



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Manager and Avaya SIP Enablement Services SIP Trunking with AT&T IP Flexible Reach Service and AT&T VPN Transport – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Communication Manager and Avaya SIP Enablement Services (SES) SIP trunking with the AT&T IP Flexible Reach service accessed through AT&T VPN transport service connections. The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T VPN (AVPN) transport service uses MPLS VPNs to allow an enterprise's sites to be connected together in a private wide area network. The convergences of various AT&T business VoIP and AVPN services allow enterprises to make voice calls over their private wide area data network connections. In these Application Notes, for brevity and clarity, the term "AT&T IP Flexible Reach service" refers specifically to the AT&T IP Flexible Reach service using AVPN as the network transport. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

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

TABLE OF CONTENTS

- 1. Introduction.....3
 - 1.1. Interoperability Compliance Testing3
 - 1.2. Support.....3
 - 1.3. Known Limitations3
- 2. Reference Configuration.....4
 - 2.1. Illustrative Configuration Information.....6
 - 2.2. Call Flows.....7
- 3. Equipment and Software Validated.....11
- 4. Avaya Communication Manager.....12
 - 4.1. System Parameters12
 - 4.2. Dial Plan and Feature Access Codes14
 - 4.3. IP Network Parameters16
 - 4.4. Outbound Calls.....22
 - 4.4.1. Outbound PSTN Calls22
 - 4.4.2. Outbound Calls To TDM Gateway Sites25
 - 4.4.3. Calling Party Number28
 - 4.5. Inbound Calls29
 - 4.5.1. Inbound PSTN Calls.....29
 - 4.5.2. Inbound Calls From TDM Gateway Sites.....32
 - 4.5.3. Connected Party Number33
 - 4.6. SIP Phones.....34
- 5. Configure Avaya SIP Enablement Services (SES)35
 - 5.1. Background.....35
 - 5.2. Host Configuration.....35
 - 5.3. Interfaces to Avaya Communication Manager.....37
 - 5.4. Call Routing.....39
 - 5.4.1. Background39
 - 5.4.2. Outbound Calls to AT&T IP Flexible Reach Service40
 - 5.4.3. Inbound Calls from AT&T IP Flexible Reach Service40
 - 5.5. Trusted Host43
- 6. General Test Approach and Test Results.....45
- 7. Verification Steps.....46
 - 7.1. Verification Tests.....46
 - 7.2. Troubleshooting Tools.....47
- 8. Conclusion47
- 9. References.....48
- 10. Change History.....48

1. Introduction

These Application Notes describe the steps for configuring Avaya Communication Manager and Avaya SIP Enablement Services (SES) SIP trunking with the AT&T IP Flexible Reach service accessed through AT&T VPN transport service connections. The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T VPN (AVPN) transport service uses MPLS VPNs to allow an enterprise's sites to be connected together in a private wide area network. The convergences of various AT&T business VoIP and AVPN services allow enterprises to make voice calls over their private wide area data network connections. In these Application Notes, for brevity and clarity, the term "AT&T IP Flexible Reach service" refers specifically to the AT&T IP Flexible Reach service using AVPN as the network transport. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. See Section 1.3 for a list of the types of calls that are not supported in AT&T IP Flexible Reach service.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying outbound and inbound call flows between Avaya Communication Manager and phones residing in a simulated PSTN and in TDM gateway sites.

1.2. Support

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. The "Connect with Avaya" section provides the worldwide support directory. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on <http://support.avaya.com>) to directly access specific support and consultation services based upon their Avaya support agreements.

1.3. Known Limitations

1. Direct IP-to-IP media is not supported on calls between SIP phones (including Avaya 4600 and 9600 Series SIP Telephones) in the Avaya site and the AT&T IP Flexible Reach service due to a known issue in Avaya Communication Manager Release 5.1.2 Service Pack 1. The administration shown in Section 4.6 disables Direct IP-to-IP media for SIP phones in the Avaya site.
2. Avaya one-X™ Communicator (in either H.323 or SIP mode) does not currently support G.729B codec, so Direct IP-to-IP media is not supported on calls between Avaya one-X™ Communicator and the AT&T IP Flexible Reach service that require G.729B codec.
3. Fax calls experiences intermittent issues with TN2602AP IP Media Resource 320 boards running build 48, hence build 47 is recommended until the issues are resolved.

4. On outbound calls from Avaya one-X™ Communicator in SIP mode to TDM gateway sites, the TDM gateway sites do not hear DTMF from Avaya one-X™ Communicator. This is due to an issue in the TDM gateway where the TDM gateway can only process RTPevent packets encoded with a specific RTP payload type, even though the TDM gateway had agreed to the RTP payload type proposed by Avaya one-X™ Communicator during the codec negotiation.
5. RTP header compression (cRTP) must be disabled in the AVPN routers connected to the Avaya site. See the AT&T document “AT&T VPN Service (AVPN) - CE Router Customer Configuration Guide for Voice over AVPN” for details.

2. Reference Configuration

The sample configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Avaya Communication Manager provides the enterprise voice communications services. In this sample configuration, Avaya Communication Manager runs on an Avaya S8720 Server. This solution is extensible to other Avaya S8xxx Servers.
- The Avaya Media Gateway provides the physical interfaces and resources for enterprise voice communications. In this sample configuration, an Avaya G650 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya SIP Enablement Services (SES) runs on an Avaya S8500 server. Avaya SES serves as a SIP proxy between Avaya Communication Manager and the AT&T IP Flexible Reach service. Avaya SES also provides registrar services to SIP phones in the enterprise.
- The Avaya “office” phones include Avaya SIP, H.323, and Digital phones, and Avaya one-X™ Communicator, which is a softphone that runs on a PC (not shown).
- Avaya Modular Messaging provides the corporate voice messaging capabilities for enterprise users.
- Enterprise sites will generally have additional or alternate routes to PSTN using analog or digital TDM trunks.
- IP Network Address Translation (NAT) devices, firewalls, Application Layer Gateway (ALG) devices, and Session Border Controller (SBC) devices that may exist between the enterprise site and the AT&T IP Flexible Reach service are not explicitly shown. Those devices generally must be SIP-aware and configured properly for SIP trunking to function properly. When configured correctly, those devices are transparent to the Avaya communications infrastructure.
- Enterprise networks of sufficient size or complexity may use Avaya SES in a separate Home/Edge server configuration, i.e., separate servers for Avaya SES Home and Avaya SES Edge roles. This configuration is functionally equivalent to the Avaya SES combined Home/Edge server configuration illustrated in these Application Notes. As appropriate, special notes have been included to clarify specific administration details related to the Avaya SES separate Home/Edge server configuration.

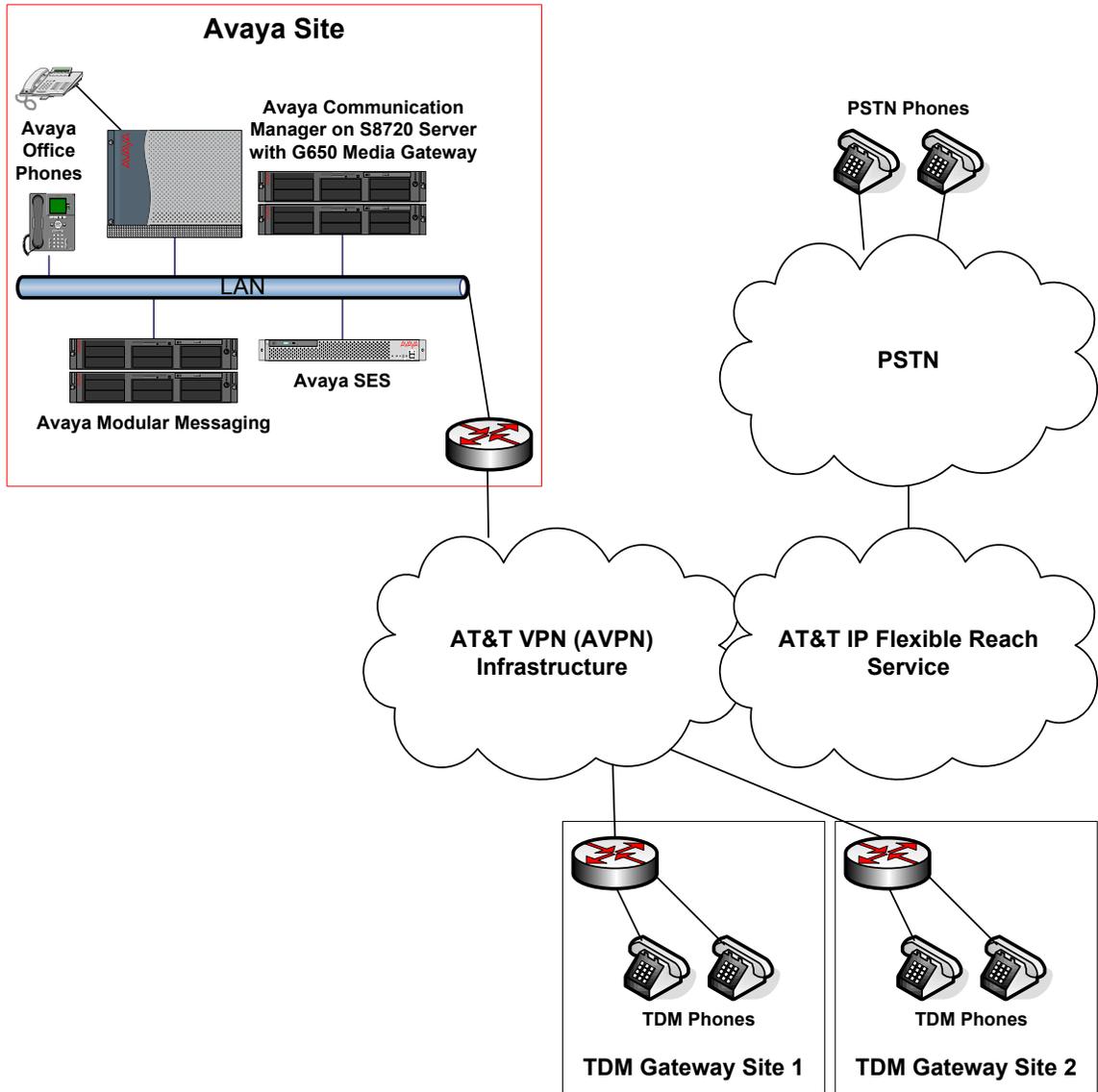


Figure 1: Sample SIP Trunking Configuration

2.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the sample configuration described in these Application Notes, and are **for illustrative purposes only**. Customers must obtain and use the specific values for their own specific configurations.

Component	Illustrative Value in these Application Notes
Avaya Site	
Extensions	26xxx
Phone Numbers (of extensions)	723-112-6xxx
AT&T IP Flexible Reach Service	
Border Element IP Address	10.94.2.12
Digits Passed in SIP Request-URI to Avaya Site	6xxx
TDM Gateway Site 1	
Phone Numbers	201-398-2xxx
TDM Gateway Site 2	
Phone Numbers	908-542-4xxx
PSTN	
Phone Numbers	732-xxx-xxxx

Table 1: Illustrative Values Used in these Application Notes

2.2. Call Flows

To understand how outbound and inbound PSTN calls, as well as calls between the Avaya site and TDM gateway sites, are routed, several call flows are described in this section.

The first call scenario illustrated in **Figure 2** is an outbound call from an Avaya Communication Manager phone to the PSTN via SIP trunking with the AT&T IP Flexible Reach service.

1. An Avaya Communication Manager phone originates a call to a PSTN number.
2. Avaya Communication Manager applies any necessary origination treatment (verifying permissions, determining the proper route, selecting the outgoing trunk, etc.) and routes the call to Avaya SES.
3. Avaya SES routes the call to the AT&T IP Flexible Reach service.
4. The AT&T IP Flexible Reach service routes the call to the PSTN.
5. The PSTN completes the call to the destination phone.

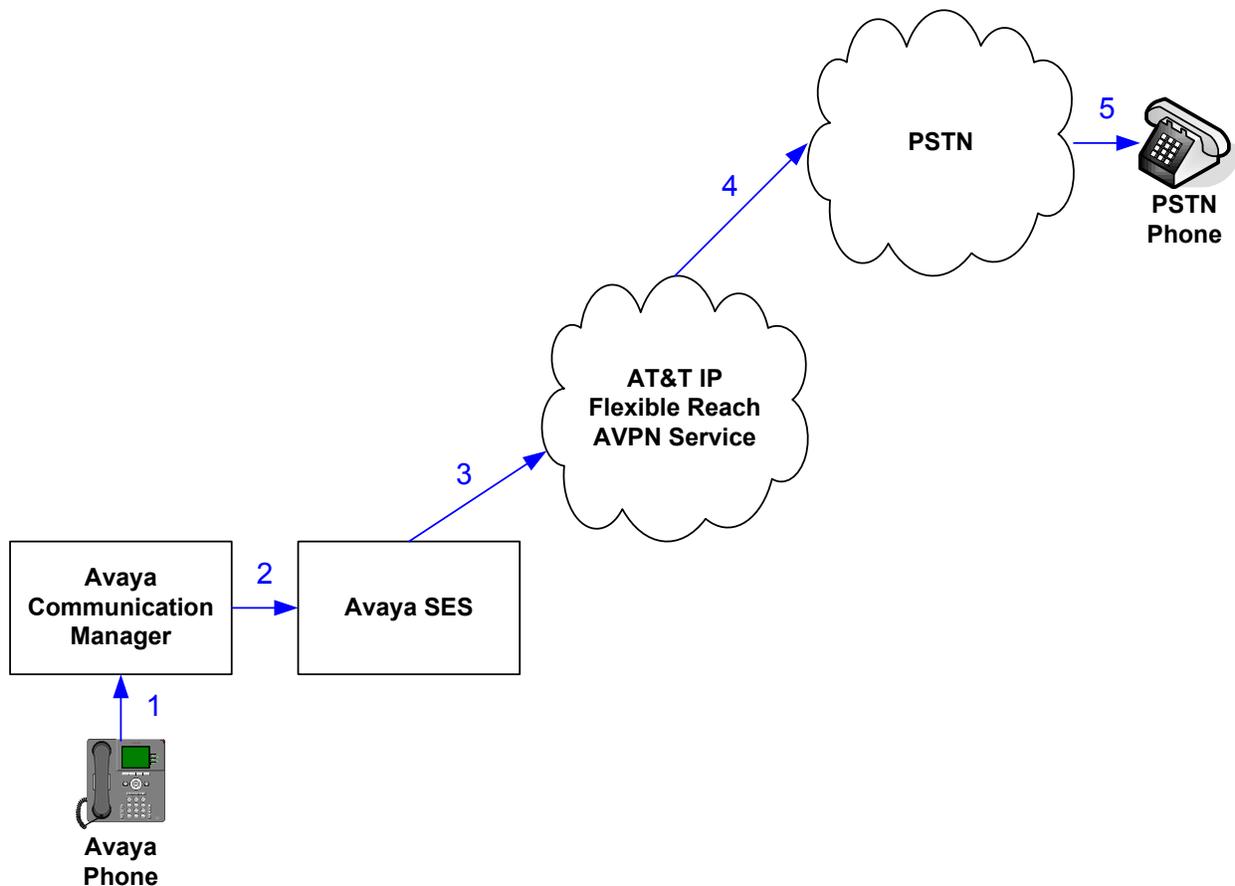


Figure 2: Outbound PSTN Call Scenario

The second call scenario illustrated in **Figure 3** is an inbound call from a PSTN phone to an Avaya Communication Manager phone via SIP trunking with the AT&T IP Flexible Reach service.

1. A PSTN phone originates a call to a DID number assigned to an Avaya Communication Manager site.
2. The PSTN routes the call to the AT&T IP Flexible Reach service.
3. The AT&T IP Flexible Reach Service routes the call to Avaya SES.
4. Avaya SES routes the call to Avaya Communication Manager.
5. Avaya Communication Manager applies any necessary termination treatment (examining and, if necessary, modifying the called party number, verifying permissions, etc.) and completes the call to the Avaya Communication Manager phone.

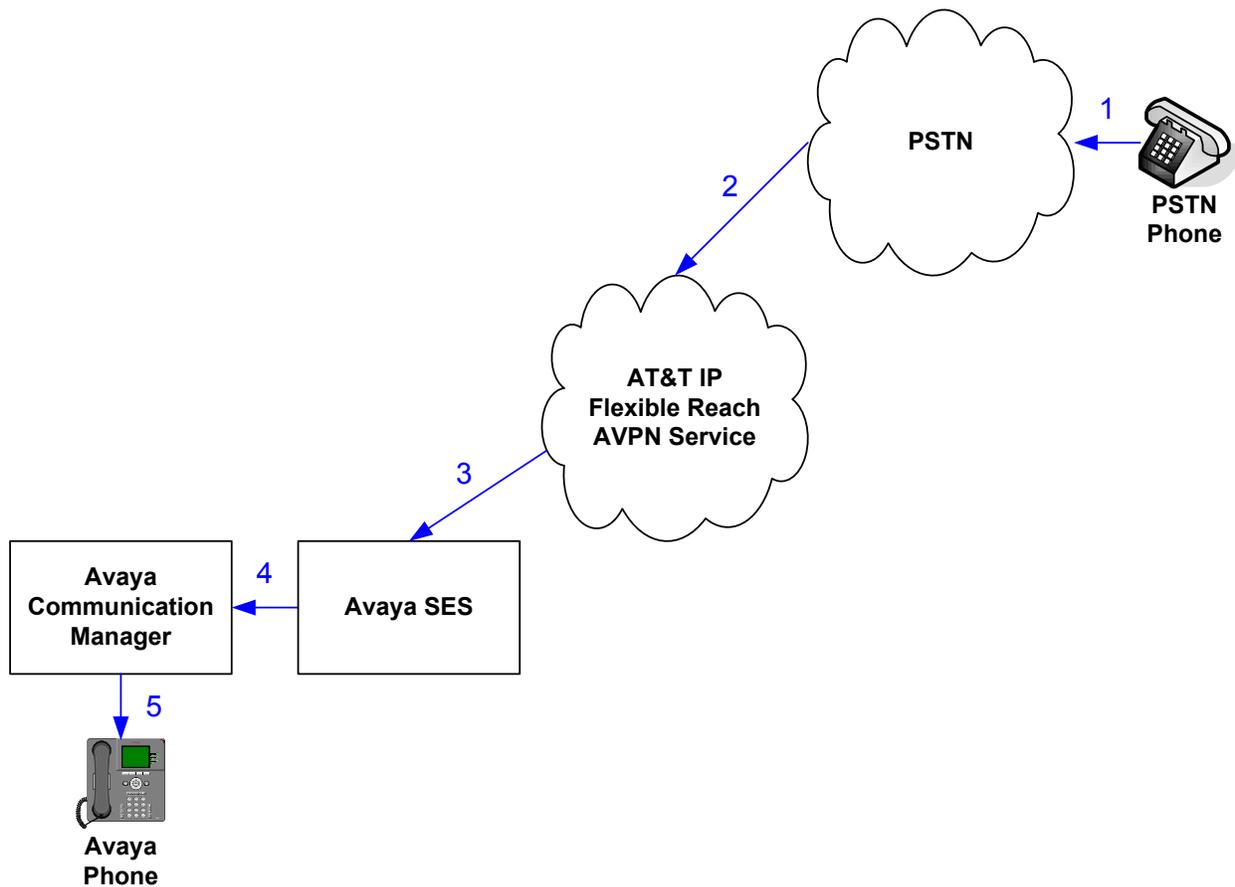


Figure 3: Inbound PSTN Call Scenario

The third call scenario illustrated in **Figure 4** is an outbound call from an Avaya Communication Manager phone to a phone residing behind a TDM gateway in another site.

1. An Avaya Communication Manager phone originates a call to a TDM gateway phone number.
2. Avaya Communication Manager applies any necessary origination treatment (verifying permissions, determining the proper route, selecting the outgoing trunk, etc.) and routes the call to Avaya SES.
3. Avaya SES routes the call to the AT&T IP Flexible Reach service.
4. The AT&T IP Flexible Reach service routes the call to the TDM gateway.
5. The TDM gateway completes the call to the called phone.

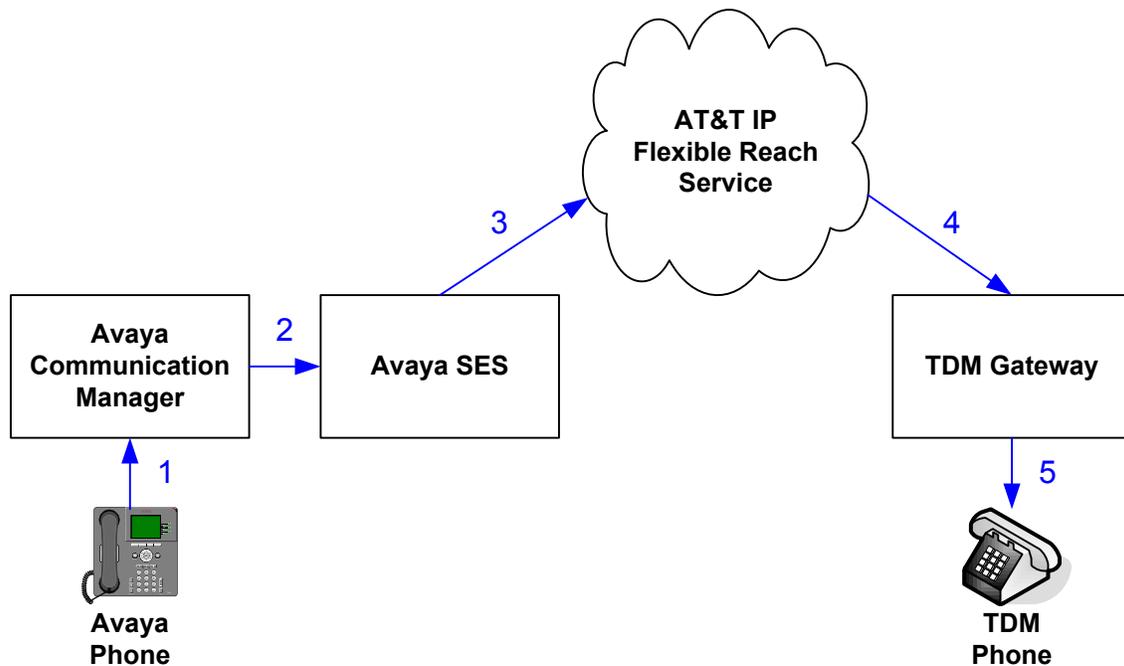


Figure 4: Outbound Call to TDM Gateway Phone Scenario

The fourth call scenario illustrated in **Figure 5** is an inbound call to an Avaya Communication Manager phone from a phone residing behind a TDM gateway in another site.

1. A phone residing behind a TDM gateway in another site originates a call to an Avaya Communication Manager phone number.
2. The TDM gateway routes the call to the AT&T IP Flexible Reach service.
3. The AT&T IP Flexible Reach service routes the call to Avaya SES.
4. Avaya SES routes the call to Avaya Communication Manager.
5. Avaya Communication Manager applies any necessary termination treatment (examining and, if necessary, modifying the called party number, verifying permissions, etc.) and completes the call to the Avaya Communication Manager phone.

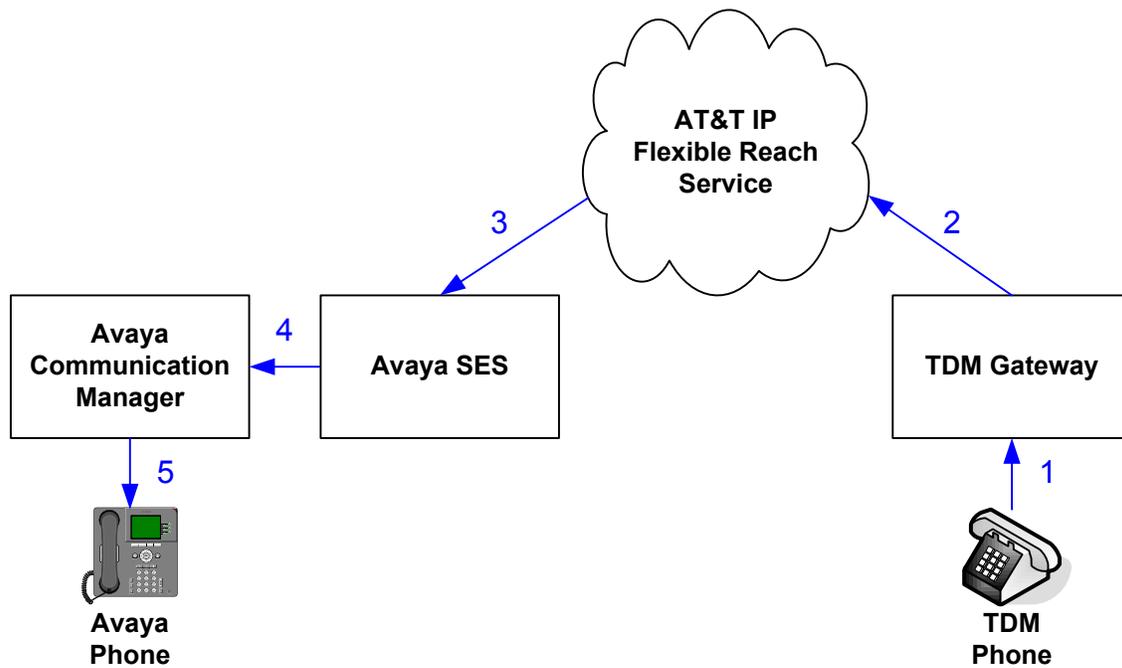


Figure 5: Inbound Call from TDM Gateway Phone Scenario

3. Equipment and Software Validated

The following equipment and software was used for the sample configuration described in these Application Notes.

Component	Version
Avaya S8720 Server	Avaya Communication Manager 5.1.2 with Service Pack 1 (R015x.01.2.416.4 with update 17067)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW15 FW045
TN799DP Control-LAN (C-LAN)	HW01 FW031
TN2602AP IP Media Resource 320 (MedPro)	HW02 FW047
TN2224CP Digital Line	HW08 FW015
TN793CP Analog Line	HW05 FW010
Avaya S8500B Server	Avaya SIP Enablement Services 5.1.2 with Service Pack 1 (SES- 5.1.2.0-416.4b with update SES- 01.2.416.4-SP1)
Avaya 9620 IP Telephone	Avaya one-X™ Deskphone Edition H.323 Release 3.0
Avaya 9630 IP Telephone	Avaya one-X™ Deskphone Edition SIP Release 2.0.5
Avaya 4610SW SIP Telephone	2.2.2
Avaya 4621SW IP Telephone	2.9.1
Avaya 6416D+M Digital Telephone	-
Avaya one-X™ Communicator	1.0 Service Pack 1 (1.0.0.77)
AT&T IP Flexible Reach Service	VNI 14

Table 2: Equipment and Software Versions

NOTE: The solution integration validated in these Application Notes (Customer Configuration Guide) should be considered valid for deployment with Avaya Aura™ Communication Manager release 5.2 and Avaya Aura™ SIP Enablement Services release 5.2. Avaya agrees to provide service and support for the integration of Avaya Aura™ Communication Manager release 5.2 and Avaya Aura™ SIP Enablement Services release 5.2 with the AT&T IP Flexible Reach service accessed through AT&T VPN transport service connections service offers in compliance with existing support agreements for Avaya Communication Manager release 5.1.2 and Avaya SIP Enablement Services release 5.1.2 and in conformance with the integration guidelines as specified in the body of this document.

4. Avaya Communication Manager

This section describes the administration steps for Avaya Communication Manager in support of SIP trunking integration with the AT&T IP Flexible Reach service. The steps are performed from the Avaya Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Avaya Communication Manager administration, including stations, C-LAN and Media Processor boards, SIP phone signaling/trunk group(s), etc., has already been performed. Consult [1], [2], and [3] for further details if necessary.

4.1. System Parameters

This section reviews the Avaya Communication Manager licenses and features that are required for the sample configuration described in these Application Notes. For required licenses that are not enabled in the steps that follow, contact an authorized Avaya account representative to obtain the licenses.

1. Enter the **display system-parameters customer-options** command. On Page 2 of the **system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

Display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:	8000	0		
Maximum Concurrently Registered IP Stations:	12000	5		
Maximum Administered Remote Office Trunks:	0	0		
Maximum Concurrently Registered Remote Office Stations:	0	0		
Maximum Concurrently Registered IP eCons:	0	0		
Max Concur Registered Unauthenticated H.323 Stations:	0	0		
Maximum Video Capable H.323 Stations:	0	0		
Maximum Video Capable IP Softphones:	0	0		
Maximum Administered SIP Trunks:	5000	150		
Maximum Administered Ad-hoc Video Conferencing Ports:	0	0		
Maximum Number of DS1 Boards with Echo Cancellation:	0	0		
Maximum TN2501 VAL Boards:	10	1		
Maximum Media Gateway VAL Sources:	0	0		
Maximum TN2602 Boards with 80 VoIP Channels:	128	0		
Maximum TN2602 Boards with 320 VoIP Channels:	128	2		
Maximum Number of Expanded Meet-me Conference Ports:	0	0		

Figure 6: System-Parameters Customer-Options Form – Page 2

2. On Pages 3 and 4 of the **system-parameters customer-options** form, verify that the bolded fields in the following screenshots are set to “y”.

```

display system-parameters customer-options                               Page 3 of 11
                                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? Y
  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
Async. Transfer Mode (ATM) Trunking? N                               Digital Loss Plan Modification? N
  ATM WAN Spare Processor? N                                       DS1 MSP? N
                                ATMS? N                               DS1 Echo Cancellation? N
  Attendant Vectoring? N

```

Figure 7: System-Parameters Customer-Options Form – Page 3

```

display system-parameters customer-options                               Page 4 of 11
                                OPTIONAL FEATURES

Emergency Access to Attendant? Y                                    IP Stations? Y
  Enable 'dadmin' Login? Y
  Enhanced Conferencing? Y                                          ISDN Feature Plus? N
  Enhanced EC500? Y                                                ISDN/SIP Network Call Redirection? N
Enterprise Survivable Server? N                                     ISDN-BRI Trunks? Y
  Enterprise Wide Licensing? N                                       ISDN-PRI? Y
  ESS Administration? Y                                              Local Survivable Processor? N
  Extended Cvg/Fwd Admin? Y                                          Malicious Call Trace? N
  External Device Alarm Admin? N                                      Media Encryption Over IP? N
Five Port Networks Max Per MCC? N                                  Mode Code for Centralized Voice Mail? N
  Flexible Billing? N
Forced Entry of Account Codes? N                                    Multifrequency Signaling? Y
  Global Call Classification? N                                        Multimedia Call Handling (Basic)? N
  Hospitality (Basic)? Y                                             Multimedia Call Handling (Enhanced)? N
Hospitality (G3V3 Enhancements)? N                                Multimedia IP SIP Trunking? N
                                IP Trunks? Y
IP Attendant Consoles? N

```

Figure 8: System-Parameters Customer-Options Form – Page 4

4.2. Dial Plan and Feature Access Codes

This section briefly describes the dial plan requirements and feature access codes for the sample configuration described in these Application Notes.

1. Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings administered in **Figure 9**:
 - 3-digit dial access codes (indicated with a **Call Type** of “**dac**”) beginning with the digit “**1**” – Trunk Access Codes (TACs) defined for trunk groups in this sample configuration conform to this format.
 - 5-digit extensions with a **Call Type** of “**ext**” beginning with the digits “**26**” – local extensions for Avaya Communication Manager stations, voicemail access, meet-me conferences, etc. in this sample configuration conform to this format.
 - Single-digit (“**9**”) feature access code (indicated with a **Call Type** of “**fac**”) – This dialed string will be interpreted as a Feature Access Codes (FAC). In this sample configuration, “**9**” is used as the user-dialed prefix for outbound calls to the PSTN.

Change dialplan analysis			DIAL PLAN ANALYSIS TABLE							Page	1 of	12
			Location: all				Percent Full:			1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type				
1	3	dac										
24	5	udp										
26	5	ext										
8	5	udp										
9	1	fac										

Figure 9: Dialplan Analysis Form

2. [Optional Step]. If extension dialing for calling the TDM gateway sites is desired, then provision entries in the dial plan accordingly. Otherwise, skip to Step 3. For example, in **Figure 10**, 5-digit extensions with a **Call Type** of “**udp**” beginning with the digits “**24**” and “**82**” are administered to allow Avaya Communication Manager users to simply dial the last five digits of the phone numbers assigned to the TDM gateway sites.

Change dialplan analysis			DIAL PLAN ANALYSIS TABLE							Page	1 of	12
			Location: all				Percent Full:			1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type				
1	3	dac										
24	5	udp										
26	5	ext										
82	5	udp										
9	1	fac										

Figure 10: Dialplan Analysis Form – With Entries for Extension Dialing to TDM Gateway Sites

Enter the **change uniform-dialplan d** command, where **d** is any digit, and provision an entry for each TDM gateway site phone number range as follows:

- **Matching Pattern** and **Len** – enter the leading digit(s) and length, respectively, of the last few digits of the TDM gateway site phone number range. For example, if the TDM gateway site phone number range is 908-542-4xxx, the **Matching Pattern** and **Len** can be “24” and “5”, respectively, as shown in **Figure 11**.
- **Del** – set to “0”.
- **Insert Digits** – enter “1” (if required by the AT&T IP Flexible Reach service) followed by the leading digits of the TDM gateway site phone number range up to, but not including, the **Matching Pattern** value above.
- **Net** – set to “aar”.

Change uniform-dialplan 0						Page	1 of	2
UNIFORM DIAL PLAN TABLE						Percent Full: 0		
Matching Pattern	Len	Del	Insert Digits	Net	Node Conv Num			
24	5	0	190854	aar	n			
82	5	0	120139	aar	n			

Figure 11: Uniform-Dialplan Form

Note: The administration shown in this step for 5-digit extensions beginning with the digits “82” will not be allowed if the single-digit “8” is already been administered as a feature access code in the dialplan analysis form, particularly when “8” is used as a user-dialed prefix for Auto Alternate Route (AAR) calls. In that case, use the **aar digit-conversion** form instead of the dialplan analysis and uniform-dialplan forms shown in this step to convert “82xxx” into “12013982xxx” and invoke AAR routing.

Change aar digit-conversion 0								Page	1 of	2
AAR DIGIT CONVERSION TABLE								Percent Full: 0		
Location: all										
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI	Req		
0	1	28	0		ars	y		n		
1	4	28	0		ars	y		n		
2xxx	4	4	0	1201398	aar	y		n		
x11	3	3	0		ars	y		n		

Figure 12: AAR Digit-Conversion Form

3. Enter the **change feature-access-codes** command. On Page 1 of the **feature-access-codes** form, provision an access code for **Auto Route Selection (ARS) – Access Code 1** that is valid under the administered dial plan in Step 1. In this sample configuration, ARS is used for routing calls to the PSTN, and the access code (“9” in **Figure 13**) entered here is used as the user-dialed prefix for outbound PSTN calls. See Section 4.4.1 for further details.

Note: If extension dialing for calling the TDM gateway sites was NOT administered in Step 2 , then ARS will also be used for routing calls to the TDM gateway sites and the ARS access code will also be used as the user-dialed prefix for outbound calls to the TDM gateway sites. See Section 4.4.2 for further details.

```

Change feature-access-codes                                     Page 1 of 9
                                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:
Answer Back Access Code:
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code:
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
Automatic Callback Activation:                        Deactivation:
  
```

Figure 13: Feature-Access-Codes Form

4.3. IP Network Parameters

These Application Notes assume that the appropriate IP network regions and IP codec sets have already been administered to support internal calls, i.e., calls within the Avaya site. For simplicity in this sample configuration, all Avaya Communication Manager elements, e.g., stations, C-LAN and MedPro boards, etc., within the Avaya site are assigned to a single IP network region and all internal calls use a single IP codec set. This section describes the steps for administering additional IP network regions to represent the PSTN and the TDM gateway sites, and another IP codec set for external calls, i.e., calls between the Avaya site and the PSTN and the TDM gateway sites.

1. Enter the **change ip-codec-set ci** command, where **ci** is the number of an IP codec set used only for internal calls. On Page 1 of the **ip-codec-set** form, ensure that “**G.729B**” and “**G.729A**” are included in the codec list as shown in **Figure 14**. Note that the **Frames Per Pkt** and **Packet Size(ms)** values for **G.729B** and **G.729A** are set according to the requirements of the AT&T IP Flexible Reach service.

```

Change ip-codec-set 1                                     Page 1 of 2
                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size (ms)
1: G.711MU      n           2          20
2: G.729B      n           3          30
3: G.729A      n           3          30
  
```

Figure 14: IP-Codec-Set Form for Internal Calls – Page 1

On Page 2 of the **ip-codec-set** form, set **FAX Mode** to “**t.38-standard**”.

```

Change ip-codec-set 1                                     Page 2 of 2
                IP Codec Set
                Allow Direct-IP Multimedia? N

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

Figure 15: IP-Codec-Set Form for Internal Calls – Page 2

Repeat this step as necessary for each IP codec set used only for internal calls.

2. Enter the **change ip-codec-set ce** command, where **ce** is the number of an unused IP codec set. This IP codec set will be used for external calls. On Page 1 of the **ip-codec-set** form, provision the codecs in the order shown in **Figure 16**. Note that the **Frames Per Pkt** and **Packet Size(ms)** values for **G.729B** and **G.729A** are set according to the requirements of the AT&T IP Flexible Reach service.

```

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                3          30
2: G.729A      n                3          30
3: G.711MU     n                2          20
    
```

Figure 16: IP-Codec-Set Form for External Calls – Page 1

On Page 2 of the **ip-codec-set** form, set **FAX Mode** to “**t.38-standard**”.

```

Change ip-codec-set 2                                     Page 2 of 2
                                                         IP Codec Set
                                                         Allow Direct-IP Multimedia? N

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

```

Figure 17: IP-Codec-Set Form for External Calls – Page 2

3. Enter the **change ip-network-region nrp**, where **nrp** is the number of an unused IP network region. This IP network region will be used to represent the PSTN. On Page 1 of the **ip-network-region** form, set the **UDP Port Min** and **UDP Port Max** to “**16384**” and “**32767**” (this port range is an AT&T IP Flexible Reach service requirement).

```

Change ip-network-region 14                             Page 1 of 19
                                                         IP NETWORK REGION
Region: 14
Location:          Authoritative Domain:
Name: AVPN PSTN
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 1          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 16384      IP Audio Hairpinning? N
UDP Port Max: 32767
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 18: IP-Network-Region Form for the Network Region Representing the PSTN

- Repeat Step 3 to administer another IP network region to represent the TDM gateway sites.

```

Change ip-network-region 13                                     Page 1 of 19
                                                                IP NETWORK REGION
Region: 13
Location:                Authoritative Domain:
Name: AVPN TDM GW Sites
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
Codecs Set: 1                Inter-region IP-IP Direct Audio: yes
                               IP Audio Hairpinning? N
UDP Port Min: 16384
UDP Port Max: 32767
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 19: IP-Network-Region Form for the Network Region Representing the TDM Gateway Sites

5. Enter the **change ip-network-region nrl**, where **nrl** is the number of an IP network region administered for local Avaya Communication Manager elements within the Avaya site. On Page 1 of the **ip-network-region** form, set the **UDP Port Min** and **UDP Port Max** to “**16384**” and “**32767**”.

Change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: Authoritative Domain: main.customera.com		
Name: Local		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 16384		IP Audio Hairpinning? Y
UDP Port Max: 32767		
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? Y
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46		Use Default Server Parameters? Y
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? Y		RSVP Enabled? N
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Figure 20: IP-Network-Region Form for a Network Region Administered for Local Avaya Communication Manager Elements – Page 1

On Page 3 of the **ip-network-region** form, for each IP network region pair consisting of this IP network region as the **src rgn** and the IP network region assigned to the PSTN or TDM gateway sites as the **dst rgn**, provision the following:

- **codec set** – Set to the codec set administered in Step 2.
- **direct WAN** – Set to “y”.
- **WAN-BW-limits** – Set to the maximum number of calls or bandwidth allowed between the two IP network regions. The setting shown in **Figure 21** was used for testing purposes only.

Inter Network Region Connection Management

src rgn	dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC IGAR AGL
1	1	1					all
1	2						
1	3						
1	4						
1	5						
1	6						
1	7						
1	8						
1	9						
1	10						
1	11						
1	12						
1	13	2	y	NoLimit			n all
1	14	2	y	NoLimit			n all
1	15						

Figure 21: IP-Network-Region Form for an IP Network Region Administered for Local Avaya Communication Manager Elements – Page 3

Repeat this step as necessary for other IP network regions administered for local Avaya Communication Manager elements.

- Enter the **list node-names** command, and note the node names and IP addresses of the Avaya SES server (combined Home/Edge server or Home server in separate SES Home/Edge configurations), as well as those of two C-LAN boards that are assigned to one of the IP network regions administered for local Avaya Communication Manager elements within the Avaya site as described in Step 5. These C-LAN boards will be used in Section 4.4.1 Step 1, Section 4.4.2 Step 1, Section 4.5.1 Step 3, and Section 5.3 Steps 1 – 2 for SIP trunking.

```
List node-names
```

NODE NAMES		
Type	Name	IP Address
IP	MainCLAN1A02	192.168.67.13
IP	MainCLAN1A03	192.168.67.14
IP	MainMP1A04	192.168.67.15
IP	MainMP1A05	192.168.67.16
IP	MainSES	192.168.67.30
IP	MainVAL1A06	192.168.67.17
IP	default	0.0.0.0
IP	procr	192.168.67.11

Figure 22: List Node-Names Form

4.4. Outbound Calls

In this sample configuration, since the AT&T IP Flexible Reach service required sites to send 11-digit called party numbers for outbound calls, the administration steps that follow in this section reflect that requirement. In actual deployment, customers and AT&T must agree on the called party number length to be sent by the customer sites.

4.4.1. Outbound PSTN Calls

This section describes the steps for administering the routing of outbound calls to the PSTN.

1. Enter the **add signaling-group spo** command, where **spo** is the number of an unused signaling group, and provision the following:
 - **Group Type** – Set to “**sip**”.
 - **Transport Method** – Set to “**tls**”. Note that this is only the transport protocol used between Avaya Communication Manager and Avaya SES. The transport protocol used between Avaya SES and the AT&T IP Flexible Reach service is UDP.
 - **Near-end Node Name** – Set to the node name of the first C-LAN board noted in Section 4.3 Step 6.
 - **Far-end Node Name** – Set to the node name of the Avaya SES server noted in Section 4.3 Step 6.
 - **Near-end Listen Port** and **Far-end Listen Port** – set to “**5061**”.
 - **Far-end Network Region** – Set to the IP network region administered in Section 4.3 Step 3 to represent the PSTN.
 - **Far-end Domain** – Enter the IP address of the AT&T IP Flexible Reach service Border Element.
 - **DTMF over IP** – Set to “**rtp-payload**” to enable Avaya Communication Manager to use DTMF according to RFC 2833.
 - **Direct IP-IP Audio Connections** – Set to “**y**”, indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible.

```
Add signaling-group 14                                     Page 1 of 1
Group Number: 14          Group Type: sip
                          Transport Method: tls
Near-end Node Name: MainCLAN1A02      Far-end Node Name: MainSES
Near-end Listen Port: 5061            Far-end Listen Port: 5061
Far-end Network Region: 14
Far-end Domain: 10.94.2.12
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   Alternate Route Timer(sec): 6
```

Figure 23: Signaling-Group Form for Outbound PSTN Calls

2. Enter the **add trunk-group tp** command, where **tp** is the number of an unused trunk group. On Page 1 of the **trunk-group** form, provision the following:
 - **Group Type** – Set to “**sip**”.
 - **Group Name** – Enter a descriptive name.
 - **TAC** – Enter a trunk access code that is consistent with the dial plan.
 - **Direction** – set to “**two-way**” so that this trunk group will be used for both outbound and inbound calls with the PSTN.
 - **Service Type** – Set to “**public-ntwrk**”.
 - **Signaling Group** – Set to the number of the signaling group administered in Step 1.
 - **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group.

```

Add trunk-group 14                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 14                                     Group Type: sip                                     CDR Reports: y
  Group Name: ATT IPFRAVPN PSTN                       COR: 1                                     TN: 1                                     TAC: 114
  Direction: two-way                                   Outgoing Display? N
Dial Access? N
Queue Length: 0
Service Type: public-ntwrk

                                     Signaling Group: 14
                                     Number of Members: 20
  
```

Figure 24: Trunk-Group Form for Outbound PSTN Calls – Page 1

3. On Page 4 of the **trunk-group** form, set “**Telephone Event Payload Type**” to the RTP payload type required by the AT&T IP Flexible Reach service. Contact AT&T or examine a SIP trace of an inbound call from the AT&T IP Flexible Reach service to determine this value.

```

Add trunk-group 14                                     Page 4 of 21
                                     PROTOCOL VARIATIONS

                                     Mark Users as Phone? N
                                     Prepend '+' to Calling Number? N
                                     Send Transferring Party Information? N

                                     Telephone Event Payload Type: 100
  
```

Figure 25: Trunk-Group Form for Outbound PSTN Calls – Page 4

4. Repeat Steps 1 – 3 for any additional AT&T IP Flexible Reach service Border Elements.
5. Enter the **change ars analysis d** command, where **d** is any digit(s). In the **ars analysis** form, provision an entry for a PSTN destination as follows:

- **Dialed String** – Enter “1” (the country code in this sample configuration) followed by enough leading digits to uniquely identify a PSTN destination number range.
- **Total Min and Max** – Enter “11”.
- **Route Pattern** – Enter the number of an unused route pattern. The route pattern will specify the trunk group(s) to be used for outbound calls matching this entry.
- **Call Type** – Enter “**hnpa**” if the PSTN destination number range is in the same “home” area code as the Avaya site, and “**fnpa**” otherwise.

In addition, provision another entry to cover the case when Avaya Communication Manager users dial PSTN destinations in the same “home” area code of the Avaya site without the leading “1”. For this entry, set **Dialed String** to the leading digits of those PSTN destinations, e.g., the “home” area code, **Total Min and Max** to “10”, **Route Pattern** to the same route pattern as above, and **Call Type** to “**hnpa**”.

Change ars analysis 1732						Page 2 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 2	
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI	Reqd
1723	11	11	14	hnpa		n	
1732	11	11	14	fnpa		n	
723	10	10	14	hnpa		n	

Figure 26: ARS Analysis Form

In **Figure 26**, entries are shown for outbound calls to **723-xxx-xxxx**, **1-723-xxx-xxxx**, and **1-732-xxx-xxxx**. Typical deployments generally require additional entries, or the use of less exact or wildcard matching strings, to cover all permitted local, long distance, international, operator, N11 service, and other PSTN destination numbers, but that is beyond the scope of these Application Notes. Ensure that there are entries to cover all permitted PSTN destination numbers. Consult [1] and [2] for further information on ARS administration.

6. Enter the **change route-pattern rp** command, where **rp** is the route pattern entered in Step 5. Provision an entry as follows:
 - **Pattern Name** – Enter a descriptive name.
 - **Secure SIP** – Set to “n”.
 - **Grp No** – Enter the number of a trunk group administered in Steps 2 – 3.
 - **FRL** – Enter the minimum Facility Restriction Level necessary to use this trunk group, with 0 being the least restrictive.
 - **Pfx Mrk** – Enter “1” so that for outbound 11-digit called party numbers that begin with “1”, the prefix “1” is not removed.
 - **NPA** – [Optional] Enter the “home” area code of the Avaya site so that (in conjunction with Pfx Mrk being set to “1”) a “1” is prefixed to outbound 10-digit called party numbers in the same “home” area code as the Avaya site.

Change route-pattern 14											Page	1 of	3
Pattern Number: 14											Pattern Name: AVPN>PSTN		
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:	14	0	723	1							n	user	
2:											n	user	
3:											n	user	
4:											n	user	
5:											n	user	
6:											n	user	
	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR		
	0	1 2 M 4 W		Request					Dgts	Format			
									Subaddress				
1:	y	y y y y y	n	n			rest					none	
2:	y	y y y y y	n	n			rest					none	
3:	y	y y y y y	n	n			rest					none	
4:	y	y y y y y	n	n			rest					none	
5:	y	y y y y y	n	n			rest					none	
6:	y	y y y y y	n	n			rest					none	

Figure 27: Route-Pattern Form for Outbound PSTN Calls

Provision additional entries as necessary for any additional trunks groups administered in Step 4.

4.4.2. Outbound Calls To TDM Gateway Sites

This section describes the steps for administering the routing of outbound calls to the TDM gateway sites.

1. Enter the **add signaling-group sg** command, where **sg** is the number of an unused signaling group, and provision the following:
 - **Group Type** – Set to “sip”.
 - **Transport Method** – Set to “tls”. Note that this is only the transport protocol used between Avaya Communication Manager and Avaya SES. The transport protocol used between Avaya SES and the AT&T IP Flexible Reach service is UDP.
 - **Near-end Node Name** – Set to the node name of the second C-LAN board noted in Section 4.3 Step 6.
 - **Far-end Node Name** – Set to the node name of the Avaya SES server noted in Section 4.3 Step 6.
 - **Near-end Listen Port** and **Far-end Listen Port** – set to “5061”.
 - **Far-end Network Region** – Set to the IP network region administered in Section 4.3 Step 4 to represent the TDM gateway sites.
 - **Far-end Domain** – Enter the IP address of the AT&T IP Flexible Reach service Border Element.
 - **DTMF over IP** – Set to “rtp-payload” to enable Avaya Communication Manager to use DTMF according to RFC 2833.

- **Direct IP-IP Audio Connections** – Set to “y”, indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible.

```

Add signaling-group 13                                     Page 1 of 1

Group Number: 13                Group Type: sip
                                Transport Method: tls

Near-end Node Name: MainCLAN1A03    Far-end Node Name: MainSES
Near-end Listen Port: 5061          Far-end Listen Port: 5061
Far-end Network Region: 13

Far-end Domain: 10.94.2.12

                                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    Alternate Route Timer(sec): 6

```

Figure 28: Signaling-Group Form for Calls with TDM Gateway Sites

2. Enter the **add trunk-group tg** command, where **tg** is the number of an unused trunk group. On Page 1 of the **trunk-group** form, provision the following:
 - **Group Type** – set to “sip”.
 - **Group Name** – Enter a descriptive name.
 - **TAC** – Enter a trunk access code that is consistent with the dial plan.
 - **Direction** – set to “two-way” so that this trunk group will be used for both outbound and inbound calls with the TDM gateway sites.
 - **Service Type** – set to “public-ntwrk”.
 - **Signaling Group** – set to the number of the signaling group administered in Step 1.
 - **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group.

```

Add trunk-group 13                                     Page 1 of 21

                                TRUNK GROUP

Group Number: 13                Group Type: sip                CDR Reports: y
Group Name: ATT IPFRAVPN TDMGW Sites    COR: 1                TN: 1                TAC: 113
Direction: two-way                Outgoing Display? N

Dial Access? N

Queue Length: 0

Service Type: public-ntwrk                Auth Code? N

                                Signaling Group: 13
                                Number of Members: 20

```

Figure 29: Trunk-Group Form for Calls with TDM Gateway Sites – Page 1

- On Page 4 of the **trunk-group** form, set “**Telephone Event Payload Type**” to the RTP payload type required by the AT&T IP Flexible Reach service. Contact AT&T or examine a SIP trace of an inbound call from the AT&T IP Flexible Reach service to determine this value.

Add trunk-group 13	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? N	
Prepend '+' to Calling Number? N	
Send Transferring Party Information? N	
Telephone Event Payload Type: 100	

Figure 30: Trunk-Group Form for Calls with TDM Gateway Sites – Page 4

- Repeat Steps 1 – 3 for any additional AT&T IP Flexible Reach service Border Elements.
- If extension dialing for calling the TDM gateway sites was administered in Section 4.2 Step 2, then enter the **change aar-analysis a** command, where **a** is any digit, and provision an entry for each TDM gateway site phone number range as follows:
 - Dialed String** – enter “1”, followed by the leading digit(s) of the TDM gateway site phone number range.
 - Total Min and Max** – set to “11”.
 - Route Pattern** – enter the number of an unused route pattern. The route pattern will specify the trunk group(s) to be used for outbound calls matching this entry.
 - Call Type** – set to “aar”.

Change aar analysis 0						Page 1 of 2
AAR DIGIT ANALYSIS TABLE						
Location: all						Percent Full: 1
Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Req'd
12013982	11	11	13	aar		n
19085424	11	11	13	aar		n

Figure 31: AAR Analysis Form

If extension dialing for calling the TDM gateway sites was NOT administered in Section 4.2 Step 2, then enter the **change ars analysis d** command, where **d** is any digit(s), and provision entries for the TDM gateway site phone numbers in the same manner described in Section 4.4.1 Step 5 (remember to use a different route pattern than the one used in Section 4.4.1 Step 5).

- Enter the **change route-pattern rg** command, **rg** is the route pattern entered in Step 5. Provision an entry as follows:
 - Pattern Name** – Enter a descriptive name.
 - Secure SIP** – Set to “n”.

- **Grp No** – Enter the number of a trunk group administered in Steps 2 – 3.
- **FRL** – Enter the minimum Facility Restriction Level necessary to use this trunk group, with 0 being the least restrictive.
- **Pfx Mrk** – Enter “1” so that for outbound 11-digit called party numbers that begin with “1”, the prefix “1” is not removed.

Change route-pattern 13													Page 1 of 3		
Pattern Number: 13													Pattern Name: AVPN>TDMSites		
SCCAN? N													Secure SIP? N		
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits						DCS/ QSIG	IXC	
								Dgts						Intw	
1:	13	0	1										n	user	
2:													n	user	
3:													n	user	
4:													n	user	
5:													n	user	
6:													n	user	
BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No. Dgts	Numbering	LAR					
0	1	2	M	4	W	Request		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	

Figure 32: Route-Pattern Form for Outbound Calls to TDM Gateway Sites

Provision additional entries as necessary for any additional trunks groups administered in Step 4.

4.4.3. Calling Party Number

Enter the **change public-unknown-numbering 0** command to specify the calling party numbers sent on outbound calls. In the **public-unknown-numbering** form, for each local extension range assigned to Avaya Communication Manager phones, provision one entry for outbound PSTN calls and another entry for outbound calls to the TDM gateway sites as follows:

- **Ext Len** – Enter the total number of digits in the local extension range.
- **Ext Code** – Enter enough leading digits to identify the local extension range.
- **Trk Grp(s)** – For outbound PSTN calls, enter the number of the trunk group administered in Section 4.4.1 Steps 2 – 3. For outbound calls to the TDM gateway sites, enter the number of the trunk group administered in Section 4.4.2 Steps 2 – 3.
- **CPN Prefix** – If necessary, enter enough prefix digits to form the desired calling party number.
- **CPN Len** – Enter the total length of the calling party number to be sent.

In **Figure 33**, for outbound calls placed by Avaya Communication Manager phones with extensions 26xxx, 11-digit calling party numbers 17231126xxx are sent for outbound PSTN calls, whereas 5-digit calling party numbers 26xxx (i.e., the calling party's extension is sent without modification) are sent for outbound calls to the TDM gateway sites¹.

Provision as many entries as necessary to cover all local extension ranges assigned to Avaya Communication Manager phones.

Change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp (s)	CPN Prefix	Total CPN Len	
5	26	1		5	Total Administered: 1 Maximum Entries: 9999
5	26	13		5	
5	26	14	172311	11	

Figure 33: Public-Unknown-Numbering Form

4.5. Inbound Calls

In this sample configuration, since the AT&T IP Flexible Reach service sends 10-digit and 4-digit called party numbers on inbound calls to the sites, the administration steps that follow in this section reflect that requirement. In actual deployment, customers and AT&T must agree on the called party number length to be sent to customer sites.

4.5.1. Inbound PSTN Calls

This section describes the steps for administering the routing of inbound calls from the PSTN.

1. Enter the **change inc-call-handling-trmt trunk-group tp** command, where **tp** is the number of the trunk group administered in Section 4.4.1 Steps 2 – 3. In the **inc-call-handling-trmt trunk-group** form, provision an entry for a DID number / number range as follows:
 - **Called Len** – Enter the total number of digits in the DID number / number range.
 - **Called Number** – Enter enough leading digits to uniquely match the DID number / number range.
 - **Del and Insert** – If necessary, enter the number of leading digits that need to be deleted from the DID number / number range, and the specific leading digits that need to be prefixed to the DID number / number range (after any deletion is performed), respectively, in order to match a local Avaya Communication Manager extension / extension range.

In this sample configuration, the AT&T IP Flexible Reach service sends 10-digit called party numbers in the range 7231126xxx on inbound DID calls. Thus the entry in **Figure**

¹ In determining what calling party number length to send to the TDM gateway sites, consider what numbers users in the TDM gateway sites expect to see on incoming calls from the Avaya site, what those users normally dial to call the Avaya sites, and whether those users are able to call numbers stored their phone logs.

34 matches the called party number range 7231126xxx and deletes the leading 5 digits to match the local Avaya Communication Manager extension range 26xxx.

Provision as many entries as necessary to cover all expected DID numbers / number ranges.

Change inc-call-handling-trmt trunk-group 14				Page	1 of	30
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Called Len	Called Number	Del	Insert		
public-ntwrk	10	7231126	5			

Figure 34: Inc-Call-Handling-Trmt Trunk-Group Form for Inbound PSTN Calls

2. Repeat Step 1 for each of the PSTN trunk groups administered in Section 4.4.1 Step 4.
3. If the domain part of the SIP INVITE FROM header of inbound DID calls from the AT&T IP Flexible Reach service contains only the IP address of the AT&T IP Flexible Reach service Border Element, then skip the remainder of this section. Otherwise, enter the **add signaling-group spi** command, where **spi** is the number of an unused signaling group. Administer the signaling group in the same manner as the signaling group administered in Section 4.4.1 Step 1 for outbound calls to the PSTN, with the following exception:
 - **Far-end Domain** – Leave blank to allow this SIP signaling group to handle inbound PSTN calls from any domain.

Add signaling-group 2		Page	1 of	1
Group Number: 2	Group Type: sip			
	Transport Method: tls			
Near-end Node Name: MainCLAN1A02	Far-end Node Name: MainSES			
Near-end Listen Port: 5061	Far-end Listen Port: 5061			
Far-end Domain:	Far-end Network Region: 14			
	Bypass If IP Threshold Exceeded? N			
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? Y			
Enable Layer 3 Test? N	IP Audio Hairpinning? N			
Session Establishment Timer(min): 3	Alternate Route Timer(sec): 6			

Figure 35: Signaling-Group Form for Inbound PSTN Calls

4. Enter the **add trunk-group tpi** command, where **tpi** is the number of an unused trunk group. Administer the trunk group in the same manner as the trunk group administered in Section 4.4.1 Steps 2 – 3 for outbound calls to the PSTN, with the following exceptions:
 - **Direction** – Set to “incoming”.

- **Signaling Group** – Set to the number of the signaling group administered in Step 3.

```

Add trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 2                                     Group Type: sip           CDR Reports: y
  Group Name: ATT IPFRAVPN PSTNin                   COR: 1                 TN: 1           TAC: 102
  Direction: incoming                               Outgoing Display? N
  Dial Access? N
  Queue Length: 0
  Service Type: public-ntwrk

                                     Signaling Group: 2
                                     Number of Members: 20

```

Figure 36: Trunk-Group Form for Inbound PSTN Calls – Page 1

```

add trunk-group 2                                     Page 4 of 21
                                     PROTOCOL VARIATIONS

                                     Mark Users as Phone? N
                                     Prepend '+' to Calling Number? N
                                     Send Transferring Party Information? N

                                     Telephone Event Payload Type: 100

```

Figure 37: Trunk-Group Form for Inbound PSTN Calls – Page 4

- Repeat Step 1 for the trunk group administered in Step 4.

4.5.2. Inbound Calls From TDM Gateway Sites

Depending on the customer implementation, the called party numbers of inbound calls from the TDM gateway sites (arriving by way of the AT&T IP Flexible Reach service) may need to be modified in order to match the local Avaya Communication Manager extensions administered in the Avaya site. Enter the **change inc-call-handling-trmt trunk-group tg** command, where **tg** is the number of the trunk group administered in Section 4.4.2 Steps 2 – 3. In the **inc-call-handling-trmt trunk-group** form, provision an entry for a called party number / number range as follows:

- **Called Len** – Enter the total number of digits in the called party number / number range.
- **Called Number** – Enter enough leading digits to uniquely match the called party number / number range.
- **Del and Insert** – If necessary, enter the number of leading digits that need to be deleted from the called party number / number range, and the specific leading digits that need to be prefixed to the called party number / number range (after any deletion is performed), respectively, in order to match a local Avaya Communication Manager extension / extension range.

In this sample configuration, the TDM gateway sites send 4-digit called party numbers in the range 6xxx. Thus the entry in **Figure 38** matches the called party number range 6xxx and prefixes a leading “2” to such called party numbers to match the local Avaya Communication Manager extension range 26xxx.

Provision as many entries as necessary to cover all expected called party numbers /number ranges. Repeat the above for all trunk groups administered for any additional AT&T IP Flexible Reach service Border Elements (see Section 4.4.2 Step 4).

Change inc-call-handling-trmt trunk-group 13				Page 1 of 30
INCOMING CALL HANDLING TREATMENT				
Service/ Feature	Called Len	Called Number	Del	Insert
public-ntwrk	4 6			2

Figure 38: Inc-Call-Handling-Trmt Trunk-Group Form for Inbound Calls from TDM Gateway Sites

4.5.3. Connected Party Number

The connected party numbers sent on inbound calls can be specified in the **public-unknown-numbering** form. For inbound calls from the PSTN and TDM gateway sites, since the same trunk groups are used for both outbound and inbound calls, the administration of calling party numbers in Section 4.4.3 is also valid for connected party numbers.

If the domain part of the SIP INVITE FROM header of inbound calls from the AT&T IP Flexible Reach service contains only the IP address of the AT&T IP Flexible Reach service Border Element, i.e., Section 4.5.1 Steps 3 – 5 were skipped, then skip the remainder of this section. Otherwise, provision an entry in the **public-unknown-numbering** form as follows:

- **Ext Len** – Enter the total number of digits in the local extension range.
- **Ext Code** – Enter enough leading digits to identify the local extension range.
- **Trk Grp(s)** – Enter the number of the trunk group administered in Section 4.5.1 Step 4.
- **CPN Prefix** – If necessary, enter enough prefix digits to form the desired connected party number.
- **CPN Len** – Enter the total length of the connected party number to be sent.

Provision as many entries as necessary to cover all local extension ranges assigned to Avaya Communication Manager phones.

Change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp (s)	CPN Prefix	Total CPN Len	
5	26	1		5	Total Administered: 3
5	26	13		5	Maximum Entries: 9999
5	26	14	172311	11	
5	26	2	172311	11	

Figure 39: Public-Unknown-Numbering Form

4.6. SIP Phones

Notes:

1. A separate signaling group and trunk group needs to be administered for SIP phones, but that is beyond the scope of these Application Notes. Consult [3] and [5] for further details.
2. The DTMF_PAYLOAD_TYPE parameter in the “46xxsettings.txt” configuration file that Avaya SIP phones download (from a file server) during startup must be configured to match the RTP payload type required by the AT&T IP Flexible Reach service. Contact AT&T or examine a SIP trace of an inbound call from the AT&T IP Flexible Reach service to determine this value. See [5] for further details.
3. The rest of this section addresses a known issue in Avaya Communication Manager Release 5.1.2 Service Pack 1 involving Avaya SIP phones and Direct IP-IP media (a.k.a. “shuffling”). The rest of this section can be skipped when the issue is resolved.

Set **Direct-IP-IP Audio Connections** to “n” on the signaling group administered for SIP phones.

```
Change signaling-group 1                                     Page 1 of 1
Group Number: 1                Group Type: sip
                               Transport Method: tls
Near-end Node Name: MainCLAN1A02      Far-end Node Name: MainSES
Near-end Listen Port: 5061            Far-end Listen Port: 5061
                                       Far-end Network Region: 1
Far-end Domain: main.customera.com
                                       Bypass If IP Threshold Exceeded? N
DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? N
                                       IP Audio Hairpinning? N
Enable Layer 3 Test? N
Session Establishment Timer(min): 3    Alternate Route Timer(sec): 6
```

Figure 40: Signaling-Group Form for SIP Phones

```
change trunk-group 1                                       Page 1 of 21
TRUNK GROUP
Group Number: 1                Group Type: sip                CDR Reports: y
Group Name: Main SIP Phones    COR: 1                    TN: 1                TAC: 101
Direction: two-way            Outgoing Display? N
Dial Access? N                Night Service:
Queue Length: 0
Service Type: tie              Auth Code? N
                                       Signaling Group: 1
                                       Number of Members: 20
```

Figure 41: Trunk-Group Form for SIP Phones

5. Configure Avaya SIP Enablement Services (SES)

This section describes the administration steps for Avaya SIP Enablement Services (SES) in support of SIP trunking with the AT&T IP Flexible Reach service. These Application Notes assume that the necessary Avaya SES licenses have been installed and basic Avaya SES administration has already been performed. Consult [3], [4], and [6] for further details.

5.1. Background

The sample configuration described in these Application Notes explicitly show an Avaya SES combined Home/Edge server configuration. In this case, a single Avaya SES server simultaneously functions in both the Home and Edge roles. Note, however, that multiple Avaya SES servers may exist using a separate Home/Edge configuration as warranted by capacity considerations (predominately for the support of SIP phones). In the separate Home/Edge server configuration:

- The SIP signaling relationship with the AT&T services exists between the AT&T Border Element and the Avaya SES Edge server.
- The Avaya Communication Manager SIP signaling group relationship exists between a C-LAN (or equivalent) interface and a specific Avaya SES Home server.
- SIP message routing between the Home and Edge servers is performed automatically and transparently. However, administration is required on the Home and Edge servers; consult [3], [4], and [6] for further details.
- Only one Avaya SES Edge server exists within a given SIP domain. Multiple Home servers may exist as required.
- All Avaya SES administration is performed from a single Avaya SES server designated during installation as the master administrator.

The SIP trunking administration is generally the same for the combined and separate Home/Edge configurations. Any specific clarifications will be noted within the individual sections as necessary.

5.2. Host Configuration

1. Launch a web browser, enter `http://<IP address of the Avaya SES master administrator>/admin` in the URL, and log in with the appropriate credentials. Click on “**Launch SES Administration Interface**”.

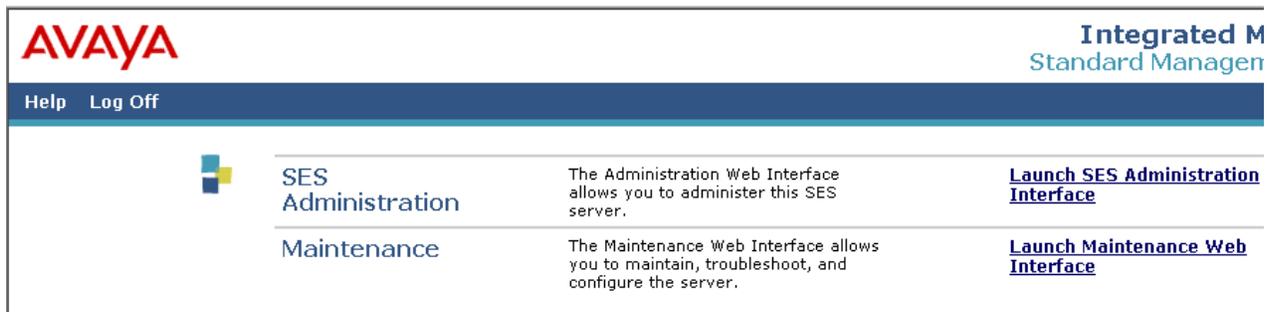


Figure 42: SES Web Interface

2. In the left pane of the SES Administration Interface, expand **Hosts**, and click on “**List**”. In the **List Hosts** page, click on “**Edit**”.

The screenshot shows the Avaya SES Administration Interface. The top header includes the Avaya logo and the text 'Integrated Management SIP Server Manager'. Below the header is a navigation menu with 'Help' and 'Exit' options. The main content area is titled 'List Hosts' and contains a table with the following data:

Commands	Host	Type	SES Version
Edit Map Go-To Test-Link Delete	192.168.67.30	SES combined home-edge	SES-5.1.2.0-416.4b

Below the table, there is a button labeled 'Migrate Home/Edge'.

Figure 43: List Hosts Page

In the **Edit Host** page, ensure that the following are provisioned:

- **Listen Protocols** – The “**UDP**”, “**TCP**”, and “**TLS**” checkboxes are checked.
- **Link Protocols** – “**TLS**” is selected.
- **Outbound Proxy** and **Outbound Direct Domains** fields are blank.

Top

- ▣ Users
 - Address Map Priorities
- ▣ Adjunct Systems
- ▣ Aggregator
- ▣ Certificate Management
- ▣ Conferences
 - Emergency Contacts
- ▣ Export/Import to ProVision
- ▣ Hosts
 - List
 - Migrate Home/Edge
 - IM logs
- ▣ Communication Manager Servers
- ▣ Communication Manager Extensions
- ▣ Server Configuration
- ▣ SIP Phone Settings
- ▣ Survivable Call Processors
 - System Status
- ▣ Trace Logger
- ▣ Trusted Hosts

Edit Host

Host IP Address*	<input type="text" value="192.168.67.30"/>		
Profile Service Password*	<input type="password" value="*****"/>		
Host Type	SES combined home-edge		
Parent	none		
Listen Protocols	<input checked="" type="checkbox"/> UDP <input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> TLS		
Link Protocols	<input type="radio"/> UDP <input type="radio"/> TCP <input checked="" type="radio"/> TLS		
Access Control Policy (Default)	<input type="radio"/> Allow All <input checked="" type="radio"/> Deny All		
Emergency Contacts Policy	<input checked="" type="radio"/> Allow <input type="radio"/> Deny		
Minimum Registration (seconds)	<input type="text" value="900"/>	Registration Expiration Timer (seconds)*	<input type="text" value="86400"/>
		Subscription Expiration Timer (seconds)*	<input type="text" value="86400"/>
Line Reservation Timer (seconds)*	<input type="text" value="30"/>		
Outbound Routing Allowed From	<input checked="" type="checkbox"/> Internal <input checked="" type="checkbox"/> External		
OutboundProxy	<input type="text"/>	Port	<input type="text"/> <input type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> TLS
Outbound Direct Domains	<input style="width: 100%;" type="text"/>		

Figure 44: Edit Host Page

Separate Home/Edge Configuration Note:

In the Avaya SES separate Home/Edge server configuration, there will be at least two SES hosts listed (Home and Edge servers).

- **Avaya SES Edge server** – Configure in the same manner as shown for the combined Home/Edge server above.
- **Avaya SES Home servers** – On each Avaya SES Home server, set the **Outbound Proxy** to the IP address of the Avaya SES Edge server, with **Port** set to “5061” and “TLS” selected.

5.3. Interfaces to Avaya Communication Manager

1. In the left pane of the SES Administration Interface, expand **Communication Manager Servers**, and click on “Add”. In the **Add Communication Manager Server Interface** page, provision the following:
 - **Communication Manager Server Interface Name** – Enter a descriptive name.
 - **Host** – Select the IP address of the Avaya SES combined Home/Edge server.
 - **SIP Trunk Link Type** – Select “TLS”.

- **SIP Trunk IP Address** – Enter the IP address of the first C-LAN board noted in Section 4.3 Step 6.

Scroll down to the bottom of the page and click on “**Add**” (not shown). Click on “**OK**” and then “**Continue**” in the subsequent confirmation pages (not shown).

Separate Home/Edge Configuration Note:

For Avaya SES separate Home/Edge server configurations, select the IP address of an Avaya SES Home server for **Host**.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The header includes the Avaya logo and the text 'Integrated Management SIP Server Management' with the server IP '192.168.67.30'. A navigation menu on the left lists various system components. The main content area is titled 'Add Communication Manager Server Interface' and contains the following form fields:

- Communication Manager Server Interface Name***: Text input field containing 'MainCLAN1A02'.
- Host**: Dropdown menu showing '192.168.67.30'.
- SIP Trunk**: Section header.
- SIP Trunk Link Type**: Radio buttons for 'TCP' and 'TLS', with 'TLS' selected.
- SIP Trunk IP Address***: Text input field containing '192.168.67.13'.
- Communication Manager Server**: Section header.
- Communication Manager Server Admin Address***: Text input field, currently empty, with a note '(see Help)' below it.

Figure 45: Add Communication Manager Server Interface Page – For First C-LAN

2. Repeat Step 1 with the following exception:
 - **SIP Trunk IP Address** – Enter the IP address of the second C-LAN board noted in Section 4.3 Step 6.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '192.168.67.30'. A navigation menu on the left lists various management options, with 'Communication Manager Servers' expanded to show 'Add' and 'List'. The main content area is titled 'Add Communication Manager Server Interface' and contains the following configuration fields:

- Communication Manager Server Interface Name***: MainCLAN1A03
- Host**: 192.168.67.30
- SIP Trunk Link Type**: TCP TLS
- SIP Trunk IP Address***: 192.168.67.14
- Communication Manager Server Admin Address***: (empty field)

Below the admin address field, there is a note: '(see Help)'. The interface also includes 'Help' and 'Exit' links in the top left corner.

Figure 46: Add Communication Manager Server Interface Page- For Second C-LAN

5.4. Call Routing

5.4.1. Background

Avaya SES functions as a SIP proxy for the SIP trunking with the AT&T IP Flexible Reach service. Avaya SES examines the Request-URI of a received SIP INVITE message (from Avaya Communication Manager for outbound calls, and from the AT&T IP Flexible Reach service for inbound calls), modifies the Request-URI and certain SIP headers, and then forwards the message to the appropriate destination.

The Request-URI generally takes the form of *sip:user@domain*, where the *user* part typically contains the called party number digits identifying the phone number being called and the *domain* part can contain a Fully Qualified Domain Name (FQDN) or an IP address. Address maps may be administered in Avaya SES to match SIP INVITE messages with certain Request-URI *user* part patterns, i.e., match certain called party numbers; if a match is found, the matching address map can modify the *user* and/or *domain* parts if necessary. The address map patterns are designed to match a range of called party numbers that require identical SIP message routing and must be specific enough to direct each unique called party number to the proper signaling contact. If the resulting *domain* part of a SIP INVITE message (whether the *user* part has been matched and possibly modified by an address map, or not matched at all) does not match the SIP domain configured on Avaya SES and the outbound proxy is not specified on Avaya SES, then Avaya SES routes the message to the IP address (FQDNs are resolved to IP addresses via DNS) indicated in the *domain* part.

In this sample configuration, for outbound calls to the AT&T IP Flexible Reach service, Avaya Communication Manager already inserts the appropriate called party number in the Request-URI *user* part and the IP address of the AT&T IP Flexible Reach service Border Element in the

domain part. Therefore, Avaya SES address maps are not required for such outbound calls. For inbound calls from the AT&T IP Flexible Reach service, the Request-URI *domain* part contains the IP address of the Avaya SES server. Therefore, one or more Avaya SES address maps are required to match the *user* part of such inbound calls and modify the *domain* part in order to properly route the calls to Avaya Communication Manager.

Note that with the AT&T IP Flexible Reach service, all calls must be routed to the AT&T IP Flexible Reach service core. Therefore, Avaya SES will route all outbound PSTN and TDM gateway site calls to the AT&T IP Flexible Reach service Border Element(s). Similarly, Avaya SES will expect to receive all inbound PSTN and TDM gateway site calls from the same AT&T IP Flexible Reach service Border Element(s).

5.4.2. Outbound Calls to AT&T IP Flexible Reach Service

The domain part of the Request-URI for outbound calls to the AT&T IP Flexible Reach service is specified by the Far-end Domain field of the Avaya Communication Manager SIP signaling groups administered in Section 4.4.1 Step 1 and Section 4.4.2 Step 1. In this sample configuration, since the IP address of the AT&T IP Flexible Reach service Border Element is specified in that Far-end Domain field, no additional Avaya SES administration is necessary for routing such outbound calls.

5.4.3. Inbound Calls from AT&T IP Flexible Reach Service

Avaya SES address maps are used to route inbound calls from the PSTN and the TDM gateway sites to Avaya Communication Manager.

1. In the left pane of the SES Administration Interface, expand **Communication Manager Servers**, and click on “List”. In the **List Communication Manager Servers** page, click on “Map” in the row corresponding to the Communication Manager Server Interface administered in Section 5.3 Step 1. The Communication Manager Server Map to be added will match inbound PSTN calls with a certain called party number / number range and route those calls to Avaya Communication Manager.



Figure 47: List Communication Manager Server Page

- In the **List Communication Manager Server Address Map** page, click on “**Add Map in New Group**”.



Figure 48: List Communication Manager Server Address Map Page

- In the **Add Communication Manager Server Address Map** page, provision the following and click on “**Add**”:
 - Name** – Enter a descriptive name.
 - Pattern** – Enter a Linux regular expression that matches the number in the user part of the Request-URI, i.e., the called party number, of inbound SIP INVITE messages for PSTN calls from the AT&T IP Flexible Reach service. In this sample configuration, for inbound calls from the PSTN, the AT&T IP Flexible Reach service inserts 10-digit numbers beginning with “7231126xxx” in the user part of the Request-URI to reach local extensions in the Avaya site. Thus, the pattern “**^sip:7231126[0-9]{3}**” shown in **Figure 49**, matches SIP INVITE messages with a Request-URI that begins with “sip:7231126” followed by any three consecutive digits.
 - Replace URI** – Ensure that the checkbox is checked.



Figure 49: Add Communication Manager Server Address Map Page – Match 10-Digit Numbers

Click on “**Continue**” in the subsequent confirmation page (not shown).

- A Contact is automatically created after creating the first Communication Manager Server Address Map (see **Figure 50**). The **Contact** specifies that the SIP messages

matched by the Communication Manager Server Address Map(s) administered in Step 3 are to be routed to the IP address of the Communication Manager Server Interface administered in Section 5.3 Step 1. The “\$(user)” string in the Contact is substituted with the user part of the original inbound Request-URI.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '192.168.67.30'. A navigation menu on the left lists various management options. The main content area is titled 'List Communication Manager Server Address Map' and contains a table with the following data:

Commands	Name	Commands	Contact
Edit Delete	ATT_7231126xxx		
		Edit Delete	sip:\$(user) @192.168.67.13:5061;transport=tls

Below the table are buttons for 'Add Another Map', 'Add Another Contact', and 'Delete Group'. At the bottom, there is a link for 'Add Map In New Group'.

Figure 50: List Communication Manager Server Address Map Page – First C-LAN

Click on “**Add Another Map**” and repeat Step 3 for each called party number / number range as necessary.

- Repeat Steps 1 – 4 for inbound calls from the TDM gateway sites, with the following exceptions:
 - Click on “**Map**” in the row corresponding to the Communication Manager Server Interface administered in Section 5.3 Step 2, i.e., for the second C-LAN board noted in Section 4.3 Step 6. The Communication Manager Server Map to be added here will match inbound calls from the TDM gateway sites with a certain called party number / number range and route those calls to Avaya Communication Manager.
 - Pattern** – Enter a Linux regular expression that matches the number in the user part of the Request-URI, i.e., the called party number, of inbound SIP INVITE messages for TDM gateway calls from the AT&T IP Flexible Reach service. In this sample configuration, for inbound calls from the TDM gateway sites, the AT&T IP Flexible Reach service inserts 4-digit numbers beginning with “6xxx” in the user part of the Request-URI to reach local extensions in the Avaya site. Thus, the pattern “**^sip:6[0-9]{3}**” shown in ???, matches SIP INVITE messages with a Request-URI that begins with “sip:6” followed by any three consecutive digits.

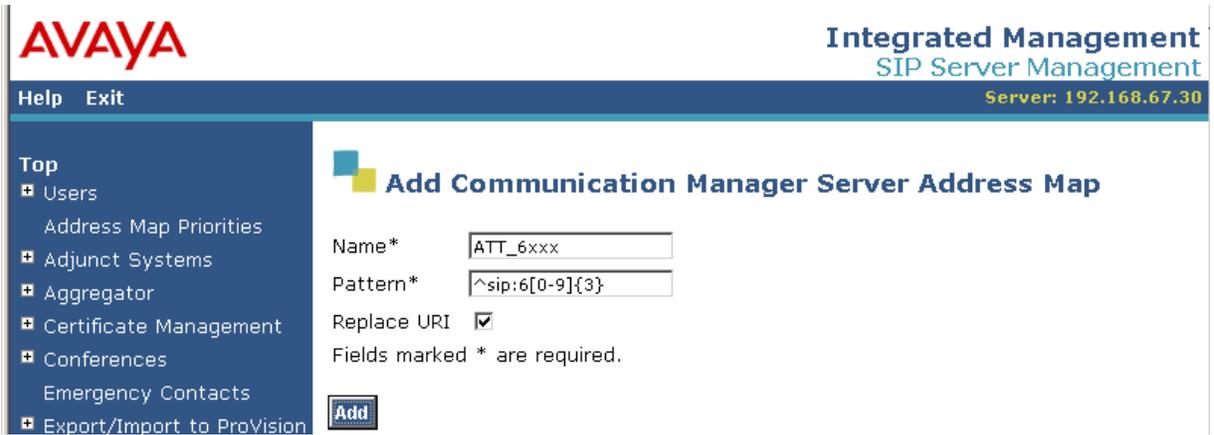


Figure 51: Add Communication Manager Server Address Map Page – Match 4-Digit Numbers



Figure 52: Figure 53: List Communication Manager Server Address Map Page – Second C-LAN

5.5. Trusted Host

The AT&T IP Flexible Reach service Border Element IP address must be added as a trusted host entry in Avaya SES. Avaya SES will not attempt to authenticate incoming requests from trusted hosts.

In the left pane of the SES Administration Interface, expand **Trusted Hosts**, and click on “**Add**”. In the **Add Trusted Host** page, provision the following:

- **IP Address** – Enter the IP address of the AT&T IP Flexible Reach service Border Element.
- **Host** – Select the IP address of the Avaya SES combined Home/Edge server.
- **Comment** – Enter a description of the trusted host.

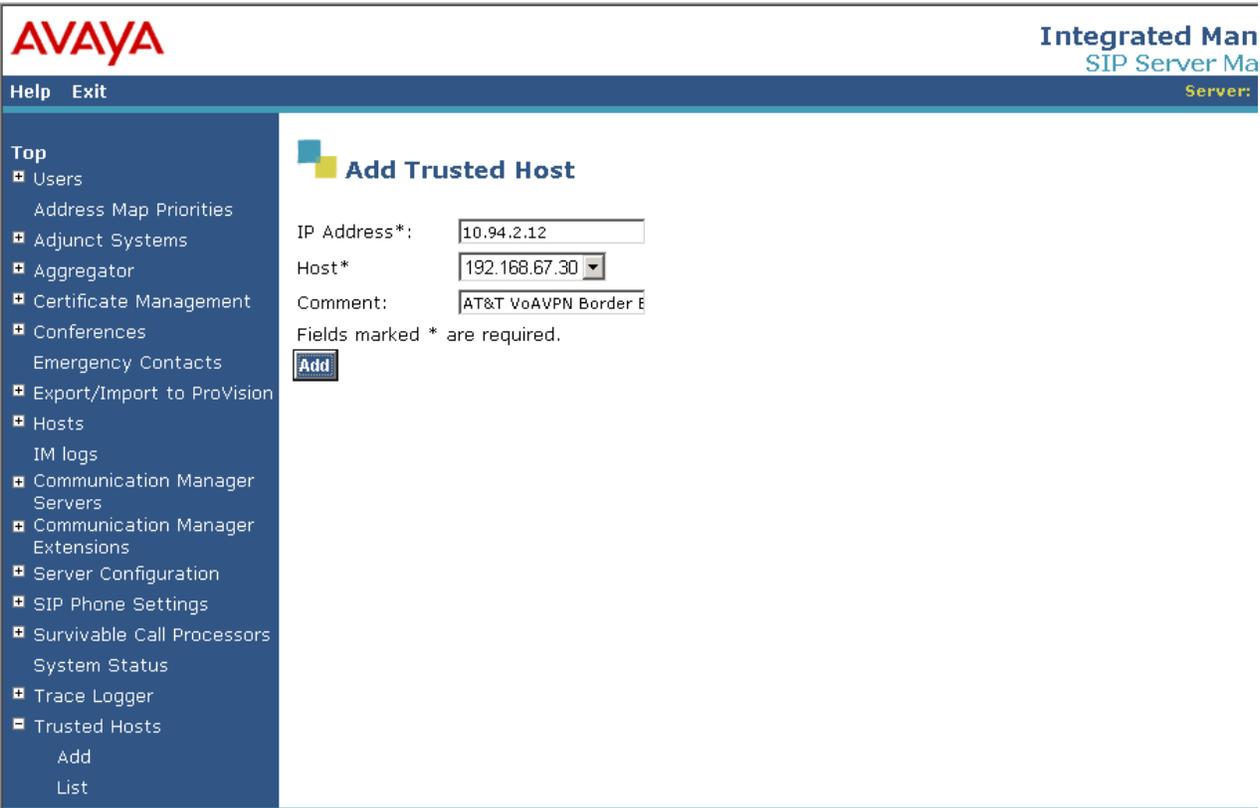


Figure 54: Add Trusted Host Page

Click on “**Continue**” in the subsequent confirmation page (not shown).

Repeat the above administration for any other AT&T IP Flexible Reach service Border Elements provided.

Separate Home/Edge Configuration Note:

In the Avaya SES separate Home/Edge server configuration, there will be at least two SES hosts listed (Home and Edge servers).

- Avaya SES Edge server – Configure the trusted host relationship on the Avaya SES Edge server.
- Avaya SES Home servers – Configure the trusted host relationship on each Avaya SES Home server.

6. General Test Approach and Test Results

The test environment consisted of:

- A simulated PSTN.
- A simulated enterprise site (“Avaya site”) with Avaya Communication Manager, Avaya SES, Avaya phones, and Avaya Modular Messaging.
- Another simulated enterprise site (“TDM gateway site) with phones residing behind a TDM gateway.
- A laboratory version of the AT&T IP Flexible Reach service, to which the simulated PSTN and enterprise sites were connected.

The main test objectives were to verify the following features and functionality:

- Outbound calls from the Avaya site to PSTN destinations.
- Inbound calls from PSTN phones to the Avaya site.
- Outbound calls from the Avaya site to TDM gateway sites destinations.
- Inbound calls from the TDM gateway sites phones to Avaya site destinations.
- Calls using Avaya 4600 and 9600 Series IP Telephones (H.323) and SIP Telephones, as well as Avaya one-X™ Communicator.
- G.729B codec for voice calls with PSTN endpoints and the TDM gateway sites.
- T.38 for fax calls with PSTN endpoints and the TDM gateway sites.
- DTMF tone transmission using RFC 2833 in both directions on calls with PSTN endpoints and the TDM gateway sites.
- Access to voicemail and Meet-Me conferences hosted on the Avaya site.
- Basic supplementary telephony features such as hold, transfer, and conference.
- Direct IP-to-IP media (also known as “shuffling”).

The following feature is not supported by Avaya with the AT&T IP Flexible Reach service and was not tested.

- Fax detection during a G.729B call with codec change to G.711Mu.

The above test objectives of Section 6 with limitations as noted in Section 1.3 were verified. Note that this configuration requires Update 17067 for Avaya Communication Manager release 5.1.2. Subsequent releases of Avaya Communication Manager are expected to incorporate this update within the primary release.

7. Verification Steps

7.1. Verification Tests

The following steps may be used to verify the configuration:

1. Verify the outbound PSTN call routing administration on Avaya Communication Manager by using the “**list ars route-chosen n**” command, where **n** is a PSTN number (including the leading country code “1” in this sample configuration but not including the ARS code). As shown below, the **ars route-chosen** form shows the **Route Pattern** that would be selected for a given dialed PSTN number.

```
List ars route-chosen 17323681042
```

ARS ROUTE CHOSEN REPORT						
Location: 1			Partitioned Group Number: 1			
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Number	Location
1732	11	11	14	fnpa		all

Figure 55: ARS Route-Chosen Form

2. If extension dialing for calling the TDM gateway sites was administered in Section 4.2 Step 2, verify the administration on Avaya Communication Manager for routing outbound calls to the TDM gateway sites by entering the “**list aar route-chosen n#**” command, where **n** is a TDM gateway site phone number (including the leading country code “1” in this sample configuration). As shown below, the **aar route-chosen** form shows the Route Pattern that would be selected for a given TDM gateway phone number.

```
List aar route-chosen 12013982001#
```

AAR ROUTE CHOSEN REPORT						
Location: all			Partitioned Group Number: 1			
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Number	Location
12013982	11	11	13	aar		all

Figure 56: AAR Route-Chosen Form

If extension dialing for calling the TDM gateway sites was NOT administered in Section 4.2 Step 2, then use the “**list ars route-chosen n**” command described in Step 1 instead, except that **n** is a TDM gateway site phone number.

- Place outbound and inbound calls, and verify that two-way talkpath exists, and that the calls remain stable for several minutes and disconnect properly.
- For trunk calls established on Avaya 4600 and 9600 Series IP Telephones (H.323), enter the “**status station e**” command, where **e** is the extension of the Avaya phone. On Page 5 of the **status station** form, verify that “**G.729AB**” is displayed and the **Audio Connection Type** is “**ip-direct**”.

```

Status station 26102                                     Page 5 of 8
                AUDIO CHANNEL Port: S00000
G.729AB      Switch-End Audio Location:
                IP Address                               Port  Node Name
Rgn
Other-End:    10. 94.  2. 12                            28588
Set-End:     192.168. 67. 72                            28838
Audio Connection Type: ip-direct

```

Figure 57: Status Station Form

7.2. 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 (Message Sequence Trace) diagnostic traces (performed by Avaya Support) can be helpful in understanding the specific interoperability issues.

The “Trace Logger” function within the Avaya SES Administration Interface may be used to capture SIP traces between Avaya SES and the AT&T IP Flexible Reach service. In addition, if port monitoring is available, a SIP protocol analyzer such as Wireshark (a.k.a. Ethereal) can be used to capture SIP traces at the various interfaces. SIP traces can be instrumental in understanding SIP protocol issues resulting from configuration problems. Note that the SIP messaging between Avaya Communication Manager and Avaya SES uses TLS encryption and cannot be viewed using Wireshark.

8. Conclusion

These Application Notes described the steps for configuring Avaya Communication Manager and Avaya SIP Enablement Services (SES) SIP trunking with the AT&T IP Flexible Reach service accessed through AT&T VPN transport service connections. The convergences of various AT&T business VoIP and AVPN services allow enterprises to make voice calls over their private wide area data network connections. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise’s sites.

The sample configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

9. References

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

- [1] *Administrator Guide for Avaya Communication Manager*, Issue 4.0, Release 5.0, January 2008, Document Number 03-300509
- [2] *Feature Description and Implementation for Avaya Communication Manager*, Issue 6, January 2008, Document Number 555-245-205
- [3] *SIP Support in Avaya Communication Manager Running on the Avaya S8xxx Servers*, Issue 8, January 2008, Document Number 555-245-206
- [4] *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services*, Issue 6.0, June 2008, Document Number 03-600768
- [5] *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Administrator Guide Release 2.0*, Issue 2, December 2007, Document Number 16-601944
- [6] *SIP Enablement Services (SES) Implementation Guide*, Issue 5, January 2008, Document Number 16-300140

AT&T IP Flexible Reach and AT&T VPN Service Descriptions:

[7] *AT&T IP Flexible Reach*

<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>

[8] *AT&T VPN*

<http://www.business.att.com/enterprise/Portfolio/vpn-services-enterprise/>

10. Change History

Issue	Date	Reason
1.0	2009-05-29	Initial issue.

©2009 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.