Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking between TelePacific SmartVoice SIP Connect and an Avaya Quick Edition Telephony Solution – 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the TelePacific SmartVoice SIP Connect service and an Avaya Quick Edition telephony solution. The Avaya solution consists of Avaya Quick Edition, and an Avaya A10 Analog Telephone Adapter (ATA) Gateway.

TelePacific Communications offers a flexible VoIP solution for customers with a SIP based network. TelePacific Communications is a facility based competitive carrier that serves customers throughout California and Nevada. Headquartered in Los Angeles, the Company is the leading competitive carrier in its markets, with customer care centers in Los Angeles and Stockton in California and Las Vegas in Nevada.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the TelePacific SmartVoice SIP Connect service and an Avaya Quick Edition telephony solution. The Avaya solution consists of Avaya Quick Edition, and an Avaya A10 Analog Telephone Adapter (ATA) Gateway.

TelePacific Communications offers a flexible VoIP solution for customers with a SIP based network. TelePacific Communications is a facility based competitive carrier that serves customers throughout California and Nevada. Headquartered in Los Angeles, the Company is the leading competitive carrier in its markets, with customer care centers in Los Angeles and Stockton in California and Las Vegas in Nevada.

Customers using the Avaya Quick Edition telephony solution with the TelePacific SmartVoice SIP Connect solution are able to place and receive PSTN calls using the SIP protocol via a dedicated broadband Internet connection. This converged network solution is an alternative to more traditional PSTN trunks such as T1 or ISDN PRI.

TelePacific can connect directly to an IP phone system as well as an external router. The TelePacific SmartVoice SIP Connect solution offers the following capabilities:

- Outbound domestic calling to local and long distance services
- Outbound international calling
- Incoming Direct Inward Dial (DID) service

Figure 1 illustrates a sample Avaya IP telephony solution connected to the TelePacific SmartVoice SIP Connect solution. This configuration was utilized for compliance testing.

Figure 2 illustrates the same configuration with the addition of a Juniper SSG 520M performing Port Network Address Translation (NAT) functionality. In a typical enterprise deployment, a firewall device will be installed to perform Network and/or Port Address Translation (PAT) functionality for security purposes as well as to minimize use of public IP addresses. The firewall device is managed by the enterprise customer and not TelePacific. This configuration was utilized to verify proper operation through a sample firewall/NAT device recommended by TelePacific. TelePacific performs their own certification testing with other firewall/NAT devices such as: Cisco Pix, ASA, IOS FW, Fortigate, or Juniper Netscreen; which they end up recommending to their customers.

Note: The IP addresses shown in **Figure 1** and **Figure 2** throughout this document are not the actual addresses used during testing. They are used as an example for these Application Notes. The real IP addresses are not revealed for security purposes.

The following Avaya IP telephony solution simulated a customer site:

- Avaya 4621SW IP Quick Edition station
- Avaya 4610SW IP Quick Edition station
- Avaya A10 ATA Gateway

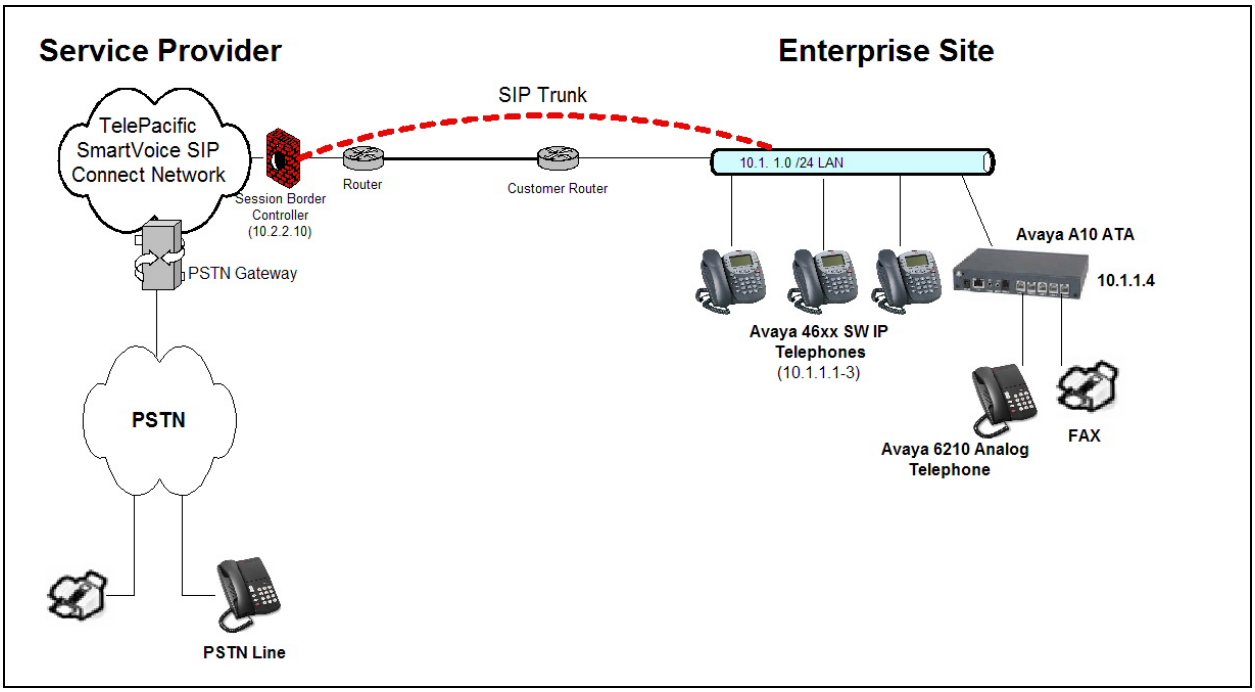


Figure 1: Avaya IP Telephony Network using TelePacific SIP Trunking Solution

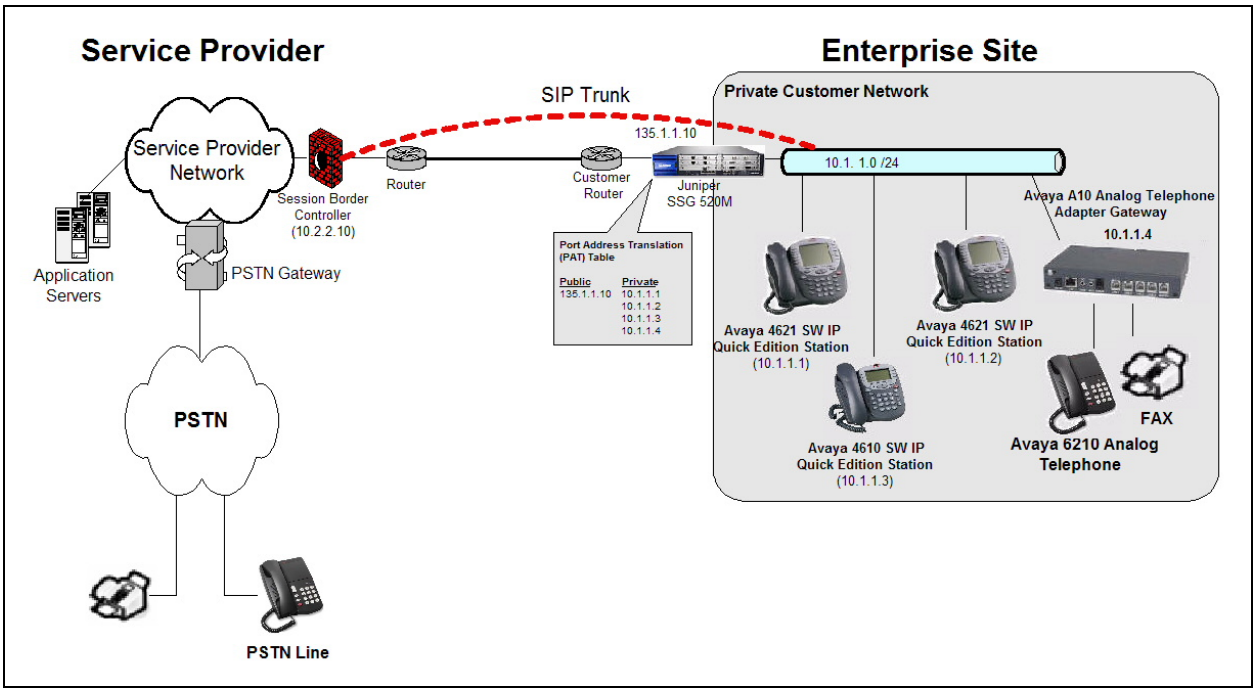


Figure 2: Avaya IP Telephony Network using Firewall Device Performing NAT

2. Equipment and Software Validated

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

Product	Software/Version
Avaya Quick Edition	3.2.5
Avaya Quick Edition A10 Analog Gateway	3.21.0
Avaya 4610SW IP Telephone	3.2.5 (Avaya Quick Edition)
Avaya 4621SW IP Telephone	3.2.5 (Avaya Quick Edition)
TelePacific SmartVoice SIP Connect	R1.0

Table 1: Equipment and Software Tested

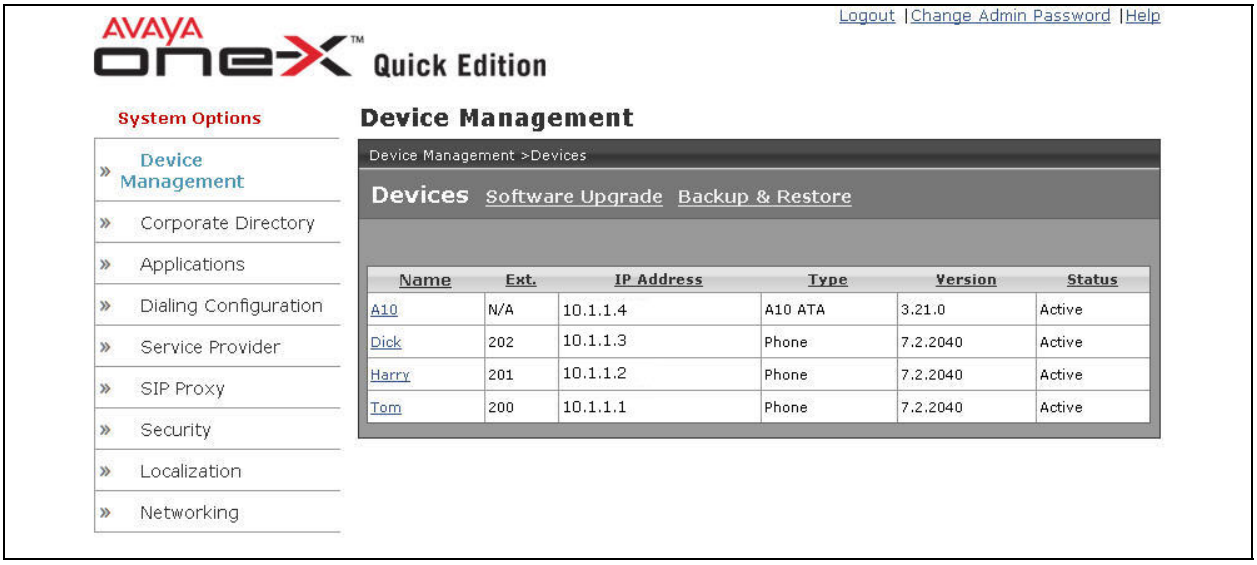
2. Configure Avaya Quick Edition

The initial configuration for an Avaya Quick Edition network is performed by directly interacting with the keypad present on the Avaya Quick Edition telephone. For information on how to perform an initial configuration for an Avaya Quick Edition network and the process for installing the A10 Analog gateway, refer to [1] and [4].

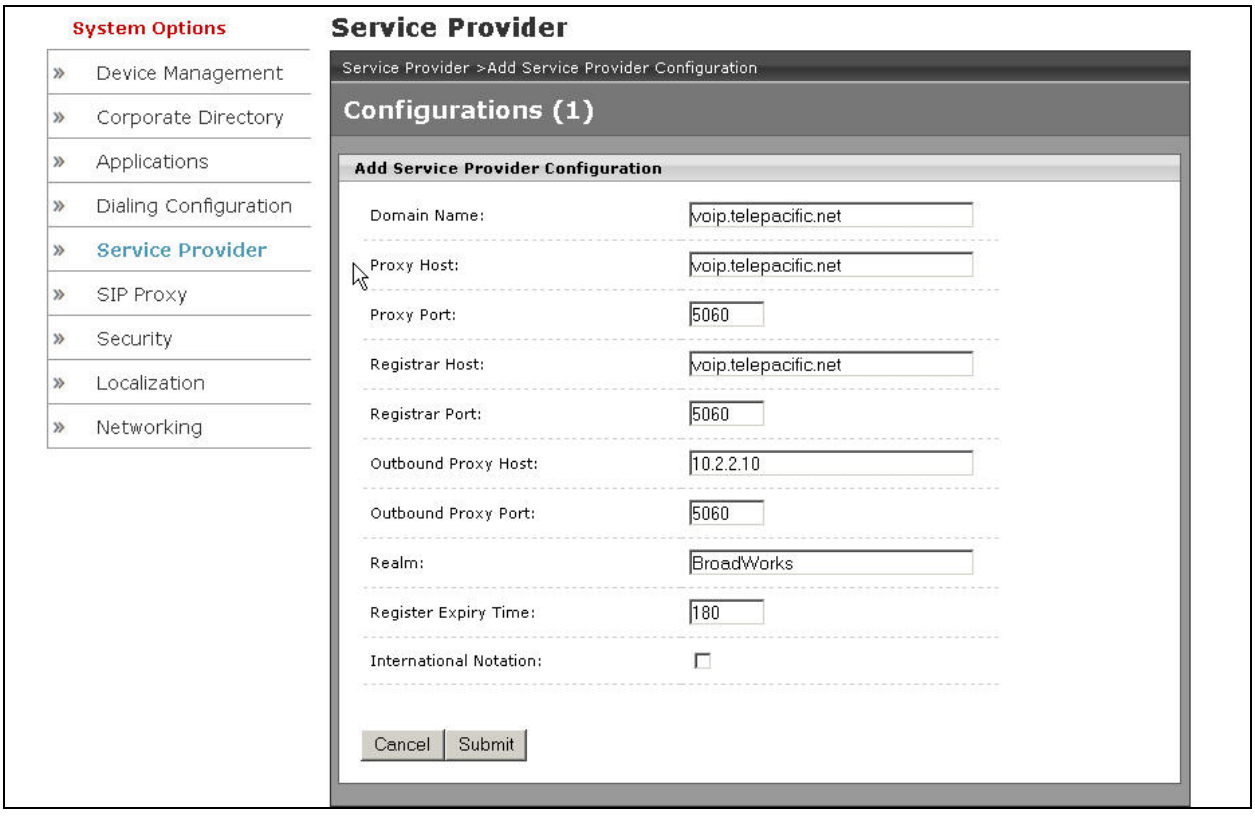
This section describes the steps for configuring a SIP trunk on Avaya Quick Edition.

Once the initial configuration has been performed, access the Avaya Quick Edition web configuration utility by using any web browser to open a secure connection to any of the IP addresses assigned to any Avaya Quick Edition telephone.

1. Once logged in, the **Device Management** web page is displayed. This page lists all of the Avaya Quick Edition devices that have been found on the network. This page can be used to quickly gauge the number and types of Avaya Quick Edition devices present within the network.



2. *Configure Service Provider Functionality*. Navigate to the Service Provider web page by clicking **Service Provider → Configuration → Add**.
   - For **Domain Name**, enter the domain name for the registration server, this value will be used as part of the From Header URI for outgoing SIP INVITE messages.
   - For **Proxy Host**, enter the Fully Qualified Domain Name (FQDN) of the proxy server provided by TelePacific. The example below uses "voip.telepacifc.net".
   - For **Proxy Port**, enter the standard well known SIP port 5060.
   - For **Registrar Host**, enter the FQDN of the registration server provided by TelePacific. The example below uses "voip.telepacifc.net".
   - For **Registration Port**, enter the standard well known SIP port 5060.
   - For **Outbound Proxy Host**, enter the FQDN provided by TelePacific. The example below uses "voip.telepacifc.net".
   - For **Outbound Proxy Port**, enter the standard well known SIP port 5060.
   - For **Realm**, enter "BroadWorks". This value will be used during the SIP digest authentication process.
   - For **Register Expiry Timer**, enter a value in seconds that represents time interval between subsequent registration attempts. Below, a value of 180 seconds is used. Depending upon how the network firewall is configured, a value as low as 60 seconds may be needed to keep the pinhole opened.
   - For **International Notation**, the default of unchecked should be accepted.

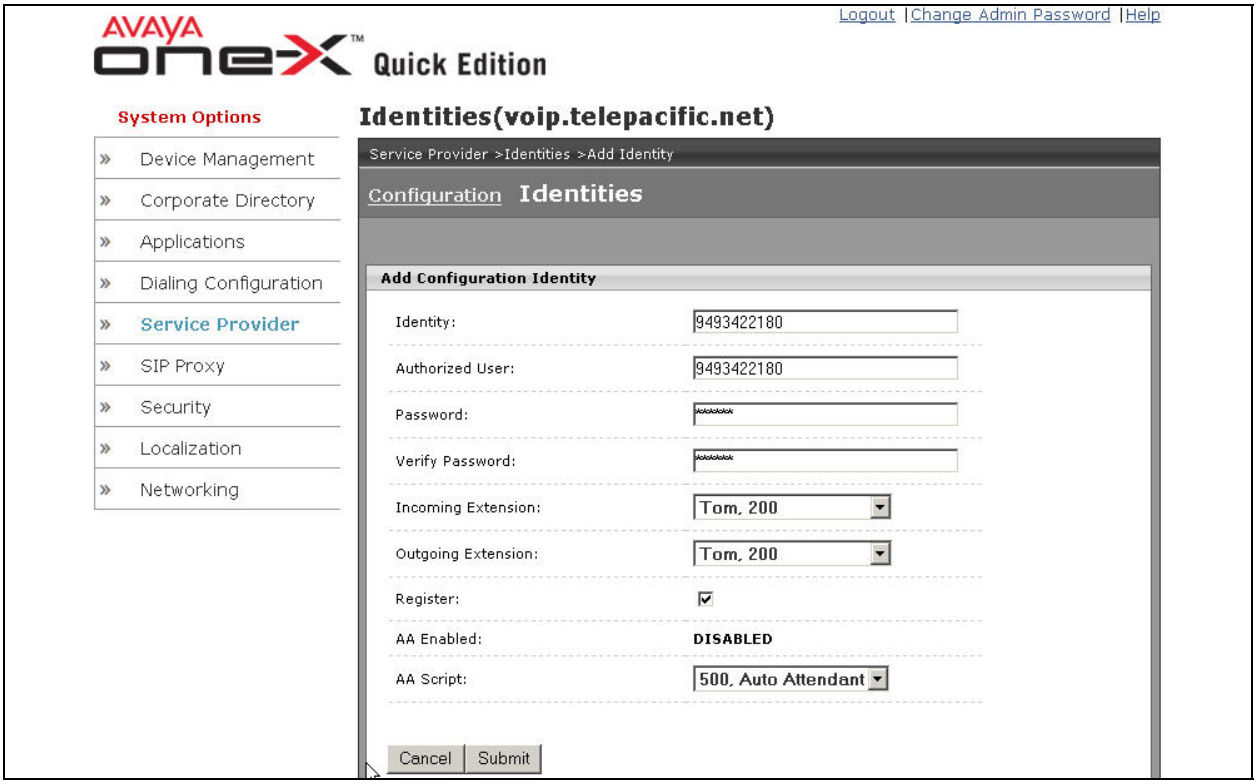


3. *Create SIP Identities for each Avaya Quick Edition telephone*. SIP Identities serve two purposes:
   - Instructs Avaya Quick Edition to register with the Service Provider.
   - Allows incoming calls to be mapped to the desired Avaya Quick Edition telephone.

Navigate to the Service Provider web page by clicking **Service Provider → Identities → Add**.

Select the following:

- For the **Identity** field, enter a unique numerical value provided by TelePacific. Typically, this value will be a DID number that will be used to access the Avaya Quick Edition telephone network from the PSTN. This value is unique for each SIP Identity created in the system.
- For the **Authorized User** field, enter the numerical value provided by TelePacific. This value will be the same for all additional SIP Identities.
- For the **Password** and **Verify Password** fields, enter the numerical value provided by TelePacific. This value will be the same for all additional SIP Identities.
- For **Incoming Extension**, select the Avaya Quick Edition set that will receive calls for the specified Identity.
- For **Outgoing Extension**, select the Avaya Quick Edition set that will be allowed to use this SIP Identity for outgoing calls. For Direct Line or DID configurations, the **Incoming Extension** and **Outgoing Extension** values are the same.
- For **Register**, enable registration by checking the box.



4. *Configure Codec preference*. For outbound SIP calls, Avaya Quick Edition offers G.711mu, G.711a and G.729a. The order of preference in the outbound INVITE message can be altered to reflect the following to options:
   a) G.711mu, G.711a, G.729a
   b) G.729a, G.711mu, G.711a

   To configure either one of the options above, navigate to the **Networking → Audio Bandwidth → Edit** screen. For option a), select **High** which indicates the preference of the higher bit rate codec G.711. For option b), select **Low** which indicates the preference of the lower bit rate codec G.729a.

4. TelePacific Services Configuration

Service is ordered through a TelePacific Account Manager or through a TelePacific Agent. To establish a relationship with TelePacific, contact at: http://www.telepacific.com or call 800-399-4925 for more details.

5. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify SIP trunking interoperability between TelePacific Service and an Avaya IP Office telephony solution. This section covers the general test approach and the test results.

5.1. General Test Approach

A simulated enterprise site consisting of an Avaya IP Office telephony solution supporting SIP trunking was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to use the commercially available SmartVoice SIP Connect solution provided by TelePacific. This allowed the enterprise site to use SIP trunking for calls to the PSTN.

The following features and functionality were covered during the SIP trunking interoperability compliance test:

- DID Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by TelePacific.
- Outgoing calls from the enterprise site were completed via TelePacific to the PSTN destinations.
- Calls using the 4610SW IP and 4621SW IP Quick Edition endpoints.
- Various call types including: local, long distance, international, and directory assistance calls.
- Calls using the G.729a and G.711MU codec types.
- Fax calls from the A10 ATA Gateway using the G.711MU codec.
- DTMF tone transmission using RFC 2833 with successful voice mail navigation with the G.729a codec and G.711mu codec types.
- Telephony features such as hold, transfer, park and conference.

6.2. Test Results

Interoperability testing of the sample configuration was completed with successful results. A subset of the original testing was also successfully completed with the firewall in place as depicted in Figure 2.

The following observations were noted.

- For outbound calls to the PSTN, if a PSTN end point is busy, the Avaya Quick Edition phone will not play a busy signal.
- When the Service Provider DTMF Payload Type Identifier (PTI) value does not match Avaya Quick Edition's default PTI of 101, DTMF events may not function properly. The workaround is to configure the Service Provider PTI value to 101 in order to match the default value of Avaya Quick Edition.

7. Verification Steps

This section provides verification steps that may be performed to verify that the Avaya Quick Edition and analog endpoints can place outbound and receive inbound calls through the TelePacific service.

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers. Verify through the IP Office Monitor and System Trace tools that the call is using the appropriate SIP Line and and that the proper SIP messages are exchanged.

2. Verify that endpoints at the enterprise site can receive a call from the PSTN and that the call can remain active for more than 35 seconds. Verify through the IP Office Monitor and System Trace tools that the call is using the appropriate SIP Line and that the proper SIP messages are exchanged.

3. Verify that the user on the PSTN can terminate an active call by hanging up.

4. Verify that an endpoint at the enterprise site can terminate an active call by hanging up.

8. Support

All TelePacific customers have 24 hours access to live technical support. Customer Care may be reached by calling 877-487-TPAC or visiting:
http://www.telepacific.com/contact/customerService.

9. Conclusion

These Application Notes describe the configuration steps required to connect customers using an Avaya IP Office telephony solution to TelePacific SmartVoice SIP Connect service. TelePacific offers a flexible VoIP solution for customers with a SIP based network. SIP trunks use the Session Initiation Protocol to connect private company networks to the public telephone network via converged IP access, providing an alternative to traditional hardwired telephony trunk lines.

10. References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at http://support.avaya.com.

[1] *Avaya one-X Quick Edition Release 3.2.0 System Administration Guide*, Document ID 16-601412, August 2007

[2] *Quick Edition Trouble Shooting Guide, Document ID 16-602443*, August 2007

[3] *Avaya one-X Quick Edition 46xx SW IP Telephone Safety and Quick Installation Instructions*, Document ID 16-601408, May 2007

[4] *Avaya one-X Quick Edition Safety and Quick Installation Instructions for G11 Global Analog Gateway, G20 ISDN BRI Gateway and A10 Analog Telephone Adapter*, Document ID 16-601414, May 2007

Non-Avaya Documentation:

[5] RFC 3261 *SIP: Session Initiation Protocol* http://www.ietf.org/

[6] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals* http://www.ietf.org/

APPENDIX A: Sample SIP INVITE Messages

This section displays the format of the SIP INVITE messages sent by TelePacific and the Avaya SIP network at the enterprise site. Customers may use these INVITE messages for comparison and troubleshooting purposes. Differences in these messages may indicate different configuration options selected.

Sample SIP INVITE Message from TelePacific to Avaya Quick Edition:

INVITE sip:9493422182@10.1.1.1;srcadr=10.1.1.1 SIP/2.0
Via: SIP/2.0/UDP 10.2.2.10:5060;branch=z9hG4bKsrmos7208g81fe4go1g1.1
From: "AVAYA INC "<sip:7324500819@10.255.224.100;user=phone>;tag=918933125-1201809664247-
To: "9493422182 9493422182"<sip:9493422182@voip.telepacific.net>
Call-ID: BW120104247310108-61647394@10.255.224.100
CSeq: 683152508 INVITE
Contact: <sip:7324500819@10.2.2.10:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,UPDATE,NOTIFY,UPDATE
Accept: multipart/mixed,application/media_control+xml,application/sdp
Max-Forwards: 9
Content-Type: application/sdp
Content-Length: 303
P-Media-Release: hngl5rp9pu6vivh05pvumhj1r8jof8do6u7g8gsnmkmj2c0el4v1004082

Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): BroadWorks 21569 1 IN IP4 10.2.2.10
Session Name (s): -
Connection Information (c): IN IP4 10.2.2.10
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 17812 RTP/AVP 18 0 2 4 100
Media Attribute (a): rtpmap:18 G729/8000/1
Media Attribute (a): fmtp:18 annexb=no
Media Attribute (a): rtpmap:0 PCMU/8000/1
Media Attribute (a): rtpmap:2 G726-32/8000/1
Media Attribute (a): rtpmap:4 G723/8000/1
Media Attribute (a): rtpmap:100 telephone-event/8000
Media Attribute (a): fmtp:100 0-15
Media Attribute (a): sendrecv

Sample SIP INVITE Message from Avaya Quick Edition to TelePacific:

INVITE sip:10.2.2.10:5060 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.1;branch=z9hG4bKeca049ec2
Max-Forwards: 70
Content-Length: 324
To: "UNKNOWN" <sip:17324500819@voip.telepacific.net>
From: "Harry" <sip:9493422182@voip.telepacific.net>;tag=75ceb1c18050ad2
Call-ID: 39a0a5d824629afb2fa11b750e2d9de2@voip.telepacific.net
CSeq: 390214244 INVITE
P-Asserted-Identity: "Harry" <sip:9493422182@voip.telepacific.net>
Allow: INVITE
Allow: CANCEL
Allow: OPTIONS
Allow: BYE
Allow: REFER
Allow: INFO
Allow: UPDATE
Content-Type: application/sdp
Contact: "Harry" <sip:9493422182@10.1.1.1>
Supported: replaces
User-Agent: Avaya 4600SW 7.2.2040 00040DE97629 MxSF/v3.2.6.26
Route: <sip:17324500819@voip.telepacific.net>

Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): dn201 1167775872 1167775873 IN IP4 10.1.1.1
Session Name (s): -
Connection Information (c): IN IP4 10.1.1.1
Time Description, active time (t): 0 0
Session Attribute (a): sendrecv
Media Description, name and address (m): audio 20018 RTP/AVP 0 8 18 101
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute (a): rtpmap:101 telephone-event/8000
Media Attribute (a): fmtp:18 annexb=no
Media Attribute (a): fmtp:101 0-15
Media Attribute (a): ptime:20
Media Attribute (a): rtcp:20019 IN IP4 10.1.1.1

APPENDIX B: Juniper SSG 520M Configuration

Below is a sample configuration used to achieve Port Address Translation as displayed in Figure 2 of this document. The "bolded" lines are those that pertain to the PAT configuration.

```
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
unset alg sip enable
set alg appleichat enable
unset alg appleichat re-assembly enable
set alg sctp enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 27911
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin http redirect
set admin auth web timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Untrust"
set interface ethernet0/0 ip 10.1.1.2/24
set interface ethernet0/0 nat
```

unset interface vlan1 ip
set interface ethernet0/1 ip 10.10.10.15/24
set interface ethernet0/1 nat
set interface ethernet0/2 ip 135.1.1.10/24
set interface ethernet0/2 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/1 ip manageable
set interface ethernet0/2 ip manageable
set interface vlan1 manage mtrace
set interface ethernet0/2 dip 4 135.1.1.10 135.1.1.10
set interface ethernet0/2 dip interface-ip incoming
unset flow no-tcp-seq-check
set flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set ike respond-bad-spi 1
set ike ikev2 ike-sa-soft-lifetime 60
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
set url protocol websense
exit
set policy id 1 name "QE" from "Trust" to "Untrust" "Any" "Any" "ANY" permit log
set policy id 1
exit
set policy id 2 from "Untrust" to "Trust" "Any" "Any" "ANY" permit log
set policy id 2
exit
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
unset license-key auto-update
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 0.0.0.0/0 interface ethernet0/2 gateway 135.1.1.1

```
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

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.