



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring SIP Trunking Using Qwest iQ SIP Trunk Service and Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services – Issue 1.0**

### **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Qwest iQ SIP Trunk Service and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura™ SIP Enablement Services, Avaya Aura™ Communication Manager, and various Avaya SIP and H.323 endpoints. These Application Notes correspond to the Qwest iQ SIP Trunk Service offered using a Network Border Switch in the network.

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

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the PSTN and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura™ SIP Enablement Services, Avaya Aura™ Communication Manager, and various Avaya SIP and H.323 endpoints. These Application Notes correspond to the Qwest iQ SIP Trunk Service offered using a Network Border Switch (NBS) in the network.

Customers using this Avaya IP telephony solution with the Qwest iQ SIP Trunk Service are able to place and receive PSTN calls via a dedicated broadband Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI. The text and coverage diagram below summarizes the Qwest iQ SIP Trunk Service at the time of writing these Application Notes. Please consult Qwest for the most current description of capabilities.

## 1.1 Qwest iQ SIP Trunk

Qwest iQ SIP Trunk enables the origination and termination of local voice, dedicated long-distance, as well as domestic and international toll-free service across a single broadband connection. It is designed to work in conjunction with the Qwest iQ Networking service, which includes a secure, managed, fully interoperable and scalable suite of wide area network (WAN) services. Qwest iQ Networking service is comprised of advanced Internet protocol (IP)-centric, multi-protocol label switching (MPLS)-based solutions.

### 1.1.1. Features

- Scalability
- Dedicated long-distance\*
- Domestic and International Toll-Free service\*
- Supports emergency 911 calling
- Inherent Security with purchase of MPLS Private and Enhanced Ports
- Switch Diversity\*
- Qwest Control® Network Management Portal
- Competitive service level agreements ([SLAs](#))
- Supports Local Number Portability

\*Off-Net Long Distance, domestic and international Toll Free, and Switch Diversity are available as an option. Additional charges apply. Qwest iQ Networking ports are purchased separately from the Qwest iQ SIP Trunk service.

### 1.1.2. How It Works

Qwest iQ SIP Trunk routes voice calls from your IP-PBX across secure MPLS communication paths using Session Initiation Protocol (SIP)—a signaling protocol that delivers real-time, IP-

based communications. Depending on where the calls terminate, they are either delivered to the Local Exchange Carrier in the customer's area or delivered off-network as a domestic or international long distance call. For calls to existing Qwest® VoIP subscribers, they are delivered on-network, which avoids ordinary toll service fees for domestic long distance.

## 1.2. Interoperability Compliance Testing

A simulated enterprise site using an Avaya IP telephony solution was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to use the commercially available SIP Trunk Service provided by Qwest.

To verify SIP trunk interoperability between the PSTN and an Avaya SIP-based network, the following features and functionality were covered during the interoperability compliance test:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by Qwest. Incoming PSTN calls were made to H.323, digital, and SIP telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Qwest to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, digital, and SIP telephones.
- Various call types were tested including: local, long distance, international, outbound toll-free, operator, and directory assistance.
- Calls using G.729A, G.729B, G.711MU, and G.711A codecs.
- DTMF transmission using RFC 2833 with successful vector navigation for inbound, and voice mail menu navigation for outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and extension to cellular, when the call arrived from the SIP Trunk from Qwest, or when the call forwarding destination and extension to cellular mobile number routed out the SIP Trunk to Qwest, or both.
- Caller ID Presentation and Caller ID Restriction.
- Avaya IP Agent in both “Road Warrior” and “Telecommuter” modes, where incoming PSTN calls arrived from Qwest, or the telecommute number routed out the SIP Trunk to Qwest, or both.

**Please refer to Section 7 for complete test results, known limitations, observations and any necessary workarounds.**

## 1.3. Support

For technical support on the Qwest iQ SIP Trunk services, contact Qwest Customer Service at <http://www.qwest.com/business/products/bundled-solutions/qwest-iq-sip-trunk/qwest-iq-sip-trunk.html>. Select the Contact a Rep link to send an e-mail inquiry or under the Contact a Rep link select Get Phone Numbers for a list of the support phone numbers available.

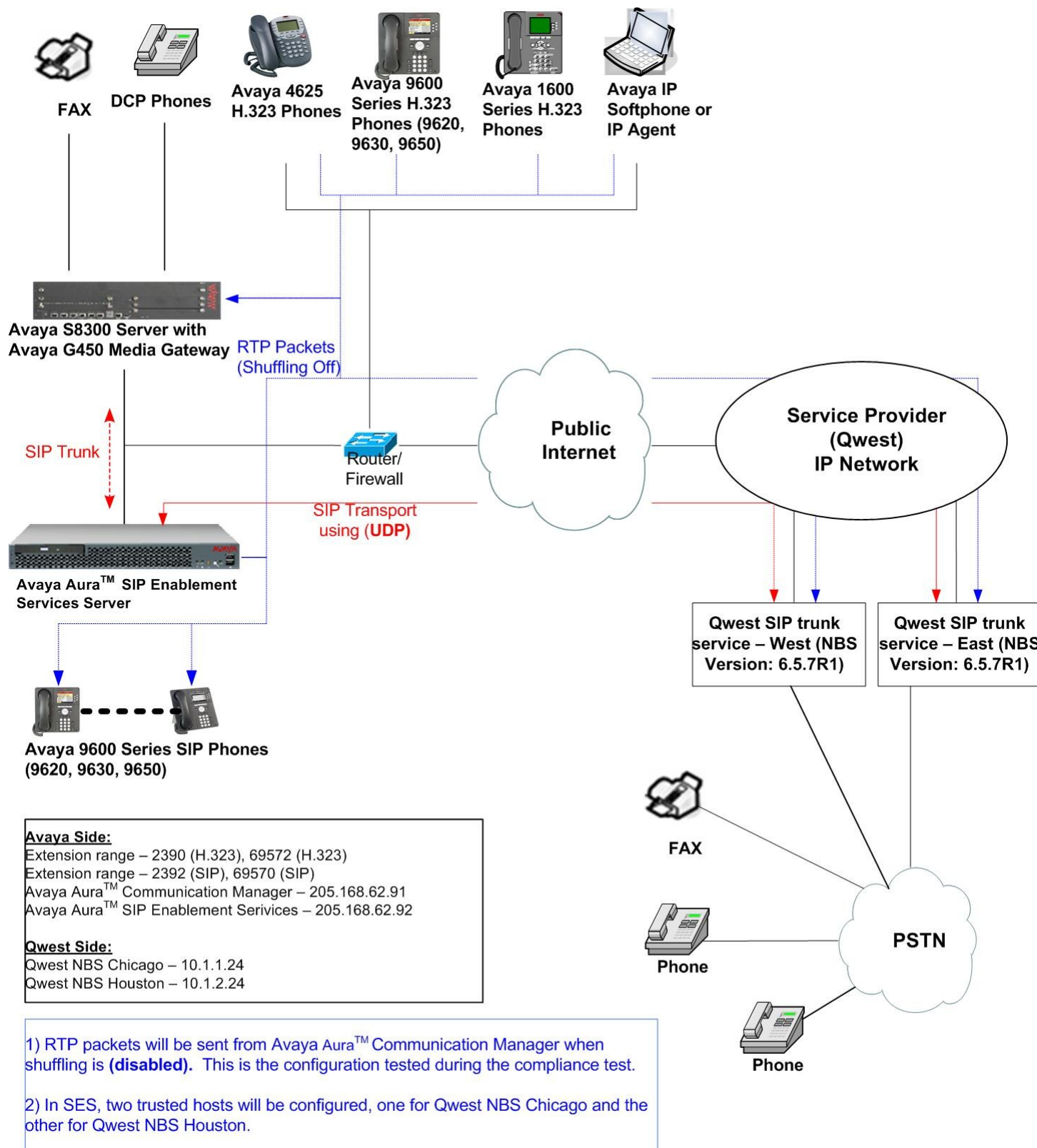
## 2. Reference Configuration

**Figure 1** illustrates an example Avaya IP telephony solution connected to the Qwest iQ SIP Trunk Service. This is the configuration used for DevConnect compliance testing.

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

- Avaya S8300 Server running Communication Manager
- Avaya G450 Media Gateway and associated hardware
- SIP Enablement Services (SES) on an Avaya S8500B Server platform
- Avaya 9600-Series IP telephones (configured for the SIP protocol)
- Avaya 9600-Series IP telephones (configured for the H.323 protocol)
- Avaya 1600-Series IP telephones (configured for the H.323 protocol)
- Avaya 4625 IP Telephone
- Avaya digital phones
- Fax machine
- Avaya IP Agent

For security reasons, the public IP addresses shown in these Application Notes have been replaced with private addresses. Any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.



**Figure 1: Avaya IP Telephony Network using the Qwest iQ SIP Trunk Service**

For incoming calls, the SES uses address maps to direct the incoming SIP messages to Communication Manager, as shown in **Section 5.2.2**. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic routing selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signaling is routed to the SES. The SES directs the outbound SIP messages to the Qwest network.

The dial plan for the configuration described in these Application Notes requires the user to use 1+10 digit dialing for local and long-distance calls over the PSTN. The Qwest iQ SIP Trunk service supports both 10 digit and 1+10 digit dialing. However, the configuration in these Application Notes only sends 10 digits to the service provider in most cases (See **Section 4.2.7**). In addition, Directory Assistance calls (411) and International calls (011+Country Code) were also supported. Communication Manager routes all calls to the Qwest Session Border Controller (NBS) using automatic routing selection.

### 3. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura™ Communication Manager running on an Avaya S8300 Server	5.2.1 (R015x.02.1.016.4) with patch 02.1.016.4-17971
Avaya G450 Media Gateway	
Avaya Aura™ SIP Enablement Services running on an Avaya S8500B Server	5.2.1 (SES05.2.1-02.1.016.4)
Avaya 9600 Series IP Telephone (H.323)	Avaya one-X Deskphone Edition (H.323)
9620	3.1
9630	3.1
9650	3.1
Avaya 4625 IP Telephone (H.323)	2.9
Avaya 9600 Series IP Telephone (SIP)	Avaya one-X Deskphone Edition (SIP)
9620	2.5
9630	2.5
Avaya 1616 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.2
Avaya IP Agent	R7.0 SP7
Qwest iQ SIP Trunk Service Solution Components	
Component	Release
Qwest iQ SIP Trunk service (NBS)	6.5.7R1

**Table 1: Equipment and Software Tested**

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

### 4. Configure Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and SIP Enablement Services (SES). One trunk is created as part of the initial SES installation and is meant to carry SIP signaling between SIP endpoints within the SES domain. A second trunk is created specifically to carry SIP signaling between the SES domain and the Qwest iQ SIP Trunk Service.

It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and SIP Enablement Services has been previously completed and is not discussed here. In addition, it is also assumed that any initial SIP configuration on Communication Manager that is

required to support the SES installation has also been completed. For more information on these installation procedures, refer to [5].

This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. This section will not attempt to show the installation procedures in their entirety.

**Section 4.2** will describe the procedures beyond the initial SIP installation that are necessary to configure SIP trunking to the Qwest iQ SIP Trunk Service.

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 IP Addresses of the network elements and public PSTN numbers are not revealed.

## 4.1. Summarize Initial SIP Configuration

This section summarizes the Communication Manager configuration in the test environment **prior** to adding SIP trunking to the Qwest iQ SIP Trunk Service.

### 4.1.1. Configure IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and SES. Use the **change node-names ip** command to create a mapping between a logical name and an IP address. In the test environment, node-name *procr* is mapped to IP address **205.168.62.91** (an Avaya S8300 Server processor Ethernet) and node name *SES* is mapped to **205.168.62.92** (the IP address of the SIP Enablement Services server).

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
IA770	10.64.41.22	
SES	205.168.62.92	
default	0.0.0.0	
procr	205.168.62.91	

### 4.1.2. Configure IP Network Regions

In the test environment, the Avaya S8300 Server, Avaya G450 Media Gateway, SES server, IP (H.323/SIP) endpoints, and Qwest SIP endpoints are located in a single IP network region. These components are located in the default IP network region 1. The **change ip-network-region 1** command was used to configure the region with the parameters described below.

- Set the **Authoritative Domain** field to match the domain name configured on SES. In this configuration, the domain name is *testroom.avaya.com*. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name for the **Name** field.



- Set the **Codec Set** field to the IP codec set to be used for calls within this IP network region. In this case, IP codec set **1** was selected.
- Default values may be used for all other fields.

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

                                IP NETWORK REGION

Region: 1
Location: Authoritative Domain: testroom.avaya.com
Name: Avaya Devices
MEDIA PARAMETERS                                             Intra-region IP-IP Direct Audio: yes
Codec Set: 1                                                 Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                           IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                                     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
H.323 IP ENDPOINTS                                         AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y                                RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

### 4.1.3. Configure Codecs

Use the **change ip-codec-set 1** command to define the codec(s) contained in this set which is used for calls as defined in the previous section. Which codecs are used and their order of preference is defined by the end customer. The example below uses only G.711MU.

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

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt   Size (ms)
1: G.711MU      n           2        20
2:
3:
4:
```

### 4.1.4. Signaling Group

The **add signaling-group** command was used to create a signaling group between Communication Manager and the SES for use by intra-site traffic. For the compliance test, signaling group 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.

- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to **5061**.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the processor Ethernet in the Avaya S8300 Server that terminates the SIP trunk. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to *SES*. This node name maps to the IP address of SES as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined **Section 4.1.2**.
- Set the **Far-end Domain** to the domain of the SES.
- Set **Direct IP-IP Audio Connections** to *n*. This field will disable media shuffling on the SIP trunk. During the DevConnect test, shuffling was disabled.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```

add signaling-group 3                                     Page 1 of 1
                                SIGNALING GROUP

Group Number: 3                                Group Type: sip
                                           Transport Method: tls

IMS Enabled? n

Near-end Node Name: procr                        Far-end Node Name: SES
Near-end Listen Port: 5061                    Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain: testroom.avaya.com

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? n
Session Establishment Timer(min): 3            IP Audio Hairpinning? n
Enable Layer 3 Test? n

                                           Alternate Route Timer(sec): 6

```

#### 4.1.5. Configure Trunk Group

The **add trunk-group** command was used to create a trunk group for the signaling group created in the previous section. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

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

- The default values were used for all other fields.

```

add trunk-group 3                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 3                                     Group Type: sip          CDR Reports: y
Group Name: ToSES                                   COR: 1                TN: 1          TAC: 1003
Direction: two-way                                Outgoing Display? n
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n

                                     Signaling Group: 3
                                     Number of Members: 20

```

## 4.2. Qwest Specific Configuration

### 4.2.1. Configure Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunk** 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. Each Avaya SIP telephone on a 2-party call with the SIP service provider uses two SIP trunk members for the duration of the call. Each non-SIP telephone (i.e., analog, digital, H.323) on a 2-party call with SIP service provider uses one SIP trunk member. The example shows that 100 licenses are available and 90 are in use. The license file installed on the system controls the maximum values for these attributes.

If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```

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

IP PORT CAPACITIES                                USED
Maximum Administered H.323 Trunks: 100            20
Maximum Concurrently Registered IP Stations: 450    3
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: 100  0
Maximum Video Capable H.323 Stations: 5            0
Maximum Video Capable IP Softphones: 5            0
Maximum Administered SIP Trunks: 100              90
Maximum Administered Ad-hoc Video Conferencing Ports: 0  0
Maximum Number of DS1 Boards with Echo Cancellation: 0  0
Maximum TN2501 VAL Boards: 0                      0
Maximum Media Gateway VAL Sources: 0              0
Maximum TN2602 Boards with 80 VoIP Channels: 0      0
Maximum TN2602 Boards with 320 VoIP Channels: 0     0
Maximum Number of Expanded Meet-me Conference Ports: 0  0

```

### 4.2.2. Configure System Features

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

```
change system-parameters features                                     Page 1 of 18
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      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
      Music/Tone on Hold: none
      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
      Internal Auto-Answer of Att'd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

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 **Block** for both fields.

```
change system-parameters features                                     Page 9 of 18
      FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

### 4.2.3. Configure Fax Configuration

Use the **change ip-codec-set 1** command to define FAX Mode contained in this set. On **Page 2** of the ip-codec-set form, set the **Fax Mode** field to **t.38-standard** for allowing faxing to and from the Qwest side. Retain the default values for the remaining fields, and submit these changes.

change ip-codec-set 1			Page 2 of 2
IP Codec Set			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	
FAX	t.38-standard	0	
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

### 4.2.4. Configure Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the SES 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 95 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to **5061**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the processor Ethernet in the Avaya S8300 Server that terminates the SIP trunk. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to **SES**. This node name maps to the IP address of SES as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined for the service provider. During the compliance test, the network region 1 was used.
- Set the **Far-end Domain** to the domain of the service provider. This may be a fully qualified domain name or an IP address but it must match the domain that the service provider expects to see in the SIP "To" header. In the case of the compliance test, this field was set to the IP address of the Qwest NBS, the edge of the Qwest iQ SIP Trunk service.
- Set **Direct IP-IP Audio Connections** to **n<sup>1</sup>**. This field will disable media shuffling on the SIP trunk. During the DevConnect test, shuffling was disabled.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

<sup>1</sup> Direct IP-IP Audio Connections, otherwise known as shuffling, did not work due to issues with the transfer scenarios; thus the recommendation was to turn the shuffling off.

add signaling-group 95		Page 1 of 1
SIGNALING GROUP		
Group Number: 95	Group Type: sip	
	Transport Method: tls	
IMS Enabled? n		
Near-end Node Name: procr		
		Far-end Node Name: SES
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: 10.1.1.24		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
	DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? n	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
Alternate Route Timer(sec): 6		

## 4.2.5. Configure Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 4.2.4**. During the compliance test, two Qwest NBS were utilized depending upon area codes. When an outbound call uses route-pattern 95, the call utilizes trunk group 95 first. If the call is not deliverable, then the call utilizes trunk group 96. The following screen shows trunk group 95 that was configured for the compliance test:

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

add trunk-group 95		Page 1 of 21
TRUNK GROUP		
Group Number: 95	Group Type: sip	CDR Reports: y
Group Name: Qwest-Chicago	COR: 1	TN: 1
Direction: two-way	Outgoing Display? n	TAC: 1095
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
		Signaling Group: 95
		Number of Members: 20

On **Page 2**, 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 Qwest iQ SIP Trunk Service the value of **600** seconds was used.

add trunk-group 95		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: yes		
Redirect On OPTIM Failure: 5000		
SCCAN? n	Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 600		

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end. Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 4.2.2**, if the inbound call is from an anonymous or restricted caller. Default values were used for all other fields.

add trunk-group 95		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 **Send Diversion Header** field to **y**. This field provides additional information to the destination party if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

add trunk-group 95		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Send Diversion Header? y		
Support Request History? y		
Telephone Event Payload Type:		

#### 4.2.6. Configure Calling Party Information

Public unknown numbering defines the calling party number to be sent to the far-end. This calling party number is sent in the SIP “From” header. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

During the compliance test, four DID numbers were assigned for testing. These four numbers were assigned to the four extensions 2390, 2392, 69570 and 69572. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these four extensions.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. In the example below, all stations with a 4-digit extension beginning with 2 and a 5-digit extension beginning with 6 will send the calling party number as the **CPN Prefix** plus the extension number.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
4	2	95	303389	10	Total Administered: 2
5	6	95	40855	10	Maximum Entries: 240

#### 4.2.7. Configure 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”. The 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: 3		
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
String	Length	Type	String	Length	Type	String	Length	Type
0	1	attd	7	5	ext			
10	4	dac	79000	5	ext			
11	4	dac	8	1	fac			
12	3	fac	9	1	fac			
13	3	fac	*	3	fac			
14	3	fac	#	3	fac			
2	5	ext						
23	4	ext						



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:	#06
Auto Alternate Routing (AAR) Access Code:	8
Auto Route Selection (ARS) - Access Code 1:	9
Access Code 2:	
Automatic Callback Activation:	*09
Deactivation:	#09
Call Forwarding Activation Busy/DA:	#11 All: *10
Deactivation:	#10
Call Forwarding Enhanced Status:	Act:
Deactivation:	
Call Park Access Code:	

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 including domestic long-distance calls, international calls, toll-free calls, operator calls, and 411 calls. The highlighted section shown below describes the area code with 73X will go out through the route pattern 95. See **Section 7** for the complete list of call types tested.

change ars analysis 173

Page 1 of 2

ARS DIGIT ANALYSIS TABLE

Location: all

Percent Full: 3

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
173	11	11	95	fnpa	n	
174	11	11	deny	fnpa	n	
175	11	11	deny	fnpa	n	
176	11	11	deny	fnpa	n	

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 95 during the compliance test. During the compliance test, two Qwest NBS were utilized depending upon area codes. When an outbound call comes into the route-pattern 95, the call utilizes the trunk-group 95 first. If the call is not deliverable, then the call utilizes the trunk 96.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 95 was connected to Qwest.
- **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:** The prefix mark (Pfx Mrk) is left blank.

- **LAR: Set to next.**

change route-pattern 95													Page 1 of 3					
Pattern Number: 95										Pattern Name: SIP-Qwest								
SCCAN? n										Secure SIP? n								
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC				
No			Mrk	Lmt	List	Del	Digits						QSIG					
										Dgts						Intw		
1:	95	0											n	user				
2:	96	0											n	user				
3:											n	user						
4:											n	user						
5:											n	user						
6:											n	user						
BCC		VALUE		TSC	CA-TSC	ITC				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				

#### 4.2.8. Configure Inbound Routing

Incoming call handling treatment is applied to inbound calls to direct them to the proper destination. Use the **change inc-call-handling-trmt trunk-group x** command (where *x* is the service provider trunk group) to define the proper digit manipulation for each DID number to map it to an internal extension. The example below shows the DID numbers used in the compliance test.

change inc-call-handling-trmt trunk-group 95										Page		1 of		3	
INCOMING CALL HANDLING TREATMENT															
Service/		Number		Number		Del		Insert							
Feature		Len		Digits											
public-ntwrk		10		303389				6							
public-ntwrk		10		408556				5							
public-ntwrk															
public-ntwrk															
public-ntwrk															

## 5. Configure SES

This section covers the configuration of SES. SES is configured via an Internet browser using the administration web interface. It is assumed that the SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure SES. For additional information on these installation tasks, refer to [5].

Each SIP endpoint at the enterprise used in the compliance test requires that a user and Communication Manager extension be created on SES. This configuration is not directly related to SIP Trunking, so it is not included here. These procedures are covered in [4].

This section is divided into two parts. **Section 5.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. This section will not attempt to show the installation procedures in their entirety. It will describe any deviations from the standard procedures, if any. **Section 5.2** will describe procedures beyond the initial SIP installation procedures that are necessary to support the Qwest iQ SIP Trunk Service.

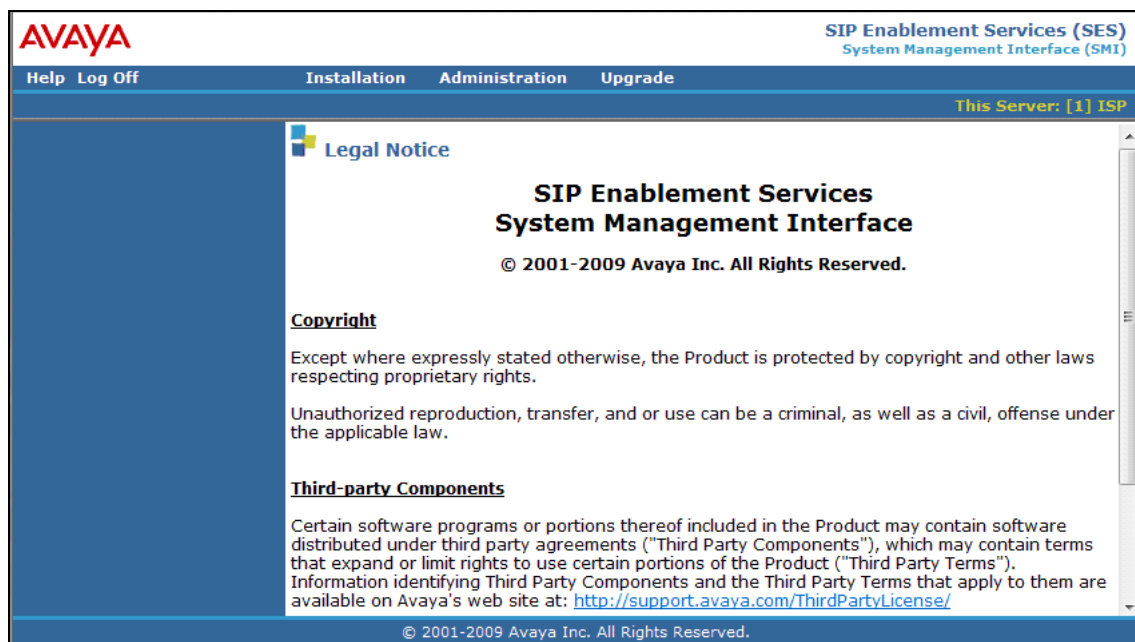
## 5.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

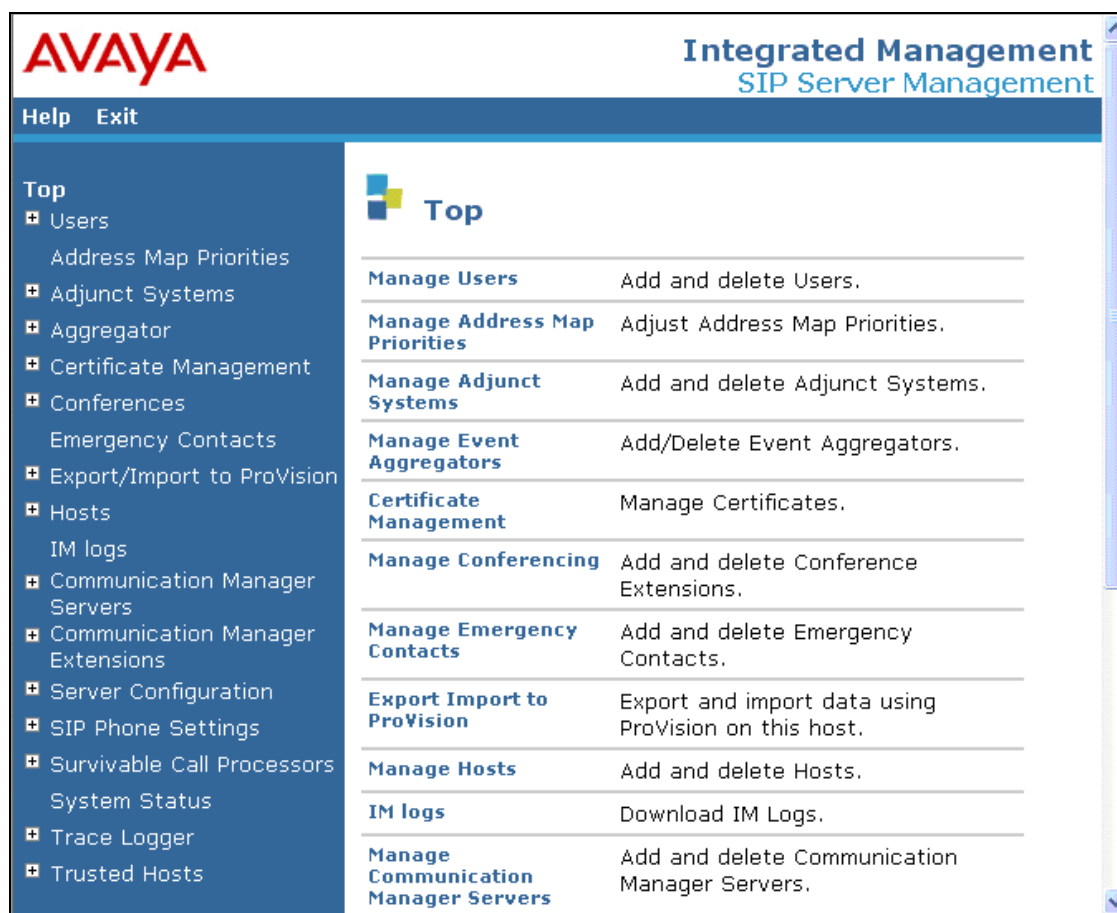
### 5.1.1. Login

Access the SES administration web interface by entering <http://<ip-addr>/admin> as the URL in an Internet browser, where <ip-addr> is the IP address of the SES.

Log in with the appropriate credentials and then navigate to the **Administration** → **SIP Enablement Services** link from the main page shown below.



The SES **Top** page will be displayed as shown below.



### 5.1.2. Initial Configuration Parameters

As part of the SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the SES administration home page shown in the previous step.

- SIP Domain: **testroom.avaya.com**  
(To view, navigate to **Server Configuration**→**System Parameters**)
- Host IP Address (SES IP address): **205.168.62.92**
- Host Type: **SES combined home-edge**  
(To view, navigate to **Host**→**List**; click **Edit**)
- Communication Manager Server Interface Name: **S8300G450**
- SIP Trunk Link Type: **TLS**
- SIP Trunk IP Address (procr IP address): **205.168.62.91**

(To view, navigate to **Communication Manager Servers**→**List**; click **Edit**)

## 5.2. Qwest Specific Configuration

This section describes additional SES configuration necessary for supporting the Qwest iQ SIP Trunk Service.

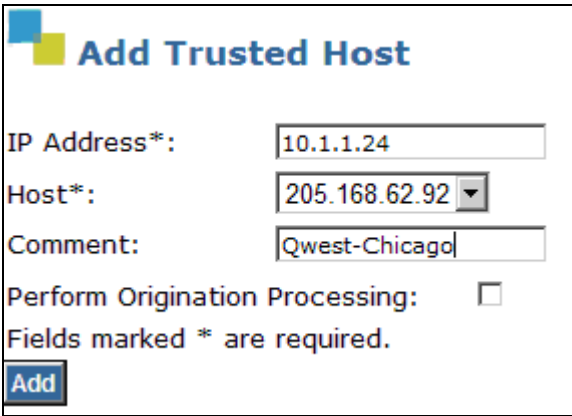
### 5.2.1. Trusted Host

Define the Qwest iQ SIP Trunk Service NBS to be a trusted host. Navigate to **Trusted Hosts**→**Add** in the left pane (see **Section 5.1.1**). In the **Add Trusted Host** window that appears, configure the following:

- **IP Address:** Enter the IP address of the Qwest NBS.
- **Host:** Select the SES IP address from the drop-down menu.
- **Comment:** Enter a description of the trusted host being added.

Click the **Add** button.

Repeat this step as necessary to configure additional trusted hosts if needed. During the Qwest DevConnect Compliance test, two trusted hosts were utilized (NBS-East and NBS-West), as shown in **Figure 1**.



**Add Trusted Host**

IP Address\*: 10.1.1.24

Host\*: 205.168.62.92

Comment: Qwest-Chicago

Perform Origination Processing: ☐

Fields marked \* are required.

**Add**

### 5.2.2. Communication Manager Address Map

A Communication Manager address map is needed to route calls from the PSTN via the SIP trunk to the enterprise. This is necessary because neither the caller nor the called party is a registered user on the SES with a Communication Manager extension assigned to it. As a result, SES does not know to route this call to Communication Manager. Thus to accomplish this task, a Communication Manager address map is needed.

Each map defines a call matching criteria based on the contents of the SIP Request-URI of the call. If a call matches the map, then the call is directed to the specified destination or contact.

The URI usually takes the form of *sip:user@domain*, where *user* is the destination number and *domain* is a domain name or an IP address.

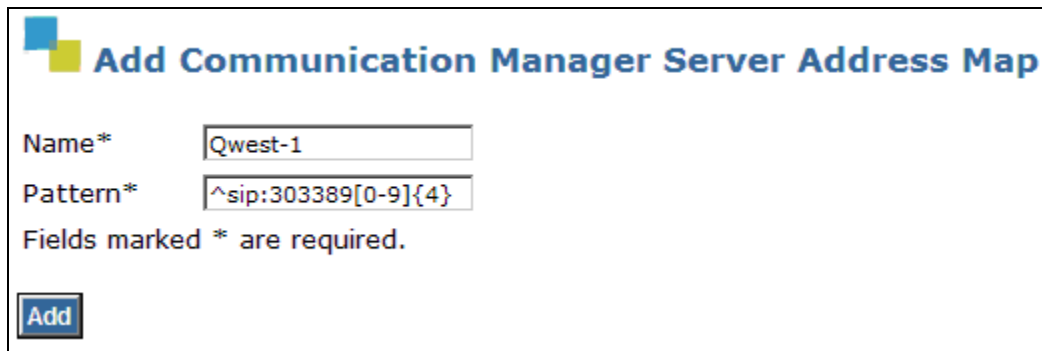
To configure a **Communication Manager Server Address Map**:

- Navigate to **Communication Manager Servers**→**List** in the left pane of the Administration web interface.
- Click on the **Map** link associated with the appropriate server.
- Click on the **Add Map In New Group** link. If other maps exist that point to the correct destination (contact) then click on **Add Another Map**.

In either case, the **Add Communication Manager Server Address Map** window appears as shown below. Configure the address map as follows:

- **Name**: Enter any descriptive name.
- **Pattern**: Enter an expression to define the matching criteria for calls to be routed from the PSTN to Communication Manager. For the address map named *Qwest-1*, the expression will match any URI that begins with *sip:303389* followed by any digit between *0-9* for the next *4* digits. Additional information on the syntax used for address map patterns can be found in [5].

Click **Add**.



After adding the address map, the **List Communication Manager Server Address Map** screen will appear, as shown below. When the first **Communication Manager Server Address Map** is added, a **Contact** is created automatically. For the **Communication Manager Server Address Map** previously added, the following contact was created:

**sip:\$(user)@205.168.62.91:5061;transport=tl**

This contact directs the calls to Communication Manager via IP address (*205.168.62.91*) using port *5061* and *TLS* as the transport protocol. The incoming DID number sent in the user part of the original request URI is substituted for *\$(user)* in the **Contact** expression.



## List Communication Manager Server Address Map

<u>Commands</u>	<u>Name</u>	<u>Commands</u>	<u>Contact</u>
Edit Delete	Quest-1		
Edit Delete	Quest-2		
		Edit Delete	sip:\$(user) @205.168.62.91:5061;transport=tls
Add Another Map		Add Another Contact	
			Delete Group
Add Map In New Group			

## 6. Qwest Services Configuration

To use the Qwest iQ SIP Trunk Service, a customer must request service from Qwest using their sales processes. The process can be started by contacting Qwest via the corporate web site at <http://www.qwest.com> and requesting information via the online sales links or telephone numbers.

## 7. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify SIP trunk interoperability between the Qwest iQ SIP Trunk Service and an Avaya IP Telephony Solution.

A simulated enterprise site using an Avaya IP telephony solution was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to use the commercially available SIP Trunk Service provided by Qwest.

The compliance test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by Qwest. Incoming PSTN calls were made to H.323, digital, analog, and SIP telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Qwest to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, digital, analog, and SIP telephones.
- Various call types were tested including: local, long distance, international, outbound toll-free, operator, and directory assistance.
- Calls using G.729A, G.729B, G.711MU, and G.711A coders.
- DTMF transmission using RFC 2833 with successful vector navigation for inbound calls and voice mail menu navigation for outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and extension to cellular, when the call arrived across the SIP Trunk from Qwest, or when the call forwarding destination and extension to cellular mobile number routed out the SIP Trunk to Qwest, or both.
- Caller ID Presentation and Caller ID Restriction.
- Avaya IP Agent in both “Road Warrior” and “Telecommuter” modes, where incoming PSTN calls arrived from Qwest, or the telecommute number routed out the SIP Trunk to Qwest, or both.
- EC500 features were tested

Interoperability testing of the sample configuration was completed with successful results for the Qwest iQ SIP Trunk Service. Qwest provided the following services, and calls were made during the compliance test:

- Fax: T.38 fax is supported and tested by Qwest.
- Inbound toll-free calls
- Outbound toll-free calls



- Operator Assisted call
- International call
- Emergency call
- Local Directory Assistance call

During the compliance test, the following limitations are observed:

- Direct IP-IP Audio Connections, otherwise known as shuffling, did not work due to issues with the transfer scenarios. Shuffling was turned off during the compliance test. With this configuration, all calls using the Qwest iQ SIP Trunk Service will require the use of an Avaya media processing resource.
- During the compliance test, REFER did not work. Thus, during transfer test cases, REFER messages were not utilized.

## 8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the SIP, H.323, digital and analog endpoints can place outbound and receive inbound PSTN calls using the Qwest iQ SIP Trunk Service.

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

## 9. Conclusion

These Application Notes describe the configuration necessary to connect Communication Manager and SIP Enablement Services to the Qwest iQ SIP Trunk Service. The Qwest iQ SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The Qwest iQ SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunk lines.

During DevConnect testing with the Qwest iQ SIP Trunk Service, Direct IP-IP Audio Connections, otherwise known as shuffling, did not work due to issues with the transfer scenarios. Therefore, the shuffling was disabled during the compliance test.

## 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 Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide*, June 2005, Document Number 210-100-500.
- [4] *Avaya Aura™ SIP Enablement Services Implementation Guide*, May 2009, Document Number 16-300140
- [5] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, May 2009, Document Number 555-245-206.
- [6] *4600 Series IP Telephone LAN Administrator Guide*, October 2007, Document Number 555-233-507
- [7] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, November 2009, Document Number 16-300698
- [8] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.0*, Dec 2007, 16-601944
- [9] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [10] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [11] RFC 4244, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

---

**©2010 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](mailto:devconnect@avaya.com).