



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Manager SIP Trunking to a Typical SIP Service Provider – Issue 1.1

Abstract

These Application Notes describe the steps for configuring SIP trunking using an Avaya Communication Manager based SIP telephony solution (including Avaya SIP Enablement Services) with a typical, but hypothetical, SIP Service Provider.

SIP trunking is an emerging access method supported by leading Service Providers to allow Public Switch Telephone Network (PSTN) calling using a Voice over IP (VoIP) access method. It may bring opportunities for cost reduction, new service opportunities and resiliency.

The configuration shown in these Application Notes is representative of a typical SIP trunking solution. It is intended to provide configuration guidance to supplement other Avaya product documentation.

Following these guidelines DOES NOT imply that successful interoperability with any specific SIP Service Provider is ensured. Compliance testing with a specific Service Provider (performed as part of the Avaya DeveloperConnection program) is necessary to formally validate the interoperability of specific configurations.

The Avaya DeveloperConnection website (<http://www.avaya.com/gcm/master-usa/en-us/corporate/alliances/developerconnection/index.htm>) should be consulted to determine the actual interoperability testing status with specific Service Providers.

1. Introduction

These Application Notes describe the steps for configuring SIP trunking between an Avaya Communication Manager based SIP telephony solution and a typical (but hypothetical) SIP Service Provider.

SIP (Session Initiation Protocol) is a standards-based communications approach designed to provide a common framework to support multimedia communication. RFC 3261 [7] is the primary specification governing this protocol. Within these Application Notes, SIP is used as the signaling protocol between the Avaya components and the network service offered by the SIP Service Provider. SIP manages the establishment and termination of connections and the transfer of related information such as the desired codec, calling party identity, etc.

SIP trunking is an emerging access method supported by leading Service Providers to allow Public Switch Telephone Network (PSTN) calling using Voice over IP (VoIP) techniques via Internet Protocol (IP) based access and network services. The Avaya SIP telephony solution described within these Application Notes consists of Avaya Communication Manager, Avaya SIP Enablement Services (SES), and various Avaya telephony endpoints.

SIP trunking may bring opportunities for cost reduction, new service opportunities and resiliency. It may reduce or eliminate the need for existing TDM trunks to Service Providers.

The configuration shown in these Application Notes is representative of a typical (but hypothetical) SIP trunking solution. It is intended to provide configuration guidance to supplement other Avaya product documentation.

Following these guidelines DOES NOT imply that successful interoperability with any specific SIP Service Provider is ensured. Formal compliance testing with specific Service Providers (performed as part of the Avaya Developer*Connection* program) is necessary to validate interoperability of specific release configurations.

The Avaya Developer*Connection* website (<http://www.avaya.com/gcm/master-usa/en-us/corporate/alliances/developerconnection/index.htm>) should be consulted to determine the actual interoperability testing status with specific Service Providers.

1.1. Typical SIP Trunking Service Offering

A SIP trunking configuration with a typical SIP Service Provider supporting enterprise business customers is illustrated in **Figure 1**.

Each SIP Service Provider's offering varies widely but generally they have some or all of the following characteristics:

- IP-based access methods. The nature of this access may vary (ranging from general purpose Internet access to end-to-end MPLS based service offerings).
- Converged voice and data via the IP access.
- Interoperability with PSTN destinations.
- Interoperability with other locations also using VoIP access methods.

- Varying outbound and inbound calling capabilities.
 - Local, long distance and international.
 - Direct Inward Dialing (DID) number assignments.
 - Toll-free numbers.
 - Operator services.
 - N11 services.
 - Virtual private network services.
- SIP signaling in a “trusted host” configuration (that does not use a challenge/response authentication method when peering with Avaya SIP infrastructure).
- G.711mu and G.729B voice codecs.
- T.38 fax interoperability.

These SIP trunking service offers are not “IP-Centrex” or “Hosted-PBX” configurations that support end users directly. They do not involve the direct registration and support (by the SIP Service Provider) of telephones.

1.2. Typical Enterprise Customer Location

Figure 1 also illustrates a typical enterprise customer location using an Avaya Communication Manager based solution to support SIP trunking with the SIP Service Provider. This typical configuration includes:

- Avaya Communication Manager providing the communication services for this customer location. Associated with Avaya Communication Manager is:
 - An Avaya S8500 Server serving as the host processor for the Avaya Communication Manager software.
 - An Avaya G650 Media Gateway supporting various VoIP resources and port cards.
- Avaya SIP Enablement Services operating on an Avaya S8500 server. Avaya SES serves as the SIP proxy between the SIP Service Provider and one or more Avaya Communication Manager systems.
- Various Avaya telephones and other endpoints.
- IP routing and data network infrastructure to support IP connectivity between the enterprise location and the SIP Service Provider.

For simplicity, these Application Notes and **Figure 1** does not describe several aspects that may exist in actual customer configurations but are beyond the scope of these Application Notes.

- Avaya Communication Manager operates on the entire family of Avaya S8xxx servers and supports configurations with all of Avaya’s Gxxx Media Gateways. The concepts presented in this Application Notes apply to all valid configurations but the specifics may vary with different S8xxx Servers and Gxxx Media Gateways.
- Customer locations will generally have additional or alternate routes to the PSTN using analog or digital TDM trunks.
- The use of Avaya SIP telephones.
- IP Network Address Translation (NAT), firewalls, Application Layer Gateway (ALG), and Session Border Controller (SBC) devices that may be sitting between the SIP Service

Provider and the Enterprise's communications infrastructure are not explicitly shown. It is assumed that these devices can be deployed in the SIP Service Provider's DMZ, the Enterprise's DMZ, or both. These devices generally must be SIP aware and configured properly for SIP trunking to function properly. When configured correctly, they are transparent to the Avaya communications infrastructure.

- Enterprise networks often have multiple geographic locations tied together via an IP network. These configurations may be supported by one or more Avaya Communication Manager systems and/or multiple media gateways. In all cases a single Avaya SES edge server will serve as the SIP proxy gateway interfacing with SIP trunking to the SIP Service Provider services.

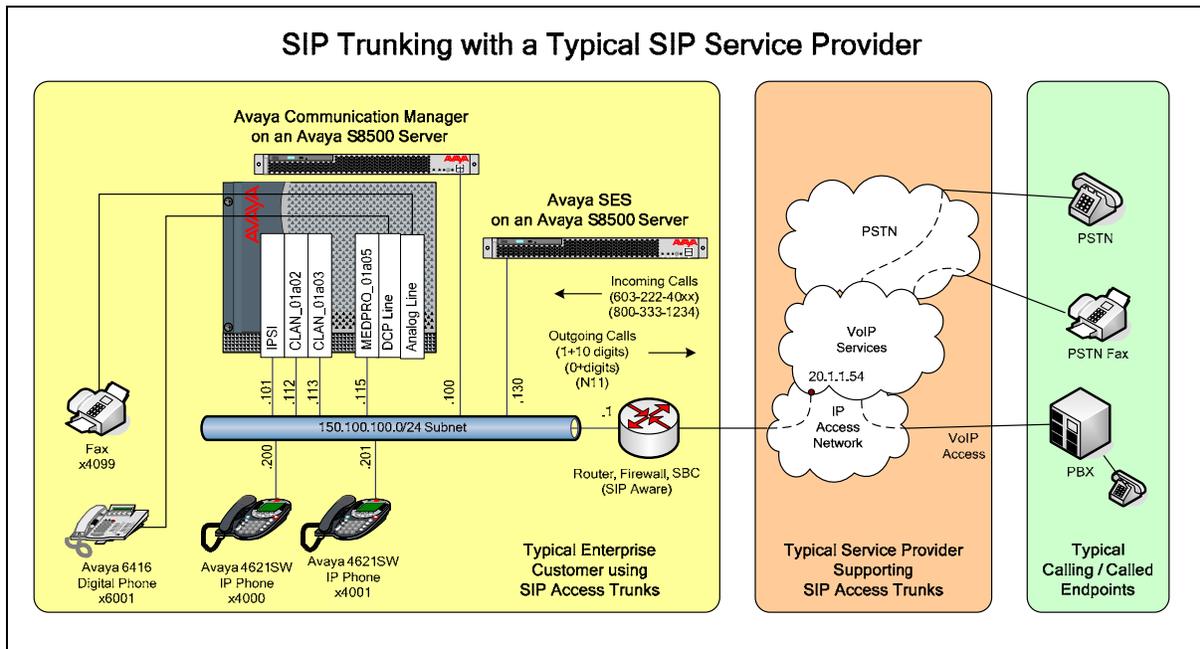


Figure 1 – Typical SIP Trunking Configuration

1.3. Call Flows

To better understand how calls are routed between the PSTN and the enterprise site shown in **Figure 1** using SIP trunks, two call flows are described in this section.

The first call scenario illustrated in **Figure 2** is a PSTN call to the enterprise site terminating on a telephone supported by Avaya Communication Manager.

1. A user on the PSTN dials a DID number assigned by the SIP Service Provider to the customer location. The PSTN routes the call to the SIP Service Provider network.
2. Based on the DID number, the SIP Service Provider offers the call to Avaya SES using SIP signaling messages sent over the IP access facility. Note that the assignment of the DID number and the address of the Avaya SES server was previously established during

the ordering and provisioning of the service.

3. Avaya SES routes the call to the Avaya S8500 Server running Avaya Communication Manager over a SIP trunk.
4. Avaya Communication Manager terminates the call to the Avaya telephone as shown in **Figure 2**.

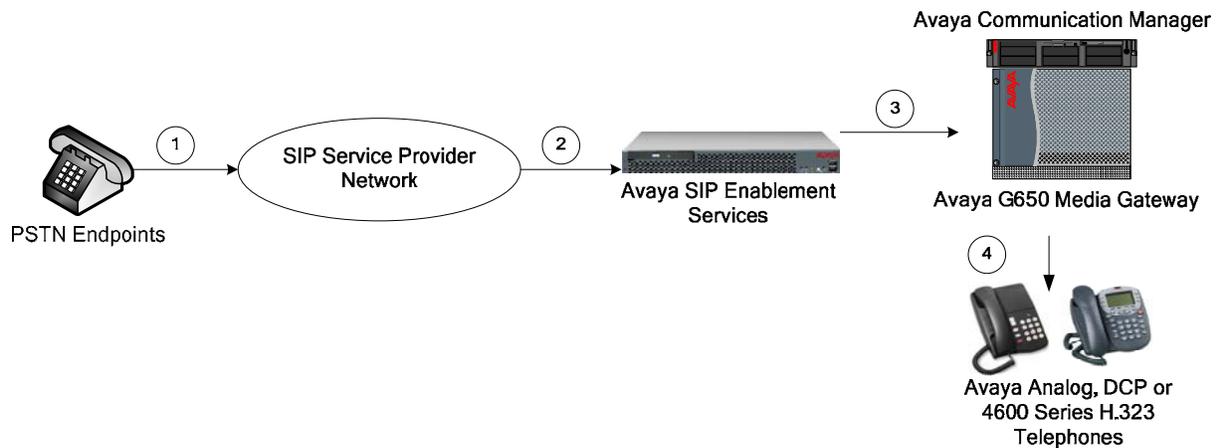


Figure 2: Incoming PSTN Calls to Avaya Communication Manager

The second call scenario illustrated in **Figure 3** is an outgoing call from an Avaya telephone at the enterprise site to the PSTN via the SIP trunk to the SIP Service Provider.

1. An Avaya telephone served by Avaya Communication Manager originates a call to a user on the PSTN.
2. The call request is handled by Avaya Communication Manager where origination treatment such as Class of Restrictions (COR) and Automatic Route Selection (ARS) is performed. Avaya Communication Manager selects the SIP trunk and sends the SIP signaling messages to Avaya SES.
3. Avaya SES routes the call to SIP Service Provider.
4. The SIP Service Provider completes the call to the PSTN.

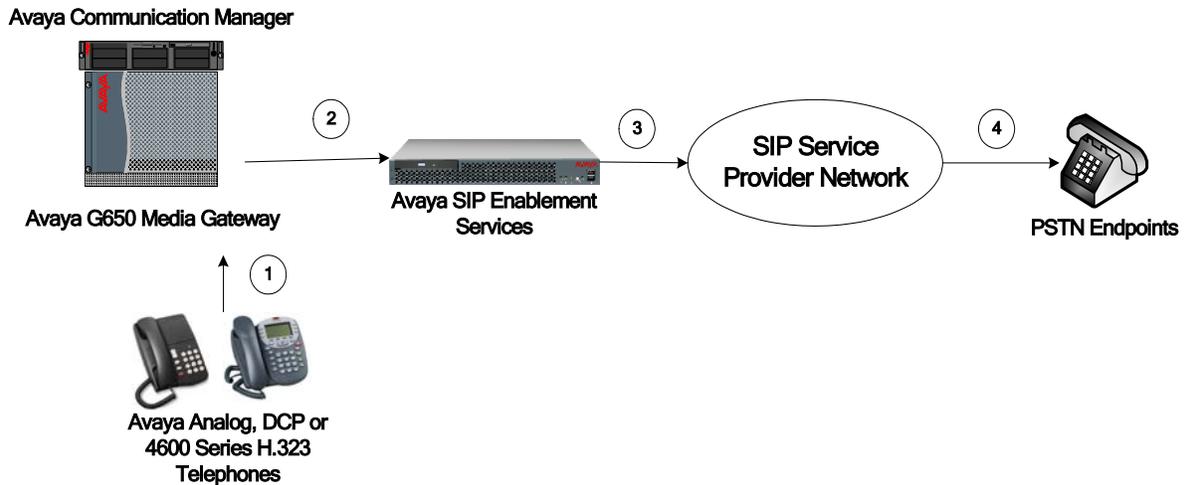


Figure 3: Outgoing Calls from Avaya Communication Manager to the PSTN

Appendix A illustrates examples of the SIP INVITE messages sent on the SIP trunk to begin each call.

2. Equipment and Software Validated

These Application Notes discuss the configuration with a typical (but hypothetical) SIP Service Provider providing SIP trunk access to their services.

The following products and software are representative of a typical Avaya Communication Manager-based SIP Trunking solution (as shown in **Figure 1**) that would be validated during formal DeveloperConnection testing with a Service Provider. Corresponding information for our “hypothetical” SIP Service Provider would be known if these Application Notes were produced as the result of actual compliance testing.

Component	Version
Avaya	
Avaya S8500B Server	Avaya Communication Manager 4.0
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW12 FW036
TN799DP Control-LAN (C-LAN)	HW01 FW017
TN2602AP IP Media Processor (Medpro)	HW02 FW031
TN2224CP Digital Line	HW08 FW015
TN793CP Analog Line	HW09 FW09
Avaya 4621SW IP (H.323) Telephones	Release 2.2
Avaya 6416D+M Digital Telephone	n/a
Avaya S8500B Server	Avaya SIP Enablement Services 3.1.2

Table 1 – Equipment and Version

3. Configure Avaya Communication Manager

Avaya Communication Manager was installed and configured for basic station to station calling prior to beginning the configuration shown in these Application Notes. These basic configuration details are outside the scope of the SIP trunking application and not included here.

3.1. SIP Trunk Configuration

3.1.1. Verify System Capacity and Required Features

The Avaya Communication Manager license controls the customer options. Contact an authorized Avaya sales representative for assistance if insufficient capacity exists or a required feature is not enabled.

Verify that there is sufficient remaining Communication Manager SIP trunk capacity available for the SIP Trunks to the SIP Service Provider, taking other applications that may require Communication Manager SIP trunk resources into consideration.

This is done by displaying Page 2 of the **System-Parameters Customer-Options** form. The number of SIP trunks available to assign to new or existing trunk groups is the difference between the **Maximum Administered SIP Trunks** and the **USED** value.

```
display system-parameters customer-options                               Page 2 of 10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 0                            0
    Maximum Concurrently Registered IP Stations: 5                    2
    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: 100 20

    Maximum Number of DS1 Boards with Echo Cancellation: 0           0
      Maximum TN2501 VAL Boards: 10                                  1
      Maximum Media Gateway VAL Sources: 0                           0
    Maximum TN2602 Boards with 80 VoIP Channels: 128                 2
    Maximum TN2602 Boards with 320 VoIP Channels: 128               0
    Maximum Number of Expanded Meet-me Conference Ports: 0           0

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

Figure 4: System-Parameters Customer-Options Form – Page 2

Verify that the Automatic Route Selection (ARS) feature is enabled on Page 3 of the **System-Parameters Customer-Options** form.

```

display system-parameters customer-options                               Page 3 of 10
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? n      Audible Message Waiting? n
Access Security Gateway (ASG)? n          Authorization Codes? n
Analog Trunk Incoming Call ID? n          CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? n   CAS Main? n
Answer Supervision by Call Classifier? n   Change COR by FAC? n
ARS? y                                     Computer Telephony Adjunct Links? n
ARS/AAR Partitioning? y                   Cvg Of Calls Redirected Off-net? n
ARS/AAR Dialing without FAC? n            DCS (Basic)? n
ASAI Link Core Capabilities? n            DCS Call Coverage? n
ASAI Link Plus Capabilities? n            DCS with Rerouting? n
Async. Transfer Mode (ATM) PNC? n         Digital Loss Plan Modification? n
Async. Transfer Mode (ATM) Trunking? n    DS1 MSP? n
ATM WAN Spare Processor? n                DS1 Echo Cancellation? n
ATMS? n
Attendant Vectoring? n

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

```

Figure 5: System-Parameters Customer-Options Form – Page 3

3.1.2. Determine Node Names

Use the “change node-names ip” command to view (or assign) the node names to be used in this configuration.

- “ses” and “150.100.100.130” are the **Name** and **IP Address** of the Avaya SIP Enablement Services server interface where Avaya Communication Manager SIP trunk messages are sent.
- “clan_01a03” and “150.100.100.113” are the **Name** and **IP Address** of the TN799DP C-LAN interface used for the SIP signaling group.

```

change node-names ip                                                  Page 1 of 2
                                IP NODE NAMES
Name                          IP Address
clan_01a02                    150.100.100.112
clan_01a03                    150.100.100.113
default                        0.0.0.0
medpro_01a05                  150.100.100.115
procr                          150.100.100.100
ses                            150.100.100.130
val_01a08                     150.100.100.118

```

Figure 6: IP Node Names

3.1.3. Define IP Codec Sets

This configuration uses two IP codec sets.

- G.711mu codec is used for local voice calls between Avaya telephones. This is IP codec set 1.

- G.729b and G.711mu codecs (in that priority) are used for voice calls via the SIP trunks to the SIP Service Provider. T.38 will be used for group 3 fax calls to PSTN connected fax machines via the SIP Service Provider. This is IP codec set 2.

Using “change ip-codec-set 1” command, enter “**G.711MU**” as the only **Audio Codec**. Retain the defaults for the remaining fields.

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

                               IP Codec Set

Codec Set: 1

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

Figure 7: IP Codec Set 1

Using “change ip-codec-set 2” command, enter “**G.729B**” and “**G.711MU**” as the first and second **Audio Codec** values on page 1 of the form. Again, retain the defaults for the remaining fields. On page 2 of the form, enter “**t38.standard**” for **FAX** and “**off**” for **Modem** and **TTD/TTY** 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.729B      n           2          20
2: G.711MU      n           2          20
3:
```

Figure 8: IP Codec Set 2 – Audio Codec Settings

```
change ip-codec-set 7                                     Page 2 of 2

                               IP Codec Set

                               Allow Direct-IP Multimedia? n

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

Figure 9: IP Codec Set 2 – Fax, Modem, TTD/TTY Mode Settings

3.1.4. Verify Near End IP Network Region

These Application Notes use IP network region 1 (the normal default) for the G650 Media Gateway, the IP telephones and the C-LAN (in slot 1a02) used for IP telephone registration. This will be the near-end network region for calls to the SIP Trunk from the SIP Service Provider.

Use the “display cabinet n” command (when “n” is “1” in this case) to verify the **IP Network Region** assignment of the G650-port carrier.

```
display cabinet 1
CABINET
CABINET DESCRIPTION
  Cabinet: 1
  Cabinet Layout: G650-rack-mount-stack
  Cabinet Type: expansion-portnetwork
Location: 1      IP Network Region: 1
Rack: row6      Room: sit1      Floor:      Building:
CARRIER DESCRIPTION
Carrier      Carrier Type      Number
E      not-used      PN 01
D      not-used      PN 01
C      not-used      PN 01
B      not-used      PN 01
A      G650-port      PN 01
```

Use the “change ip-network-map” command to assign the IP telephones to **Region 1**. In these Application Notes, the IP telephone addresses are within the range specified by the **From IP Address** and **To IP Address** fields (as shown in **Figure 1**.)

```
change ip-network-map
IP ADDRESS MAPPING
Page 1 of 32
Emergency
Location
Extension
From IP Address (To IP Address or Mask) Region VLAN
150.100.100.200 150.100.100.210 1 n
. . . . . n
. . . . . n
. . . . . n
```

Figure 10: IP Network Map for IP Telephones

3.1.5. Configure the C-LAN IP Network Region Assignment

In these Application Notes, two C-LANs are assumed to have been previously installed as part of the initial Avaya Communication Manager basic installation (using the procedures as described in [2]) and assigned the Node Names shown in **Figure 6**. The configuration in this section will assign them to the Network Regions appropriate for this SIP Trunking application.

Using the “change ip-interface uucss” command (where uu is the cabinet, c is carrier, and ss is the slot of the respective C-LAN), assign the **Network Region** value as follows:

- C-LAN “1a02” to Network Region 1
- C-LAN “1a03” to Network Region 2

Note: In order to change an existing ip-interface, the **Enable Ethernet Port** must first be set to “n”, the form saved and then the “change ip-interface uucss” done again. The **Enable Ethernet Port** must then be re-enabled with “y” when the **Network Region** value is set.

The resulting ip-interface of the C-LAN used for IP (H.323) telephone registration is:

```
change ip-interface 1a02                                     Page 1 of 1
                                                           IP INTERFACES

Type: C-LAN
Slot: 01A02
Code/Suffix: TN799 D
Node Name: clan_01a02
IP Address: 150.100.100.112
Subnet Mask: 255.255.255.0                               Link: 12
Gateway Address: . . .
Enable Ethernet Port? y                                  Allow H.323 Endpoints? y
Network Region: 1                                       Allow H.248 Gateways? y
VLAN: n                                                  Gatekeeper Priority: 5

Target socket load and Warning level: 400
Receive Buffer TCP Window Size: 8320
                                                           ETHERNET OPTIONS
Auto? n
Speed: 100Mbps
Duplex: Full
```

Figure 11: IP Interface of C-LAN 1a02 used for IP Telephones

The resulting ip-interface of the C-LAN to be used for SIP signaling group 3 is:

```
change ip-interface 01a03                                    Page 1 of 1
                                                           IP INTERFACES

Type: C-LAN
Slot: 01A03
Code/Suffix: TN799 D
Node Name: clan_01a03
IP Address: 150.100.100.113
Subnet Mask: 255.255.255.0                               Link: 13
Gateway Address: . . .
Enable Ethernet Port? y                                  Allow H.323 Endpoints? y
Network Region: 2                                       Allow H.248 Gateways? y
VLAN: n                                                  Gatekeeper Priority: 5

Target socket load and Warning level: 400
Receive Buffer TCP Window Size: 8320
                                                           ETHERNET OPTIONS
Auto? n
Speed: 100Mbps
Duplex: Full
```

Figure 12: IP Interface of C-LAN 1a03 used for SIP Signaling Group 3

3.1.6. Define IP Network Regions

IP network regions set various IP network properties for SIP trunk groups and other IP elements (such as IP telephones, media processor cards, etc.) assigned to the region.

In these Application Notes, two distinct IP network regions are defined.

- “IP Network Region 1” serves as the default region for Avaya Communication Manager and defines properties for local extension to extension calling.
- “IP Network Region 2” defines the properties for calls routed via SIP trunks to the SIP Service Provider.

Using the “change ip-network-region 1” command, enter on Page 1:

- **Name:** a descriptive string such as “Avaya CM Main Location”.
- **Authoritative Domain:** enter the SIP Domain of the Avaya SES used to reach the SIP Service Provider. In this case, “customer-sipdomain.com” is used. This value must match the **SIP Domain** field provisioned in the SES Administration Web Interface. Refer to Section 4.1.2 below for further details.
- **Codec Set:** the value “1” corresponding to the ip-codec-set defined in Section 3.1.3 for local calls between telephones on Avaya Communication Manager.
- **Intra-region IP-IP Direct Audio:** the value “yes” (the default).
- **Inter-region IP-IP Direct Audio:** the value “yes” (the default).

The IP-IP Direct Audio settings ensure the most efficient use of TN2602AP Media Processor resources.

Defaults for the remaining values are also used.

```
change ip-network-region 1                                     Page 1 of 19
                                     IP NETWORK REGION
Region: 1
Location: 1          Authoritative Domain: customer-sipdomain.com
Name: Avaya CM Main Location
MEDIA PARAMETERS
  Codec Set: 1          Intra-region IP-IP Direct Audio: yes
                        Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048    IP Audio Hairpinning? n
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46    RTCP Reporting Enabled? y
  Audio PHB Value: 46          RTCP MONITOR SERVER PARAMETERS
  Video PHB Value: 26          Use Default Server Parameters? y
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
  H.323 Link Bounce Recovery? y    RSVP Enabled? n
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

Figure 13: IP Network Region 1 – Page 1

Page 3 of the IP network region form is used to define the codec set and connectivity characteristics between IP network regions.

In these Application Notes, region 1 and 2 are directly connected (using the local LAN) without bandwidth restrictions. Calls between these regions are to use codec set 2 (as defined within Section 3.1.3).

On Page 3, configure the “src rgn 1 dst rgn 2” row as follows:

- **codec set:** enter “2”, to use the codec choices defined in Section 3.1.3 for calls with the SIP PSTN gateway.
- **direct WAN:** enter “y” to indicate that regions 1 and 2 are directly connected.
- **Total WAN-BW-limits:** enter “:NoLimit” to indicate that there is no explicit limit on the bandwidth or number of simultaneous calls between the regions.

```
change ip-network-region 1 Page 3 of 19
```

Inter Network Region Connection Management

src rgn	dst rgn	codec set	direct WAN	Total WAN-BW-limits	Video Norm	Prio	Shr	Intervening-regions	Dyn CAC	IGAR
1	1	1								
1	2	2	y	:NoLimit			n			n
1	3									
1	4									

Figure 14: IP Network Region 1 – Page 3

Configure IP Network Region 2, using the “change ip-network-region 2” command.

Enter:

- **Name:** a descriptive string such as “SIP Trks PSTN SP”
- **Authoritative Domain:** enter the SIP Domain of the Avaya SES used to reach the SIP Service Provider. In this case, “customer-sipdomain.com” is used. This value must match the **SIP Domain** field provisioned in the SES Administration Web Interface. Refer to Section 4.1.2 below for further details.
- **Codec Set:** the value “2” corresponding to the ip-codec-set defined in Section 3.1.3 for calls to the SIP PSTN Service Provider.
- **Intra-region IP-IP Direct Audio:** the value “yes” (the default).
- **Inter-region IP-IP Direct Audio:** the value “yes” (the default).

```

change ip-network-region 2                                     Page 1 of 19
                                                           IP NETWORK REGION

  Region: 2
Location: 1          Authoritative Domain: customer-sipdomain.com
  Name: SIP Trks PSTN SP
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
  Codec Set: 2           Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 20000    IP Audio Hairpinning? n
  UDP Port Max: 20999
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

```

Figure 15: IP Network Region 2 – Page 1

Verify that Page 3 of the “change ip-network-region 2” command appears as shown below without any additional entries. The codec set and inter-region connectivity characteristics for the **src rgn 2 dst rgn 1** row were established during the configuration of IP network region 1.

```

change ip-network-region 2                                     Page 3 of 19
                                                           Inter Network Region Connection Management

src dst codec direct   Total           Video           Dyn
rgn rgn set   WAN  WAN-BW-limits  Norm Prio  Shr Intervening-regions  CAC IGAR
2  1  2   y    :NoLimit           n
2  2  2
2  3
2  4

```

Figure 16: IP Network Region 2 – Page 3

3.1.7. Define SIP Trunk Group

One SIP trunk group is defined for calls with the SIP Service Provider (routed via the Avaya SES). Both incoming Direct Inward Dialed (DID) calls and outbound calls to the PSTN use this trunk group. This SIP trunk group requires a corresponding SIP signaling group to define the characteristics of the signaling relationship.

3.1.7.1 Establish the SIP Signaling Group

Using the “add signaling-group 3” command, configure signaling group 3 as follows:

- **Group Type:** set to “sip”.
- **Transport Method:** automatically set to “tls”. The Transport Layer Security (TLS) transport protocol is used between the Avaya Communication Manager and the Avaya SES. Note this is not the transport protocol used to communicate between the Avaya SES and the SIP Service Provider.

- **Near-end Node Name:** set to the C-LAN node name (defined in Section 3.1.2) used for the respective signaling group. In these Application Notes, “clan_01a03” is used for signaling group 3.
- **Far-end Node Name:** set to the Avaya SES used to route messages to the SIP Service Provider. In these Application Notes, the node name “ses” is used as defined in Section 3.1.2
- **Near-end Listen Port:** set to “5061”, the default port for SIP signaling using tls transport.
- **Far-end Listen Port:** set to “5061”.
- **Far-end Network Region:** set to “2”, the network region defined for SIP Service Provider calls as defined in Section 3.1.6.
- **Far-end Domain:** set to the IP address or domain name (e.g., serviceprovider.com) provided by the SIP Service Provider as their node that will send and receive SIP messages. In these Application Notes, the IP address “20.1.1.54” will be used.
- **Direct IP-IP Audio Connections:** set to “y”, indicating the RTP paths should be optimized to reduce the use of media processing resources when possible.
- **DTMF over IP:** set to “rtp-payload”. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833 [8].

The default values for the other fields may be used.

The resulting form for signaling group 3 is shown below.

```

add signaling-group 3                                     Page 1 of 1
                                     SIGNALING GROUP
Group Number: 3           Group Type: sip
                          Transport Method: tls

Near-end Node Name: clan_01a03           Far-end Node Name: ses
Near-end Listen Port: 5061               Far-end Listen Port: 5061
Far-end Domain: 20.1.1.54               Far-end Network Region: 2

                                          Bypass If IP Threshold Exceeded? n

DTMF over IP: rtp-payload               Direct IP-IP Audio Connections? y
                                          IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 3

```

Figure 17: Signaling Group 3

3.1.7.2 Establish the SIP Trunk Group

Using the “add trunk-group 3” command, configure trunk group 3 as follows.

On Page 1 of the Trunk Group form:

- **Group Type:** set to “sip”.
- **Group Name:** enter a descriptive string such as “SIP-PSTN-SP-TG3”.
- **TAC:** enter a trunk access code such as “#003”.
- **Service Type:** set to “public-ntwrk” for trunks to the PSTN.
- **Signaling Group:** set to “3” as defined within Section 3.1.7.1.
- **Number of Members:** set to the maximum number of simultaneous calls permitted for each trunk group. Within these Application Notes, “10” was used.

The default values may be used on the remaining pages of the trunk-group form.

The resulting form for trunk-group 3 is shown below.

```
add trunk-group 3                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 3                                     Group Type: sip          CDR Reports: y
  Group Name: SIP-PSTN-TG3                          COR: 1                 TN: 1          TAC: #003
  Direction: two-way                                Outgoing Display? n
  Dial Access? n                                    Night Service:
  Queue Length: 0
  Service Type: public-ntwrk                        Auth Code? n
                                                    Signaling Group: 3
                                                    Number of Members: 10
```

Figure 18: Trunk Group 3

3.1.8. Configure Calling Party Number Information

The SIP “From” header shown below contains information about the calling party. The header contains the calling party number (e.g., “16032224001”) in the userinfo segment and a domain (or IP address) in the hostname segment separated by an “@” sign.

```
From: "Jane Smith" <sip:16032224001@customer-sipdomain.com>;tag=80f839da25
```

The “public-unknown-numbering” command controls the calling party number sent in the userinfo segment. The **Authoritative Domain** field of the IP Network Region form completed in **Figure 15** associated with the SIP trunk group sets the hostname segment.

Public-unknown-numbering must always be setup, if no additional CPN prefix digits are sent. In these Application Notes the public-unknown-numbering is configured to send an 11 digit number corresponding to the DID or 800 number assigned by the SIP Service Provider.

Using the “change public-unknown-numbering n” command (where “n” is the leading digit of the extension range), specify the calling party number information as follows:

- **Ext Len:** set to “4”, the length of the extensions used.
- **Ext Code:** set to the leading digit of the extension used. In these Application Notes “40” and “6001” are entered to cover the assigned extensions of 40xx and 6001.
- **Trk Grp(s):** by default, leave blank to perform the same conversion across all SIP (and ISDN) trunk groups.
- **CPN Prefix:** set to the leading digits (e.g., “1603222”) that are to be sent as the calling party number.
- **Total CPN Len:** set to the total length (e.g., “11”) of the calling party number to be sent. The extension number will be appended to the **CPN Prefix** to form complete calling party number of **Total CPN Len** digits.

The completed public-unknown-numbering form is shown below.

change public-unknown-numbering 4					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	40		1603222	11	Total Administered: 2 Maximum Entries: 9999
4	6001		18003331234	11	

Figure 19: Public Unknown Numbering

3.1.9. Configure Call Routing

3.1.9.1 Outbound Calls

In these Application Notes, Automatic Route Selection (ARS) is used to route outbound calls via the SIP trunk groups to the SIP Service Provider. Each SIP Service Provider specifies the type of outbound calls supported (such as Local, Long Distance, International, etc.) and required digits to be sent for each call type. In this Application Notes those rules are specified in Table 2 found within Section 4.1.5. The rules may differ among the various Service Providers.

In addition the ARS route patterns support alternate routing (via an alternate trunk group 4)¹ when the first choice trunk group is fully utilized or unavailable. Note the configuration details for trunk group 4 is not described within these Application Notes.

Here, the configuration of one outbound calling pattern supporting calls to 1-733-xxx-xxx is shown. Routing will select SIP trunk group 3 as the first choice, with overflow to trunk group 4 as required. In this case as note in Table 2, the SIP Service Provider requires all calls within the North American Numbering plan will always be sent a 1 plus 10 digits.

¹ Note that this alternate trunk group does not necessarily need to use SIP. It would typically be an ISDN PRI or other “more traditional” method for placing PSTN calls, but can be any of the trunk types supported by Communication Manager.

A typical installation will generally require additional dial string and route pattern entries but that is beyond the scope of these Application Notes. Further information on ARS administration is discussed in References [1] and [3].

ARS administration begins by verifying the availability of the feature as shown in Section 3.1.1.

Following the verification, use the “change dialplan analysis” command to create a feature access code (fac) for ARS use.

- **Dialed String:** enter “9” that will become the user dialed prefix for outbound calls.
- **Total Length:** enter “1” as the length of the prefix.
- **Call Type:** enter “fac” as the type of prefix.

```
change dialplan analysis                                     Page 1 of 12
```

DIAL PLAN ANALYSIS TABLE								
Percent Full: 1								
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	attd						
4	4	ext						
5	4	ext						
6	4	ext						
9	1	fac						
*	3	dac						
#	4	dac						

Figure 20: Dial Plan Analysis

Use the “change feature-access-codes” command to assign the feature access code “9” to **Auto Route Selection (ARS) - Access Code 1** as shown below.

```
change feature-access-codes                               Page 1 of 7
```

FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *71		
Answer Back Access Code:		
Auto Alternate Routing (AAR) Access Code:		
Auto Route Selection (ARS) - Access Code 1: 9	Access Code 2:	
Automatic Callback Activation:	Deactivation:	
Call Forwarding Activation Busy/DA: *61 All: *62	Deactivation: *60	
Call Forwarding Enhanced Status: Act:	Deactivation:	
Call Park Access Code:		
Call Pickup Access Code:		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Contact Closure Open Code:	Close Code:	

Figure 21: ARS Feature Access Code

Use the “change ars analysis nn” command to configure the ARS route pattern selection rules as follows. Here “nn” is “17”, the first two digits of the dialed number after the ARS access code.

- **Dialed String:** enter the leading digits (e.g., “1733”) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., “11”) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., “11”) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., “3”) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used calls matching the dialed number.
- **Call Type:** enter “fnpa”, the call type for North American 1+10 digit calls.

change ars analysis 17						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 1			
Dialed String	Total Min Max	Route Pattern	Call Type	Node Num	ANI Reqd		
1733	11 11	3	fnpa		n		

Figure 22: ARS Digit Analysis Entries

Use the “change route-pattern n” command (where “n” is the **Route Pattern** number used above) to specify the SIP trunk groups selected for the outbound call.

In the form:

- **Pattern Name:** enter a descriptive string such as “PSTN LD” to describe the routing pattern.
- **Secure SIP?:** leave as “n”, the default.
- **Grp No:** enter the trunk groups to be used in priority order. Trunk group 3 is the first choice route followed by trunk group 4 in this configuration.
- **FRL:** enter the minimum facility restriction level (e.g., 1) necessary to use this trunk group, with 0 being the least restrictive. The FRL within the Class of Restriction (COR) assigned to the station must be greater than or equal to 1 in this case to use these trunk groups.
- **Pfx Mrk:** enter “1”, to always send the prefix 1 on 10 digit calls as specified for this Service Provider.
- **LAR:** enter the routing behavior to be followed if the call is not successfully completed using the trunk group. “Next” will cause the call to attempt to use the next choice in the routing pattern. “None” indicates that no further attempts will be made to complete the call. In the example below, a call that fails when attempting to use trunk group 3, will automatically attempt to use trunk group 4 before being abandoned.

The defaults values for the remaining fields may be used.

The completed route pattern form is shown below.

```

change route-pattern 3                                     Page 1 of 3
                Pattern Number: 3  Pattern Name: PSTN LD
                Secure SIP? n
  Grp FRL NPA Pfx Hop Toll No.  Inserted          DCS/ IXC
  No   Mrk Lmt List Del  Digits          QSIG
                                     Intw
1: 3   1     1
2: 4   1     1
3:
4:
5:
6:
                                     n  user
                                     n  user
                                     n  user
                                     n  user
                                     n  user
                                     n  user

  BCC VALUE TSC CA-TSC  ITC BCIE Service/Feature PARM No. Numbering LAR
  0 1 2 M 4 W      Request          Dgts Format
                                     Subaddress
1: Y Y Y Y Y n n          rest          next
2: Y Y Y Y Y n n          rest          none
3: Y Y Y Y Y n n          rest          none
4: Y Y Y Y Y n n          rest          none
5: Y Y Y Y Y n n          rest          none
6: Y Y Y Y Y n n          rest          none

```

Figure 23: Route Pattern 3

Use the “change locations” command to designate the SIP trunk route pattern (route pattern “3” below) in the **Proxy Sel. Rte. Pat.** field.

```

change locations                                         Page 1 of 16
                LOCATIONS
  ARS Prefix 1 Required For 10-Digit NANP Calls? y
  Loc Name          Timezone Rule  NPA ARS Atd  Disp Prefix  Proxy Sel
  No   Offset          FAC  FAC  Parm          Rte Pat
1: Main          + 00:00  0          1          3
2:

```

Figure 24: Location Form Administration

3.1.9.2 Incoming Calls

This step configures the routing of incoming DID numbers to the proper extensions.

In these Application Notes, incoming DID numbers 603-222-4000 through 4099 and the toll-free 800 number 800-333-1234 are assigned by the SIP Service Provider as noted in **Table 3** within Section 4.1.5 . These incoming digits are defined by the SIP Service Provider and must match what they send in order for incoming calls to route correctly. They are assigned to extensions (or hunt groups, VDNs, etc) as shown below.

Digits Received (within SIP INVITE message)	Extension (or Hunt Group) Answering
603 222 40xx	40xx
800 333 1234	6001

Use the “change inc-call-handling-trmt trunk-group n” command (where “n” is the SIP trunk group number) to administer the incoming number routing. This administration must be done for each incoming trunk group.

- **Called Len:** enter the total number of incoming digits received (e.g., “10”).
- **Called Number:** enter the specific digit pattern to be matched.
- **Del:** enter the number of leading digits that should be deleted
- **Insert:** enter the specific digits to be inserted at the beginning of the adjusted incoming digit string (to form what should be the complete number).

The completed inc-call-handling-trmt form for trunk group 3 is shown below.

change inc-call-handling-trmt trunk-group 3					Page 1 of 30
Service/ Feature	INCOMING CALL		HANDLING TREATMENT		
	Called Len	Called Number	Del	Insert	
public-ntwrk	10	60322240		6	
public-ntwrk	10	8003331234	10	6001	

3.1.10. Save Avaya Communication Manager Changes

This completes the configuration of the Avaya Communication Manager.

Use the “save translation” command to make the changes permanent.

4. Configure Avaya SIP Enablement Services

This section covers the administration of Avaya SIP Enablement Services. Avaya SIP Enablement Services is configured via an Internet browser using SIP Server Management screens. It is assumed that Avaya SIP Enablement Services software and the license file have already been installed. During the software installation, the install script is run on the Linux shell of the server to specify the IP network properties of the server including DNS server address(es). For additional information on these installation tasks, refer to Reference [6].

4.1. SIP Trunking to the SIP Service Provider

4.1.1. Log in to Avaya SIP Enablement Services

Access the Avaya SES SIP Server Management pages by entering “http://<ip-addr>/admin” as the URL in an Internet browser, where “<ip-addr>” is the IP address of Avaya SIP Enablement Services server. In these Application Notes, the URL “http://150.100.100.130/admin” was used.

Log in with the appropriate credentials and then select the **Launch Administration Web Interface** link from the main page as shown in **Figure 25**.



Figure 25: Avaya SES Main Page

The Avaya SES administration home page shown in **Figure 26** is displayed.



Figure 26: Avaya SES Administration Home Page

4.1.2. Verify System Properties

From the left pane of any SIP Server Management page, expand the **Server Configuration** option and select **System Properties**. This page displays the Avaya **SES Version** and the **Network Properties** entered via the install script during the installation process.

In the **Edit System Properties**, page note the **SIP Domain** entered during the initial installation. The **SIP Domain** “customer-sipdomain.com” is used in these Application Notes.

Note that throughout the SES administration screens, the Help link may be used at anytime for further information regarding the meaning of any fields.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The header includes the Avaya logo, the title "Integrated Management SIP Server Management", and the server IP "150.100.100.130". A navigation menu on the left lists various system management options. The main content area is titled "Edit System Properties" and contains several sections:

- System Properties:** Includes fields for SES Version (SES-3.1.2.0-309.0), System Configuration (simplex), Host Type (home/edge), and SIP Domain* (customer-sipdomain.cc). A note below the SIP Domain field states: "Note that the DNS domain is: customer-sipdomain.com. If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com".
- License Host*:** A text input field containing "localhost".
- Network Properties:** Includes fields for Local IP (150.100.100.130), Local Name (ses8300.customer-sipdomain.com), Logical IP (150.100.100.130), Logical Name (ses8300.customer-sipdomain.com), and Gateway IP Address (150.100.100.1).
- Redundant Properties:** Includes a field for Management Device (SAMP).

At the bottom of the form, there is a note "Fields marked * are required." and an "Update" button.

Figure 27: System Properties

4.1.3. Verify the Avaya SES Host Information

Verify the Avaya SES Host information using the **Edit Host** page. In these Application Notes the Avaya SES **Host Type** is a combined “home/edge”. This means that both the SIP Service Provider and Avaya Communication Manager communicate via a common home/edge Avaya SES. (Note that separate Avaya SES home and edge servers may exist in other configurations. Communications with the SIP Service Provider will always occur via the edge Avaya SES.)

Navigate to the **Edit Host** page (**Figure 28**) by following the **Hosts** link in the left navigation pane and then clicking on the **Edit** option under the **Commands** section of the **List Hosts** screen.

On the **Edit Host** screen:

- Verify that the IP address of this combined Avaya SES Home/Edge server is in the **Host IP Address** field.
- Do not modify the **DB Password** or **Profile Service Password** fields. If these fields are changed, exit the form without using the **Update** button. These values must match the values entered during the Avaya SES installation; incorrect changes may disable the Avaya SES.
- Verify that the **UDP**, **TCP** and **TLS** checkboxes are enabled as **Listen Protocols**.
- Verify that **TLS** is selected as the **Link Protocol**.
- Ensure that the SIP Service Provider IP address or domain name is not in the **Outbound Proxy** or **Outbound Direct Domains** fields.
- Default values for the remaining fields may be used.
- Click the **Update** button only if changes are necessary. Otherwise, exit the **Edit Host** page by selecting the **Top** link on the left navigation bar.

AVAYA Integrated Management
SIP Server Management
Server: 150.100.100.130

Help Exit

Edit Host

Host IP Address* 150.100.100.130

DB Password

Profile Service Password

Host Type home/edge

Parent none

Listen Protocols UDP TCP TLS

Link Protocols UDP TCP TLS

Presence Access Policy Allow All Deny All (Default)

Emergency Contacts Policy Allow Deny

Minimum Registration (seconds) 300 Registration Expiration Timer (seconds)* 86400

Line Reservation Timer (seconds)* 30

Outbound Routing Allowed From Internal External

OutboundProxy _____ Port _____ UDP TCP TLS

Outbound Direct Domains _____

Default Ringer Volume* 5 Default Ringer Cadence* 2

Default Receiver Volume* 5 Default Speaker Volume* 5

VMM Server Address _____

VMM Server Port 5005 VMM Report Period 5

Fields marked * are required.

Update

Figure 28: Edit Host

4.1.4. Add Avaya Communication Manager Media Server Interface

In these Application Notes, one media server signaling interface named “CLAN-1A03-5061” is used with Avaya Communication Manager.

Expand the **Media Servers** option within any Avaya SES SIP Server Management page, and select **Add** to display the Add Media Server page (**Figure 29**).

In the Add Media Server Interface page, enter information corresponding to the signaling group “3” entry performed in section 3.1.7.1.

- Enter “CLAN-1A03-5061” as the descriptive name in the **Media Server Interface Name** field.
- Select the Avaya SES home/edge IP address in the **Host** field.
- Select “TLS” (Transport Link Security) for the **SIP Trunk Link Type**. TLS provides encryption at the transport layer between Avaya Communication Manager and the Avaya SES.

- Enter the IP address of the “clan-1a03” interface in the **SIP Trunk IP Address** field as defined in **Figure 6**. Note: This may be the IP address of the “proc” interface in other Avaya Communication Manager configurations.

After completing the **Add Media Server Interface** page, click on the **Add** button.

AVAYA

Help Exit

Top

- Users
- Conferences
- Media Server Extensions
 - Emergency Contacts
- Hosts
- Media Servers
 - List
 - Add
- Adjunct Systems
 - Services
- Server Configuration
- Certificate Management
 - IM Logs
- Trace Logger
- Export/Import to ProVision

Add Media Server Interface

Media Server Interface Name*

Host

SIP Trunk

SIP Trunk Link Type TCP TLS

SIP Trunk IP Address*

Media Server

Media Server Admin Address (see Help)

Media Server Admin Login

Media Server Admin Password

Media Server Admin Password Confirm

Fields marked * are required.

Add

Figure 29: Add Media Server Interface for Voice Calls

When these operations are completed, the List Media Servers page will appear as shown in **Figure 30**.

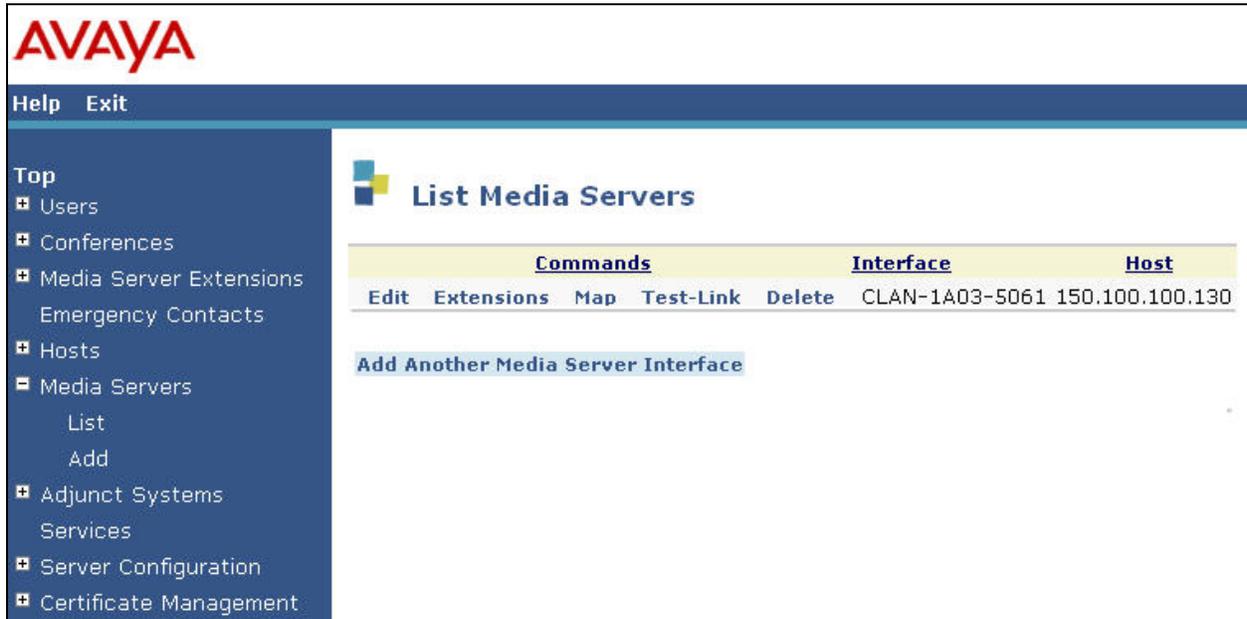


Figure 30: Completed List Media Servers

4.1.5. Configure Call Routing

Avaya SIP Enablement Services functions as a SIP proxy server for the SIP trunking with the SIP Service Provider. In this role, for outbound calls the Avaya SES must direct SIP messages originating from Avaya Communication Manager to the IP address designated by the SIP Service Provider. In a similar manner for incoming DID calls, the Avaya SES must route messages received from the SIP Service Provider to the proper signaling interface on Avaya Communication Manager.

In these Application Notes, the SIP message routing will be done for both outbound and inbound calls using Address Maps that examine some or all of the *called number* (using a Pattern) and route to a specific predetermined destination (called a Contact). The outbound proxy and direct domain routing feature is not used due to possible interactions with the SES Trusted Host capabilities.

The *called number* is contained within the *user* part of the Request URI of an incoming SIP INVITE message. The URI usually takes the form of *sip:user@domain*, where *domain* can be a fully qualified domain name or an IP address. The *user* part for SIP trunking in these Application Notes will only contain digits².

² SIP does permit mnemonic addressing such as “sip:john.doe@customer.com”. However, this convention is not used in these Application Notes for SIP Trunking. Further discussion of this topic is beyond the scope of this document.

The Address Map Patterns are specified using Linux regular expression syntax. Patterns are generally designed to match a collection of *called numbers* that require identical SIP message routing. However, each Pattern must also be specific enough to direct each unique *called number* to the proper signaling Contact. The Address Map Patterns must also be mutually exclusive (non-overlapping) from all other Address Map Patterns used in the Avaya SES to ensure proper operation.

Appendix B provides a detailed description of the Linux regular expression syntax used within the address map patterns.

4.1.5.1 Outbound PSTN Calls

SIP signaling for outbound calls is directed to Avaya SIP Enablement Services using the trunk groups selected by Automatic Route Selection in Avaya Communication Manager. The ARS routing patterns and SIP trunk group definitions control the digits used to populate the user portion of the Request URI for the SIP INVITE message and the codec(s) requested. SES receives the SIP INVITE message from Communication Manager and performs digit matching on the user portion of the Request URI using the regular expression provisioned in its Host Address Map Patterns to route the SIP INVITE to the SIP Service Provider using the Contact information corresponding to the Host Address Map.

In these Application Notes, the Avaya SES routing rules will send outbound PSTN calls to the SIP Service Provider. **Table 2** contains the rules used to configure the Avaya SES Host Address Maps in the following sections.

Type of Call	Digits Sent	Host Address Map Name	Host Address Map Pattern
Local and Long Distance in North American Numbering Plan	Digit 1 plus any 10 digits	LD_1plus10	^sip:1[0-9]{10}
Operator and International Calling	Digit 0 with or without additional digits; overall length indeterminate	0or0plusAny	^sip:0
N11 Service Calls	Digits 2 thru 9 followed only by the digits 11	N11	^sip:[2-9]11

Table 2: Outbound Host Address Map Rules

Note that additional or more specific pattern matches would be used if necessary to selectively route SIP traffic to different destinations (such as multiple service providers serving different geographic regions). Also note that a user dialed access code (such as 9 to place a PSTN call) has been previously deleted by Communication Manager (via ARS) prior to seizing the outbound SIP trunk.

4.1.5.1.1 Outbound Routing - Host Maps

Begin the outbound routing configuration by navigating to the Add Host Address Map pages.

- From any SIP Server Management page, expand the **Hosts** link and choose the **List** link causing the List Hosts page to appear.
- Select the **Map** link on the List Hosts page (**Figure 31**) causing the List Host Address Map page to appear.

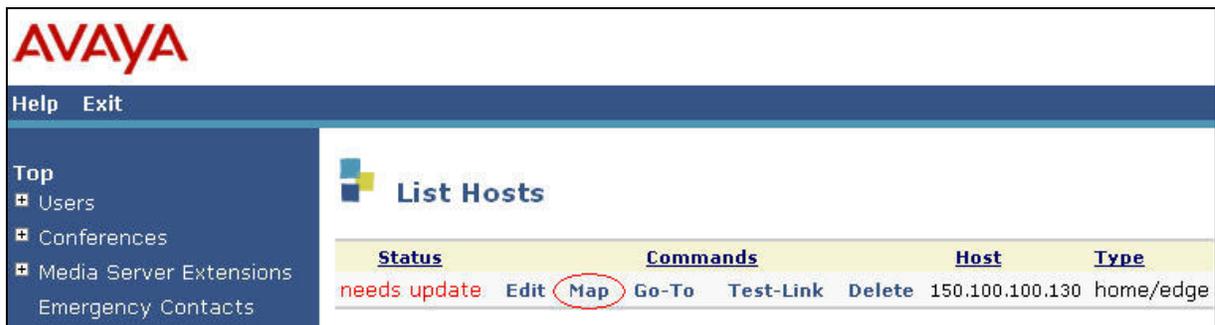


Figure 31: Accessing Host Address Maps from List Hosts Screen

- Select the **Add Map In New Group** link on the List Host Address Map page (**Figure 32**). This will display the Add Host Address Map screen (**Figure 33**).

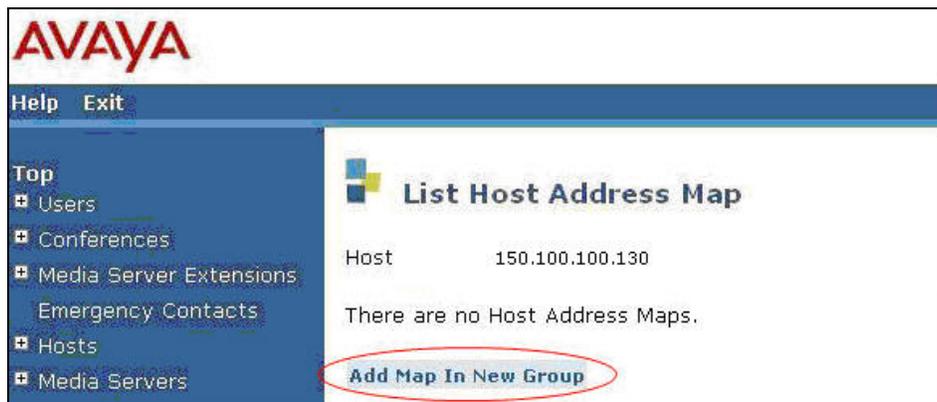


Figure 32: Adding a Host Address Map Group

The configuration of the Host Address Map for all 1 plus 10 digit North American calls is shown in **Figure 33**.

- Enter a descriptive **Name** for the map, such as “LD_1Plus10”.
- Enter the appropriate pattern for the call type. In this example, the pattern used for North American calls is “^sip:1[0-9]{10}” as noted in **Table 2**.
- Leave the **Replace URI** checkbox selected.
- Click the **Add** button.

The screenshot shows the Avaya web interface for adding a host address map. The left sidebar contains a navigation menu with 'Hosts' selected. The main content area is titled 'Add Host Address Map' and contains the following fields:

- Host: 150.100.100.130
- Name*: LD_1Plus10
- Pattern*: ^sip:1[0-9]{10}
- Replace URI:

Below the fields is a note: 'Fields marked * are required.' and an 'Add' button.

Figure 33: Address Map for 1+10 Digit Dialing

The remaining Host Address Map patterns for outbound calling are added in a similar manner. **Figure 34** illustrates the entry for Operator “zero” and “zero-plus” dialing.

The screenshot shows the Avaya web interface for adding a host address map. The left sidebar contains a navigation menu with 'Hosts' selected. The main content area is titled 'Add Host Address Map' and contains the following fields:

- Host: 150.100.100.130
- Name*: 0or0plusAny
- Pattern*: ^sip:0
- Replace URI:

Below the fields is a note: 'Fields marked * are required.' and an 'Add' button.

Figure 34: Address Map for 0 and 0+ Dialing

Figure 35 illustrates the host address map for the N11 service codes.

The screenshot shows the Avaya SIP Server Management interface. At the top left is the Avaya logo. Below it is a navigation menu with 'Help' and 'Exit' buttons. The main content area is titled 'Add Host Address Map'. It contains the following fields and options:

- Host: 150.100.100.130
- Name*: N11
- Pattern*: ^sip:[2-9]11
- Replace URI:
- Fields marked * are required.
- An 'Add' button is located at the bottom left of the form area.

The left sidebar contains the following navigation options:

- Top
- Users
- Conferences
- Media Server Extensions
- Emergency Contacts
- Hosts
- Update All
- List
- Migrate Home/Edge
- Media Servers

Figure 35: Address Map for N11 Dialing

4.1.5.1.2 Outbound Routing – Host Contact

The next step is to enter the host contact information for the SIP Service Provider. The SIP Service Provider must provide the IP address (or domain name), port and transport method to be used.

In these Application Notes, the IP address “20.1.1.54”, port “5060” and “udp” transport is used.

To enter the host contact information:

- Access the Host Address Map page by expanding the **Hosts** link in the left pane of any SIP Server Management page, selecting **List** and then clicking on the **Map** link associated with the appropriate **Host** (e.g., the Avaya SES at 150.100.100.130).

The List Host Address Map page is displayed as shown in **Figure 36**. Notice that there is no **Contact** information (above the **Add Another Contact** link) when first creating this entry.

Note: Should an entry already exist due to prior administration, the entry should be edited or deleted instead of using **Add Another Contact**.

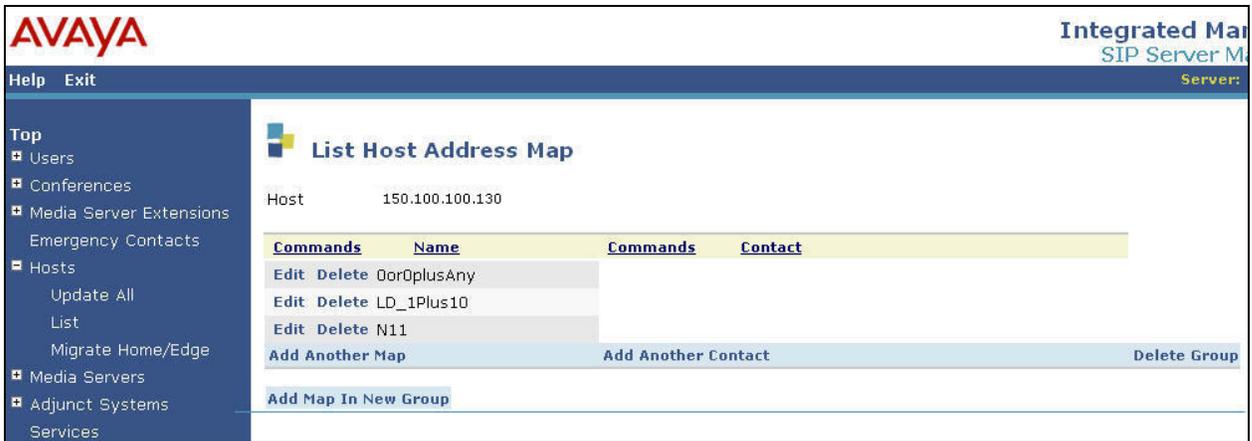


Figure 36: List Host Address Map – Prior to Contact Entry

- Click on the **Add Another Contact** link to open the Add Host Contact page as shown in **Figure 37**.
- In the Add Host Contact page, the **Contact** field specifies the destination for the call. In these Application Notes (using an IP address) the Contact field is entered as:

sip:\$(user)@20.1.1.54:5060;transport=udp

Note that if the SIP PSTN Server Provider requires a domain name (e.g. serviceprovider.com), SES will use a DNS SRV query to resolve the domain name into the appropriate IP address, port, and transport protocol. As such, the port or transport notation must NOT be included in this string if a domain name is used instead of an IP address (e.g., sip:\$(user)@serviceprovider.com).

- Click the **Add** button when completed.

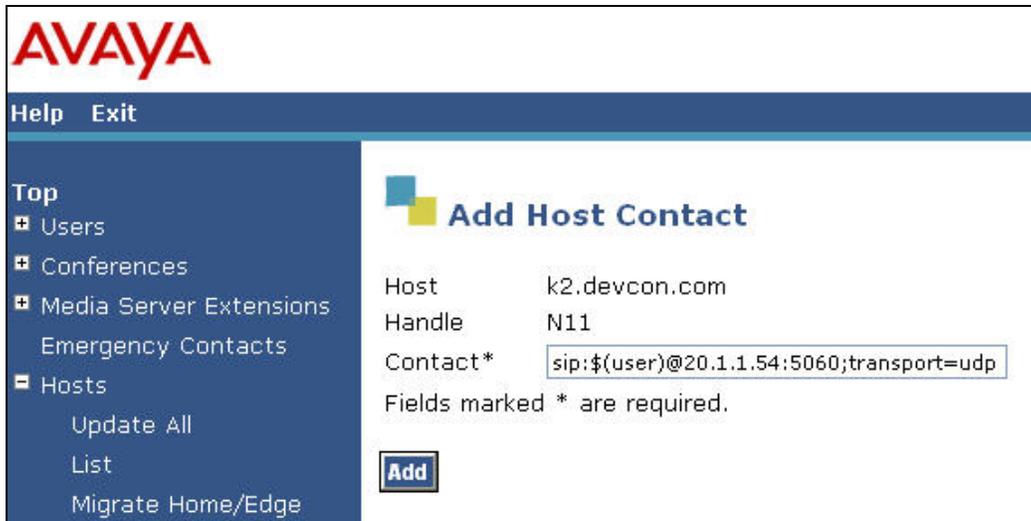


Figure 37 - Add Host Contact

After configuring the **Maps** and **Contact** information, the List Host Address Map page will appear as shown in **Figure 38**.

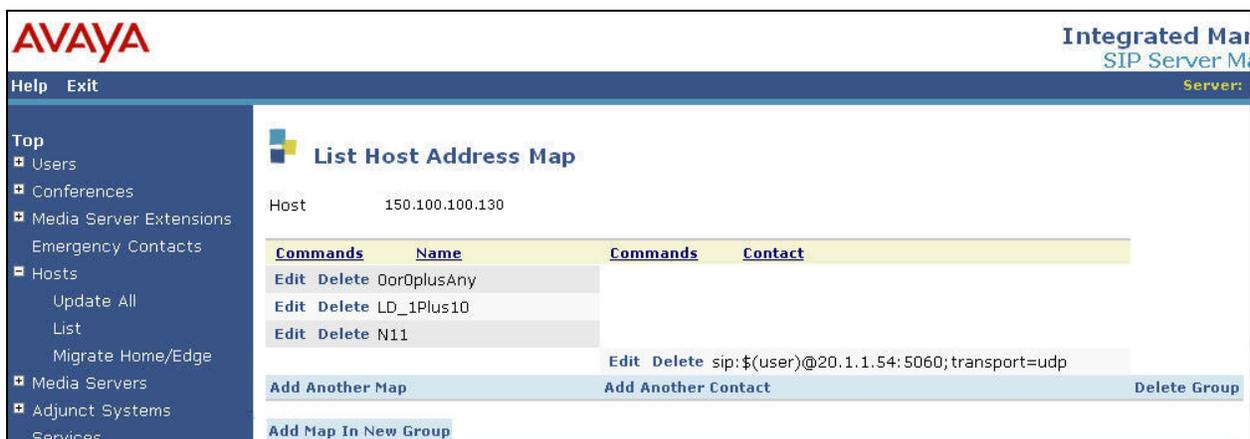


Figure 38: Completed List Host Address Map

4.1.5.2 Inbound Direct Inward Dialed Calls

SIP messages for incoming calls from the SIP Service Provider are sent to the Avaya SIP Enablement Services server. The Avaya SES then routes these messages to the appropriate Avaya Communication Manager using an Avaya SES media server address map.

In these Application Notes, the incoming PSTN calls use media server address map patterns matching the 10-digit called number in the user part of the SIP URI.

An example of a SIP URI in an INVITE message received from the SIP Service Provider for the DID number 603-222-4009 is:

sip:6032224009@150.100.100.130

The user part in this case is the 10-digit number “6032224009”.

Table 3 below summarizes the media server address map strategy used in these Application Notes for incoming calls.

DID Number Range	SIP URI User Portion	Address Map Pattern	Media Server Interface
603-222-4000 through 4099	6032224000 through 6032224099	^sip:60322240[0-9]{2}	CLAN-1A03-5061
800-333-1234	8003331234	^sip:8003331234	CLAN-1A03-5061

Table 3: Incoming DID Address Map Rules

To configure the media server address map for voice calls:

- Expand the **Media Servers** link in the left navigation menu of any SIP Server Management page. Select **List** to display the List Media Servers screen shown in **Figure 39**.
- Click on the **Map** link to display the List Media Server Address Map screen associated with the “CLAN-1A03-5061” **Interface**.

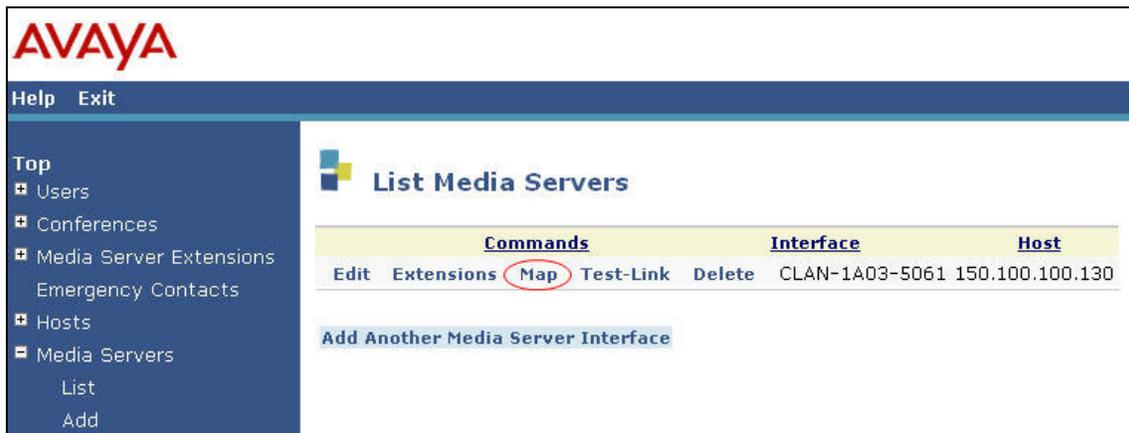


Figure 39: List Media Servers

- Since no previous media server address map exists, click on the **Add Map In New Group** link as shown in **Figure 40**. The **Host** field displays the name of the media server interface to which this map applies.

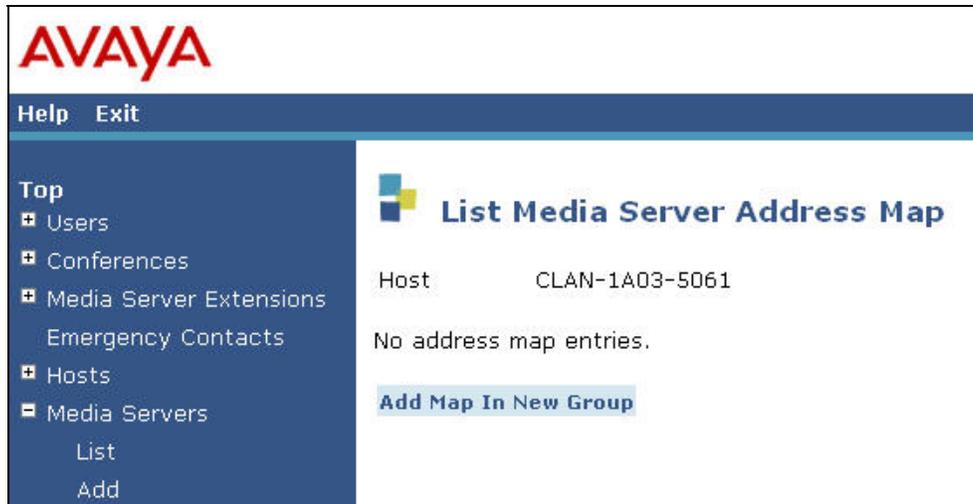


Figure 40 - List Media Server Address Map

The Add Media Server Address Map page shown in **Figure 41** is displayed.

- Enter a descriptive name in the **Name** field, such as “DID-60355540xx”.
- Enter the **Address Map Pattern** for incoming DID calls (from **Table 3**) into the **Pattern** field.

In this case, the DID numbers provided by the SIP Service Provider are 603-222-4000 thru 4099. The pattern specification for these DID numbers is:

`^sip:60322240[0-9]{2}`

This means that URIs beginning with “sip:60322240” followed any other 2 digits will match the pattern and be routed to the interface defined as “CLAN-1A03-5061”.

- Click the **Add** button once the form is completed.

The screenshot shows the Avaya web interface with the 'Add Media Server Address Map' page. The left sidebar contains a navigation menu with 'Media Servers' expanded to show 'List' and 'Add' options. The main content area has the following fields:

- Host: CLAN-1A03-5061
- Name*: DID-60355540xx
- Pattern*: ^sip:60322240[0-9]{2}
- Replace URI:

Fields marked * are required. An 'Add' button is located at the bottom left of the form area.

Figure 41: Incoming DID Calls - Media Server Address Map

A second media server address map is created for the assigned 800 number found in **Table 3**. The Name and Pattern will be entered as shown in **Figure 42**.

The screenshot shows the Avaya web interface with the 'Add Media Server Address Map' page. The left sidebar contains a navigation menu with 'Media Servers' expanded to show 'List' and 'Add' options. The main content area has the following fields:

- Host: CLAN-1A03-5061
- Name*: DID-8003331234
- Pattern*: ^sip:8003331234
- Replace URI:

Fields marked * are required. An 'Add' button is located at the bottom left of the form area.

Figure 42: Incoming 800 Call - Media Server Address Map

After configuring the media server address maps, the **List Media Server Address Map** page appears as shown in **Figure 43**.

The screenshot shows the Avaya SIP Administration Web Interface. The main content area is titled "List Media Server Address Map". It displays the host "CLAN-1A03-5061". Below this, there is a table with the following structure:

Commands	Name	Commands	Contact
Edit Delete	DID-60355540xx		
Edit Delete	DID-8003331234	Edit Delete	sip:\$(user)@150.100.100.113:5061;transport=tls

Below the table, there are several buttons: "Add Another Map", "Add Another Contact", "Delete Group", and "Add Map In New Group".

Figure 43: List Media Server Address Map

Note that after the first media server address map is created, a corresponding media server **Contact** entry is created automatically.

sip:\$(user)@150.100.100.113:5061;transport=tls

This **Contact** entry contains the IP address of the “CLAN-1A03” interface on Avaya Communication Manager, the port (5061) and the transport protocol (tls) to be used. The incoming digits sent in the user part of the original request URI will replace the \$(user) string when the message is sent.

4.1.6. Specify the SIP Service Provider as a Trusted Host

The IP address (or domain name) used by the SIP Service Provider (e.g., 20.1.1.54) must be added as a trusted host entry in the Avaya SES. As a trusted host, the Avaya SES will not attempt to authenticate incoming requests from the designated IP address.³

To configure a trusted host⁴:

- Log into the Avaya SES Linux shell using the administrative login and password.

³ If the trusted host step is not done, authentication challenges to incoming SIP messages (such as INVITES and BYEs) will be issued by Avaya SES. This may cause call setup to fail, active calls to be disconnected after timeout periods, and/or SIP protocol errors.

⁴ In SES release 4.0, the trusted host configuration is performed using the Trusted Host link found on the SES Administration Web Interface.

- Enter the following trustedhost command at the Linux shell prompt.

```
trustedhost -a 20.1.1.54 -n 150.100.100.130 -c SPsipProxy
```

The `-a` argument specifies the fully qualified domain name or IP address to be trusted; `-n` specifies the Avaya SES host name; `-c` adds a comment.

- Use the following **trustedhost** command to verify the entry is correct.

```
trustedhost -L
```

Figure 44 illustrates the results of the above trustedhost commands.⁵

```
admin@sesS8500> trustedhost -a 20.1.1.54 -n 150.100.100.130 -c SPsipProxy
20.1.1.54 is added to trusted host list.

admin@sesS8500> trustedhost -L
Third party trusted hosts.
   Trusted Host           |           CCS Host Name           |           Comment
-----+-----+-----
20.1.1.54                | 150.100.100.130                  | SPsipProxy
```

Figure 44: Results of Trusted Host Commands

- The trusted host configuration will not take effect until the **Update** action done in Section 4.1.7 is performed.

Note: In some cases the **Update** link may not be visible immediately following a trusted host command. Refreshing a SIP Server Management page by selecting **Top** from the left navigation menu will cause the **Update** link to appear.

4.1.7. Save the Avaya SES Changes

After making any changes within Avaya SES, commit the database changes by using the **Update** link.

Perform this step by clicking on the **Update** link found in the bottom of the blue navigation bar on the left side of any SIP Server Management page as shown in **Figure 45**.

⁵ For completeness, the `-d` argument allows the trust relationship to be deleted. For example,

```
trustedhost -d vzb-sip.net -n 192.168.0.11
```

removes a previously entered trust relationship.

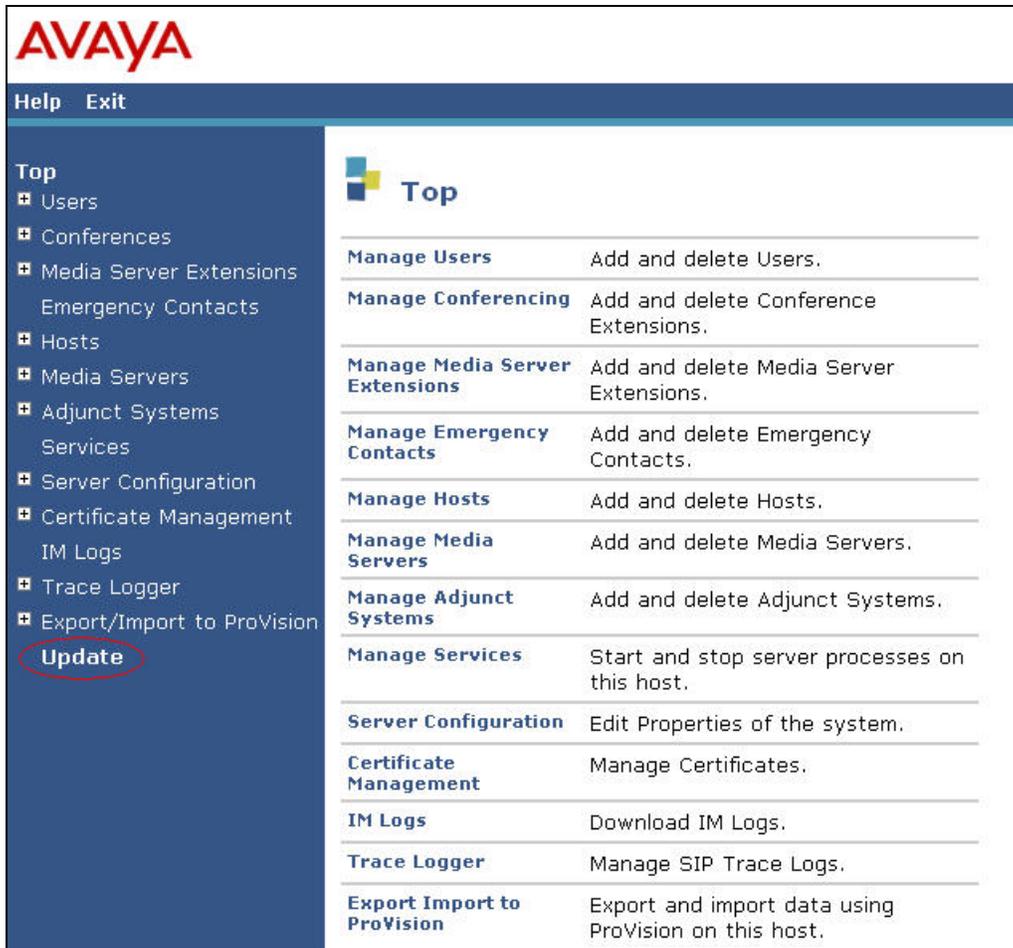


Figure 45: Update Displayed After an Avaya SES Administrative Change

5. Verification Steps

5.1. Verification Tests

This section provides steps that may be performed to verify the operation of the SIP trunking configuration described in the Application Notes.

- Incoming Calls – Verify that calls placed from a PSTN telephone to the DID number assigned are properly routed via the SIP trunk group(s) to the expected telephone, hunt group, ACD split, etc. Verify the talk-path exists in both directions, that calls remain stable for several minutes and disconnect properly.
- Outbound Calls – Verify that calls placed to a PSTN telephone are properly routed via the SIP trunk group(s) defined in the ARS route patterns. Verify that the talk-path exists

in both directions and that calls remain stable and disconnect properly.

- Direct IP-IP Connections – This applies if IP telephones and Direct IP-IP are used. Verify that stable calls are using Direct IP-IP talk paths using the “status station” or “status trunk-group” commands. When Direct IP-IP is used, the Audio Connection field will indicate “ip-direct” instead of “ip-tdm”.

5.2. Troubleshooting Tools

The Avaya Communication Manager “list trace station”, “list trace tac”, “status station” and/or “status trunk-group” commands are helpful diagnostic tools to verify correct operation and to troubleshoot problems. MST diagnostic traces (performed by Avaya support) can be helpful in understanding the specific SIP interoperability issues.

The “Trace Logger” function within the Avaya SES Administration Web Interface may be used to capture SIP traces between Avaya SES and the SIP Service Provider. These traces can be instrumental in understanding SIP protocol issues resulting from configuration problems.

If port monitoring is available, a SIP protocol analyzer such as WireShark (a.k.a., Ethereal) to monitor the SIP messaging at the various interfaces (C-LAN, Acme Packet and/or SIP PSTN gateway) is a very powerful tool for troubleshooting. Note that SIP messaging between Avaya Communication Manager and Avaya SES uses TLS encryption and cannot be viewed using WireShark..

6. Conclusion

These Application Notes describe the steps for configuring SIP trunking between an Avaya Communication Manager based SIP telephony solution and a typical (but hypothetical) SIP Service Provider.

The configuration shown in these Application Notes is representative of a typical (but hypothetical) SIP trunking solution and is intended to provide configuration guidance to supplement other Avaya product documentation.

Following these guidelines DOES NOT imply that successful interoperability with any specific SIP Service Provider is ensured.

Formal compliance testing with specific Service Providers is performed as part of the Avaya DeveloperConnection program to validate interoperability of specific release configurations involving Avaya products and the Service Provider’s service offerings.

The Avaya DeveloperConnection website (<http://www.avaya.com/gcm/master-usa/en-us/corporate/alliances/developerconnection/index.htm>) should be consulted to determine the interoperability testing status with specific Service Providers.

7. References

The Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3.1, Document Number 03-300509.
- [2] *Adding New Hardware for Avaya Media Servers and Gateways*, February 2007, Issue 2, Release 4.0, Document Number 03-300684
- [3] *Feature Description and Implementation for Avaya Communication Manager*, Issue 5, Document Number 555-245-205
- [4] *SIP Support in Avaya Communication Manager Running on the Avaya S8300, S8400, S8500 series and S8700 series Media Server*, March 2007, Issue 6.1, Document Number 555-245-206.
- [5] *4600 Series IP Telephone Release 2.6 LAN Administrator Guide*, August 2006, Issue 4, Document Number 555-233-507
- [6] *Installing and Administering SIP Enablement Services*, March 2007, Issue 2.1, Document Number 03-600768

Several Internet Engineering Task Force (IETF) standards track RFC documents were referenced within these Application Notes. The RFC documents may be obtained at: <http://www.rfc-editor.org/rfcsearch.html>.

- [7] RFC 3261 - *SIP (Session Initiation Protocol)*, June 2002, Proposed Standard
- [8] RFC 2833 - *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, May 2000, Proposed Standard

APPENDIX A: Sample SIP INVITE Messages

This section displays the format of typical SIP INVITE messages sent between the SIP Service Provider and the Avaya SES at the enterprise site. These INVITE messages may be used for comparison and troubleshooting purposes. Differences in these messages may indicate that different configuration options were selected.

Sample SIP INVITE Message from a SIP Service Provider to the Avaya SES:

```
INVITE sip:6023334000@150.100.100.130 SIP/2.0
Via:SIP/2.0/UDP 20.1.1.54;branch=z9hG4bK-xyz.20.1.1.54-V5060-0-951040837
From:<sip:7336731730@20.1.1.54;user=phone>;tag=26074514-1178723120777-
To:"ABC Corp"<sip:6023334000@150.100.100.130>
Call-ID:BW110520777090507561442054@20.1.1.54
CSeq:951040837 INVITE
Contact:<sip:20.1.1.54:5060>
Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,UPDATE,NOTIFY
Supported:100rel
Accept:multipart/mixed,application/sdp
Max-Forwards:10
Content-Type:application/sdp
Content-Length:285
```

```
v=0
o=xyz 57542641 1 IN IP4 20.211.120.15
s=-
c=IN IP4 20.211.120.15
t=0 0
m=audio 17040 RTP/AVP 18 0 8 101
c=IN IP4 20.211.120.15
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

Sample SIP INVITE Message from Avaya SES to the SIP Service Provider:

```
INVITE sip:17337425413@20.1.1.54 SIP/2.0
Call-ID: 80105628dbddc1835a465d72c600
CSeq: 1 INVITE
From: "SIP Trunk Demol" <sip:16023334000@customer-
sipdomain.com:5061>;tag=80105628dbddc1825a465d72c600
Record-Route: <sip:150.100.100.130:5060;lr>,<sip:1150.100.100.113:5061;lr;transport=tls>
To: "17337425413" <sip:17337425413@150.100.100.130>
Via: SIP/2.0/UDP 150.100.100.130:5060;branch=z9hG4bK8383830303031313135f96.0,SIP/2.0/TLS
150.100.100.113;psrrposn=2;received=150.100.100.113;branch=z9hG4bK80105628dbddc1845a465d72c600
Content-Length: 201
Content-Type: application/sdp
Contact: "SIP Trunk Demol" <sip:6023334000@150.100.100.113:5061;transport=tls>
Max-Forwards: 69
User-Agent: Avaya CM/R014x.00.0.730.5
Allow: INVITE,CANCEL,BYE,ACK,PRACK,SUBSCRIBE,NOTIFY,REFER,OPTIONS
History-Info: <sip:17337425413@>;index=1
History-Info: "17337425413" <sip:17337425413@>;index=1.1
Supported: 100rel,timer,replaces,join,histinfo
Min-SE: 1200
Session-Expires: 1200;refresher=uac
P-Asserted-Identity: "SIP Trunk Demol" <sip:16023334000@customer-sipdomain.com:5061>

v=0
o=- 1 1 IN IP4 150.100.100.113
s=-
c=IN IP4 150.100.100.116
t=0 0
m=audio 2052 RTP/AVP 18 0 127
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:127 telephone-event/8000
```

APPENDIX B: Specifying Pattern Strings in Address Maps

The syntax for the pattern matching used within the Avaya SES is a Linux regular expression used to match against the URI string found in the SIP INVITE message.

Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special *metacharacters*, which may represent items like quantity, location or types of character(s).

In the pattern matching string used in the Avaya SES:

- Normal text characters and numbers match themselves.
- Common metacharacters used are:
 - A period `.` matches any character once (and only once).
 - An asterisk `*` matches zero or more of the preceding characters.
 - Square brackets enclose a list of any character to be matched. Ranges are designated by using a hyphen. Thus the expression `[12345]` or `[1-5]` both describe a pattern that will match any single digit between 1 and 5.
 - Curly brackets containing an integer 'n' indicate that the preceding character must be matched exactly 'n' times. Thus `5{3}` matches '555' and `[0-9]{10}` indicates any 10 digit number.
 - The circumflex character `^` as the first character in the pattern indicates that the string must begin with the character following the circumflex.

Putting these constructs together as used in this document, the pattern to match the SIP INVITE string for any valid 1+ 10 digit number in the North American dial plan would be:

`^sip:1[0-9]{10}`

This reads as: "Strings that begin with exactly **sip:1** and having any 10 digits following will match.

A typical INVITE request below uses the shaded portion to illustrate the matching pattern.

```
INVITE sip:17325551638@20.1.1.54:5060;transport=udp SIP/2.0
```

©2007 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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com