



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring TELUS SIP Trunking with Avaya Aura® Communication Manager 5.2.1 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 TELUS SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 5.2.1, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

TELUS 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 TELUS SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 5.2.1, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to TELUS SIP Trunking via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager and the Acme Packet 3800 Net-Net SBC.

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

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test. Please note that enterprise SIP endpoints are not supported in this configuration and so were not tested.

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various enterprise phone types including H.323, digital, and analog telephones. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various enterprise phone types including H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client)
Avaya one-X® Communicator can place calls from the local computer or control a remote phone. Both of these modes were tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Only the H.323 version of Avaya one-X® Communicator was tested.
- Inbound and outbound calls to/from TELUS Derived Voice endpoints
- Inbound and outbound calls to/from TELUS Mobility endpoints

- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, and local directory assistance (411).
- Codec G.711MU, G.711A and G.729A.
- 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
- Voicemail Message Waiting Indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and enterprise mobility (extension to cellular)
- T.38 Fax (established from an initial G.711MU/A call)
- Network Call Redirection using the SIP REFER method

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested.
- Call redirection requested by a 302 response is not supported by TELUS.
- Establishment of a T.38 fax from a G.729 call could not be tested due to a limitation of the lab environment.

2.2. Test Results

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

- **OPTIONS Max-Forwards Value:** TELUS requires that SIP OPTIONS messages sent from the enterprise contain a Max-Forwards value of zero. The SBC was configured to originate OPTIONS messages to the network with Max-Forward set to zero. See the **ping-method** setting in **Section 6.8.1**.
- **Use of SA8965:** TELUS requires re-INVITEs to contain Session Description Protocol (SDP) information. Thus, the Communication Manager special application SA8965 must be enabled. (See **Section 5.2**)
- **Incorrect Error Indication if No Matching Codec Offered:** If the Communication Manager SIP trunk is improperly configured to have no matching codec with the service provider and an inbound call is placed, Communication Manager returns a “500 Service Unavailable” response instead of a “488 Not Acceptable Here” response. The user hears a network announcement.
- **Re-INVITE When Covering to Voicemail Does Not Contain SDP:** In the scenario of an inbound call to an enterprise extension that covers to voicemail, the resulting re-INVITE to redirect media between the SBC/network and the voicemail server does not contain SDP. This seems to be an issue with special application SA8965 and is being investigated by Avaya development. This scenario did not cause any user perceivable problems. Voicemail messages could be left by the caller and retrieved by the recipient.
- **Codecs:** G.711MU is the preferred/default codec used by TELUS. G.729 is supported but is not available on all media gateways in the TELUS network.

- **Call Forwarding and EC500:** Inbound PSTN calls that are call forwarded back to the PSTN or ring to an EC500 (enterprise mobility) endpoint, will display the forwarding party/EC500 host at the destination instead of the original PSTN caller. This is the result of differences in the interpretation/implementation of the SIP Diversion header between TELUS and Communication Manager. A SIP header manipulation was created on the SBC to create the P-Asserted-ID header with information contained in the Diversion header. (See **Sections 6.10.2.12** and **6.10.2.13**) This allows the call to complete but results in the incorrect calling party displayed at the destination as described above.
- **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. Communication Manager provides the new connected party information by updating the Contact header in a re-INVITE message. TELUS does not use the updated Contact header for displaying calling party information.
- **Coverage to Voicemail for TELUS Mobility Users:** Calls from the enterprise to TELUS mobility users that cover to voicemail could result in one-way audio. If this occurs, the caller will not be able to hear the voicemail announcements and menus. A software change was made on Communication Manager to address this issue and was built on top of Release 5.2.1 Service Pack 11. The change was tested and passed compliance testing using an early development release. The change will be available in a future service pack release. Customers who encounter this problem should use the standard escalation process to request a patch from Avaya Global Services.
- **Use of REFER:** Enabling of the Network Call Redirection feature on the Communication Manager SIP trunk activates the use of the SIP REFER method for various inbound PSTN calls redirected back to the PSTN. The use of the REFER method resulted in dropped calls for blind transfer and vector redirection scenarios. Enabling of Network Call Redirection is not recommended.
- **T.38 Fax – Network Coverage:** Not all media gateways in the TELUS network support T.38 fax. Communication Manager does not support fallback to G.711 pass-through fax from T.38 fax. Thus, if a T.38 fax call encounters a media gateway in the TELUS network that does not support T.38 then the call will terminate.
- **Transitioning to T.38 for Outbound Calls:** In general, the answering side of a fax call will send a re-INVITE to transition to T.38. For outbound fax calls to the PSTN, this means the network would typically send the re-INVITE to transition to T.38. However, TELUS requires Communication Manager to transition to T.38 for both inbound and outbound fax calls. Relying on Communication Manager to transition to T.38 on an outbound call may have the following impact:
 - On an outbound call, sending of the T.38 INVITE happens on detection of the V.21 preamble of the originating fax machine's Digital Command Signal (DCS) message. This is part of the T.30 exchange. This request to transition to T.38 may happen too late for some terminating gateways to accommodate the switch to T.38.
 - If the initial call is using the G.729 codec, the compression of the V.21 preamble may cause its detection to be less reliable than if the call was initially using G.711.

- The ability to transition to T.38 in the middle of the T.30 exchange is supported on the following Avaya media platforms (G430/G450/TN2602). Older platforms (G350/G700/TN2302) may have different behavior.

Compliance testing was conducted with the TN2602 media platform (part of the G650 media gateway) using codec G.711MU to initially establish the call. Outbound T.38 fax calls in this environment were successful.

- **G.711 Pass-through Fax:** Communication Manager does not support G.711 pass-through fax over SIP trunks. These calls are treated like any other voice call by Communication Manager. If a customer chooses to use G.711 pass-through fax, success is not guaranteed.
- **Inbound Calls With Calling Party Number (CPN) Block Enabled:** Communication Manager will accept calls from SIP domains/hosts that it recognizes. This is determined by comparing the uri-host portion of the P-Asserted-Identity (PAI) header or From header in the incoming INVITE with the Far-end domain configured in the Communication Manager signaling group. If Communication Manager finds a match in any signaling group, the call is accepted. TELUS does not include the PAI header in the INVITE and in the case of CPN block, the uri-host in the From header is masked with the value of **anonymous.invalid**. In order to allow these calls to complete, a second signaling/trunk group was created on Communication Manager to accept calls from domain **anonymous.invalid**. See Sections 5.7 and 5.8 for details.

2.3. Support

For technical support on the TELUS system, please contact your TELUS Account Executive or visit <http://telus.com>.

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

3. Reference Configuration

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

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

- Duplex Avaya S8710 Servers running Communication Manager
- Avaya G650 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 3800 Net-Net 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 3800 Net-Net SBC. In this way, the 3800 Net-Net SBC can protect the enterprise against any SIP-based attacks. The 3800 Net-Net 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.

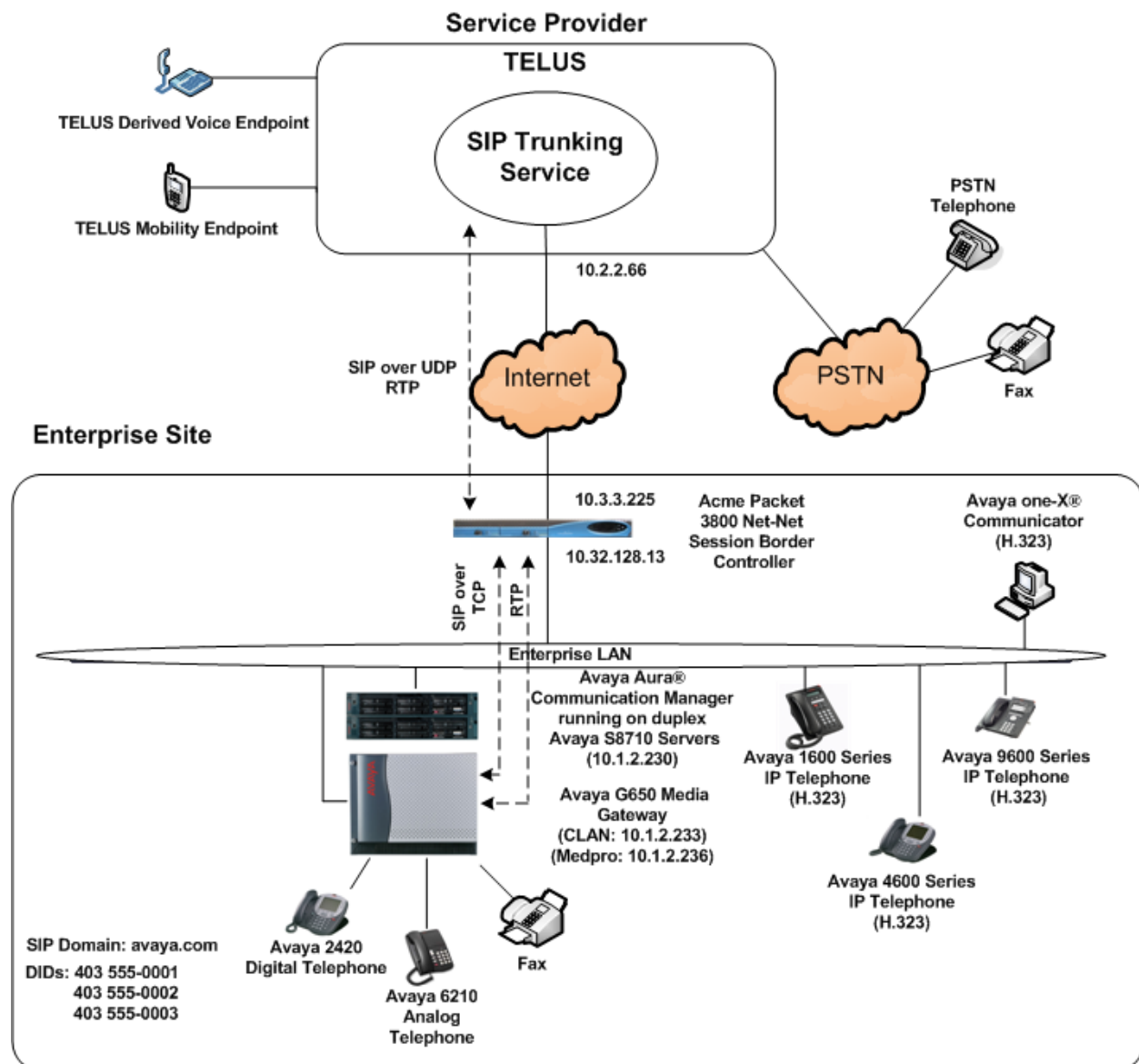


Figure 1: Avaya IP Telephony Network using TELUS SIP Trunking

For inbound calls, the calls flow from the service provider to the 3800 Net-Net 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 3800 Net-Net SBC. From the 3800 Net-Net SBC, the call is sent to TELUS SIP Trunking.

For outbound calls, the enterprise was configured to send 11 digits in the SIP destination headers (Request URI and To) and 10 digits in the SIP source headers (i.e., From, Contact, and P-Asserted-Identity). For inbound calls, TELUS sent 10 digits in both the source headers and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on duplex Avaya S8710 Servers	5.2.1 SP11 + dev patch (R015x.02.1.016.4-19308) + dev patch
Avaya G650 Media Gateway <ul style="list-style-type: none"> IP Server Interface (IPSI) TN2312BP Control LAN (CLAN) TN799DP IP Media Processor (MEDPRO) TN2602AP 	HW15 FW054 HW01 FW040 HW02 FW061
Avaya 1608 IP Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.3.1
Avaya 4621SW IP Telephone (H.323)	2.9.2
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1 SP4 (3.1.04S)
Avaya one-X® Communicator (H.323)	6.1 (Build 6.1.0.12-GA-30334)
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Acme Packet 3800 Net-Net Session Border Controller	SCX6.2.0 MR-3 GA (Build 619)
TELUS SIP Trunking Solution Components	
Component	Release
Acme Packet 4520 Net-Net Session Border Controller	6.1m7p5
Nokia Siemens Networks HiQ 4200	Version 14.0

Table 1: Equipment and Software Tested

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for TELUS SIP Trunking. A SIP trunk is established between Communication Manager and the 3800 Net-Net SBC for use by traffic to and from TELUS. It is assumed the general installation of Communication Manager, Avaya Media Gateway and 3800 Net-Net SBC has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 800 SIP trunks are available and 208 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page	2 of 10
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	800	200	
Maximum Concurrently Registered IP Stations:	18000	5	
Maximum Administered Remote Office Trunks:	0	0	
Maximum Concurrently Registered Remote Office Stations:	0	0	
Maximum Concurrently Registered IP eCons:	0	0	
Max Concur Registered Unauthenticated H.323 Stations:	0	0	
Maximum Video Capable H.323 Stations:	0	0	
Maximum Video Capable IP Softphones:	0	0	
Maximum Administered SIP Trunks:	800	208	
Maximum Administered Ad-hoc Video Conferencing Ports:	0	0	
Maximum Number of DS1 Boards with Echo Cancellation:	0	0	
Maximum TN2501 VAL Boards:	10	1	
Maximum Media Gateway VAL Sources:	0	0	
Maximum TN2602 Boards with 80 VoIP Channels:	128	0	
Maximum TN2602 Boards with 320 VoIP Channels:	128	2	
Maximum Number of Expanded Meet-me Conference Ports:	0	0	

5.2. Special Application SA8965

TELUS requires that all INVITE messages contain SDP information, including re-INVITES. In general, when Communication Manager sends a re-INVITE to perform a media shuffling operation (redirect media directly between two endpoints) the re-INVITE will not include SDP information. In order to change this behavior, special application SA8965 must be enabled. This is done via the **change system-parameters special-applications** command. Navigate to **Page 7** and enter a **y** next to the special application titled **SA8965 - SIP Shuffling with SDP** in the list below. By enabling this feature, a new protocol variation parameter will appear on **Page 3** of the trunk form (See **Section 5.8**).

```
change system-parameters special-applications                               Page 7 of 9
                                SPECIAL APPLICATIONS

                                (SA8888) - Per Station Music On Hold? n
(SA8889) - Verizon VoiceGenie SIP MIME Message Bodies? n
                                (SA8891) - Verizon VoiceGenie SIP Headers? n
                                    (SA8893) - Blast Conference? n
                                (SA8896) - IP Softphone Lamp Control? n
                                (SA8900) - Support for NTT Call Screening? n
                                (SA8904) - Location Based Call Type Analysis? n
                                (SA8911) - Expanded Public Unknown Table? n
(SA8917) - LSP Redirect using special coverage point? n
                                    (SA8927) - Increase Paging Groups? n
(SA8928) - Display Names on Bridged Appearance Labels? n
                                (SA8931) - Send IE with EC500 Extension Number? n
                                (SA8942) - Multiple Unicode Message File Support? n
                                (SA8944) - Multiple Logins for Single IP Address? n
                                    (SA8946) - Site Data Expansion? n
(SA8958) - Increase BSR Polling/Interflow Pairs to 40000? n
                                    (SA8965) - SIP Shuffling with SDP? y
(SA8967) - Mask CLI and Station Name for QSIG/ISDN Calls? y
```

5.3. System Features

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

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

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

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

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

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

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

ENBLOC DIALING PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

5.4. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the CLAN circuit pack (**clan1**) and for the 3800 Net-Net SBC (**spAcme1**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
bvSM	10.32.24.235	
clan1	10.1.2.233	
default	0.0.0.0	
medpro2	10.1.2.236	
procr	. . .	
procr1	10.1.2.11	
procr2	10.1.2.21	
spAcme1	10.32.128.13	

5.5. 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. G.711MU is the preferred/default codec used by TELUS. G.729 is supported but is not available on all media gateways in the TELUS network. Thus, the list of offered codecs must include G.711Mu. For the compliance test, G.729A, G.711Mu and G.711A were defined in IP codec set 4. To use these codecs, enter **G.729A**, **G.711MU** and **G.711A** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

change ip-codec-set 4

Page 1 of 2

IP Codec Set

Codec Set: 4

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

On **Page 2**, to enable T.38 fax, set the **Fax Mode** to **t.38-standard**. Otherwise, set the **Fax Mode** to **off**.

change ip-codec-set 4			Page 2 of 2
IP Codec Set			
Allow Direct-IP Multimedia? n			
FAX	Mode	Redundancy	
	t.38-standard	0	
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

5.6. IP Network Region

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

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.5**.
- Default values can be used for all other fields.

```
change ip-network-region 4                                     Page 1 of 19

                                IP NETWORK REGION

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

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

change ip-network-region 4										Page	3	of	19
Source Region: 4										Inter Network Region Connection Management			
										I			M
										G	A		t
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c				
rgn	set	WAN	Units	Total Norm	Prio Shr Regions	CAC	R	L	e				
1	4	y	NoLimit				n		t				
2													
3													
4	4											all	

5.7. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the 3800 Net-Net 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 36 was used and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to **tcp**. The transport method specified here is used between Communication Manager and 3800 Net-Net SBC.
- Set the **IMS Enabled** field to **n**.
- Set the **Near-end Node Name** to **clan1**. This node name maps to the IP address of the CLAN circuit pack as defined in **Section 5.4**.
- Set the **Far-end Node Name** to **spAcme1**. This node name maps to the IP address of 3800 Net-Net SBC as defined in **Section 5.4**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5060**. This is the standard port value for SIP over TCP.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**.
- Set the **Far-end Domain** to the IP address of the TELUS SIP proxy.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media

Gateway, these resources may be depleted during high call volume preventing additional calls from completing.

- 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 36                                     Page 1 of 1
                                     SIGNALING GROUP

Group Number: 36                Group Type: sip
                                Transport Method: tcp

IMS Enabled? n

Near-end Node Name: clan1        Far-end Node Name: spAcme1
Near-end Listen Port: 5060        Far-end Listen Port: 5060
Far-end Network Region: 4
Far-end Domain: 10.2.2.66

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

In order to allow inbound calls with CPN block enabled (see **Section 2.2** for details), a second signaling group (signaling group 37) was created with the **Far-end Domain** set to **anonymous.invalid**. All other settings should be the same as signaling group 36 above.

```
add signaling-group 37                                     Page 1 of 1
                                     SIGNALING GROUP

Group Number: 37                Group Type: sip
                                Transport Method: tcp

IMS Enabled? n

Near-end Node Name: clan1        Far-end Node Name: spAcme1
Near-end Listen Port: 5060        Far-end Listen Port: 5060
Far-end Network Region: 4
Far-end Domain: anonymous.invalid

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

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for each of the signaling groups created in **Section 5.7**. For the compliance test, the first trunk group (trunk group 36) was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group **36** shown in **Section 5.7**.
- 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 36                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 36                Group Type: sip        CDR Reports: y
  Group Name: DirectToSPAcme1    COR: 1              TN: 1        TAC: 136
  Direction: two-way            Outgoing Display? n
  Dial Access? n                Night Service:
  Queue Length: 0
  Service Type: public-ntwrk     Auth Code? n
                                   Signaling Group: 36
                                   Number of Members: 10
```


On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.7**.

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 **900** seconds was used.

add trunk-group 36 Group Type: sip	Page 2 of 21
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 15000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 900	

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 5.3**, 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 36	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: public	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
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** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been re-directed. These settings are needed by TELUS 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 TELUS.

Set the **Shuffling with SDP** field to **y**. This will instruct Communication Manager to send SDP information in shuffling re-INVITEs on calls that use this trunk. This parameter only appears if special application SA8965 is enabled. See **Section 5.2** for full details.

add trunk-group 36	Page 4 of 21
<p style="text-align: center;">PROTOCOL VARIATIONS</p> <p> Mark Users as Phone? n Prepend '+' to Calling Number? n Send Transferring Party Information? n Network Call Redirection? n Send Diversion Header? y Support Request History? n Telephone Event Payload Type: 101 Shuffling with SDP? y </p>	

In order to allow inbound calls with CPN block enabled (see **Section 2.2** for details), a second trunk group (trunk group 37) was created for the signaling group 37 created in **Section 5.7**. Use the instructions for creating trunk group 36 to create trunk group 37. Use a unique value for the **Group Name** and **TAC**. Set the **Direction** to **incoming** so only inbound calls will be allowed on this trunk. Set the **Signaling Group** to **37**. **Page 1** of trunk group 37 is shown below. All other settings on all other pages are the same as trunk 36.

add trunk-group 37	Page 1 of 21
<p style="text-align: center;">TRUNK GROUP</p> <p> Group Number: 37 Group Type: sip CDR Reports: y Group Name: Inbound from Telus COR: 1 TN: 1 TAC: 137 Direction: incoming Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: public-ntwrk Auth Code? n <p style="text-align: right;"> Signaling Group: 37 Number of Members: 10 </p> </p>	

5.9. 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 5.8**), 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 by the SIP service provider. It is used to authenticate the caller.

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

change public-unknown-numbering 0					Page 1 of 1
NUMBERING - PUBLIC/UNKNOWN FORMAT					
				Total	
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	CPN Len	
5	3			5	Total Administered: 4
5	30023	34	4035550001	10	Maximum Entries: 9999
5	30024	34	4035550002	10	
5	30025	34	4035550003	10	

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

change public-unknown-numbering 0					Page 1 of 1
NUMBERING - PUBLIC/UNKNOWN FORMAT					
				Total	
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	CPN Len	
5	3	34	40355	10	Total Administered: 1
					Maximum Entries: 9999

5.10. Outbound Routing

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

change dialplan analysis							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 2		
	Dialed String	Total Length	Call Type		Dialed String	Total Length	Call Type		Dialed String
	1	3	dac						
	2	5	ext						
	222	5	aar						
	3	5	ext						
	3234	7	ext						
	4	5	ext						
	5	5	ext						
	6	5	ext						
	7	7	ext						
	8	1	fac						
	9	1	fac						
	*	3	fac						
	#	3	fac						

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

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

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 36 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	36	op		n
0		11	11	36	op		n
011		10	18	36	intl		n
1403		11	11	36	fpna		n
1647		11	11	36	fpna		n
1780		11	11	36	fpna		n
1800		11	11	36	fpna		n
1877		11	11	36	fpna		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 route pattern in the following manner. The example below shows the values used for route pattern 36 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 36 was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk: 1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers.
- **LAR: next**

change route-pattern 36													Page	1 of	3
Pattern Number: 34 Pattern Name: AcmeSBC Route															
SCCAN? n Secure SIP? n															
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits						QSIG		
													Intw		
1:	36	0	1										n	user	
2:												n	user		
3:												n	user		
4:												n	user		
5:												n	user		
6:												n	user		
BCC VALUE			TSC	CA-TSC	ITC BCIE			Service/Feature	PARM	No.	Numbering	LAR			
0 1 2 M 4 W				Request							Dgts Format				
													Subaddress		
1:	y	y	y	y	y	n	n						rest		next
2:	y	y	y	y	y	n	n						rest		none
3:	y	y	y	y	y	n	n						rest		none
4:	y	y	y	y	y	n	n						rest		none
5:	y	y	y	y	y	n	n						rest		none
6:	y	y	y	y	y	n	n						rest		none

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 Acme Packet 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-configuration** to save the configuration.
11. Type **activate-configuration** 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 to the private enterprise and public networks.

6.1.1. Public Interface

Create a phy-interface to the public 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 → 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 to the private enterprise 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** → **1**
6. **virtual-mac** → **00:08:25:a0:f4:8a**

Virtual MAC addresses are assigned based on the MAC address assigned to the Acme. This MAC address is found by entering the command → **show prom-info mainboard** (e.g. **00 08 25 a0 fa 80**). To define a virtual MAC address, replace the last digit with **8** thru **f**.

7. Enter **duplex-mode** → **FULL**
8. Enter **speed** → **100**
9. Enter **done**
10. Enter **exit**

6.2. Network Interfaces

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

6.2.1. Public Interface

Create a network-interface to the public side of the Acme. The compliance test was performed with a direct Internet connection to the service using the settings below.

1. Enter **system** → **network-interface**
2. Enter **name** → **s0p0**
3. Enter **ip-address** → **10.3.3.225**
4. Enter **netmask** → **255.255.255.224**
5. Enter **gateway** → **10.3.3.254**
6. Enter **dns-ip-primary** → **10.3.184.199**
7. Enter **hip-ip-list** → **10.3.3.225**
8. Enter **icmp-ip-list** → **10.3.3.225**
9. Enter **done**
10. Enter **exit**

6.2.2. Private Interface

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

1. Enter **system** → **network-interface**
2. Enter **name** → **s1p0**
3. Enter **ip-address** → **10.32.128.13**
4. Enter **netmask** → **255.255.255.0**
5. Enter **gateway** → **10.32.128.254**
6. Enter **hip-ip-list** → **10.32.128.13**

7. Enter **icmp-ip-list** → **10.32.128.13**
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** → **EXTERNAL**
3. Enter **network-interfaces** → **s0p0:0**
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** → **INTERNAL2**
3. Enter **network-interfaces** → **s1p0:0**
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 3800 Net-Net SBC.

6.4.1. Outside Steering-Pool

Create a steering-pool for the outside network. The start-port and end-port values should specify a range acceptable to the service provider. For the compliance test, no specific range was specified by the service provider, so the start and end ports shown below were chosen arbitrarily.

1. Enter **media-manager** → **steering-pool**
2. Enter **ip-address** → **10.3.3.225**
3. Enter **start-port** → **49152**
4. Enter **end-port** → **65535**
5. Enter **realm-id** → **EXTERNAL**
6. Enter **done**
7. Enter **exit**

6.4.2. Inside Steering-Pool

Create a steering-pool for the inside network. The start-port and end-port values should specify a range acceptable to the internal enterprise network and include the port range used by Communication Manager. For the compliance test, a wide range was selected that included the default port range that Communication Manager uses and shown on the ip-network-region form in **Section 5.6**.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 10.32.128.13**
3. Enter **start-port → 2048**
4. Enter **end-port → 65535**
5. Enter **realm-id → INTERNAL2**
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 3800 Net-Net SBC SIP operating parameters. The home-realm is the internal default realm for the 3800 Net-Net SBC and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere. If the egress-realm is blank, the home-realm is used instead.

1. Enter **session-router → sip-config**
2. Enter **state → enabled**
3. Enter **operation-mode → dialog**
4. Enter **home-realm-id → INTERNAL2**
5. Enter **egress-realm-id →**
6. Enter **nat-mode → Public**
7. Enter **done**
8. Enter **exit**

6.7. SIP Interfaces

The SIP interface defines the SIP signaling interface (IP address and port) on the 3800 Net-Net SBC.

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** → **EXTERNAL**
4. Enter **sip-port**
 - a. Enter **address** → **10.3.3.225**
 - b. Enter **port** → **5060**
 - c. Enter **transport-protocol** → **UDP**
 - d. Enter **allow-anonymous** → **agents-only**
 - 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** → **INTERNAL2**
4. Enter **sip-port**
 - a. Enter **address** → **10.32.128.13**
 - 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 Communication Manager CLAN (inside). SIP header manipulations can be applied to the 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** → **10.2.2.66**

3. Enter **ip-address** → 10.2.2.66
4. Enter **port** → 5060
5. Enter **state** → enabled
6. Enter **app-protocol** → SIP
7. Enter **transport-method** → UDP
8. Enter **realm-id** → EXTERNAL
9. Enter **description** → TELUS
10. Enter **ping-method** → OPTIONS;hops=0
11. Enter **ping-interval** → 60
12. Enter **ping-send-mode** → keep-alive
13. Enter **in-manipulationid** →
14. Enter **out-manipulationid** → outManToSP
15. Enter **done**
16. 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** → 10.1.2.233
3. Enter **ip-address** → 10.1.2.233
4. Enter **port** → 5060
5. Enter **state** → enabled
6. Enter **app-protocol** → SIP
7. Enter **transport-method** → StaticTCP
8. Enter **realm-id** → INTERNAL2
9. Enter **description** → TrentonClan1
10. Enter **ping-method** →
11. Enter **ping-interval** → 0
12. Enter **ping-send-mode** → keep-alive
13. Enter **in-manipulationid** → inManFromCM
14. Enter **done**
15. Enter **exit**

6.9. Local Policies

Local policies allow SIP requests from the **INTERNAL2** realm to be routed to the service provider session agent in the **EXTERNAL** realm (and vice-versa).

6.9.1. INTERNAL2 to EXTERNAL

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

1. Enter **session-router** → local-policy
2. Enter **from-address** → *
3. Enter **to-address** → *
4. Enter **source-realm** → INTERNAL2

5. Enter **state** → **enabled**
6. Enter **policy-attributes**
 - a. Enter **next-hop** → **10.2.2.66**
 - b. Enter **realm** → **EXTERNAL**
 - 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. EXTERNAL to INTERNAL2

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

1. Enter **session-router** → **local-policy**
2. Enter **from-address** → *
3. Enter **to-address** → *
4. Enter **source-realm** → **EXTERNAL**
5. Enter **state** → **enabled**
6. Enter **policy-attributes**
 - a. Enter **next-hop** → **10.1.2.233**
 - b. Enter **realm** → **INTERNAL2**
 - 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**

6.10. SIP Manipulations

SIP manipulation specifies rules for manipulating the contents of specified SIP headers. Two separate sets of SIP manipulations were required for the compliance test listed below.

- **inManFromCM** – A set of SIP header manipulation rules (HMRs) on traffic from Communication Manager to the SBC.
- **outManToSP** - A set of SIP header manipulation rules on traffic from the SBC to service provider (TELUS).

6.10.1. Communication Manager to SBC

The following set of SIP HMRs is applied to traffic from Communication Manager to the SBC. In some call flows the user part of the SIP Contact header received from Communication Manager was not passed unaltered to the public side of the SBC. To correct this, the user part of the Contact header is stored when received from Communication Manager and used to create a

temporary header called X-Contact that will be deleted on the outbound (public) side of the SBC. The information contained in the X-Contact header will be used to recreate the proper Contact header on the public side of the SBC as shown in **Sections 6.10.2.7 and 6.10.2.8**.

To create this set of SIP HMRs:

1. Enter **session-router** → **sip-manipulation**
2. Enter **name** → **inManFromCM**
3. Enter **description** → **“Inbound SIP HMRs From CM”**
4. Proceed to the following sections. Once all sections are completed then proceed with **Steps 5 and 6** below.
5. Enter **done**
6. Enter **exit**

6.10.1.1 Store Contact

This rule stores the user part of the incoming Contact header.

1. Enter **header-rule**
2. Enter **name** → **strcon**
3. Enter **header-name** → **Contact**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule**
 - a. Enter **name** → **strval**
 - b. Enter **type** → **uri-user**
 - c. Enter **action** → **store**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **match-value** → **(.*)**
 - g. Enter **done**
 - h. Enter **exit**
9. Enter **done**
10. Enter **exit**

6.10.1.2 Create X-Contact

This rule creates a temporary header called X-Contact containing only the user part of the incoming Contact header as stored by the rule defined in the previous section.

1. Enter **header-rule**
2. Enter **name** → **addXcontact**
3. Enter **header-name** → **X-Contact**
4. Enter **action** → **add**
5. Enter **comparison-type** → **pattern-rule**

6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule**
 - a. Enter **name** → **addX**
 - b. Enter **type** → **header-value**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **pattern-rule**
 - f. Enter **new-value** → **\$strcon.\$strval.\$0**
 - g. Enter **done**
 - h. Enter **exit**
9. Enter **done**
10. Enter **exit**

6.10.2. SBC to TELUS

The following set of SIP HMRs is applied to traffic from the SBC to TELUS.

To create this set of SIP HMRs:

1. Enter **session-router** → **sip-manipulation**
2. Enter **name** → **outManToSP**
3. Enter **description** → **“outbound SIP HMRs To SP”**
4. Proceed to the following sections. Once all sections are completed then proceed with **Steps 5 and 6** below.
5. Enter **done**
6. Enter **exit**

6.10.2.1 Change Host of the To Header

This rule replaces the host part of the To header with the service provider's IP address.

1. Enter **header-rule**
2. Enter **name** → **manipTo**
3. Enter **header-name** → **To**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **pattern-rule**
6. Enter **msg-type** → **request**
7. Enter **element-rule**
 - a. Enter **name** → **chgToHost**
 - b. Enter **type** → **uri-host**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **new-value** → **\$REMOTE_IP**
 - g. Enter **done**
 - h. Enter **exit**

8. Enter **done**
9. Enter **exit**

6.10.2.2 Change Host of the From Header

This rule replaces the host part of the From header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipFrom**
3. Enter **header-name** → **From**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule**
 - a. Enter **name** → **From**
 - b. Enter **type** → **uri-host**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **new-value** → **\$LOCAL_IP**
 - g. Enter **done**
 - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

6.10.2.3 Change Host of the History Info Header

This rule replaces the host part of the History-Info header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipHistInfo**
3. Enter **header-name** → **History-Info**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule**
 - a. Enter **name** → **HistoryInfo**
 - b. Enter **type** → **uri-host**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **new-value** → **\$LOCAL_IP**
 - g. Enter **done**
 - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

6.10.2.4 Change Host of the PAI Header

This rule replaces the host part of the P-Asserted-Identity header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipPAI**
3. Enter **header-name** → **P-Asserted-Identity**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule**
 - a. Enter **name** → **Pai**
 - b. Enter **type** → **uri-host**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **new-value** → **\$LOCAL_IP**
 - g. Enter **done**
 - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

6.10.2.5 Change Host of the Diversion Header

This rule replaces the host part of the Diversion header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipDiversion**
3. Enter **header-name** → **Diversion**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule**
 - a. Enter **name** → **Diversion**
 - b. Enter **type** → **uri-host**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **new-value** → **\$LOCAL_IP**
 - g. Enter **done**
 - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

6.10.2.6 Change Host of the Refer-To Header

This rule replaces the host part of the Refer-To header with the service provider's IP address.

1. Enter **header-rule**
2. Enter **name** → **manipRefer**
3. Enter **header-name** → **Refer-To**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule**
 - a. Enter **name** → **chgHostRefer**
 - b. Enter **type** → **uri-host**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **new-value** → **\$REMOTE_IP**
 - g. Enter **done**
 - h. Enter **exit**
8. Enter **done**
9. Enter **exit**

6.10.2.7 Store X-Contact Header

This rule stores the contents of the X-Contact header so it can be used later. The X-Contact header contains only the user part of the Contact header as it was originally received from Communication Manager as described in **Section 6.10.1**.

1. Enter **header-rule**
2. Enter **name** → **storexcontact**
3. Enter **header-name** → **X-Contact**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule**
 - a. Enter **name** → **storexcontact**
 - b. Enter **type** → **header-value**
 - c. Enter **action** → **store**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **match-value** → **(.*)**
 - g. Enter **done**
 - h. Enter **exit**
9. Enter **done**
10. Enter **exit**

6.10.2.8 Replace Contact Header

This rule uses the data stored from the X-Contact header to overwrite the user part of the outbound Contact header.

1. Enter **header-rule**
2. Enter **name** → **replacecontact**
3. Enter **header-name** → **Contact**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **pattern-rule**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **element-rule**
 - a. Enter **name** → **replacecontact**
 - b. Enter **type** → **uri-user**
 - c. Enter **action** → **replace**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **pattern-rule**
 - f. Enter **match-value** → **(.*)**
 - g. Enter **new-value** **\$storexcontact.\$storexcontact.\$0**
 - h. Enter **done**
 - i. Enter **exit**
9. Enter **done**
10. Enter **exit**

6.10.2.9 Delete X-Contact Header

This rule deletes the temporary X-Contact header before sending the message to the service provider.

1. Enter **header-rule**
2. Enter **name** → **delxcontact**
3. Enter **header-name** → **X-Contact**
4. Enter **action** → **delete**
5. Enter **comparison-type** → **pattern-rule**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE,UPDATE**
8. Enter **done**
9. Enter **exit**

6.10.2.10 Delete P-Location Header

This rule deletes the P-Location header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

1. Enter **header-rule**
2. Enter **name** → **delPloc**

3. Enter **header-name** → **P-Location**
4. Enter **action** → **delete**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **any**
7. Enter **methods** →
8. Enter **done**
9. Enter **exit**

6.10.2.11 Delete Alert-Info Header

This rule deletes the Alert-Info header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

1. Enter **header-rule**
2. Enter **name** → **delAlert**
3. Enter **header-name** → **Alert-Info**
4. Enter **action** → **delete**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **any**
7. Enter **methods** →
8. Enter **done**
9. Enter **exit**

6.10.2.12 Store Diversion Header User and Display Name

This rule stores the user and the display name parts of the Diversion header to be used in the next section to modify the PAI header. This is necessary to complete calls from the PSTN which are redirected back to the PSTN. See **Section 2.2** for more details.

1. Enter **header-rule**
2. Enter **name** → **strDivNum**
3. Enter **header-name** → **Diversion**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE**
8. Enter **element-rule**
 - a. Enter **name** → **strval**
 - b. Enter **type** → **uri-user**
 - c. Enter **action** → **store**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **case-sensitive**
 - f. Enter **match-value** → **(.*)**
 - g. Enter **done**
 - h. Enter **exit**
9. Enter **element-rule**

- a. Enter **name** → **strDisName**
- b. Enter **type** → **uri-display**
- c. Enter **action** → **store**
- d. Enter **match-val-type** → **any**
- e. Enter **comparison-type** → **case-sensitive**
- f. Enter **match-value** → **(.*)**
- g. Enter **done**
- h. Enter **exit**
10. Enter **done**
11. Enter **exit**

6.10.2.13 Create PAI Header with Diversion Header Information

This rule creates the PAI header using the information stored from the Diversion header in the last section. It only creates the PAI header in the INVITE message if the Diversion header is present. This is determined by checking if any value was stored for the Diversion user from the previous rule. This rule is necessary to complete calls from the PSTN which are redirected back to the PSTN. See **Section 2.2** for more details.

1. Enter **header-rule**
2. Enter **name** → **makePAIfromDiv**
3. Enter **header-name** → **P-Asserted-Identity**
4. Enter **action** → **add**
5. Enter **comparison-type** → **boolean**
6. Enter **msg-type** → **request**
7. Enter **methods** → **INVITE**
8. Enter **match-value** → **\$strDivNum.\$strval.\$0**
9. Enter **element-rule**
 - a. Enter **name** → **newPAIval**
 - b. Enter **type** → **header-value**
 - c. Enter **action** → **add**
 - d. Enter **match-val-type** → **any**
 - e. Enter **comparison-type** → **pattern-rule**
 - f. Enter **match-value** → **(.*)**
 - g. Enter **new-value** →
`"+$strDivNum.$strDisName.$0+"<sip:+$strDivNum.$strval.$0+@+$LOC
AL_IP+>`
 - h. Enter **done**
 - i. Enter **exit**
10. Enter **done**
11. Enter **exit**

6.10.2.14 Delete Diversion Header

This rule deletes the Diversion header. The Diversion header is no longer needed once the PAI has been modified. It may also cause unexpected behavior if forwarded on to the TELUS network.

1. Enter **header-rule**
2. Enter **name** → **delDiv**
3. Enter **header-name** → **Diversion**
4. Enter **action** → **delete**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **any**
7. Enter **methods** →
8. Enter **done**
9. Enter **exit**

7. TELUS SIP Trunking Configuration

TELUS is responsible for the network configuration of the TELUS SIP Trunking service.

TELUS will require that the customer provide the public IP address used to reach the 3800 Net-Net SBC at the edge of the enterprise. TELUS will provide the IP address of the TELUS 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 TELUS and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the TELUS 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:

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

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and Acme Packet 3800 Net-Net Session Border Controller to TELUS SIP Trunking. This solution successfully passed compliance testing via the Avaya DevConnect Program. 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*, May 2009, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, May 2009, Document Number 555-245-205.
- [3] *Avaya 1600 Series IP Deskphones Administrator Guide Release Release 1.3.x*, May 2010, Document Number 16-601443.
- [4] *4600 Series IP Telephone LAN Administrator Guide*, October 2007, Document Number 555-233-507.
- [5] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, November 2009, Document Number 16-300698.
- [6] *Administering Avaya one-X® Communicator*, July 2011.
- [7] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [8] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

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

```

host-routes
    dest-network      10.1.2.0
    netmask           255.255.255.0
    gateway           10.32.128.254
    description
    last-modified-by  admin@192.168.168.37
    last-modified-date 2011-10-27 16:57:53
host-routes
    dest-network      10.32.0.0
    netmask           255.255.0.0
    gateway           10.32.128.254
    description       DevConnectLAN
    last-modified-by  admin@135.11.141.118
    last-modified-date 2010-08-05 15:25:58
host-routes
    dest-network      192.168.0.0
    netmask           255.255.0.0
    gateway           10.32.128.254
    description       Route to remote testers
    last-modified-by  admin@192.168.168.37
    last-modified-date 2011-09-10 10:50:25
local-policy
    from-address
    to-address
    source-realm
    description
    activate-time     N/A
    deactivate-time   N/A
    state             enabled
    policy-priority    none
    last-modified-by  admin@192.168.168.37
    last-modified-date 2011-12-19 13:06:16
    policy-attribute
        next-hop      10.2.2.66
        realm          EXTERNAL
        action         none
        terminate-recursion enabled
        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	EXTERNAL
description	
activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	none
last-modified-by	admin@192.168.168.37
last-modified-date	2012-03-26 12:59:18
policy-attribute	
next-hop	10.1.2.233
realm	INTERNAL2
action	none
terminate-recursion	enabled
carrier	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	
state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	
media-manager	
state	enabled
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      enabled
min-media-allocation        2000
min-trusted-allocation      4000
deny-allocation             64000
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
dnalg-server-failover       disabled
last-modified-by            admin@135.11.141.142
last-modified-date          2010-06-16 05:40:01
network-interface
  name                       s0p0
  sub-port-id                0
  description
  hostname
  ip-address                 10.3.3.225
  pri-utility-addr
  sec-utility-addr
  netmask                   255.255.255.224
  gateway                   10.3.3.254
  sec-gateway
  gw-heartbeat
    state                    disabled
    heartbeat                0
    retry-count              0
    retry-timeout            1
    health-score             0
  dns-ip-primary            10.3.184.199
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout               11
    hip-ip-list              10.3.3.225
  ftp-address
    icmp-address             10.3.3.225
  snmp-address
  telnet-address
  ssh-address
  last-modified-by          admin@192.168.168.37
  last-modified-date        2011-09-10 10:08:47
network-interface
  name                       s1p0
  sub-port-id                0
  description
  hostname
  ip-address                 10.32.128.13
  pri-utility-addr

```

sec-utility-addr	
netmask	255.255.255.0
gateway	10.32.128.254
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	10.32.128.13
ftp-address	10.32.128.13
icmp-address	10.32.128.13
snmp-address	
telnet-address	10.32.128.13
ssh-address	
last-modified-by	admin@192.168.168.37
last-modified-date	2011-11-03 11:42:43
phy-interface	
name	s0p0
operation-type	Media
port	0
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	
speed	
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-09-09 19:39:05
phy-interface	
name	slp0
operation-type	Media
port	0
slot	1
virtual-mac	00:08:25:a0:f4:8a
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-09-09 19:38:24
realm-config	
identifier	EXTERNAL
description	
addr-prefix	0.0.0.0
network-interfaces	
s0p0:0	
mm-in-realm	disabled

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@135.11.207.156
last-modified-date	2010-11-03 08:55:21
realm-config	
identifier	INTERNAL2
description	
addr-prefix	0.0.0.0
network-interfaces	
	slp0:0
mm-in-realm	disabled
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@135.11.207.156
last-modified-date	2010-12-16 17:25:01
session-agent	
hostname	10.2.2.66
ip-address	10.2.2.66
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	EXTERNAL
egress-realm-id	
description	TELUS
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=0
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	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	outManToSP
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@192.168.168.37
last-modified-date	2011-10-10 12:21:24

session-agent	
hostname	10.1.2.233
ip-address	10.1.2.233
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	StaticTCP
realm-id	INTERNAL2
egress-realm-id	
description	TrentonClan1
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	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	inManFromCM
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@192.168.168.37
last-modified-date	2012-02-16 16:02:33
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	enabled
home-realm-id	INTERNAL2
egress-realm-id	
nat-mode	Public
registrar-domain	*
registrar-host	*
registrar-port	5060
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180
inactive-dynamic-conn	32
enforcement-profile	
pac-method	
pac-interval	10
pac-strategy	PropDist
pac-load-weight	1
pac-session-weight	1
pac-route-weight	1
pac-callid-lifetime	600
pac-user-lifetime	3600
red-sip-port	1988
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
add-reason-header	disabled
sip-message-len	4096
enum-sag-match	disabled
extra-method-stats	enabled
registration-cache-limit	0
register-use-to-for-lp	disabled
options	max-udp-length=0
refer-src-routing	disabled

add-ucid-header	disabled
proxy-sub-events	
pass-gruu-contact	disabled
sag-lookup-on-redirect	disabled
last-modified-by	admin@192.168.168.37
last-modified-date	2012-02-16 13:46:26
sip-interface	
state	enabled
realm-id	EXTERNAL
description	
sip-port	
address	10.3.3.225
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	agents-only
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@192.168.168.37
last-modified-date            2011-11-18 10:38:42
sip-interface
state                          enabled
realm-id                       INTERNAL2
description
sip-port
    address                    10.32.128.13
    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@135.105.224.163
last-modified-date	2011-08-03 16:00:53
sip-manipulation	
name	outManToSP
description	Outbound SIP HMRs To SP
split-headers	
join-headers	
header-rule	
name	manipTo
header-name	To
action	manipulate
comparison-type	pattern-rule
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	chgToHost
parameter-name	
type	uri-host
action	replace
match-val-type	any

comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	manipFrom
header-name	From
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	From
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	manipDiversion
header-name	Diversion
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	Diversion
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	manipHistInfo
header-name	History-Info
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	HistoryInfo
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	

	new-value	\$LOCAL_IP
header-rule		
	name	manipPAI
	header-name	P-Asserted-Identity
	action	manipulate
	comparison-type	case-sensitive
	msg-type	request
	methods	
	match-value	
	new-value	
	element-rule	
	name	Pai
	parameter-name	
	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	\$LOCAL_IP
header-rule		
	name	storeXcontact
	header-name	X-Contact
	action	manipulate
	comparison-type	case-sensitive
	msg-type	request
	methods	INVITE,UPDATE
	match-value	
	new-value	
	element-rule	
	name	storeXcontact
	parameter-name	
	type	header-value
	action	store
	match-val-type	any
	comparison-type	case-sensitive
	match-value	(.*)
	new-value	
header-rule		
	name	replacecontact
	header-name	Contact
	action	manipulate
	comparison-type	pattern-rule
	msg-type	request
	methods	INVITE,UPDATE
	match-value	
	new-value	
	element-rule	
	name	replacecontact
	parameter-name	
	type	uri-user
	action	replace
	match-val-type	any
	comparison-type	pattern-rule
	match-value	(.*)
	new-value	

\$storeXcontact.\$storeXcontact.\$0

header-rule	
name	delXcontact
header-name	X-Contact
action	delete
comparison-type	pattern-rule
msg-type	request
methods	INVITE, UPDATE
match-value	
new-value	
header-rule	
name	strDivNum
header-name	Diversion
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	INVITE
match-value	
new-value	
element-rule	
name	strval
parameter-name	
type	uri-user
action	store
match-val-type	any
comparison-type	case-sensitive
match-value	(.*)
new-value	
element-rule	
name	strDisName
parameter-name	
type	uri-display
action	store
match-val-type	any
comparison-type	case-sensitive
match-value	(.*)
new-value	
header-rule	
name	manipRefer
header-name	Refer-To
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	chgHostRefer
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	delPloc

header-name	P-Location
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	delAlert
header-name	Alert-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	delDiv
header-name	Diversion
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	makePAIfromDiv
header-name	P-Asserted-Identity
action	add
comparison-type	boolean
msg-type	request
methods	INVITE
match-value	\$strDivNum.\$strval.\$0
new-value	
element-rule	
name	newPAIval
parameter-name	
type	header-value
action	add
match-val-type	any
comparison-type	pattern-rule
match-value	(.*)
new-value	
\"+\$strDivNum.\$strDisName.\$0+\<+sip:\$strDivNum.\$strval.\$0+@+\$LOCAL_IP+>	
last-modified-by	admin@192.168.168.37
last-modified-date	2012-04-02 11:30:18
sip-manipulation	
name	inManFromCM
description	Inbound SIP HMRs From CM
split-headers	
join-headers	
header-rule	
name	strcon
header-name	Contact
action	manipulate
comparison-type	case-sensitive

msg-type	request
methods	INVITE,UPDATE
match-value	
new-value	
element-rule	
name	strval
parameter-name	
type	uri-user
action	store
match-val-type	any
comparison-type	case-sensitive
match-value	(.*)
new-value	
header-rule	
name	addXcontact
header-name	X-Contact
action	add
comparison-type	pattern-rule
msg-type	request
methods	INVITE,UPDATE
match-value	
new-value	
element-rule	
name	addX
parameter-name	
type	header-value
action	replace
match-val-type	any
comparison-type	pattern-rule
match-value	
new-value	\$strcon.\$strval.\$0
last-modified-by	admin@135.11.207.156
last-modified-date	2011-01-03 17:14:28
steering-pool	
ip-address	10.3.3.225
start-port	49152
end-port	65535
realm-id	EXTERNAL
network-interface	
last-modified-by	admin@192.168.168.37
last-modified-date	2011-09-10 10:11:31
steering-pool	
ip-address	10.32.128.13
start-port	2048
end-port	65535
realm-id	INTERNAL2
network-interface	
last-modified-by	admin@135.11.141.118
last-modified-date	2010-10-06 11:28:26
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	enabled
internal-trace	enabled
log-filter	all
default-gateway	10.3.3.254
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@192.168.168.37
last-modified-date	2011-09-10 11:04:14

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.