



Application Notes for Configuring SIP Trunking Using PAETEC Dynamic IP SIP Trunk Service using the Broadsoft Platform 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 PAETEC Dynamic IP SIP Trunk Service and an Avaya IP telephony solution. PAETEC can offer the Dynamic IP SIP Trunk Service using several different platform technologies in the PAETEC network. These Application Notes correspond to the Dynamic IP SIP Trunk Service offered using a Broadsoft platform in the network. The Avaya solution consists of Avaya Aura™ SIP Enablement Services, Avaya Aura™ Communication Manager, and various Avaya SIP, H.323, digital and analog endpoints.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the PAETEC Dynamic IP SIP Trunk service and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura™ SIP Enablement Services, Avaya Aura™ Communication Manager, and various Avaya SIP, H.323, digital and analog endpoints.

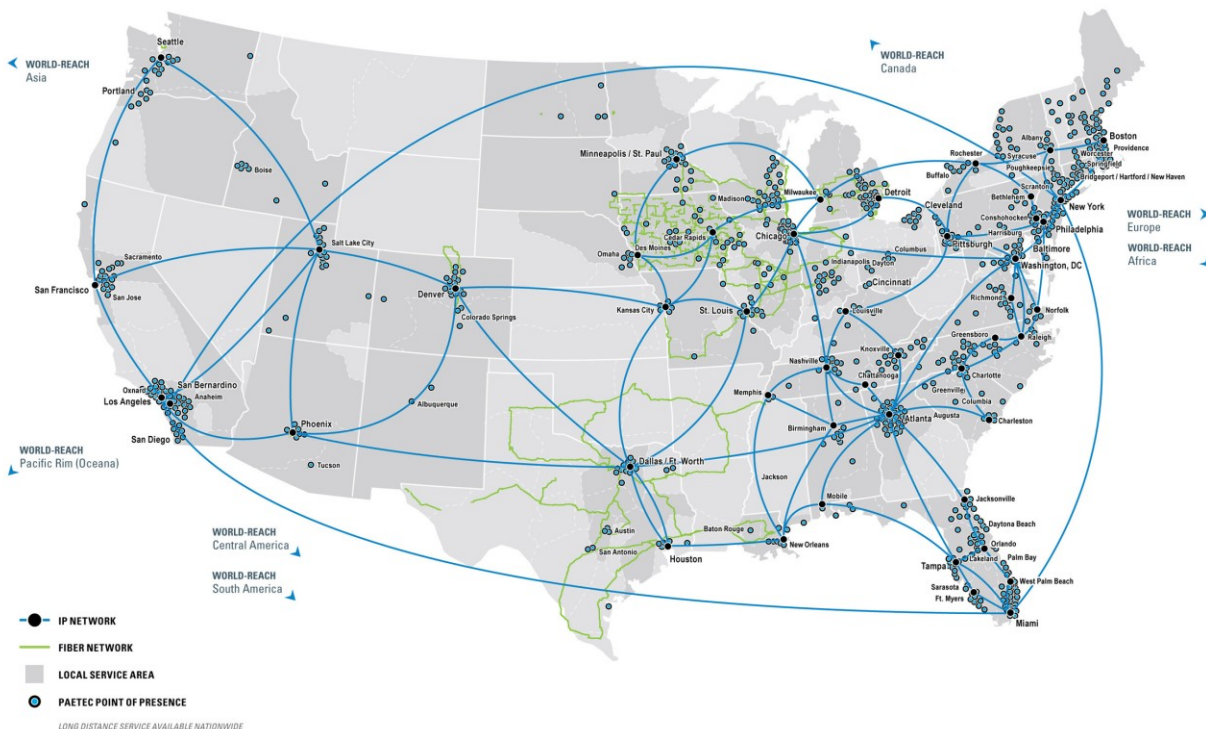
PAETEC can offer the Dynamic IP SIP Trunk Service using several different platform technologies in the PAETEC network. These Application Notes correspond to the Dynamic IP SIP Trunk Service offered using a Broadsoft platform in the network.

Customers using this Avaya IP telephony solution with the PAETEC Dynamic IP 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 was provided by PAETEC and summarizes the PAETEC Dynamic IP SIP Trunk Service at the time of writing these Application Notes. Please consult PAETEC for the most current description of capabilities. PAETEC serves 82 of the top 100 Metropolitan Statistical Areas, and offers data, voice, and value-added services throughout the United States.

The PAETEC Dynamic IP SIP Trunk Service includes the following capabilities:

- Outbound PSTN calling to local, long distance and international services
- Incoming Direct Inward Dial (DID) service
- Incoming Toll-free service
- Operator, Directory Assistance and Calling Card Service
- Converged IP access via a private IP MPLS Network



1.1. 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 Dynamic IP SIP Trunk Service provided by PAETEC.

To verify SIP trunking interoperability between the PAETEC Dynamic IP SIP Trunk Service 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 PAETEC. 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 PAETEC 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.711MU, and G.711A coders.
- DTMF transmission using RFC 2833 with successful vector navigation for inbound and 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 PAETEC, or when the call forwarding destination and extension to cellular mobile number routed out the SIP Trunk to PAETEC, or both.
- Caller ID Presentation and Caller ID Restriction.
- Avaya IP Softphone in both “Road Warrior” and “Telecommuter” modes, where incoming PSTN calls arrived from PAETEC, or the telecommute number routed out the SIP Trunk to PAETEC, or both.
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones. This allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

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

1.2. Support

For technical support on PAETEC Dynamic IP SIP Trunk services, contact PAETEC Customer Care by calling 877-340-2600 or by sending email to customercare@paetec.com.

2. Reference Configuration

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

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

- Avaya S8720 Servers running Communication Manager
- Avaya G650 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 4600-Series IP telephones (configured for the H.323 protocol)
- Avaya 1600-Series IP telephones (configured for the H.323 protocol)
- Avaya digital phones
- Analog phones and fax machines
- Avaya IP Softphone

For the purposes of the compliance test, the simulated enterprise site was configured using all public IP addresses so that all devices could communicate directly with the public IP address of the Dynamic IP Trunk Service. However, in these Application Notes, these public IP addresses have been replaced with private addresses for security reasons. Any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.

In an actual customer configuration, the enterprise site may also include additional network components such as a session border controller or data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that traffic must be allowed to pass between the Dynamic IP SIP Trunk Service and the following enterprise components:

- SIP traffic to/from the SIP Enablement Services server
- RTP traffic to/from VOIP media resources in Avaya Media Gateways (e.g. MedPro circuit packs in the Avaya G650 Media Gateway or on-board integrated VOIP resources in the smaller gateways)
- RTP traffic to/from H.323 or SIP telephones
- RTP traffic to/from H.323 or SIP soft clients

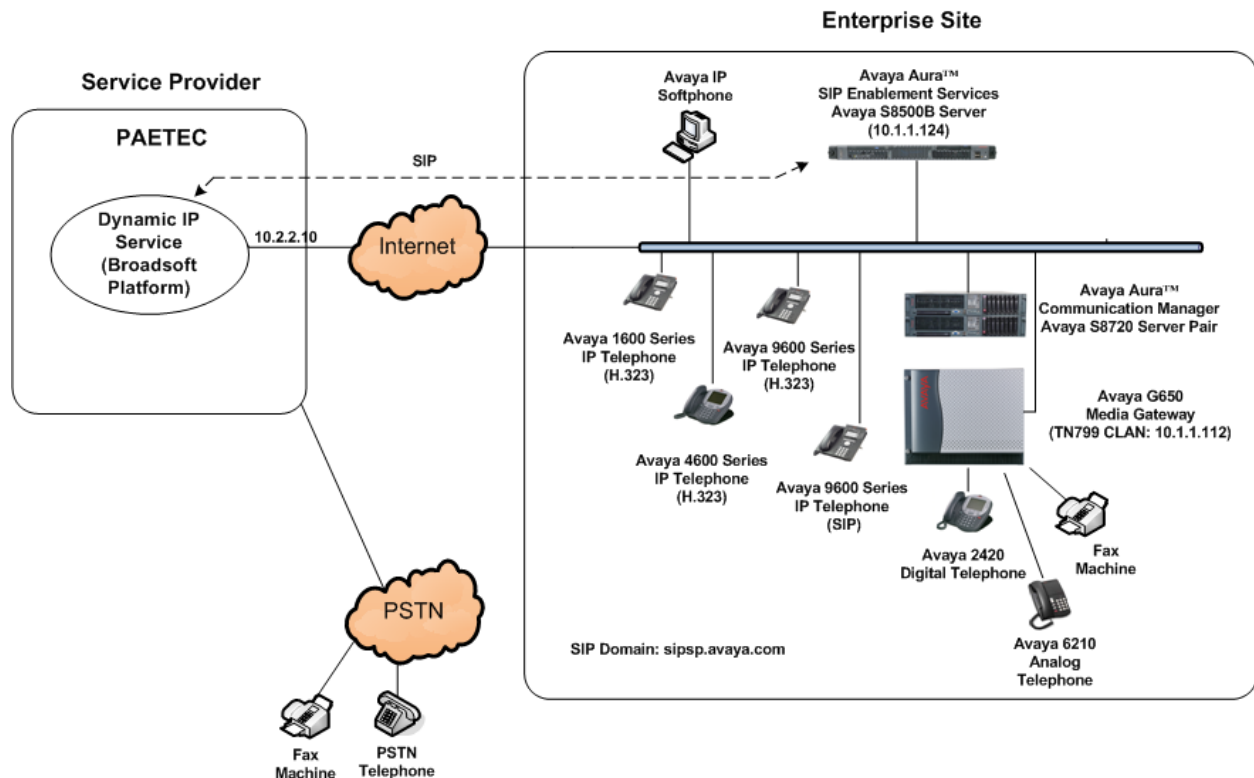


Figure 1: Avaya IP Telephony Network using the PAETEC Dynamic IP SIP Trunk Service

For incoming calls, the SES uses address maps to direct the incoming SIP messages to the appropriate 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 route 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 PAETEC 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 Dynamic IP 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 4.2.8**). In addition, Directory Assistance calls (411) and International calls (011+Country Code) are also supported. Communication Manager routes all calls to the PAETEC network using Automatic Route Selection (ARS).

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 S8720 Server Pair	5.2 SP3
Avaya G650 Media Gateway	TN2312AP(IPSI): HW12 FW45 TN799DP (CLAN): HW1 FW31 TN2302AP (MedPro):HW20 FW120 TN2602AP (MedPro):HW02 FW47
Avaya Aura™ SIP Enablement Services running on an Avaya S8500B Server	5.2 SP3
Avaya 9640 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.0 SP1 (s3.002)
Avaya 9620 IP Telephone (SIP)	Avaya one-X Deskphone Edition SIP 2.4.2
Avaya 1608 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.1.1
Avaya 4621SW IP Telephone (H.323)	2.9.1
Avaya IP Softphone	Release 6.0 SP6
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
PAETEC Dynamic IP SIP Trunk Service Solution Components	
Component	Release
Acme Packet Net-Net Session Director 4250 Session Border Controller	SC6.1.0
BroadSoft Platform	14sp9

Table 1: Equipment and Software Tested

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

It is assumed the general installation of Communication Manager, Avaya G650 Media Gateway and SES has been previously completed and is not discussed here. In addition, it is 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 PAETEC Dynamic IP 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 PAETEC Dynamic IP SIP Trunk Service.

4.1.1. 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 **08A_CLAN** is mapped to IP address **10.1.1.112** (a CLAN board in the G650 Media Gateway) and node name **SES** is mapped to **10.1.1.124** (the IP address of the SES). In other Avaya configurations such as an Avaya G250, G350, G700, or G450 Media Gateway with a standalone Avaya S8300 Server, the Avaya S8300 Server processor address (node name **procr**) is used as the SIP signaling interface to SES, rather than a C-LAN interface.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
03A_medpro	10.1.1.113	
08A_CLAN	10.1.1.112	
SES	10.1.1.124	
default	0.0.0.0	
procr	0.0.0.0	

4.1.2. IP Network Regions

In the test environment, the Avaya S8720 Servers, Avaya Media Gateway, SES server, and IP (H.323/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 *sipsp.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.
- 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. This was done for both **Intra-region** and **Inter-region IP-IP Direct Audio**. 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 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: 1          Authoritative Domain: sipsp.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: 6000          IP Audio Hairpinning? n
      UDP Port Max: 65535
  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

```

4.1.3. Codecs

Use the **change ip-codec-set 1** command to define the codec(s) contained in this set which is used for calls within the enterprise 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:

```

4.1.4. 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 *08A_CLAN*. This node name maps to the IP address of the CLAN circuit pack in the Avaya G650 Media Gateway 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 *y*. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```
add signaling-group 1                                     Page 1 of 1
                                     SIGNALING GROUP
Group Number: 1           Group Type: sip
                          Transport Method: tls
IMS Enabled? n

Near-end Node Name: 08A_CLAN      Far-end Node Name: SES
Near-end Listen Port: 5061        Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain: sipsp.avaya.com

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? y
Enable Layer 3 Test? n                    IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n    Direct IP-IP Early Media? n
                                           Alternate Route Timer(sec): 6
```

4.1.5. 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 *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 1                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 1                                     Group Type: sip          CDR Reports: y
  Group Name: SESDomain                             COR: 1              TN: 1          TAC: 1001
    Direction: two-way                             Outgoing Display? n
    Dial Access? n                                  Night Service:
    Queue Length: 0
  Service Type: public-ntwrk                         Auth Code? n

                                           Signaling Group: 1
                                           Number of Members: 20

```

4.2. PAETEC Specific Configuration

4.2.1. 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 trunks 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. The example shows that 2000 licenses are available and 72 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:	2000	0
Maximum Concurrently Registered IP Stations:	18000	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:	0	0
Maximum Video Capable H.323 Stations:	0	0
Maximum Video Capable IP Softphones:	0	0
Maximum Administered SIP Trunks:	2000	72
Maximum Administered Ad-hoc Video Conferencing Ports:	0	0
Maximum Number of DS1 Boards with Echo Cancellation:	0	0
Maximum TN2501 VAL Boards:	10	0
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

4.2.2. System Features

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

```

change system-parameters features                                     Page 1 of 17
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
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 (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
Internal Auto-Answer of AttD-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 default value of *anonymous* for both fields.

```

change system-parameters features                                     Page 9 of 17
      FEATURE-RELATED SYSTEM PARAMETERS

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

DISPLAY TEXT
  Identity When Bridging: principal

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. IP Network Region

Create a separate IP network region for the service provider trunk(s). This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk(s). Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the domain name configured on SES. In this configuration, the domain name is *sipsp.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 to be used for calls within this IP network region. In this case, IP codec set 2 was selected.
- Default values can be used for all other fields.

change ip-network-region 2
Page 1 of 19

IP NETWORK REGION

Region: 2
Location: 1 **Authoritative Domain: sipsp.avaya.com**

Name: SP Region

MEDIA PARAMETERS

Codec Set: 2

UDP Port Min: 2048

UDP Port Max: 3329

DIFFSERV/TOS PARAMETERS

Call Control PHB Value: 46

Audio PHB Value: 46

Video PHB Value: 26

802.1P/Q PARAMETERS

Call Control 802.1p Priority: 6

Audio 802.1p Priority: 6

Video 802.1p Priority: 5

H.323 IP ENDPOINTS

H.323 Link Bounce Recovery? y

Idle Traffic Interval (sec): 20

Keep-Alive Interval (sec): 5

Keep-Alive Count: 5

Intra-region IP-IP Direct Audio: yes

Inter-region IP-IP Direct Audio: yes

IP Audio Hairpinning? n

RTCP Reporting Enabled? y

RTCP MONITOR SERVER PARAMETERS

Use Default Server Parameters? y

AUDIO RESOURCE RESERVATION PARAMETERS

RSVP Enabled? n

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

change ip-network-region 2
Page 3 of 19

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

4.2.4. Codecs

Use the **change ip-codec-set 2** command to define the codec(s) contained in this set which is used for calls between the enterprise and the service provider as defined in the previous section. The PAETEC Dynamic IP SIP Trunk Service supports G.729A and G.711MU. Thus, both of these codecs were included in this set in order of preference. The order of preference is defined by the end customer. Enter **G.729A** and **G.711MU** in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 2

Page 1 of 2

IP Codec Set

Codec Set: 2

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

On **Page 2**, set the **Fax Mode** field to **none**. The PAETEC Dynamic IP SIP Trunk Service does not support T.38 fax.

change ip-codec-set 2				Page	2 of	2
IP Codec Set						
Allow Direct-IP Multimedia? n						
	Mode	Redundancy				
FAX	none	0				
Modem	off	0				
TDD/TTY	US	3				
Clear-channel	n	0				

4.2.5. 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 4 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 **08A_CLAN**. This node name maps to the IP address of the CLAN circuit pack in the Avaya G650 Media Gateway 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 in **Section 4.2.3**.
- 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. If a fully qualified domain name is used, then a DNS server must be present in the network that can resolve the name to the

appropriate IP address. In the case of the compliance test, this field was set to the IP address of the Acme SBC at the edge of the PAETEC Dynamic IP SIP Trunk service.

- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

add signaling-group 4		Page 1 of 1
SIGNALING GROUP		
Group Number: 4	Group Type: sip	
	Transport Method: tls	
IMS Enabled? n		
Near-end Node Name: 08A_CLAN	Far-end Node Name: SES	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 2	
Far-end Domain: 10.2.2.10		
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? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

4.2.6. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 4.2.5**. For the compliance test, trunk group 4 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set 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 4                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 4          Group Type: sip          CDR Reports: y
  Group Name: PAETEC Trk      COR: 1          TN: 1      TAC: 1004
    Direction: two-way      Outgoing Display? n
    Dial Access? n          Night Service:
    Queue Length: 0
  Service Type: public-ntwrk      Auth Code? n

                                     Signaling Group: 4
                                     Number of Members: 14

```

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 PAETEC Dynamic IP Trunk Service the value of **900** seconds was used.

```

add trunk-group 4                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 5000

  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 4.2.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```

change trunk-group 4                                     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.

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

4.2.7. 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.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 20000, 20004 and 20008. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	20000	4	9085551111	10	Total Administered: 3
5	20004	4	9085552222	10	Maximum Entries: 9999
5	20008	4	9085553333	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 2 will send the calling party number as the **CPN Prefix** plus the extension number.

change public-unknown-numbering 0				Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT				
				Total
Ext	Ext	Trk	CPN	CPN
Len	Code	Grp(s)	Prefix	Len
5	2	4	90855	10
				Total Administered: 3
				Maximum Entries: 9999

4.2.8. 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									
DIAL PLAN ANALYSIS TABLE									
Location: all									
Percent Full: 1									
	Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
	String	Length	Type	String	Length	Type	String	Length	Type
0		1	dac						
1		4	dac						
2		5	ext						
8		1	fac						
9		1	fac						
*		3	fac						
#		3	fac						

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

change feature-access-codes									
FEATURE ACCESS CODE (FAC)									
Abbreviated Dialing List1 Access Code: *70									
Abbreviated Dialing List2 Access Code: *80									
Abbreviated Dialing List3 Access Code:									
Abbreviated Dial - Prgm Group List Access Code:									
Announcement Access Code:									
Answer Back Access Code:									
Attendant Access Code:									
Auto Alternate Routing (AAR) Access Code: 8									
Auto Route Selection (ARS) – Access Code 1: 9									
Automatic Callback Activation:									
Access Code 2:									
Deactivation:									
Call Forwarding Activation Busy/DA: *90 All: *72 Deactivation: #73									
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. See **Section 7** for the complete list of call types tested. All dialed strings except toll-free numbers are mapped to route pattern 4 which contains the SIP trunk to the service provider (as defined below). Toll-free numbers are mapped to route pattern 6.

change ars analysis 0					Page 1 of 2		
ARS DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
0		1	11	4	op		n
00		2	2	4	iop		n
011		10	18	4	intl		n
1469		11	11	4	fnpa		n
1732		11	11	4	fnpa		n
1800		11	11	6	fnpa		n
1877		11	11	6	fnpa		n
1908		11	11	4	fnpa		n
411		3	3	4	svcl		n

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 4 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 4 was connected to PAETEC.
- **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. This will remove the prefix of one on any 1 + 10 digit dialed numbers and leave numbers of any other length unchanged. This will ensure 10 digits are sent to the service provider for North American Numbering Plan (NANP) numbers.

change route-pattern 4														Page 1 of 3	
Pattern Number: 4 Pattern Name: PAETEC															
SCCAN? n Secure SIP? n															
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits					DCS/ QSIG	IXC Intw		
1: 4	0											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. Dgts	Numbering Format	LAR	
		0	1	2	M	4	W	Request					Subaddress		
1:		y	y	y	y	y	n	n		rest				none	
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	

For toll-free numbers, PAETEC requires 1 + 10 digits be sent. Thus, route pattern 6 is used for toll-free numbers and uses a different value for the prefix mark. Route pattern 6 was configured as follows:

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 4 was connected to PAETEC.
- **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 10-digit number with a 1 and leave numbers of any other length unchanged.

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

4.2.9. 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 4					Page	1 of 30
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Number Digits	Del	Insert		
public-ntwrk	10	9085551111	10	20000		
public-ntwrk	10	9085552222	10	20004		
public-ntwrk	10	9085553333	10	20008		

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 media server 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 [3].

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 PAETEC Dynamic IP SIP Trunk Service.

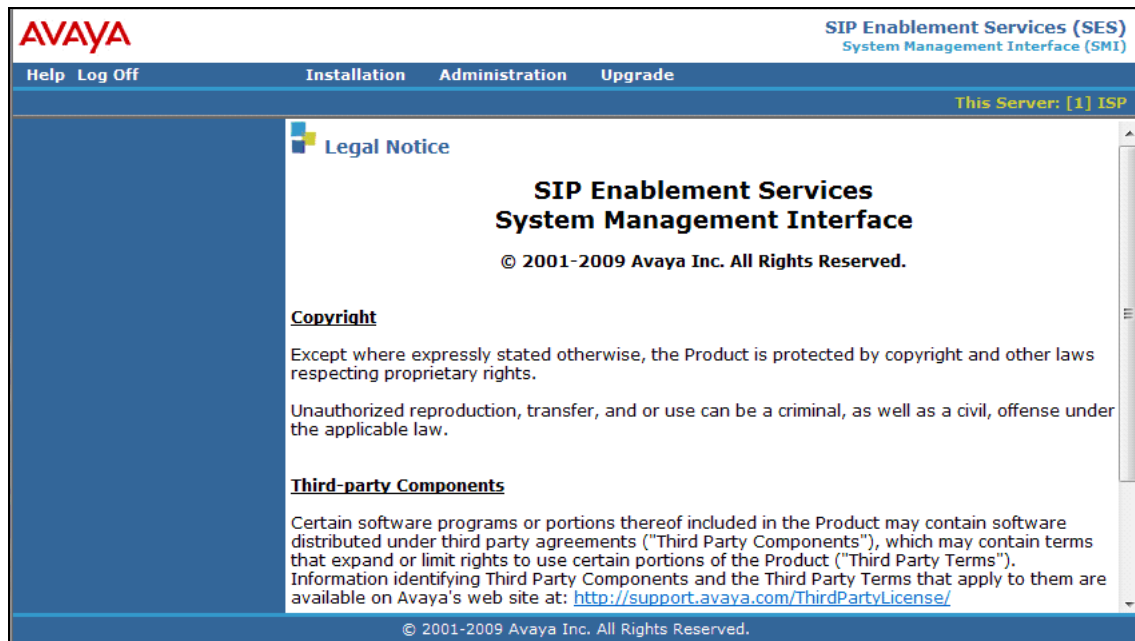
5.1. Summarize Initial Configuration Parameters

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

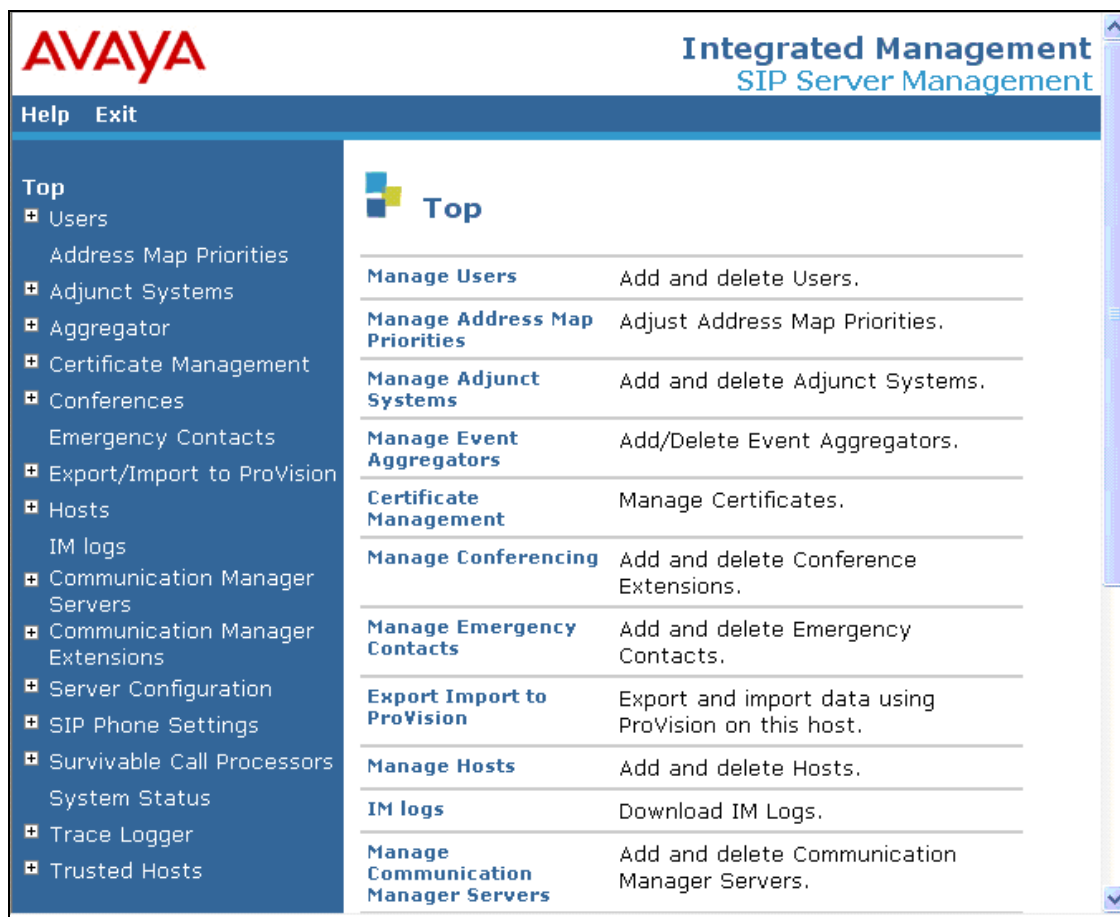
5.1.1. Login

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: *sipsp.avaya.com*
(To view, navigate to **Server Configuration**→**System Parameters**)
- Host IP Address (SES IP address): *10.1.1.124*
- Host Type: *SES combined home-edge*
(To view, navigate to **Host**→**List**; click **Edit**)
- Communication Manager Server Interface Name: *CM1*
- SIP Trunk Link Type: *TLS*
- SIP Trunk IP Address (CLAN IP address): *10.1.1.112*
(To view, navigate to **Communication Manager Servers**→**List**; click **Edit**)

5.2. PAETEC Specific Configuration

This section describes additional SES configuration necessary for supporting the PAETEC Dynamic IP SIP Trunk Service.

5.2.1. Trusted Host

Define the PAETEC Dynamic IP SIP Trunk Service SBC 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 SBC.
- **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.

Add Trusted Host

IP Address*: 10.2.2.10

Host*: 10.1.1.124 ▼

Comment: SP Proxy

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 media server 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 *AvayaDIDs*, the expression will match any URI that begins with *sip:908555* 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].
- **Replace URI:** Check the box.

Click **Add**.



Add Communication Manager Server Address Map

Name*

Pattern*

Replace URI ☒

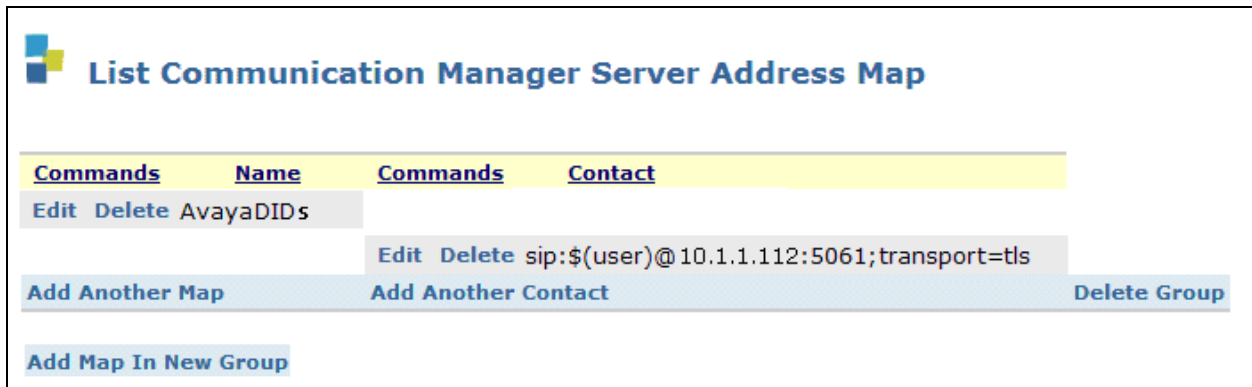
Fields marked * are required.

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)@10.1.1.112:5061;transport=tls

This contact directs the calls to Communication Manager via IP address (**10.1.1.112**) 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

Commands	Name	Commands	Contact
Edit Delete	AvayaDIDs	Edit Delete	sip:\$(user)@10.1.1.112:5061;transport=tls
Add Another Map		Add Another Contact	Delete Group
Add Map In New Group			

6. PAETEC Services Configuration

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

During the signup process, PAETEC will require that the customer provide the public IP address used to reach the SIP Enablement Services server. PAETEC provided the following information for the compliance testing: IP address of the PAETEC SIP proxy/SBC, and Direct Inward Dialed (DID) numbers. This information was used to complete the Communication Manager and SIP Enablement Services configuration discussed in the previous sections.

7. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify SIP trunk interoperability between the PAETEC Dynamic IP 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 Dynamic IP SIP Trunk Service provided by PAETEC.

The compliance test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by PAETEC. 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 PAETEC 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.711MU, and G.711A coders.
- DTMF transmission using RFC 2833 with successful vector navigation for inbound and 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 PAETEC, or when the call forwarding destination and extension to cellular mobile number routed out the SIP Trunk to PAETEC, or both.
- Caller ID Presentation and Caller ID Restriction.
- Avaya IP Softphone in both “Road Warrior” and “Telecommuter” modes, where incoming PSTN calls arrived from PAETEC, or the telecommute number routed out the SIP Trunk to PAETEC, or both.

- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones. This allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

Interoperability testing of the sample configuration was completed with successful results for the PAETEC Dynamic IP SIP Trunk Service. The following observations were made during the compliance test:

- **Asynchronous DTMF Payloads:** This capability is not supported by PAETEC. This capability allows DTMF RTP events to be sent with a different payload header in each direction of the call. If it is not supported, DTMF tones may not be passed end to end when connected to an endpoint that expects asynchronous DTMF payloads to be honored. This behavior was observed when calling a PSTN-connected IVR from an Avaya 9600 Series SIP Telephone. This particular scenario can be worked around by setting the DTMF payload value in the phone settings file to the preferred value used by PAETEC (i.e. 101). However, this scenario may arise with other endpoints or connected systems.
- **CPN Block:** Outbound calling party number (CPN) block from the enterprise is not supported. PAETEC requires the calling party number to be present in the SIP From header of the outbound call for authentication. Outbound calls with CPN block enabled will fail with a 404 User Not Found response from the network.
- **Fax:** T.38 fax is not supported by PAETEC.
- **Extension to Cellular (EC500) Extend Feature:** For active PSTN calls with an Avaya phone with EC500 enabled, the phone user can not extend the call (effectively transferring) to the associated cellular (EC500) phone. The extended call rings the EC500 phone once then the call is dropped. A possible workaround for this problem is to configure a DID number to map to an administered *Active Call Appearance Select* Feature Name Extension. The cellular (EC500) phone may then dial the DID number and bridge onto the call. The call can then be dropped by the host phone.
- **Calls Not Tested:** Inbound toll-free and 911 emergency calls are both supported but were not tested as part of the compliance test.
- **Outbound toll-free calls:** PAETEC requires outbound toll-free calls to be dialed with 1 + 10 digits while all other North American Numbering Plan (NANP) numbers can be dialed with either 10 digits or 11 digits (1 + 10).

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 PAETEC Dynamic IP 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 PAETEC Dynamic IP SIP Trunk Service. The PAETEC Dynamic IP SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The PAETEC Dynamic IP SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunk lines.

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.