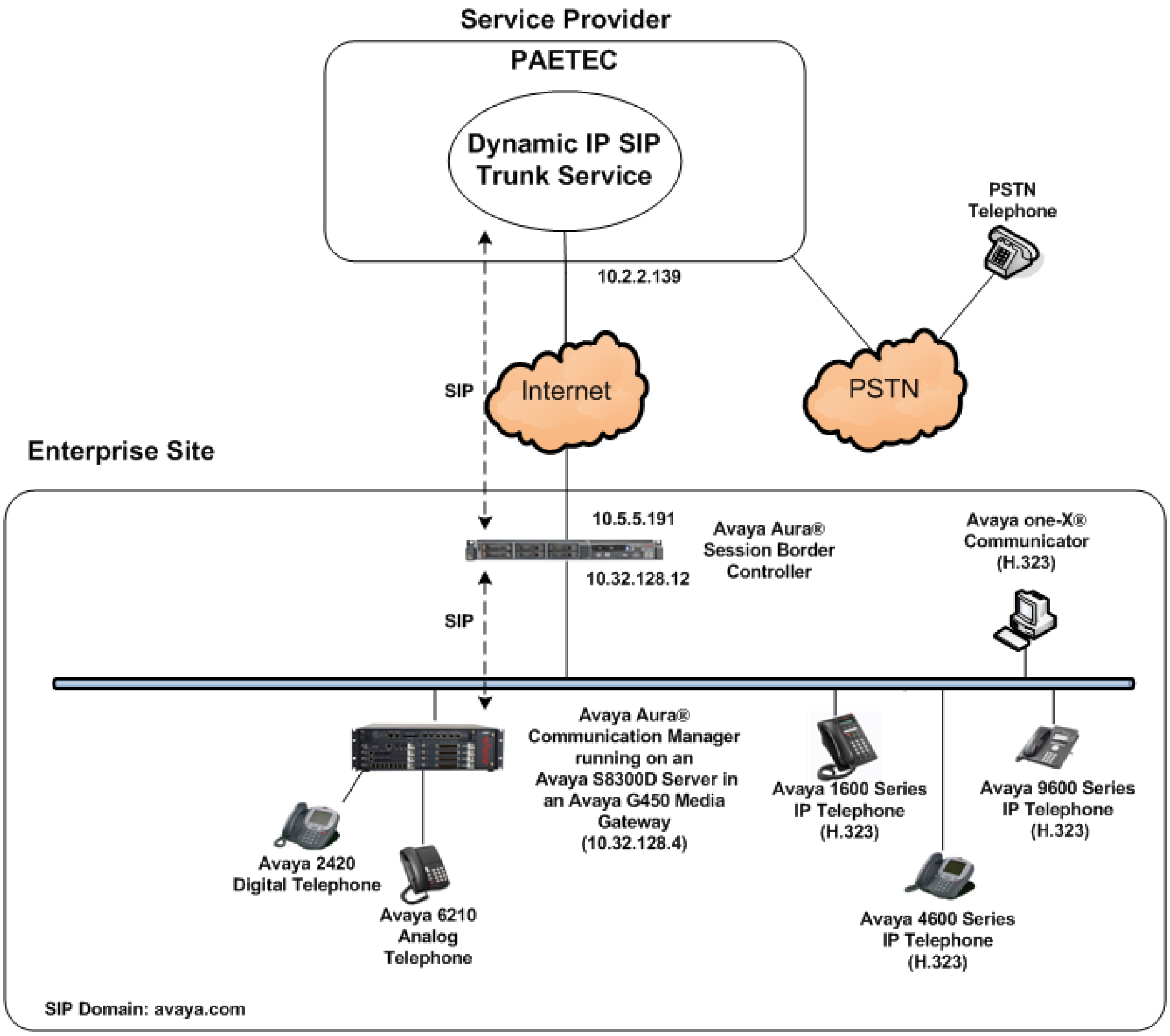


Figure 1: Avaya IP Telephony Network using the Dynamic IP SIP Trunk Service

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. 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 the Dynamic IP SIP Trunk Service.

PAETEC requires outbound toll-free calls to be dialed with 1 + 10 digits while all other North American Numbering Plan (NANP) numbers can be dialed with either 10 digits or 11 digits (1 + 10).

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)). PAETEC sent 10 digits in both the source and destination headers.

3. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on an Avaya S8300D Server	6.0 SP1 (R016x.00.0.345.0-18444) (System Platform 6.0.1.05)
Avaya G450 Media Gateway	30.14.0
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
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura™ Session Border Controller	6.0 (Build SBCT_6.0.0.1.4)
PAETEC SIP Trunking Solution Components	
Component	Release
BroadSoft Platform	14sp9

Table 1: Equipment and Software Tested

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

4. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Dynamic IP SIP Trunk Service. A SIP trunk is established between Communication Manager and the SBC for use by signaling traffic to and from PAETEC. It is assumed the general installation of Communication Manager and the Avaya G450 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.

4.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 SIP trunks are available and 20 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                                USED
                     Maximum Administered H.323 Trunks: 4000  36
           Maximum Concurrently Registered IP Stations: 2400  3
             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  20
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

4.2. System Features

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

```
change system-parameters features                              Page   1 of  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 ***anonymous*** 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: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

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

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

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

4.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8300D Server running Communication Manager ***(procr***) and for the SBC (***auraSBC***). These node names will be needed for defining the service provider signaling group in **Section 4.6**.

```
change node-names ip                                                Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
auraSBC             10.32.128.12
cmm                 10.32.128.4
default             0.0.0.0
procr               10.32.128.4
procr6              ::
```

4.4. 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, ip-codec-set 2 was used for this purpose. The Dynamic IP SIP Trunk Service supports G.729A, G.711MU and G.711A. Thus, these codecs were included in this set, in order of preference. The order of preference is defined by the end customer. Enter ***G.729A***, ***G.711MU*** and ***G.711A*** in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 2

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

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

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

4.5. 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 2 was chosen for the service provider trunk. IP network region 1 is the default IP network region and encompasses the rest of the enterprise. Use the **change ip-network-region 2** command to configure region 2 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 4.4**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              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
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). 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 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 2                                     Page   4 of  20

 Source Region: 2     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    2     y    NoLimit                                             n       t
 2    2                                                                 all
 3
```

4.6. 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 4 was used and was configured using the parameters highlighted below:

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***.
- Set the **Transport Method** to ***tcp***. Set the **Near-end Listen Port** and **Far-end Listen Port** to the default well-known port value of ***5060***.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will be set to ***Others***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Avaya S8300D Server running Communication Manager as defined in **Section 4.3**.
- Set the **Far-end Node Name** to ***auraSBC***. This node name maps to the IP address of SBC as defined in **Section 4.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 4.5**.
- Set the **Far-end Domain** to the IP address of the PAETEC SIP proxy.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to ***15***. This is the amount of time (in seconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending 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 4                                           Page   1 of   1
                                SIGNALING GROUP

 Group Number: 4             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others


   Near-end Node Name: procr                 Far-end Node Name: auraSBC
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 2

Far-end Domain: 10.2.2.139
                                             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                      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 15
```

4.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 4.6**. For the compliance test, trunk group 4 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 **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group shown **Section 4.6**.
- 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 4                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 4                    Group Type: sip           CDR Reports: y
  Group Name: DirectTrkToAuraSBC          COR: 1        TN: 1        TAC: 1004
   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: 4
                                                     Number of Members: 5
```

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 comparable to the **Alternate Route Timer** on the signaling group form described in **Section 4.6**.

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 4                                               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

                                      Delay Call Setup When Accessed Via IGAR? n
```

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

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 4.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 4                                               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

                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

On **Page 4**, set the **Network Call Redirection** field to ***n***. Set the **Send Diversion Header** field to ***y***. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to ***101***, the value preferred by PAETEC.

```
add trunk-group 3                                               Page   4 of  21
                                PROTOCOL VARIATIONS

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


        Convert 180 to 183 for Early Media? n
  Always Use re-INVITE for Display Updates? n
                              Enable Q-SIP? n
```

4.8. 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 4.7**), 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, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 40003, 40005 and 40010. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change public-unknown-numbering 0                                  Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 4
 5  4                                       5        Maximum Entries: 240
 5  40003                   7135554378      10
 5  40005                   7135554379      10    Note: If an entry applies to
 5  40010                   7135554380      10    a SIP connection to Avaya
                                                  Aura(tm) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.
```

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 entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 4 will send the calling party number as the **CPN Prefix** plus the extension number.

```
change public-unknown-numbering 0                                  Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 4
 5  4                       71355           10       Maximum Entries: 240

                                                  Note: If an entry applies to
                                                  a SIP connection to Avaya
                                                  Aura(tm) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.
```

4.9. 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. 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           4   dac
   4           5   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  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       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: *01    All: *02    Deactivation: *03
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 4 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      4        op            n
    0                     11   11     4        op            n
    00                    2    2      4        op            n
    011                   10   18     4        intl          n
    1800                  11   11     4        fpna          n
    1877                  11   11     4        fpna          n
    1908                  11   11     4        fpna          n
    411                   3    3      4        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 4 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 ***4*** 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. All HNPA 10 digit numbers are left unchanged.
- **LAR**: ***next***

```
change route-pattern 4                                              Page   1 of   3
                    Pattern Number: 4   Pattern Name: DirectToAuraSBC
                             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: 4    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
```

4.10. Inbound Routing

Inbound calls directed to a 10-digit DID number must be routed to the proper enterprise extension for termination. Use the **inc-call-handling-trmt trunk-group *x*** command, where ***x*** is the trunk group specified in **Section 4.7** to define the mapping of incoming DID numbers to extensions. Create an entry for each DID assigned to the enterprise. Enter the fields as defined below:

- **Number Len**: Length of the digit string to match on.
- **Number Digits**: The digit string to match on.
- **Del**: The number of digits to delete from the incoming number.
- **Insert**: The number of digits to insert in the resulting number.

One entry in the table will match on each DID assigned to the enterprise. All 10 digits of the incoming number are deleted and replaced with a 5-digit extension.

```
change inc-call-handling-trmt trunk-group 4                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 7135554378       10  40003
 public-ntwrk    10 7135554379       10  40005
 public-ntwrk    10 7135554380       10  40010
```

5. 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].

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**.

5.1. Installation Wizard

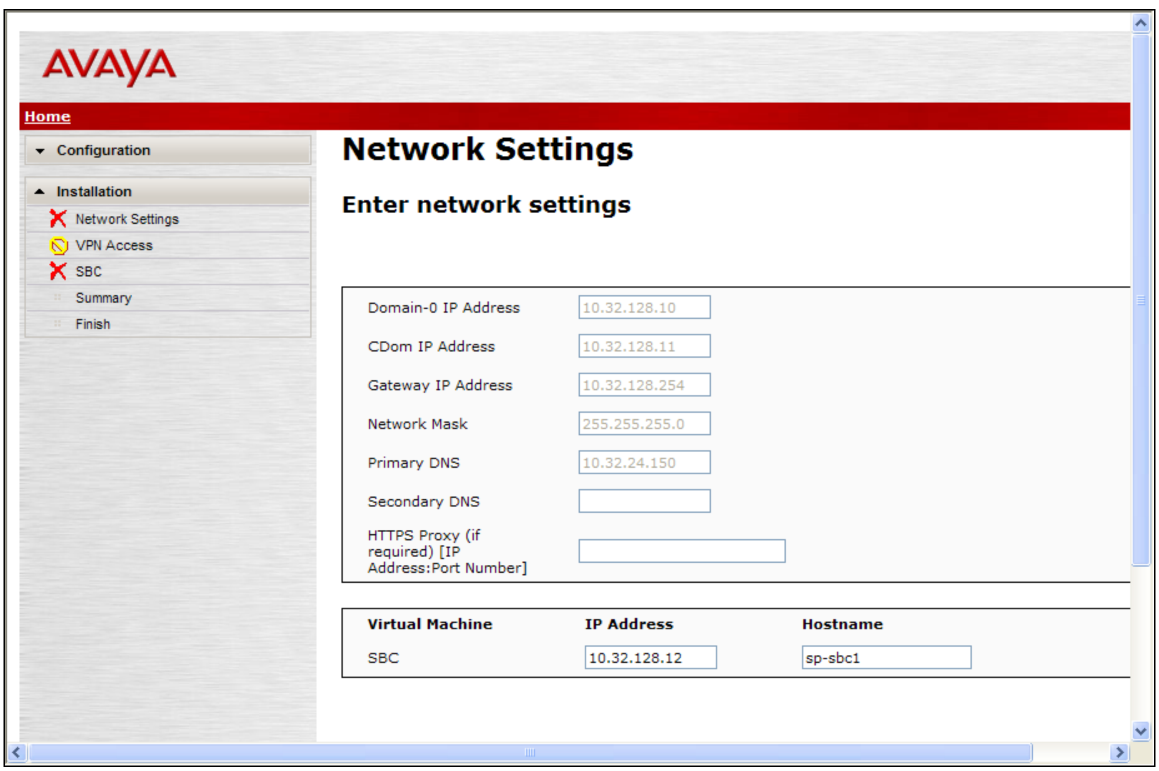
During the installation of the SBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the SBC.

5.1.1. 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 a host name for the SBC.

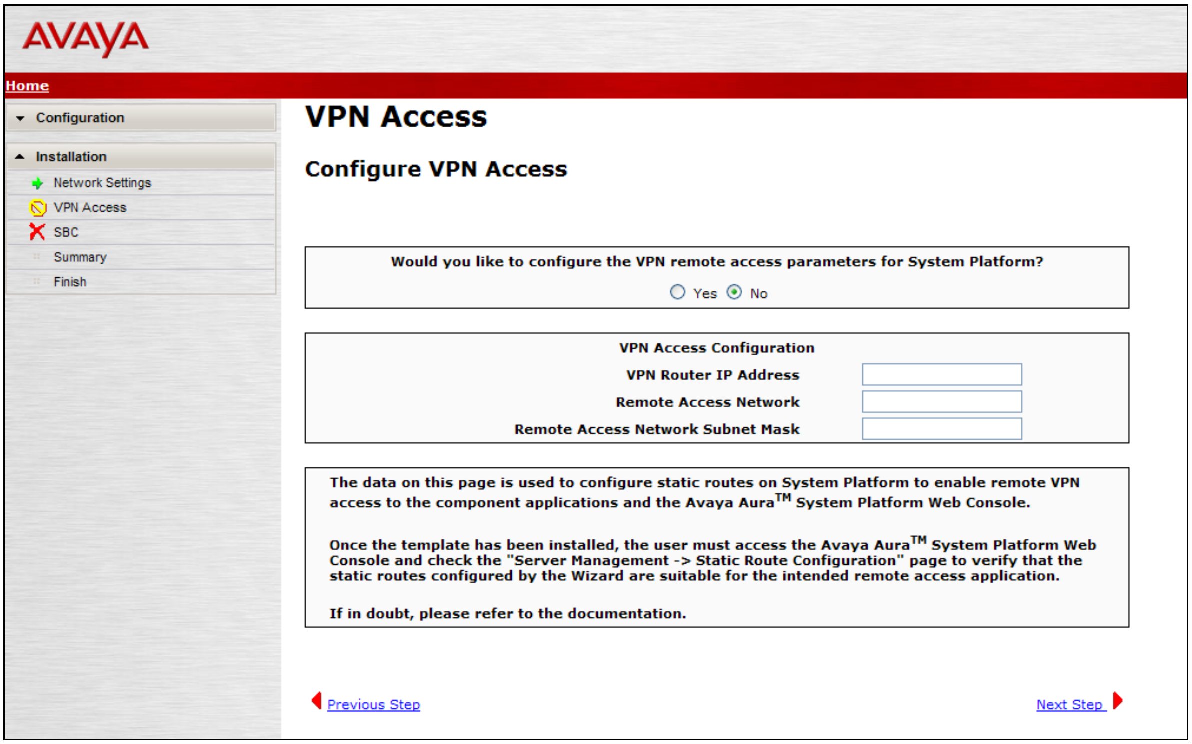
Click **Next Step** (not shown) to continue.



5.1.2. 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.



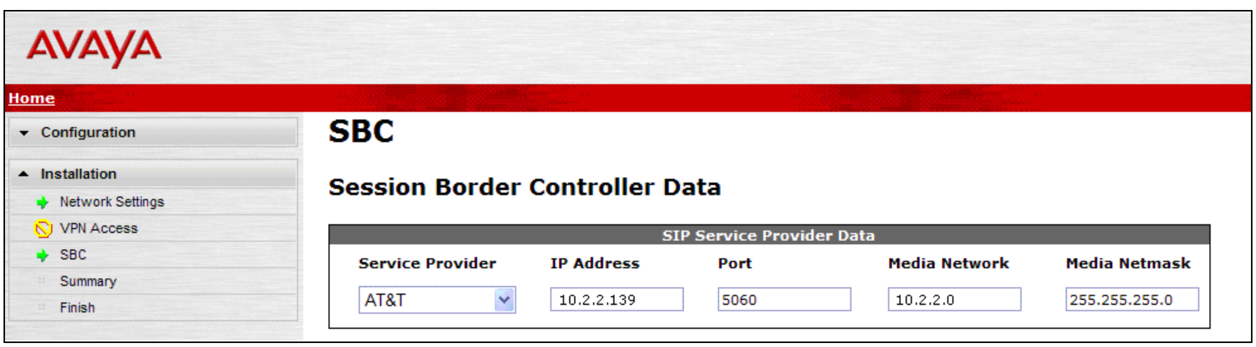
5.1.3. SBC

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 PAETEC. Thus, **AT&T** was chosen instead and further customization was done manually after the wizard was complete.
- **IP Address**: Enter the IP address of the SIP proxy of the service provider. If the service provider has multiple proxies, enter the primary proxy on this screen and additional proxies can be added after installation.
- **Port**: Enter the port number that the service provider uses to listen for SIP traffic.
- **Media Network**: Enter the network address of the network where media traffic will originate from the service provider. If media can originate from multiple networks, enter one network address on this screen and additional networks can be added after installation.
- **Media Netmask**: Enter the netmask corresponding to the **Media Network**.

Scroll down to continue.



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

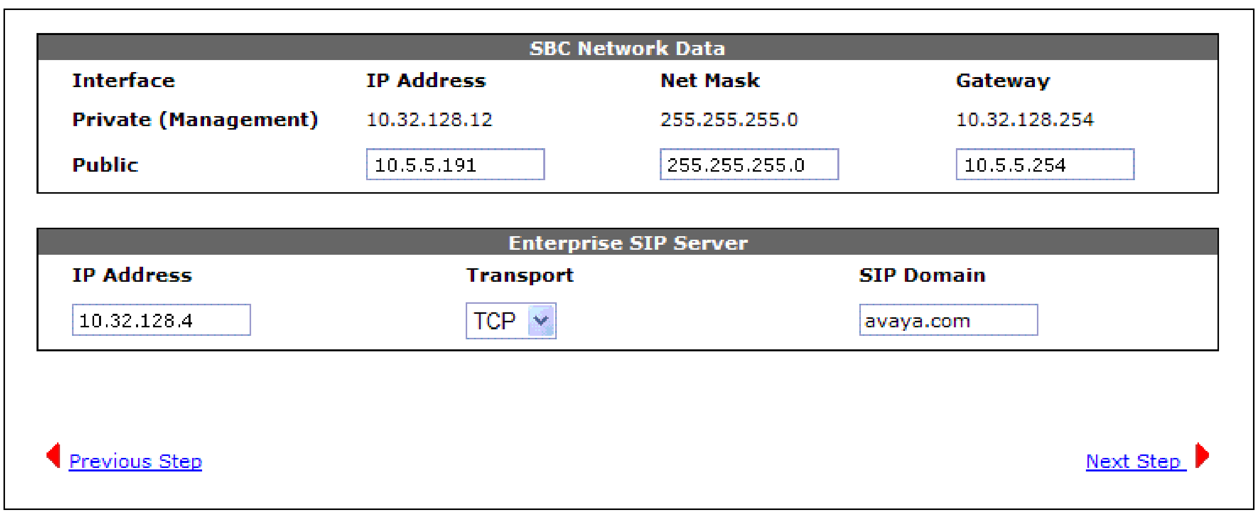
In the **SBC Network Data** section:

- **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.

In the **Enterprise SIP Server** section:

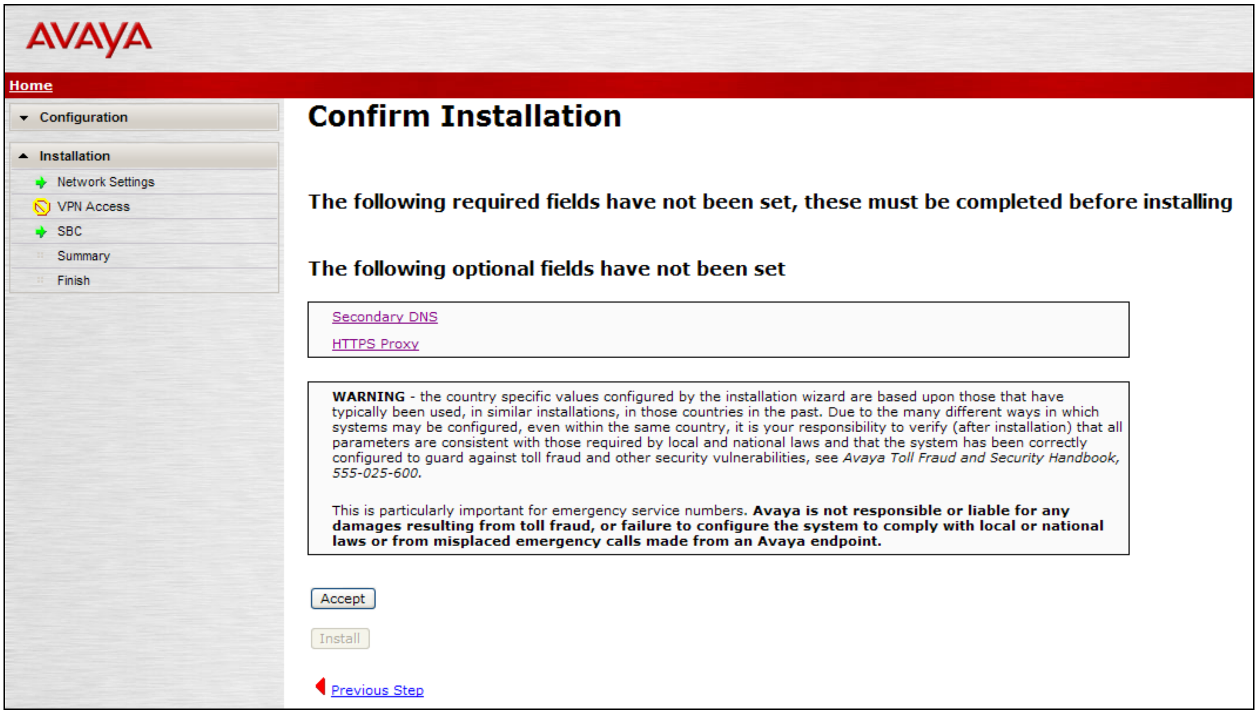
- **IP Address**: Enter the IP address of the Enterprise SIP Server to which the SBC will connect. In the case of the compliance test, this is the IP address of the Communication Manager.
- **Transport**: From the pull-down menu, select the transport protocol to be used for SIP traffic between the SBC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

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.



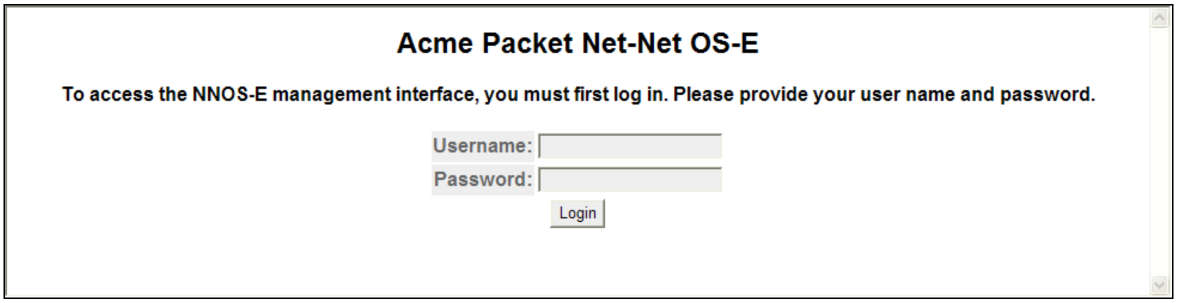
5.1.4. Confirm Installation

The **Confirm Installation** screen will indicate if any required or optional fields have not been set. The list of required fields that have not been set should be empty. If not, click **Previous Step** to navigate to the necessary screen to set the required field. Otherwise, click **Accept** to finish the wizard and to continue the overall template installation.



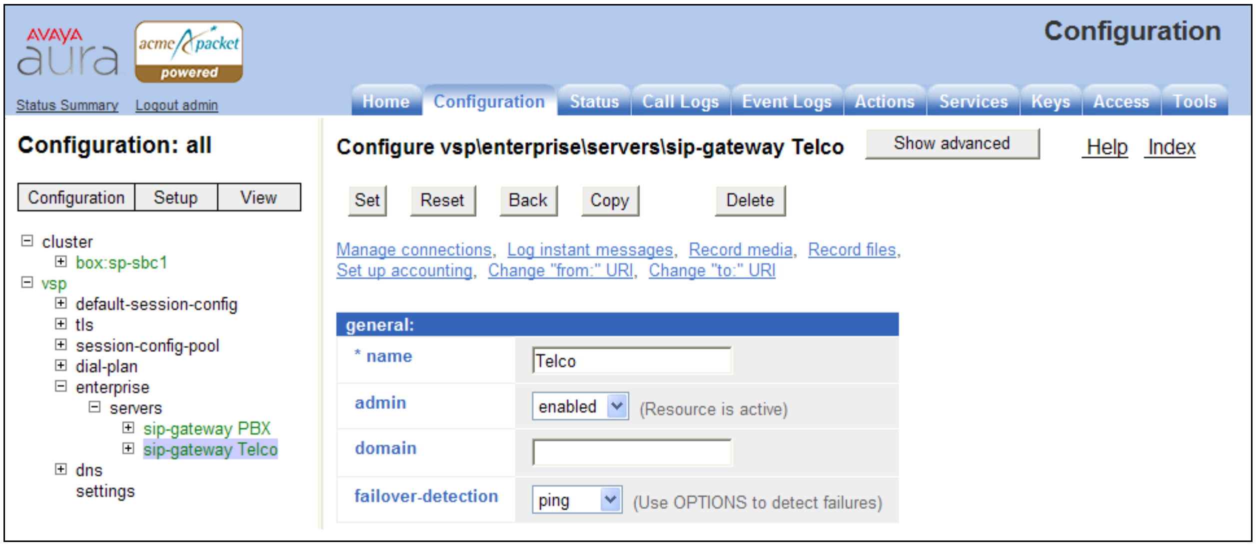
5.2. Post Installation Configuration

The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 5.1.3**. Since a different service provider other than PAETEC had to be selected in the installation wizard then additional manual changes must also be performed. These changes are performed by accessing the browser-based GUI of the Session Border Controller, using the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 5.1.3**. Log in with the appropriate credentials.

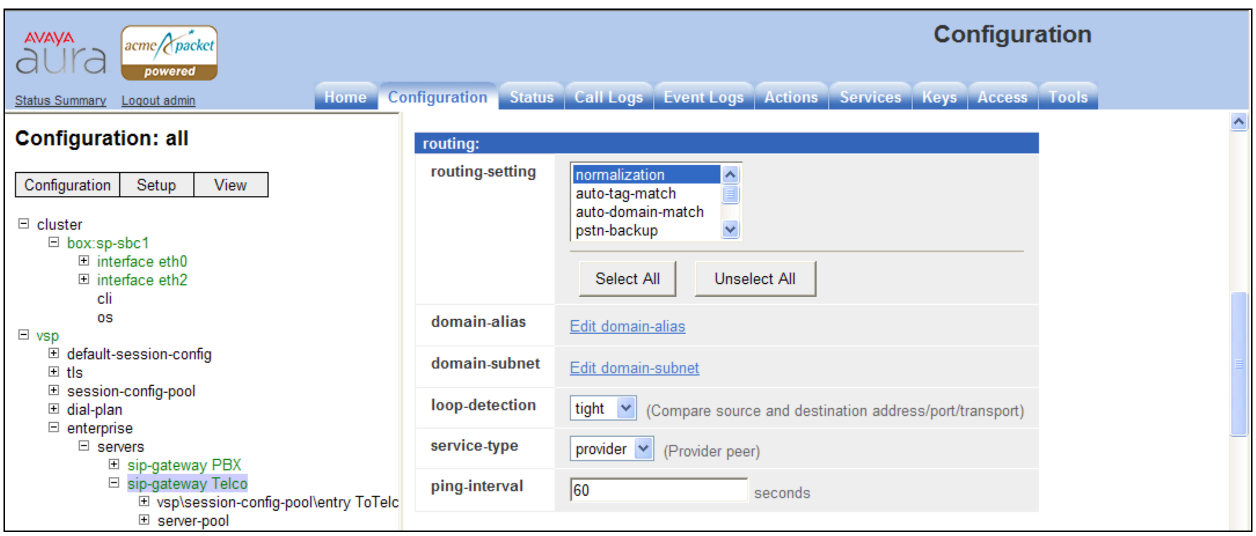


5.2.1. Options Frequency

To set the frequency of the OPTIONS messages sent from the SBC to the service provider, first navigate to **vsp → enterprise → servers → sig-gateway Telco**. Click **Show Advanced.**

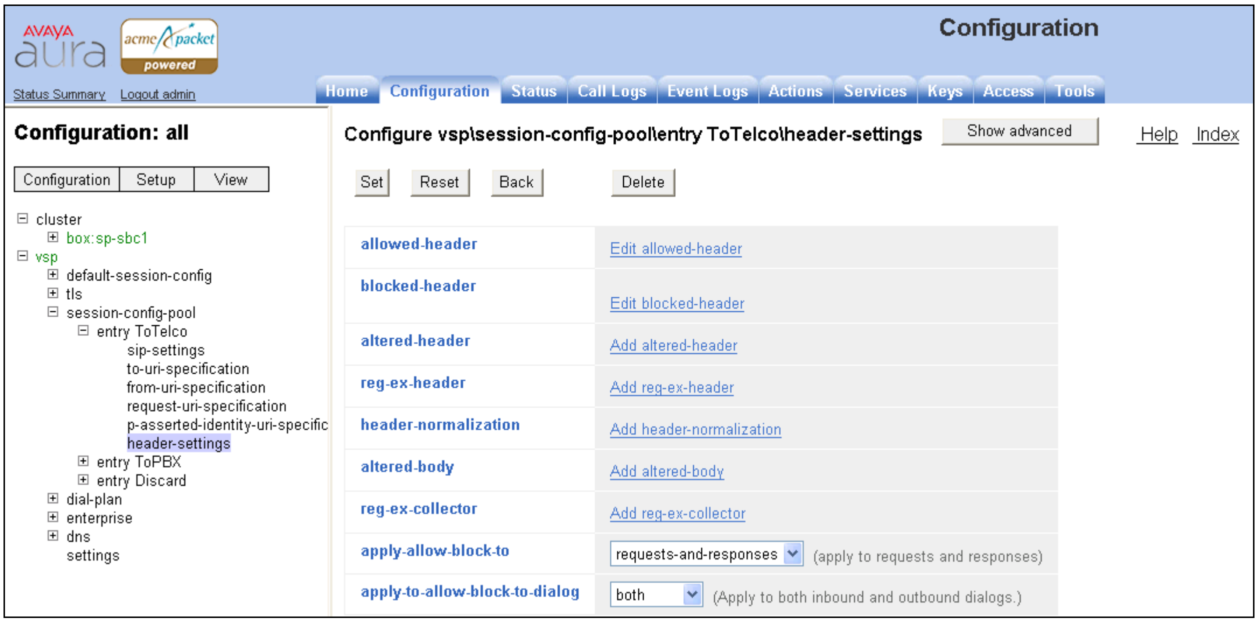


Scroll down to the **routing** section of the form. Enter the desired interval in the **ping-interval** field. Click **Set** at the top of the form (shown in previous figure).

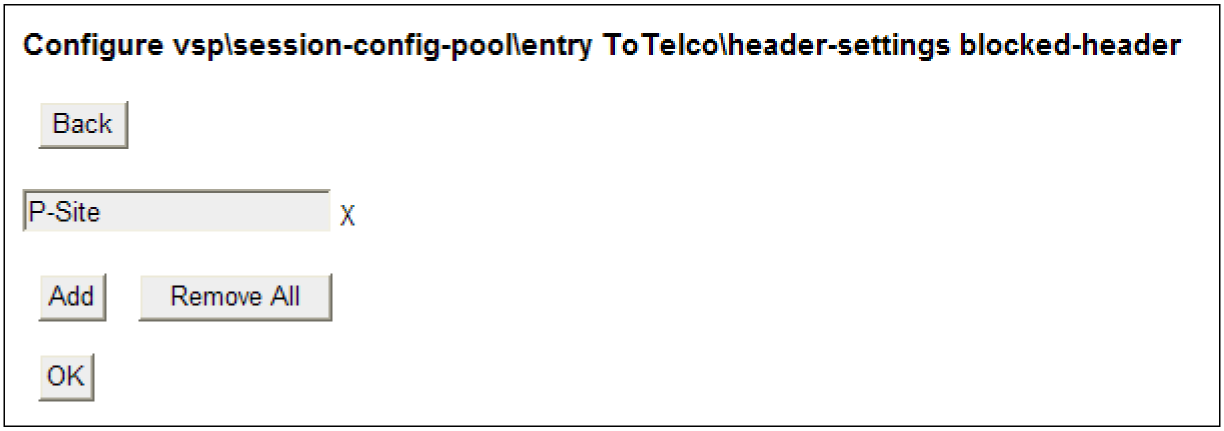


5.2.2. Blocked Headers

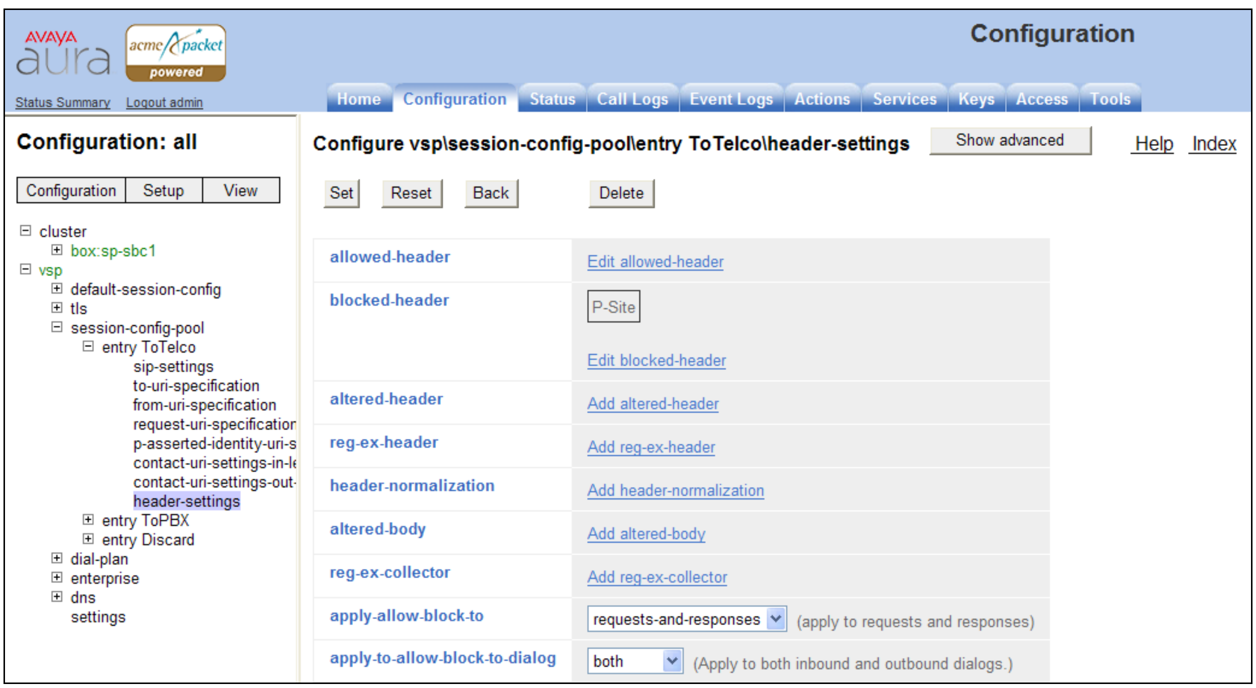
The P-Site header is sent in SIP messages from Communication Manager to the PAETEC network. This header contains private IP addresses from the enterprise. These private IP addresses should not be exposed external to the enterprise. For simplicity, this header was simply removed (blocked) from both requests and responses for both inbound and outbound calls. To create a rule for blocking a header on an outbound call, first navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. Click **Edit blocked-header**.



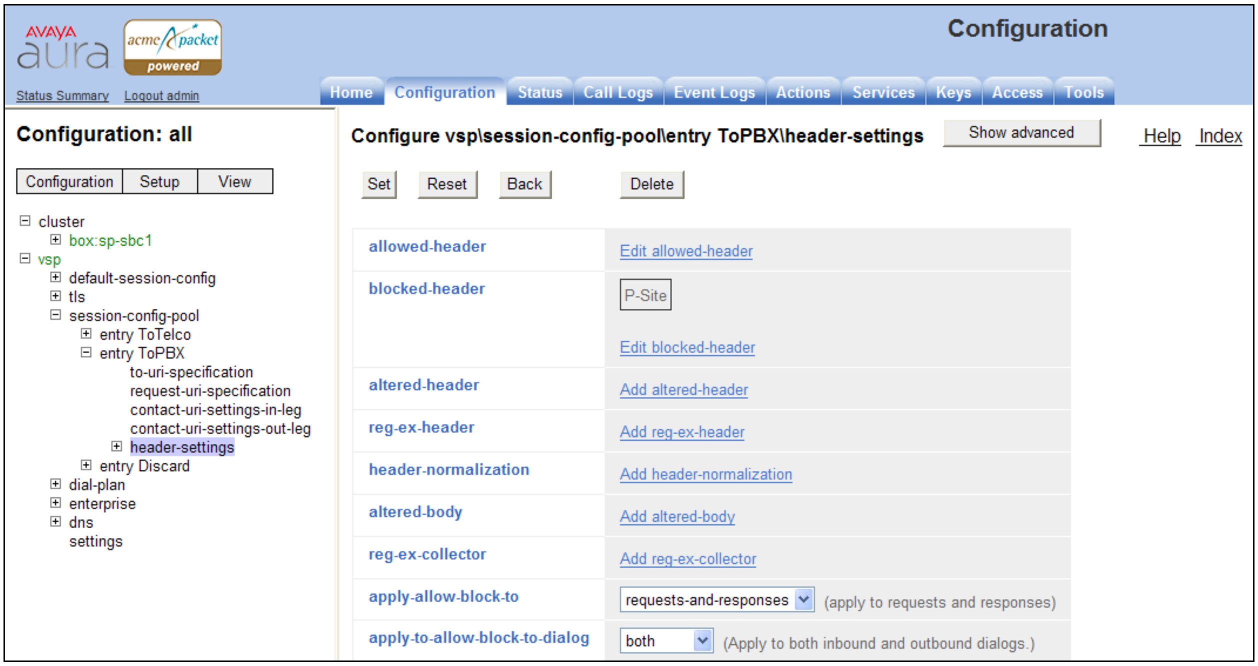
In the right pane that appears, click **Add.** In the blank field that appears, enter the name of the header to be blocked. Click **OK**. The screen below shows the **P-Site** header blocked for the compliance test.



The list of blocked headers for outbound calls will appear in the right pane as shown below. Click **Set** to complete the configuration.

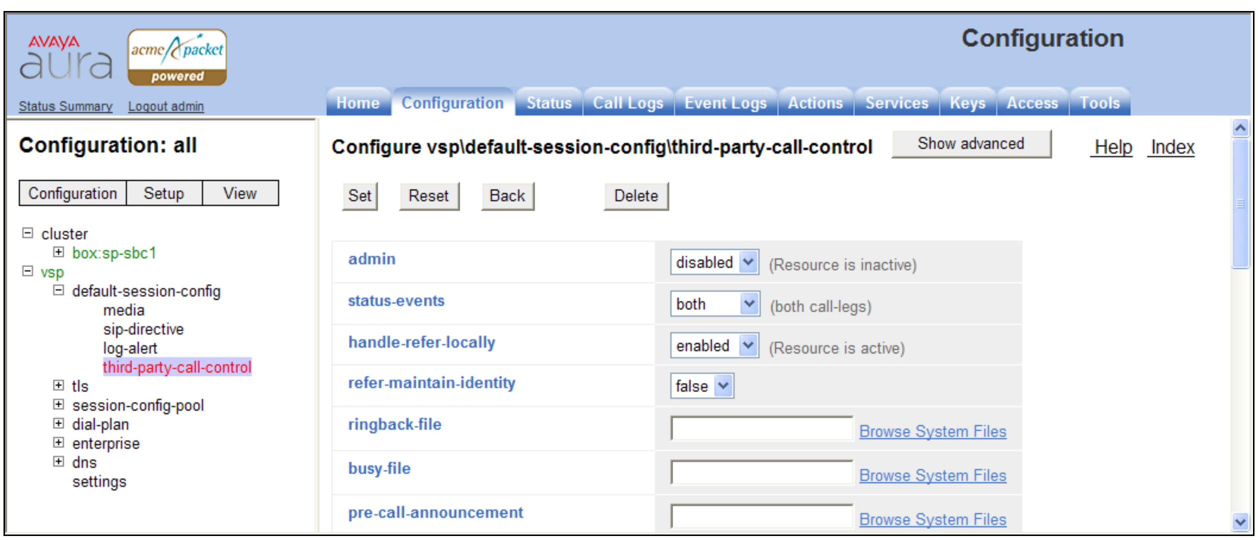


To create a rule for blocking a header on an inbound call, first navigate to **vsp → session-config-pool → entry ToPBX → header-settings**, then repeat the procedure described earlier in this section. The list of blocked headers for inbound calls is shown below.



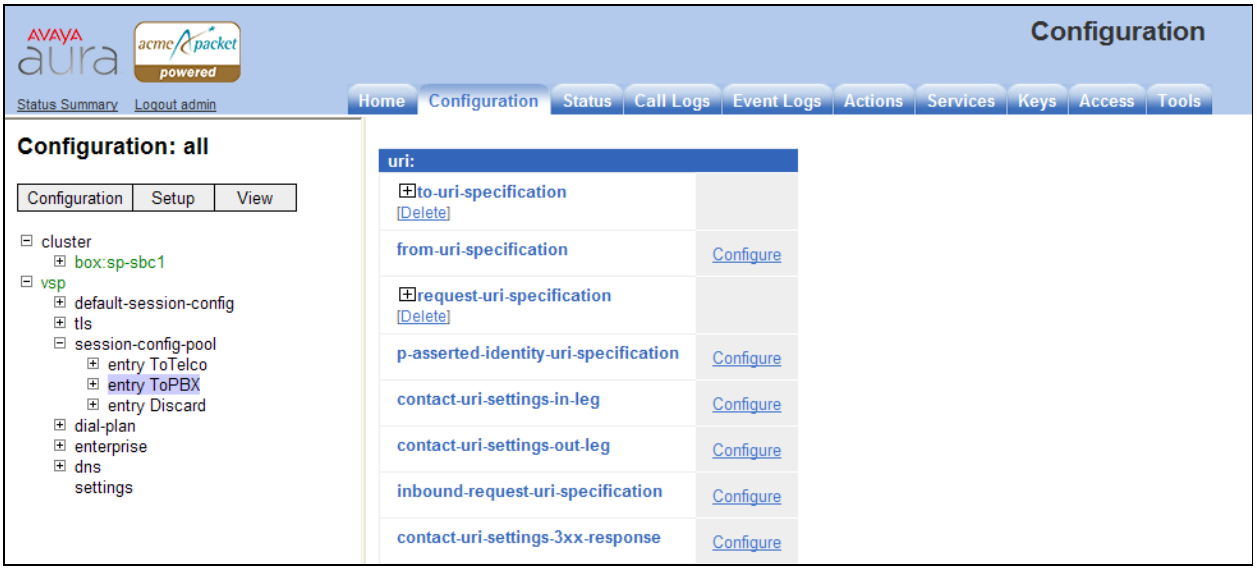
5.2.3. Third Party Call Control

Disable third party call control. Navigate to **vsp → default-session-config → third-party-call-control**. Set the **admin** field to ***disabled***.

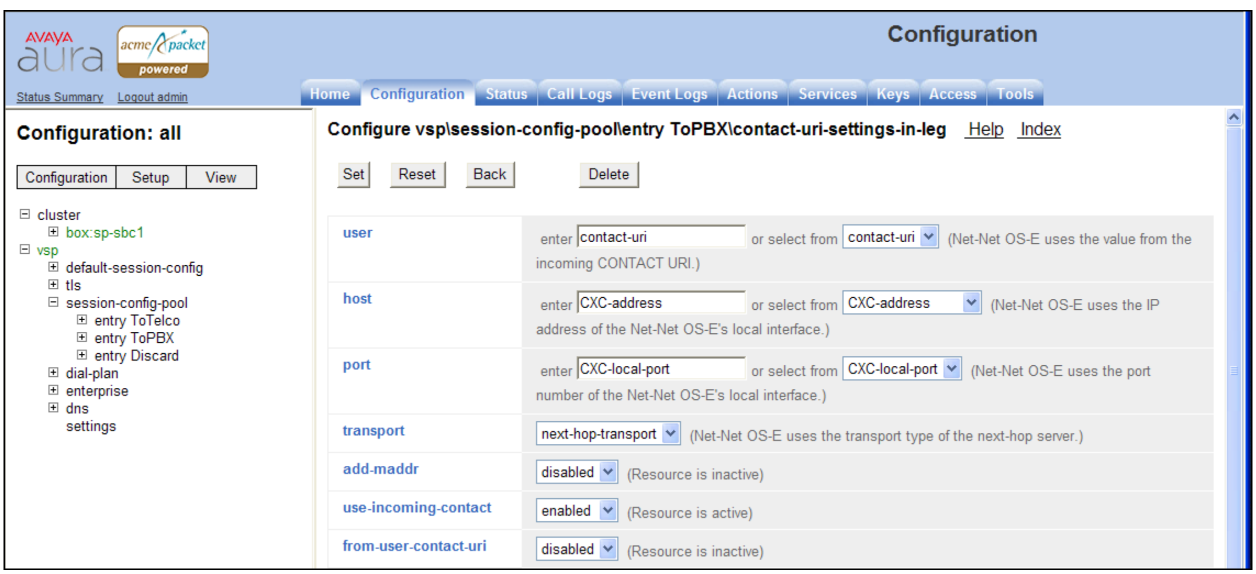


5.2.4. Contact Header

Using the settings chosen in the installation wizard, the SBC does not automatically pass to the service provider the updated Contact header that results from a redirected call. In order to have the updated Contact header passed to the service provider, first navigate to **vsp → session-config-pool → entry ToPBX**. Scroll down to the **uri** section and click **Configure** next to **contact-uri-settings-in-leg**.



In the right pane that appears, set the **add-maddr** field to ***disabled*** and the **use-incoming-contact** field to ***enabled***.



Use the same procedure described in this section to set these same values for the **contact-uri-settings-out-leg**. Repeat again for the **contact-uri-settings-in-leg** and **contact-uri-settings-out-**

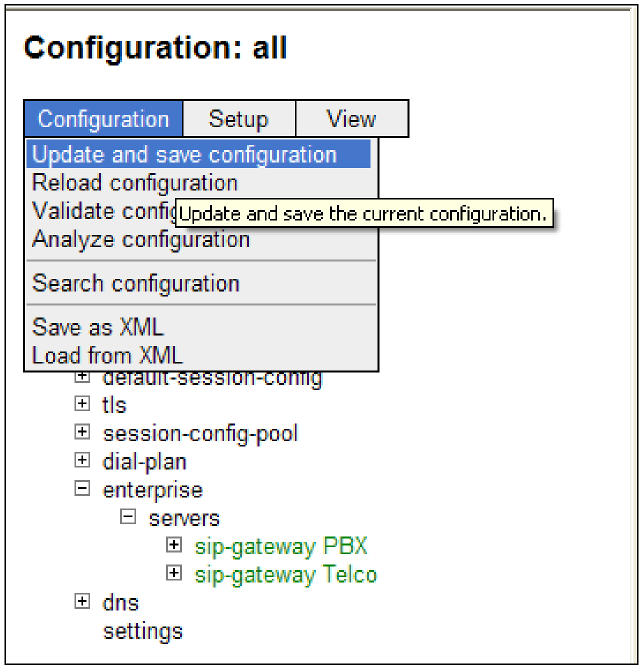
leg of the ToTelco session-config-pool by navigating to **vsp → session-config-pool → entry ToTelco**.

5.2.5. From Header

This header modification is necessary to support the acceptance of inbound calls with CPN block enabled. To accept an incoming call, Communication Manager requires the PAI header to contain a recognizable domain. In the absence of a PAI header, Communication Manager will perform the same check on the From header. PAETEC does not send a PAI header and in the case of an inbound call with CPN block enabled, the domain in the From header is purposely altered. Thus, to allow these calls to succeed, this header modification overwrites the incoming From header with the private IP address of the SBC which is recognizable to Communication Manager. This modification occurs on all incoming INVITEs, not just the ones with CPN block enabled.

5.2.6. Save the Configuration

To save the configuration, begin by clicking on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.



6. Dynamic IP SIP Trunk Service Configuration

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

During the signup process, PAETEC will require that the customer provide the public IP address used to reach the SBC at the edge of the enterprise. PAETEC will provide the IP address of the PAETEC 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.

7. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager and the SBC to connect to the Dynamic IP SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 1.1**.

The Dynamic IP SIP Trunk Service passed compliance testing.

8. Verification Steps

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

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

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and Avaya Aura® Session Border Controller to the PAETEC Dynamic IP SIP Trunk Service. The PAETEC Dynamic IP SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The PAETEC Dynamic IP SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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, Document Number 555-245-205.
[5] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x,* February 2010, Document Number 16-601443.
[6] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.
[7] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.
[8] *Avaya one-X Communicator Getting Started, November 2009.*
[9] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/
[10] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/
[11] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

11. Appendix A: Avaya Aura® SBC Configuration File

```
#
#  Copyright (c) 2004-2010  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 15:30:04 Thu 2010-12-02
#
config cluster
 config box 1
  set hostname sp-sbc1
  set timezone America/New_York
  set name sp-sbc1
  set identifier 00:ca:fe:09:42:38
  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 "" "" any 0
    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
     config route internal-sip-media
      set destination host 10.32.128.4
      set gateway 10.32.128.254
     return
    return
   return
  return
  config interface eth2
   config ip outside
    set ip-address static 10.5.5.191/24
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" any 0
    return
    config media-ports
    return
    config routing
     config route Default
      set admin disabled
     return
     config route external-sip-media
      set destination network 10.2.2.0/24
      set gateway 10.5.5.254
     return
    return
   return
  return
  config cli
   set prompt sp-sbc1
  return
  config os
  return
 return
return

config services
 config event-log
  config file access
```

```
   set filter access info
  return
  config file system
   set filter general info
   set filter system info
  return
  config file errorlog
   set filter all error
  return
  config file db
   set filter db debug
   set filter dosDatabase info
  return
  config file management
   set filter management info
  return
  config file peer
   set filter sipSvr info
  return
  config file cac
   set filter sipCAC warning
  return
  config file dos
   set filter dos alert
   set filter dosSip alert
   set filter dosTransport alert
   set filter dosUrl alert
  return
  config file krnlsys
   set filter krnlsys debug
  return
  config file acct
   set filter acct debug
  return
 return
return

config master-services
 config accounting
 return
 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 header-settings
   return
   config third-party-call-control
   return
  return
  config tls
   config certificate ws-cert
    set certificate-file /cxc/certs/ws.cert
   return
  return
  config session-config-pool
   config entry ToTelco
    config sip-settings
    return
    config to-uri-specification
     set host next-hop
    return
    config from-uri-specification
     set host local-ip
    return
    config request-uri-specification
     set host next-hop
    return
    config p-asserted-identity-uri-specification
     set host local-ip
    return
    config contact-uri-settings-in-leg
     set add-maddr disabled
     set use-incoming-contact enabled
    return
    config contact-uri-settings-out-leg
     set add-maddr disabled
     set use-incoming-contact enabled
    return
    config header-settings
     set blocked-header P-Site
    return
   return
   config entry ToPBX
    config to-uri-specification
     set host next-hop-domain
    return
    config from-uri-specification
     set host local-ip
    return
    config request-uri-specification
     set host next-hop-domain
    return
    config contact-uri-settings-in-leg
     set add-maddr disabled
     set use-incoming-contact enabled
    return
    config contact-uri-settings-out-leg
     set add-maddr disabled
```

```
    set use-incoming-contact enabled
   return
   config header-settings
    set blocked-header P-Site
   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 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
     config server PBX1
      set host 10.32.128.4
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set failover-detection ping
    set ping-interval 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
     config server Telco1
      set host 10.2.2.139
     return
    return
   return
  return
 return
 config dns
  config resolver
```

```
   config server 10.32.24.150
   return
  return
 return
 config settings
  set stack-socket-threads-max 2
 return
return

config external-services
return

config preferences
 config gui-preferences
  set enum-strings SIPSourceHeader Refer-To
  set enum-strings SIPSourceHeader Max-Forwards
  set enum-strings RequestURIStringSource 10.2.2.139
 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 0x002bdd5d9fea2fefeb97b0115854a47db2c8b27a2fe0187e0274977f4b
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x004803cd9fae4ee1b2462598359d6c5e179008f9083caa7b30b9b19b43
   set permissions access\permissions read-only
  return
 return
return

config features
return
```

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.