Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Century Link SIP Trunking with Avaya Aura® Communication Manager Evolution Server 6.0.1 and Acme Packet 3800 Net-Net Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server and an Acme Packet 3800 Net-Net Session Border Controller, along with 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 required to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server and an Acme Packet 3800 Net-Net Session Border Controller (SBC), along with 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 IP 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 Avaya Aura® Communication Manager, the Acme Packet 3800 Net-Net SBC, and various Avaya endpoints.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types.
  Phone types included H.323, digital, and analog telephones at the enterprise. 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. 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).
- Codecs G.711MU and G.729A were tested but only codec G.711Mu is currently supported in the CenturyLink production environment.
- 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).

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.

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.

- **No Error Indication if No Matching Codec Offered**: If the Communication Manager SIP trunk is improperly configured to have no matching codecs with the service provider and an outbound call is placed, the service provider only returns a "100 Trying" response and no error indication. As a result, Communication Manager cancels the call when the Alternate Route Timer expires (generally 6 seconds by default).
- **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. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink solution. It is listed here simply as an observation.
- **Asynchronous DTMF payload header values are not supported**: CenturyLink does not support the use of a different DTMF payload header value in each direction of a single call. This may occur if the media is re-directed from Communication Manager to an endpoint, and the endpoint wishes to use a different DTMF payload header value than was negotiated when the call was initially established. CenturyLink will send a re-INVITE to force the DTMF payload header value to be the same in each direction. In response, Communication Manager will send a re-INVITE to force the DTMF payload header value back to the original asynchronous values which allow the DTMF payload header value to be the same end-to-end in the same direction (even though the values are different in each direction). These re-INVITEs continue for several minutes before one side gives up and tears down the call. This issue manifested itself in two separate call scenarios during the compliance test as described in these Application Notes. This issue may occur in other call scenarios that were not tested.

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. . Alternatively, in the United States, the phone number (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:

- Avaya S8800 Server running Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya 9600-Series IP telephones (H.323)
- Avaya 4600-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 Acme Packet 3800 Net-Net Session Director (SBC). It has a public side that connects to the external service provider network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flow 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 throughout this document. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

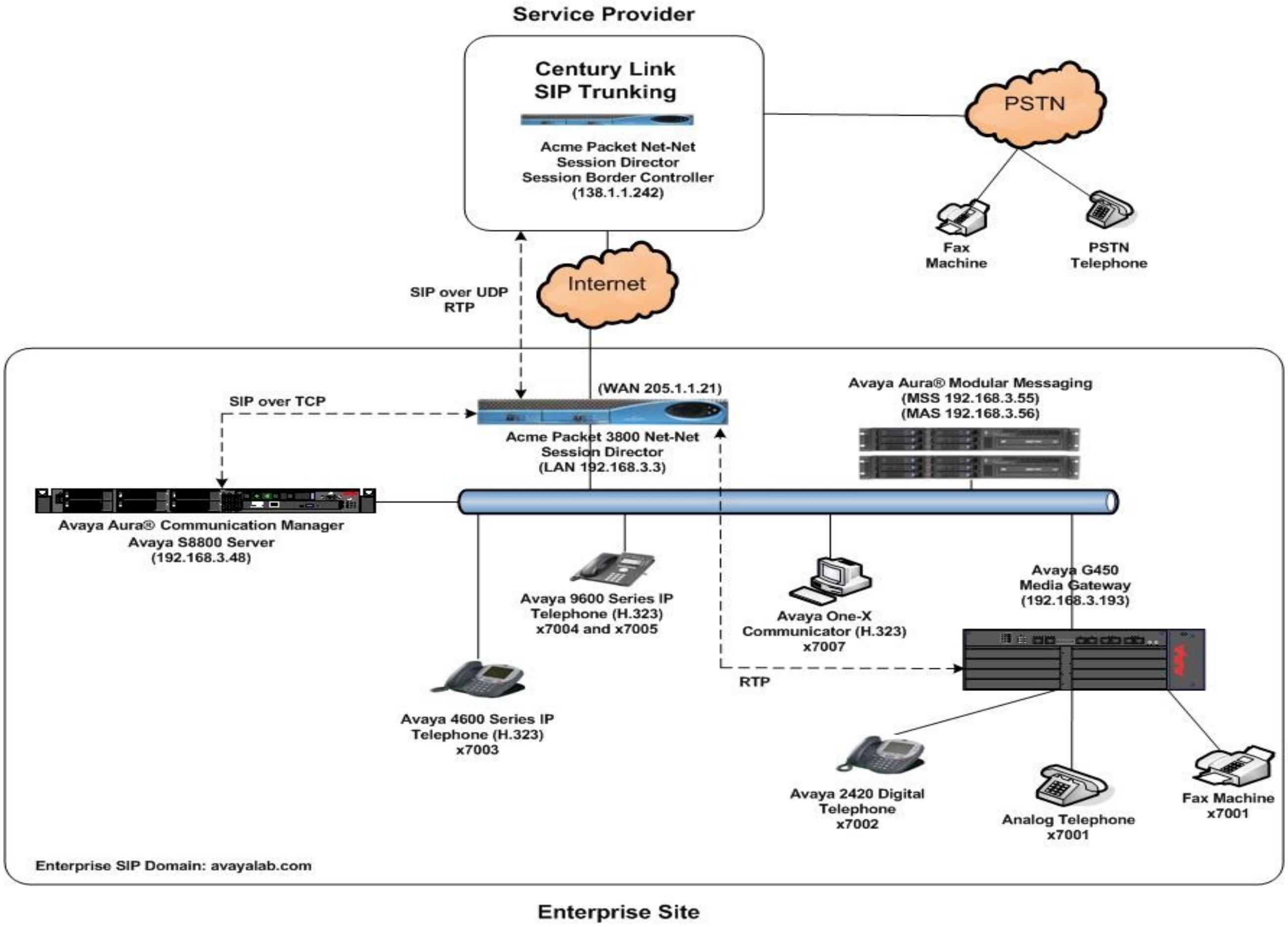


Figure 1: Avaya IP Telephony Network using CenturyLink SIP Trunking

A separate trunk was created between Avaya Aura® 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 enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

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

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

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). 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:

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on an Avaya S8800 Server	6.0.1 (R016x.00.1.510.1) (System Platform 6.0.2.0.5)
Avaya G450 Media Gateway	30.14.0
Avaya 4610SW IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 9620 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 9630 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 Analog Telephone	n/a
Acme Packet 3800 Net-Net Session Border Controller	SCX6.2.0 M3P3 GA
CenturyLink SIP Trunking Solution Components	
Component	Release
Acme Packet Net-Net Session Border Controller	6.1
BroadSoft Softswitch	R16 sp1
Sonus Media Gateway	V07.02.05R000

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 Avaya Aura® Communication Manager.

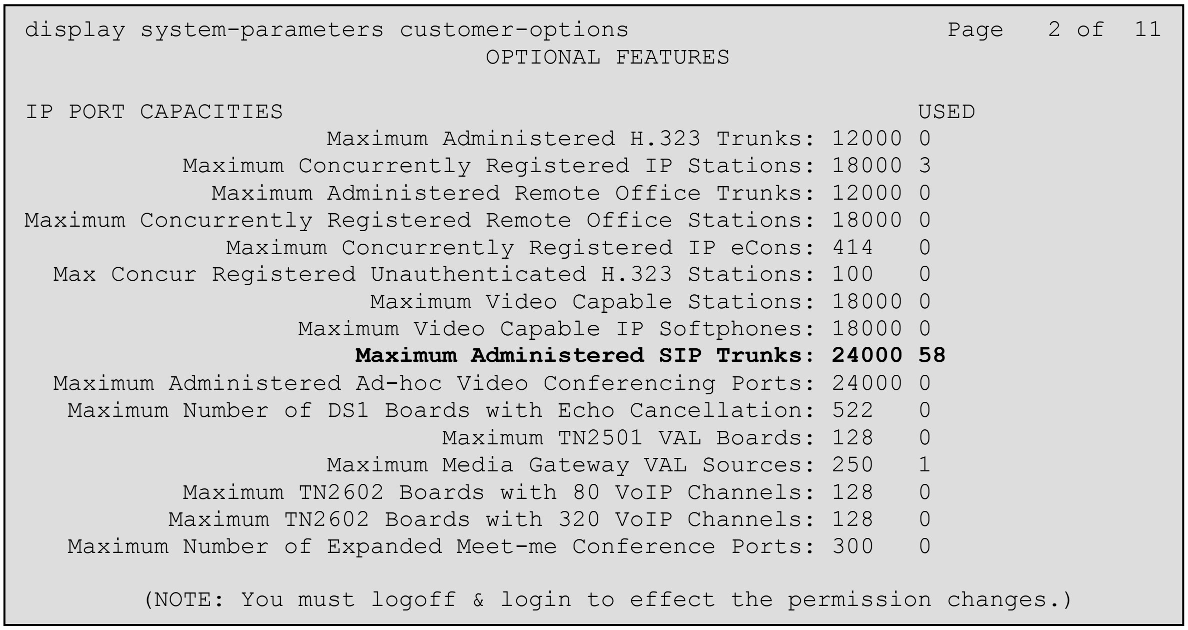
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Avaya Aura® Communication Manager for CenturyLink SIP Trunking. A SIP trunk is established between Avaya Aura® Communication Manager and the enterprise SBC for use by signaling traffic to and from CenturyLink. It is assumed that the basic installation tasks for Avaya Aura® Communication Manager, the Avaya G450 Media Gateway, and the Acme Packet enterprise SBC have been previously completed and are not discussed here.

The Avaya Aura® 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

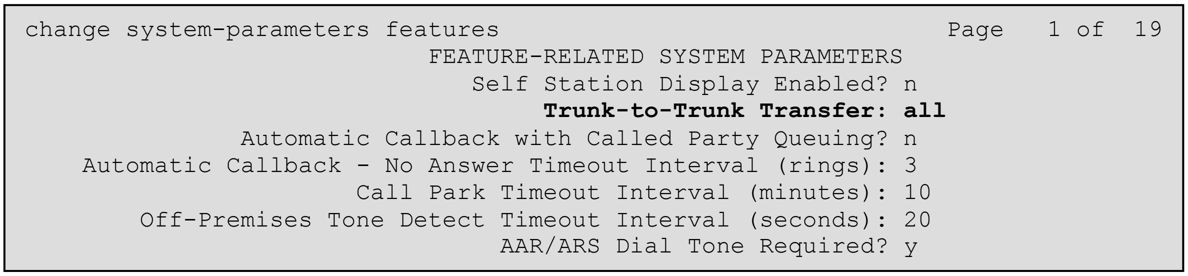
Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 24000 SIP trunks are available and 58 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: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 58
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

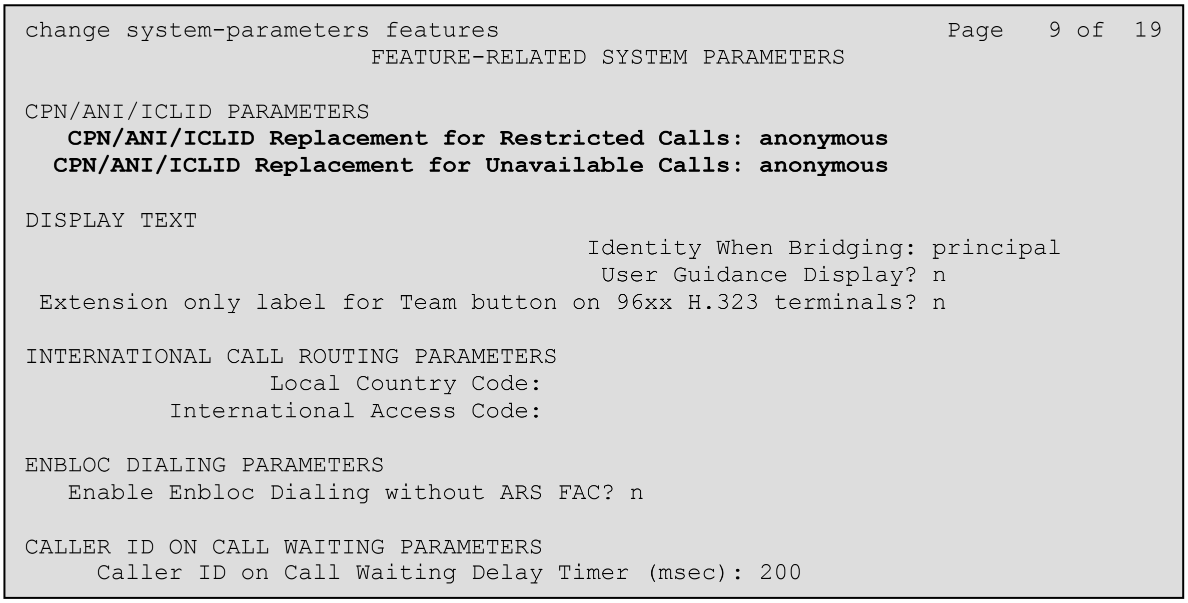
5.2. System Features

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
```

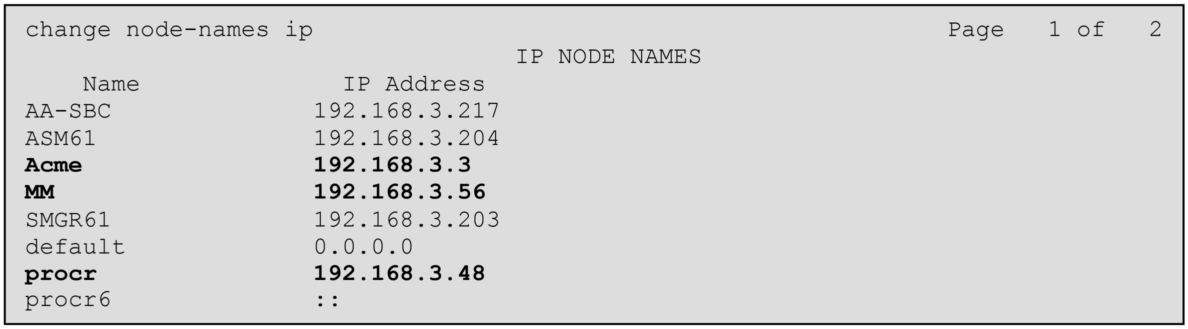
On **Page 9,** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of ***anonymous*** for both.



```
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
```

5.3. IP Node Names

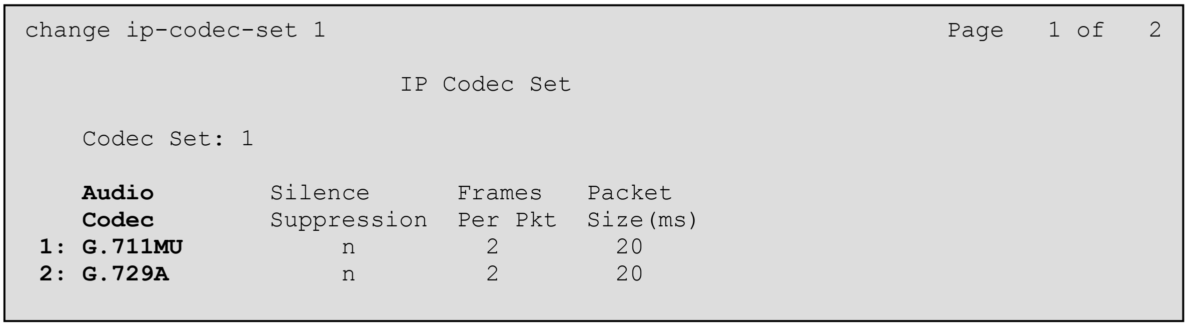
Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8800 Server running Communication Manager ***(procr***) and for the inside IP address of the enterprise SBC (**Acme**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.



```
change node-names ip                                               Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
AA-SBC              192.168.3.217
ASM61               192.168.3.204
Acme                192.168.3.3
MM                  192.168.3.56
SMGR61              192.168.3.203
default             0.0.0.0
procr               192.168.3.48
procr6              ::
```

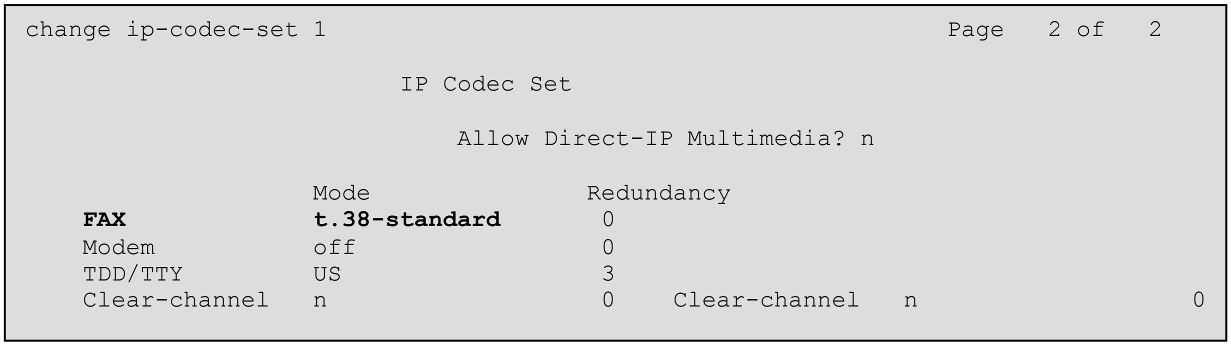
5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls within the enterprise. For the compliance test, codecs G.711MU and G.729A were tested using ip-codec-set 1. To use these codecs, enter ***G.711MU*** and ***G.729A*** in the **Audio Codec** column of the table in order of preference. Default values can be used for all other fields.



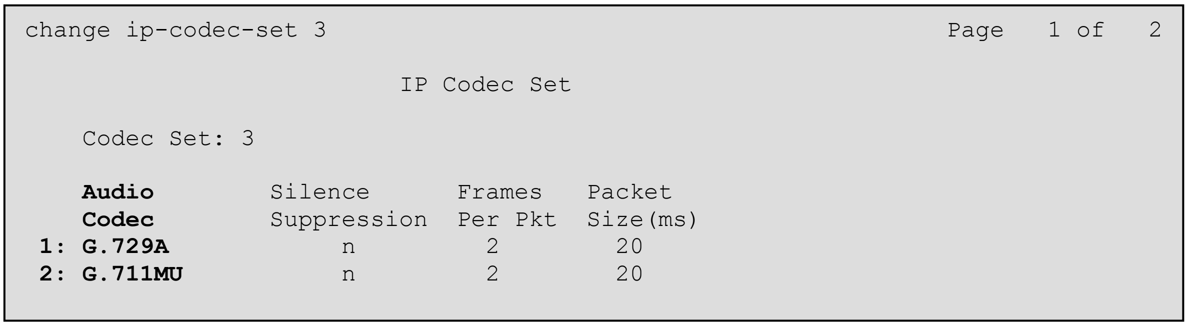
```
change ip-codec-set 1                                              Page   1 of   2

                           IP Codec Set

    Codec Set: 1

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

On **Page 2**, set the **Fax Mode** to ***T.38-Standard*** to support T.38 faxing *within* the enterprise.



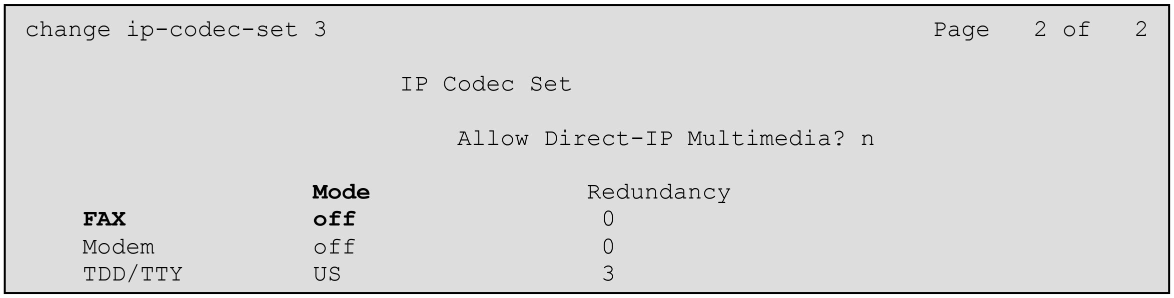
```
change ip-codec-set 1                                              Page   2 of   2

                           IP Codec Set

                               Allow Direct-IP Multimedia? n

                Mode                Redundancy
   FAX          t.38-standard        0
   Modem        off                  0
   TDD/TTY      US                   3
   Clear-channel  n                  0    Clear-channel   n                   0
```

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, codecs G.729A and G.711MU were tested using ip-codec-set 3. To use these codecs, enter ***G.729A*** and ***G.711MU*** in the **Audio Codec** column of the table in order of preference. Default values can be used for all other fields.



```
change ip-codec-set 3                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 3

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

On **Page 2**, set the **Fax Mode** to ***off*** since T.38 faxing is not currently supported by CenturyLink's SIP Trunking service.



```
change ip-codec-set 3                                           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 Regions

Create an IP-Network-Region for devices within the enterprise. For the compliance test, IP-network-region 1 was chosen for the enterprise. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***avayalab.com***. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field. In this case **Enterprise** was used.
- 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 for the enterprise in **Section 5.4**.
- Default values can be used for all other fields.

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

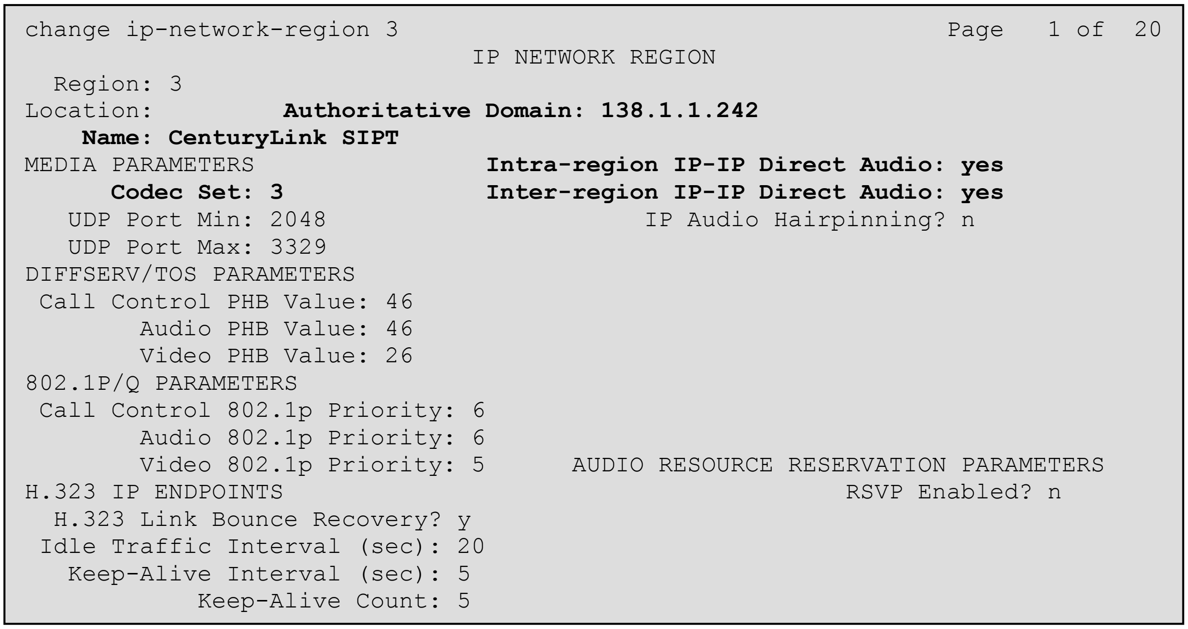
On **Page 4**, define the IP codec set to be used for traffic between region 3 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 3. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for ip network region 1 will automatically create a complementary table entry on the ip network region 3 form for destination region 1. This complementary table entry can be viewed using the **display ip-network-region 3** command and navigating to **Page 4**.

```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     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    1                                                                all
 2
 3    3     y    NoLimit                                             n       t
 4
```

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 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 with the following parameters:

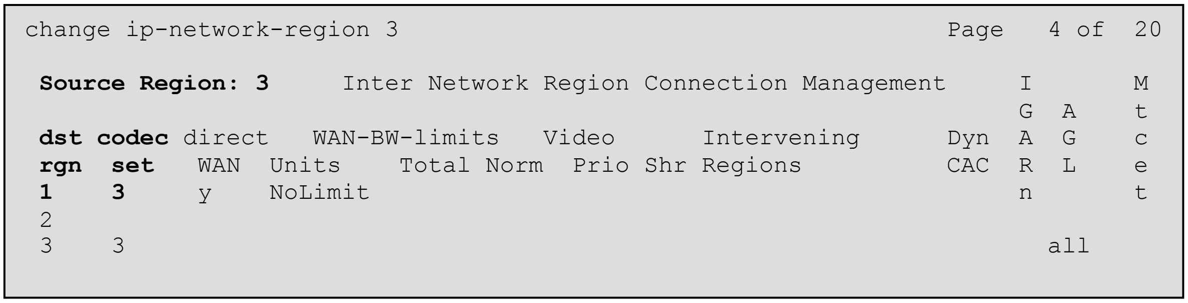
- Set the **Authoritative Domain** field to match the SIP domain or IP address of the service providers SBC or SIP proxy. In this configuration, an IP address of the service provider SBC, ***138.1.1.242*,** was used. This appears in the Host portion of the “From” header of SIP messages originating from this IP region.

- Enter a descriptive name in the **Name** field. In this case **CenturyLink SIPT** was used.
- 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 for calls between the enterprise and CenturyLink in **Section 5.4**.
- Default values can be used for all other fields.



```
change ip-network-region 3                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 3
Location:         Authoritative Domain: 138.1.1.242
    Name: CenturyLink SIPT
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              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 3 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 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for ip network region 3 will automatically create a complementary table entry on the ip network region 1 form for destination region 3. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4**.

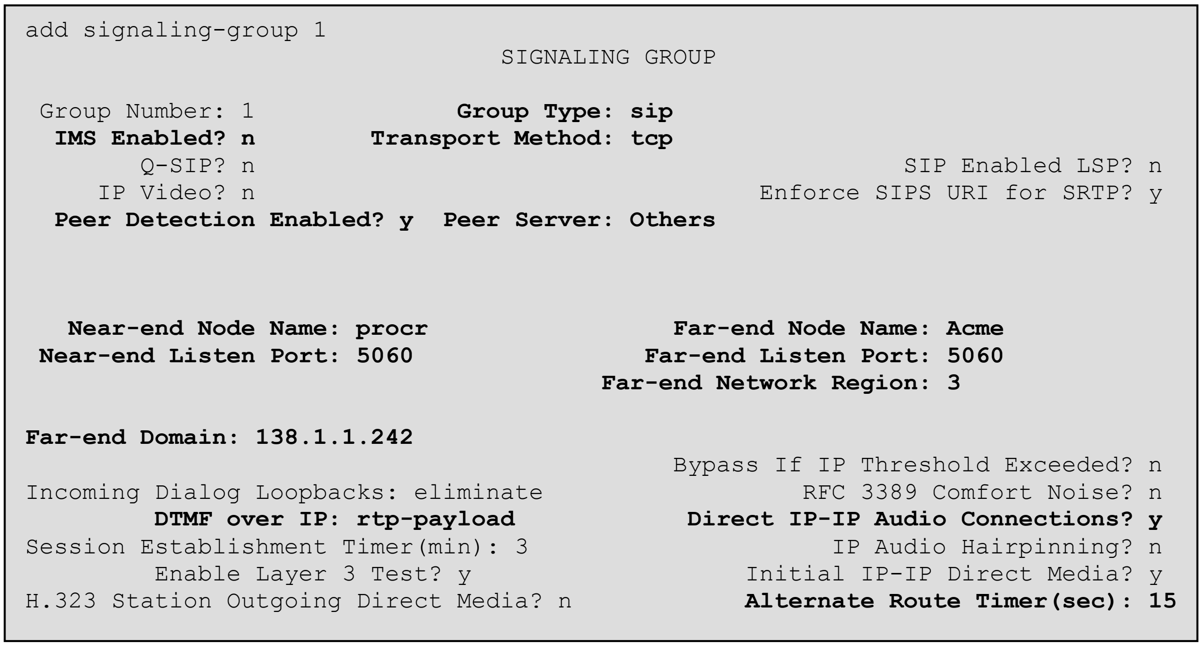


```
change ip-network-region 3                                      Page   4 of  20

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Acme Packet 3800 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 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to ***tcp***. The transport method specified here is used between the Communication Manager and the Acme Packet 3800 SBC.
- Set the **IMS Enabled** field to ***n***.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port which can be a random unused port or the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5060***.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer Server** field will initially be set to ***Others*** and cannot be changed via administration. The **Peer Server** field would automatically change to ***SM*** if Communication Manager detected an Avaya Aura® Session Manager peer. No Avaya Aura® Session Manager was used in this compliance test configuration, so the **Peer Server** field value of ***Others*** is the proper setting.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***Acme***. This node name maps to the IP address of the Acme Packet 3800 SBC as defined in **Section 5.3**.
- 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 SBC.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk associated with this signaling group 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 1
                                 SIGNALING GROUP

 Group Number: 1              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: Acme
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 3

Far-end Domain: 138.1.1.242
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? 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 1 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 configured 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.
- Default values were used for all other fields.

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

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: CenturyLink                 COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                  Member Assignment Method: auto
                                                           Signaling Group: 1
                                                         Number of Members: 14
```

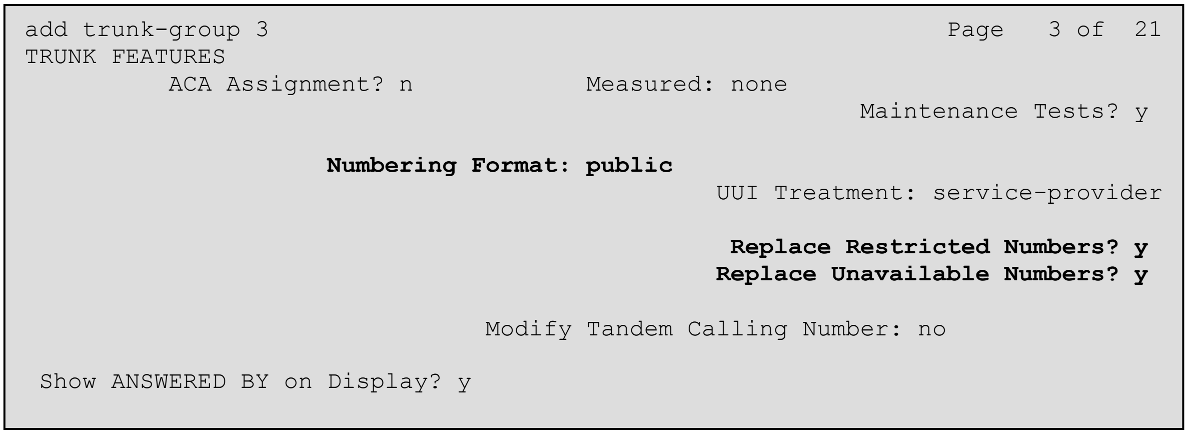
On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call 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 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 1                                               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

             XOIP Treatment: auto    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.

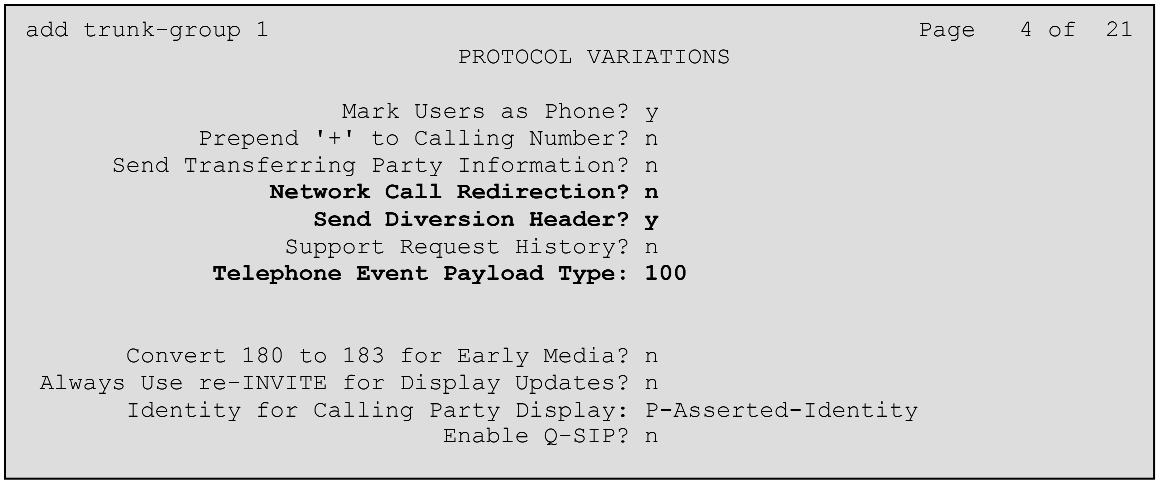
Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2** if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block 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 3                                               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***, which 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 ***100***, the value preferred by CenturyLink.

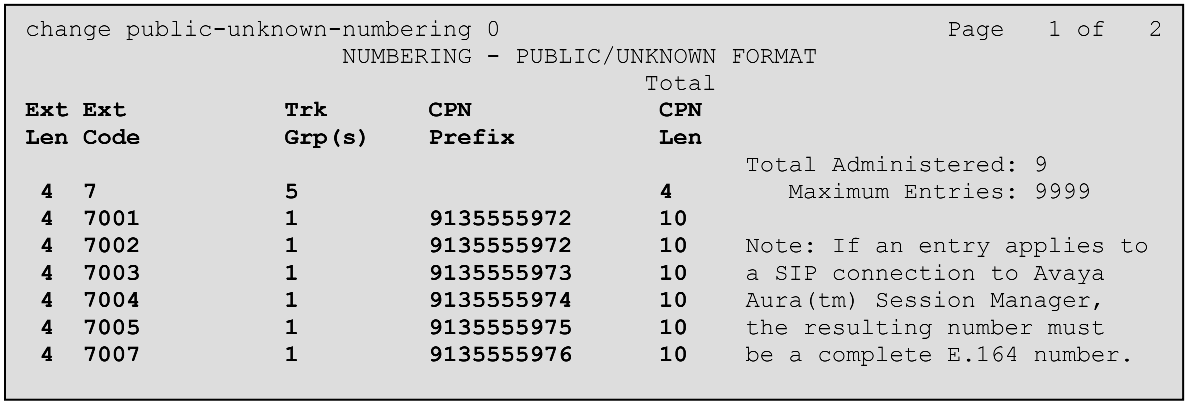


```
add trunk-group 1                                             Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? y
            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


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

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 assigned and provided by the SIP service provider. It is used to authenticate the caller.

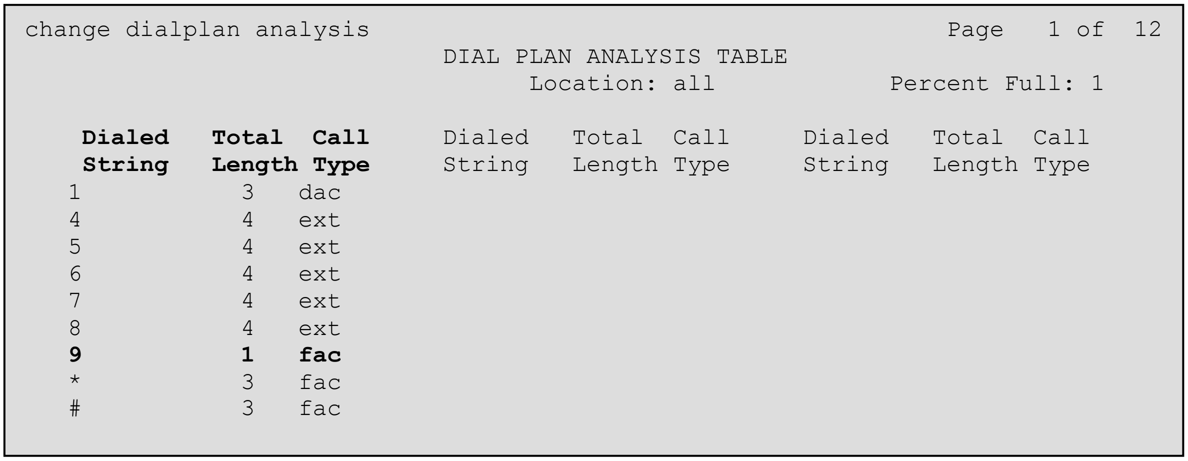
In the sample configuration, five DID numbers were assigned for testing. These five DID numbers were assigned to six extensions (7001 thru 7005, and 7007). These 10-digit DID numbers were used for the outbound calling party information on the service provider trunk whenever calls were originated from these six extensions. **NOTE**: Extensions 7001 and 7002, the analog and digital phones respectively, used the same DID of 913-555-5972 for their outbound calling party information due to only having five DIDs for this compliance test.



```
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: 9
 4  7             5                         4       Maximum Entries: 9999
 4  7001          1         9135555972      10
 4  7002          1         9135555972      10   Note: If an entry applies to
 4  7003          1         9135555973      10   a SIP connection to Avaya
 4  7004          1         9135555974      10   Aura(tm) Session Manager,
 4  7005          1         9135555975      10   the resulting number must
 4  7007          1         9135555976      10   be a complete E.164 number.
```

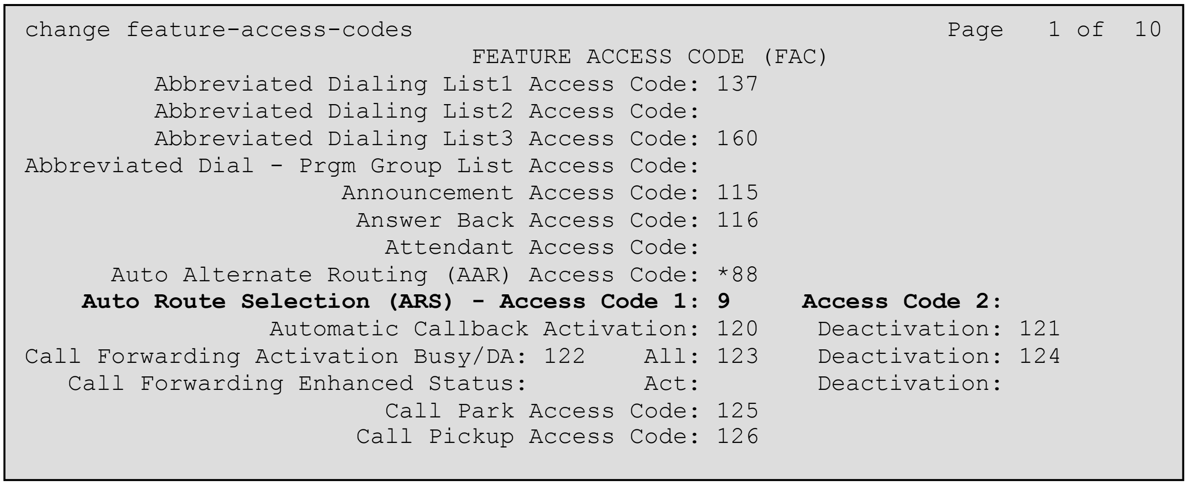
5.9. Outbound Routing

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 and having a total length of 1 digit, as a feature access code (**fac**).



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

    Dialed   Total  Call     Dialed   Total  Call      Dialed   Total  Call
    String   Length Type     String   Length Type      String   Length Type
   1           3   dac
   4           4   ext
   5           4   ext
   6           4   ext
   7           4   ext
   8           4   ext
   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**.



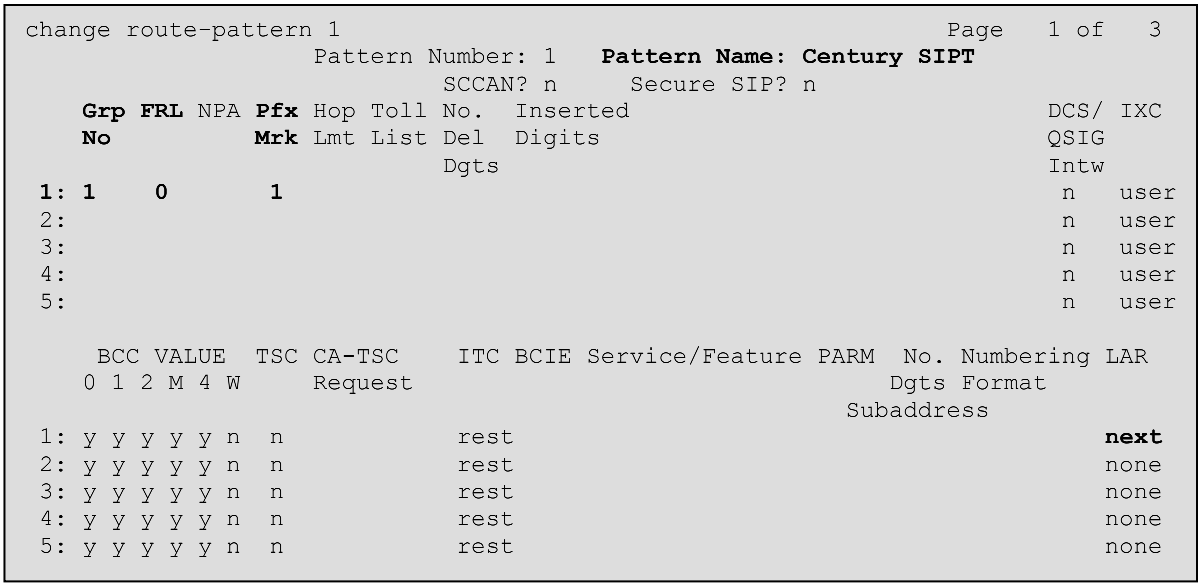
```
change feature-access-codes                                     Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: 137
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code: 160
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: 115
                       Answer Back Access Code: 116
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *88
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: 120    Deactivation: 121
Call Forwarding Activation Busy/DA: 122    All: 123    Deactivation: 124
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: 125
                       Call Pickup Access Code: 126
```

Use the **change ars analysis x** command to configure the routing of dialed digits following the first digit 9, where **x** is the next digit in the string to be matched against the table below. The example below shows a large subset of the dialed strings tested as part of the compliance test. Towards the bottom there are example entries for 10-digit dialing. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 1 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: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     1    1     1        op           n
    0                     8    8     1        op           n
    0                     11   11    1        op           n
    00                    2    2     1        op           n
    01                    9    17    1        iop          n
    011                   10   18    1        intl         n
...................... output truncated.................................
    130                   11   11    1        hnpa
    1300                  11   11    deny     fnpa
    131                   11   11    1        fnpa
    132                   11   11    1        fnpa
    133                   11   11    1        fnpa
    134                   11   11    1        fnpa
    135                   11   11    1        fnpa
    136                   11   11    1        fnpa
    137                   11   11    1        fnpa
...................... output truncated.................................
    172                   11   11    1        hnpa
    173                   11   11    1        fnpa
    174                   11   11    1        fnpa
    175                   11   11    1        fnpa
    176                   11   11    1        fnpa
    177                   11   11    1        fnpa
    178                   11   11    1        fnpa
    179                   11   11    1        fnpa
    180                   11   11    1        fnpa
......................output truncated..................................
    2                     10   10    1        fnpa
    3                     10   10    1        hnpa
    4                     10   10    1        fnpa
    411                    3    3    1        svcl
    5                     10   10    1        fnpa
    6                     10   10    1        fnpa
    611                    3    3    1        svcl
    7                     10   10    1        hnpa
    8                     10   10    1        fnpa
    811                    3    3    1        svcl
    9                     10   10    1        fnpa
    911                    3    3    1        svcl
    913                   10   10    1        fnpa
```

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 1 used for 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 ***1*** 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 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: Century SIPT
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
    No          Mrk Lmt List Del  Digits                                  QSIG
                             Dgts                                         Intw
 1: 1    0       1                                                         n   user
 2:                                                                        n   user
 3:                                                                        n   user
 4:                                                                        n   user
 5:                                                                        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. Configure Acme Packet 3800 Net-Net Session Border Controller

The following sections describe the provisioning of the Acme Packet 3800 Net-Net SBC. Only the SBC provisioning required for the reference configuration is described in these Application Notes. The resulting SBC configuration file is shown in **Appendix A**.

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

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to (*configure)#*.
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4 - 8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until returned to the Superuser prompt.
10. Type **save-config** to save the configuration.
11. Type **verify-config** to verify that no errors have been made.
12. Type **activate-config** to activate the configuration.

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

6.1. Physical Interfaces

This section defines the physical interfaces for the private enterprise and public networks.

6.1.1. Public Interface

Create a phy-interface for the public side of the Acme.

1. Enter **system → phy-interface**
2. Enter **name → s1p0**
3. Enter **operation-type → Media**
4. Enter **port → 0**
5. Enter **slot → 0**
6. Enter **duplex-mode → FULL**
7. Enter **speed → 100**
8. Enter **done**
9. Enter **exit**

6.1.2. Private Interface

Create a phy-interface for the private enterprise side of the Acme.

1. Enter **system → phy-interface**
2. Enter **name → s0p0**
3. Enter **operation-type → Media**
4. Enter **port → 0**
5. Enter **slot → 1**
6. Enter **duplex-mode → FULL**
7. Enter **speed → 100**
8. Enter **done**
9. Enter **exit**

6.2. Network Interfaces

This section defines the network interfaces for the private enterprise and public IP networks.

6.2.1. Public Interface

Create a network-interface to the public side of the Acme.

1. Enter **system → network-interface**
2. Enter **name → s1p0**
3. Enter **ip-address → 205.1.1.21**
4. Enter **netmask → 255.255.255.128**
5. Enter **gateway → 205.1.1.1**
6. Enter **dns-ip-primary →**
7. Enter **hip-ip-list → 205.1.1.21**
8. Enter **icmp-ip-list → 205.1.1.21**
9. Enter **done**
10. Enter **exit**

6.2.2. Private Interface

Create a network-interface for the private enterprise side of the Acme.

1. Enter **system → network-interface**
2. Enter **name → s0p0**
3. Enter **ip-address → 192.168.3.3**
4. Enter **netmask → 255.255.255.0**
5. Enter **gateway → 192.168.3.1**
6. Enter **hip-ip-list → 192.168.3.3**
7. Enter **icmp-ip-list → 192.168.3.3**
8. Enter **done**
9. Enter **exit**

6.3. Realms

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

6.3.1. Outside Realm

Create a realm for the external network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → CenturyLink**
3. Enter **network-interfaces → s1p0:0**
4. Enter **done**
5. Enter **exit**

6.3.2. Inside Realm

Create a realm for the internal network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → Enterprise**
3. Enter **network-interfaces → s0p0:0**
4. Enter **done**
5. Enter **exit**

6.4. Steering-Pools

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

6.4.1. Outside Steering-Pool

Create a steering-pool for the outside network.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 205.1.1.21**
3. Enter **start-port → 16384**
4. Enter **end-port → 32767**
5. Enter **realm-id → CenturyLink**
6. Enter **done**
7. Enter **exit**

6.4.2. Inside Steering-Pool

Create a steering-pool for the inside network.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 192.168.3.3**
3. Enter **start-port → 16384**
4. Enter **end-port → 32767**
5. Enter **realm-id → Enterprise**
6. Enter **done**
7. Enter **exit**

6.5. Media-Manager

Verify that the media-manager process is enabled.

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

6.6. SIP Configuration

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

1. Enter **session-router → sip-config**
2. Enter **state → enabled**
3. Enter **operation-mode → dialog**
4. Enter **home-realm-id → Enterprise**
5. Enter **egress-realm-id → Enterprise**
6. Enter **nat-mode → None**
7. Enter **done**
8. Enter **exit**

6.7. SIP Interfaces

The SIP interface defines the SIP signaling interface (IP address and port) on the Acme Packet. SIP header manipulations can be applied at the SIP interface level.

6.7.1. Outside SIP Interface

Create a sip-interface for the outside network.

1. Enter **session-router → sip-interface**
2. Enter **state → enabled**
3. Enter **realm-id → CenturyLink**
4. Enter **sip-port**
    a. Enter **address → 205.1.1.21**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → UDP**
    d. Enter **allow-anonymous → all**
    e. Enter **done**
    f. Enter **exit**
5. Enter **stop-recurse → 401,407**
6. Enter **done**
7. Enter **exit**

6.7.2. Inside SIP Interface

Create a sip-interface for the inside network.

1. Enter **session-router → sip-interface**

2. Enter **state → enabled**
3. Enter **realm-id → Enterprise**
4. Enter **sip-port**
    a. Enter **address → 192.168.3.3**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → TCP**
    d. Enter **allow-anonymous → all**
    e. Enter **done**
    f. Enter **exit**
5. Enter **stop-recurse → 401,407**
6. Enter **done**
7. Enter **exit**

6.8. Session-Agents

A session-agent defines an internal "next hop" signaling entity for the SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent is defined for the service provider (outside) and Avaya Aura® Communication Manager (inside). SIP header manipulations can be applied at the SIP Session-Agent level.

6.8.1. Outside Session-Agent

Create a session-agent for the outside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 138.1.1.242**
3. Enter **ip-address → 138.1.1.242**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP**
8. Enter **realm-id → CenturyLink**
9. Enter **description → CenturyLink**
10. Enter **ping-method → OPTIONS;hops=70**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **done**
14. Enter **exit**

6.8.2. Inside Session-Agent

Create a session-agent for the inside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → cm601**
3. Enter **ip-address → 192.168.3.48**
4. Enter **port → 5060**
5. Enter **transport-method → UDP+TCP**
6. Enter **realm-id → Enterprise**
7. Enter **description →**

8. Enter **ping-method →**
9. Enter **ping-interval → 60**
10. Enter **ping-send-mode → keep-alive**
11. Enter **done**
12. Enter **exit**

6.9. Local Policies

Local policies allow SIP requests from the **Enterprise** realm to be routed to the service provider session agent in the **CenturyLink** realm, and vice-versa.

6.9.1. Enterprise to CenturyLink

Create a local-policy for the **Enterprise** realm.

1. Enter **session-router → local-policy**
2. Enter **from-address →** *
3. Enter **to-address →** *
4. Enter **source-realm → Enterprise**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 138.1.1.242**
    b. Enter **realm → CenturyLink**
    c. Enter **terminate-recursion → enabled**
    d. Enter **app-protocol → SIP**
    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

6.9.2. CenturyLink to Enterprise

Create a local-policy for the **CenturyLink** realm.

1. Enter **session-router → local-policy**
2. Enter **from-address → ***
3. Enter **to-address → ***
4. Enter **source-realm → CenturyLink**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 192.168.3.48**
    b. Enter **realm → Enterprise**
    c. Enter **terminate-recursion → enabled**
    d. Enter **app-protocol → SIP**
    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

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.CenturyLinknetworks.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.
The configuration between CenturyLink and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the CenturyLink network.

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 commands on 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 group number> - Displays trunk group information.
- **status trunk** <trunk group 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 Acme Packet 3800 Net-Net 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] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.0, August 2010, *D*ocument Number 555-245-205.

[3] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.

[4] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* Release 3.1, November 2009, Document Number 16-300698.

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

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

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

[8] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

11. Appendix A: Acme Packet 3800 Net-Net SBC Configuration File

```
EnterpriseSBC# show run
local-policy
      from-address
                                     *
      to-address
                                     *
      source-realm
                                     Enterprise
      description
      activate-time                  N/A
      deactivate-time                N/A
      state                          enabled
      policy-priority                none
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 15:39:03
      policy-attribute
            next-hop                       138.1.1.242
            realm                          CenturyLink
            action                         none
            terminate-recursion            disabled
            carrier
            start-time                     0000
            end-time                       2400
            days-of-week                   U-S
            cost                           0
            app-protocol                   SIP
            state                          enabled
            methods
            media-profiles
            lookup                         single
            next-key
            eloc-str-lkup                  disabled
            eloc-str-match
local-policy
      from-address
                                     *
      to-address
                                     *
      source-realm
                                     CenturyLink
      description
      activate-time                  N/A
      deactivate-time                N/A
      state                          enabled
      policy-priority                none
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 15:37:26
      policy-attribute
            next-hop                       192.168.3.48
            realm                          Enterprise
            action                         none
            terminate-recursion            disabled
            carrier
            start-time                     0000
            end-time                       2400
            days-of-week                   U-S
            cost                           0
            app-protocol                   SIP
            state                          enabled
            methods
            media-profiles
            lookup                         single
            next-key
            eloc-str-lkup                  disabled
            eloc-str-match
media-manager
      state                          enabled
      latching                       enabled
      flow-time-limit                86400
      initial-guard-timer            300
      subsq-guard-timer              300
      tcp-flow-time-limit            86400
      tcp-initial-guard-timer        300
      tcp-subsq-guard-timer          300
      tcp-number-of-ports-per-flow   2
      hnt-rtcp                       disabled
      algd-log-level                 NOTICE
      mbcd-log-level                 NOTICE
      red-flow-port                  1985
      red-mgcp-port                  1986
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      media-policing                 enabled
      max-signaling-bandwidth        10000000
      max-untrusted-signaling        100
      min-untrusted-signaling        30
      app-signaling-bandwidth        0
      tolerance-window               30
      rtcp-rate-limit                0
      trap-on-demote-to-deny         disabled
      min-media-allocation           2000
      min-trusted-allocation         4000
      deny-allocation                32000
      anonymous-sdp                  disabled
      arp-msg-bandwidth              32000
      fragment-msg-bandwidth         0
      rfc2833-timestamp              disabled
      default-2833-duration          100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event    disabled
      media-supervision-traps        disabled
      dnsalg-server-failover         disabled
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-09-08 19:23:20
network-interface
      name                           wancom0
      sub-port-id                    0
      description
      hostname
      ip-address                     135.9.230.221
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        135.9.230.254
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list
      ftp-address
        icmp-address
      snmp-address
      telnet-address
      ssh-address
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-09-02 18:52:49
network-interface
      name                           s0p0
      sub-port-id                    0
      description
      hostname
      ip-address                     192.168.3.3
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        192.168.3.1
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary                 192.168.3.9
      dns-ip-backup1
      dns-ip-backup2
      dns-domain                     sprint7288.com
      dns-timeout                    11
        hip-ip-list                    192.168.3.3
      ftp-address
        icmp-address                   192.168.3.3
      snmp-address
      telnet-address
      ssh-address
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-09-02 18:20:58
network-interface
      name                           s1p0
      sub-port-id                    0
      description
      hostname
      ip-address                     205.1.1.21
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.128
      gateway                        205.1.1.1
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list                    205.1.1.21
      ftp-address
        icmp-address                   205.1.1.21
      snmp-address
      telnet-address
      ssh-address
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-05 00:48:51
ntp-config
      server                         192.168.3.9
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-09-08 19:26:51
phy-interface
      name                           wancom0
      operation-type                 Control
      port                           0
      slot                           1
      virtual-mac
      wancom-health-score            50
      overload-protection            disabled
      last-modified-by               admin@console
      last-modified-date             2010-04-20 12:15:56
phy-interface
      name                           s0p0
      operation-type                 Media
      port                           0
      slot                           0
      virtual-mac
      admin-state                    enabled
      auto-negotiation               enabled
      duplex-mode                    FULL
      speed                          100
      overload-protection            disabled
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-04-20 12:31:37
phy-interface
      name                           s1p0
      operation-type                 Media
      port                           0
      slot                           1
      virtual-mac
      admin-state                    enabled
      auto-negotiation               enabled
      duplex-mode                    FULL
      speed                          100
      overload-protection            disabled
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-04-20 14:18:05
realm-config
      identifier                     CenturyLink
      description
      addr-prefix                    0.0.0.0
      network-interfaces
                                     s1p0:0
      mm-in-realm                    enabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
      msm-release                    disabled
      generate-UDP-checksum          disabled
      max-bandwidth                  0
      fallback-bandwidth             0
      max-priority-bandwidth         0
      max-latency                    0
      max-jitter                     0
      max-packet-loss                0
      observ-window-size             0
      parent-realm
      dns-realm
      media-policy
      media-sec-policy
      in-translationid
      out-translationid
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      class-profile
      average-rate-limit             0
      access-control-trust-level     none
      invalid-signal-threshold       0
      maximum-signal-threshold       0
      untrusted-signal-threshold     0
      nat-trust-threshold            0
      deny-period                    30
      ext-policy-svr
      symmetric-latching             disabled
      pai-strip                      disabled
      trunk-context
      early-media-allow
      enforcement-profile
      additional-prefixes
      restricted-latching            none
      restriction-mask               32
      accounting-enable              enabled
      user-cac-mode                  none
      user-cac-bandwidth             0
      user-cac-sessions              0
      icmp-detect-multiplier         0
      icmp-advertisement-interval    0
      icmp-target-ip
      monthly-minutes                0
      net-management-control         disabled
      delay-media-update             disabled
      refer-call-transfer            disabled
      dyn-refer-term                 disabled
      codec-policy
      codec-manip-in-realm           disabled
      constraint-name
      call-recording-server-id
      xnq-state                      xnq-unknown
      hairpin-id                     0
      stun-enable                    disabled
      stun-server-ip                 0.0.0.0
      stun-server-port               3478
      stun-changed-ip                0.0.0.0
      stun-changed-port              3479
      match-media-profiles
      qos-constraint
      sip-profile
      sip-isup-profile
      block-rtcp                     disabled
      hide-egress-media-update       disabled
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 14:42:51
realm-config
      identifier                     Enterprise
      description
      addr-prefix                    0.0.0.0
      network-interfaces
                                     s0p0:0
      mm-in-realm                    enabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
      msm-release                    disabled
      generate-UDP-checksum          disabled
      max-bandwidth                  0
      fallback-bandwidth             0
      max-priority-bandwidth         0
      max-latency                    0
      max-jitter                     0
```

```
    max-packet-loss                0
    observ-window-size             0
    parent-realm
    dns-realm
    media-policy
    media-sec-policy
    in-translationid
    out-translationid
    in-manipulationid
    out-manipulationid
    manipulation-string
    manipulation-pattern
    class-profile
    average-rate-limit             0
    access-control-trust-level     none
    invalid-signal-threshold       0
    maximum-signal-threshold       0
    untrusted-signal-threshold     0
    nat-trust-threshold            0
    deny-period                    30
    ext-policy-svr
    symmetric-latching             disabled
    pai-strip                      disabled
    trunk-context
    early-media-allow
    enforcement-profile
    additional-prefixes
    restricted-latching            none
    restriction-mask               32
    accounting-enable              enabled
    user-cac-mode                  none
    user-cac-bandwidth             0
    user-cac-sessions              0
    icmp-detect-multiplier         0
    icmp-advertisement-interval    0
    icmp-target-ip
    monthly-minutes                0
    net-management-control         disabled
    delay-media-update             disabled
    refer-call-transfer            disabled
    dyn-refer-term                 disabled
    codec-policy
    codec-manip-in-realm           disabled
    constraint-name
    call-recording-server-id
    xnq-state                      xnq-unknown
    hairpin-id                     0
    stun-enable                    disabled
    stun-server-ip                 0.0.0.0
    stun-server-port               3478
    stun-changed-ip                0.0.0.0
    stun-changed-port              3479
    match-media-profiles
    qos-constraint
    sip-profile
    sip-isup-profile
```

```
      block-rtcp                     disabled
      hide-egress-media-update       disabled
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-05-15 23:58:52
session-agent
      hostname                       cm601
      ip-address                     192.168.3.48
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP+TCP
      realm-id                       Enterprise
      egress-realm-id
      description
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method
      ping-interval                  0
      ping-send-mode                 keep-alive
      ping-all-addresses             disabled
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
      in-translationid
      out-translationid
      trust-me                       enabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                    disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      p-asserted-id
      trunk-group
      max-register-sustain-rate      0
      early-media-allow
      invalidate-registrations       disabled
      rfc2833-mode                   none
      rfc2833-payload                0
      codec-policy
      enforcement-profile
      refer-call-transfer            disabled
      reuse-connections              NONE
      tcp-keepalive                  none
      tcp-reconn-interval            0
      max-register-burst-rate        0
      register-burst-window          0
      sip-profile
      sip-isup-profile
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 15:12:33
session-agent
      hostname                       138.1.1.242
      ip-address                     138.1.1.242
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       CenturyLink
      egress-realm-id
      description
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method                    OPTIONS;hops=70
      ping-interval                  60
      ping-send-mode                 keep-alive
      ping-all-addresses             disabled
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
      in-translationid
      out-translationid
      trust-me                       enabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                    disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      p-asserted-id
      trunk-group
      max-register-sustain-rate      0
      early-media-allow
      invalidate-registrations       disabled
      rfc2833-mode                   none
      rfc2833-payload                0
      codec-policy
      enforcement-profile
      refer-call-transfer            disabled
      reuse-connections              NONE
      tcp-keepalive                  none
      tcp-reconn-interval            0
      max-register-burst-rate        0
      register-burst-window          0
      sip-profile
      sip-isup-profile
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 15:16:51
sip-config
      state                          enabled
      operation-mode                 dialog
      dialog-transparency            enabled
      home-realm-id                  Enterprise
      egress-realm-id                Enterprise
      nat-mode                       None
      registrar-domain
      registrar-host
      registrar-port                 0
      register-service-route         always
      init-timer                     500
      max-timer                      4000
      trans-expire                   32
      invite-expire                  180
      inactive-dynamic-conn          32
      enforcement-profile
      pac-method
      pac-interval                   10
      pac-strategy                   PropDist
      pac-load-weight                1
      pac-session-weight             1
      pac-route-weight               1
      pac-callid-lifetime            600
      pac-user-lifetime              3600
      red-sip-port                   1988
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      add-reason-header              disabled
      sip-message-len                4096
      enum-sag-match                 disabled
      extra-method-stats             enabled
      registration-cache-limit       0
      register-use-to-for-lp         disabled
      options                        max-udp-length=65535
                                       set-inv-exp-at-100-resp
      refer-src-routing              disabled
      add-ucid-header                disabled
      proxy-sub-events
      pass-gruu-contact              disabled
      sag-lookup-on-redirect         disabled
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-09-09 16:43:20
sip-interface
      state                          enabled
      realm-id                       CenturyLink
      description
      sip-port
            address                        205.1.1.21
            port                           5060
            transport-protocol             UDP
            tls-profile
            allow-anonymous                all
            ims-aka-profile
      carriers
      trans-expire                   0
      invite-expire                  0
      max-redirect-contacts          0
      proxy-mode
      redirect-action
      contact-mode                   none
      nat-traversal                  none
      nat-interval                   30
      tcp-nat-interval               90
      registration-caching           disabled
      min-reg-expire                 300
      registration-interval          3600
      route-to-registrar             disabled
      secured-network                disabled
      teluri-scheme                  disabled
      uri-fqdn-domain
      trust-mode                     all
      max-nat-interval               3600
      nat-int-increment              10
      nat-test-increment             30
      sip-dynamic-hnt                disabled
      stop-recurse                   401,407
      port-map-start                 0
      port-map-end                   0
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      sip-ims-feature                disabled
      operator-identifier
      anonymous-priority             none
      max-incoming-conns             0
      per-src-ip-max-incoming-conns  0
      inactive-conn-timeout          0
      untrusted-conn-timeout         0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode           pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
      term-tgrp-mode                 none
      implicit-service-route         disabled
      rfc2833-payload                101
      rfc2833-mode                   transparent
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                disabled
      enforcement-profile
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      sip-profile
      sip-isup-profile
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 15:22:14
sip-interface
      state                          enabled
      realm-id                       Enterprise
      description
      sip-port
            address                        192.168.3.3
            port                           5060
            transport-protocol             TCP
            tls-profile
            allow-anonymous                all
            ims-aka-profile
```

```
carriers
trans-expire                   0
invite-expire                  0
max-redirect-contacts          0
proxy-mode
redirect-action
contact-mode                   none
nat-traversal                  none
nat-interval                   30
tcp-nat-interval               90
registration-caching           disabled
min-reg-expire                 300
registration-interval          3600
route-to-registrar             disabled
secured-network                disabled
teluri-scheme                  disabled
uri-fqdn-domain
trust-mode                     all
max-nat-interval               3600
nat-int-increment              10
nat-test-increment             30
sip-dynamic-hnt                disabled
stop-recurse                   401,407
port-map-start                 0
port-map-end                   0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature                disabled
operator-identifier
anonymous-priority             none
max-incoming-conns             0
per-src-ip-max-incoming-conns  0
inactive-conn-timeout          0
untrusted-conn-timeout         0
network-id
ext-policy-server
default-location-string
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                 none
implicit-service-route         disabled
rfc2833-payload                101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
ims-aka-feature                disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive                  none
add-sdp-invite                 disabled
add-sdp-profiles
```

```
      sip-profile
      sip-isup-profile
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 15:24:24
steering-pool
      ip-address                     205.1.1.21
      start-port                     16384
      end-port                       32767
      realm-id                       CenturyLink
      network-interface
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-06 15:27:07
steering-pool
      ip-address                     192.168.3.3
      start-port                     16384
      end-port                       32767
      realm-id                       Enterprise
      network-interface
      last-modified-by               admin@135.9.230.222
      last-modified-date             2010-09-09 16:12:51
system-config
      hostname
      description
      location
      mib-system-contact
      mib-system-name
      mib-system-location
      snmp-enabled                   enabled
      enable-snmp-auth-traps         disabled
      enable-snmp-syslog-notify      disabled
      enable-snmp-monitor-traps      disabled
      enable-env-monitor-traps       disabled
      snmp-syslog-his-table-length   1
      snmp-syslog-level              WARNING
      system-log-level               WARNING
      process-log-level              NOTICE
      process-log-ip-address         0.0.0.0
      process-log-port               0
      collect
            sample-interval                5
            push-interval                  15
            boot-state                     disabled
            start-time                     now
            end-time                       never
            red-collect-state              disabled
            red-max-trans                  1000
            red-sync-start-time            5000
            red-sync-comp-time             1000
            push-success-trap-state        disabled
      call-trace                     disabled
      internal-trace                 disabled
      log-filter                     all
      default-gateway                205.1.1.1
      restart                        enabled
      exceptions
      telnet-timeout                 0
      console-timeout                0
      remote-control                 enabled
      cli-audit-trail                enabled
      link-redundancy-state          disabled
      source-routing                 disabled
      cli-more                       disabled
      terminal-height                24
      debug-timeout                  0
      trap-event-lifetime            0
      default-v6-gateway             ::
      ipv6-support                   disabled
      cleanup-time-of-day            00:00
      last-modified-by               admin@135.9.230.222
      last-modified-date             2011-01-05 00:53:39
task done
EnterpriseSBC#
```

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.