AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for IP Trade Voice Trading Solution with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IP Trade Voice Trading Solution to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP Trunks.

The IP Trade solution consists of a set of IP Trade turrets, a Turret Support Server (TSS), and a Turret Proxy to Open Line Dealing (TPO) server. The trading turrets, as well as the Open Line Dealing (OLD) extensions defined in the TPO server, register as SIP endpoints with Avaya Aura® Session Manager. This enables IP Trade devices to integrate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and, in the case of the turrets, Avaya Modular Messaging.

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

Application Notes describe the procedures for configuring IP Trade's IP-based trading floor solution to communicate with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Modular Messaging (MM).

The IP Trade solution consists of the following components:

- **Turret Support Server (TSS)**: The TSS provides security extensions, end user profile management, hunt group capabilities and bridges to middle-office applications.

- **IP Trade turret**: The IP Trade turret is SIP-based VoIP trading phone. Its call handling panel uses Avaya Communication Manager feature name extensions (FNE) and/or IP Trade Profile internal features to provide a variety of call features (e.g., Hold, Transfer, Conference, Call Park, Call Forward, Call Pickup, Call Dispatch, Barge-In, etc.).

- **Turret Proxy to Open Line Dealing (TPO) Server**: The TPO server serves as a proxy phone between a remote place via private wire or lines (referred to DDI Lines) registered to the local Avaya Communication Manager and locally shared on IP Trade end-users (turrets). When a local IP Trade end-user presses the button for respective private wire to reach the remote place, all of the other local IP Trade end users see that the line is in use and can also connect to the same remote location by means of the TPO conferencing and bridging, connecting IP Trade end user to the same "Open Line" locally over a single call to the remote location, and are each able to speak publicly or privately to that remote location

- While private wires are direct (point-to-point) connections to remote places, the same concept is applied to DDI Lines that are shared among local IP Trade end users. Shared DDI Line offer the following capabilities:

  - *Common lamping* – Shared DDI lines can be mapped on programmable keys on several traders position and provide them in real-time with the state of line.

  - *Line sharing* – Once the line is engaged on a call, traders can join/leave the line without any restrictions as they would do on private wires; similarly, the distant party can be put on hold by any trader and resumed from another position.

  - *Floating & line coverage* – Whether call events are monitored - or not - and whether ringing lines are alerted in the float area - or not - can now be selected for each individual line and activated/deactivated on-demand.

  - *Telephony functions* – The main telephony functions remain available on shared DDI lines and enables traders to transfer the distant party to another extension, to conference external parties – i.e. IP phones, external lines – , to forward the line, to switch "do not disturb" on/off and to receive MWI notifications. DTMF are also supported.

In these Application Notes, the TPO server registers many SIP endpoints as Shared DDI Lines or as single lines for private wires with Avaya Aura® Session Manager . One Avaya IP extension was used for a simulated private wire remote place.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among IP Trade turret users with Avaya SIP, Avaya H.323, PSTN users, and/or the Avaya Modular Messaging voicemail pilot to verify MWI scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN connection to IP Trade TSS.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing included subscriber login, greeting, leaving and retrieving voice message, message waiting indicator, unconditional call forward, blind and attended transfer, hold and resume, conference, and Private Line Automatic Ringdown (PLAR).

The serviceability testing focused on verifying the ability of IP Trade Voice Trading Solution to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection to the TSS server.

2.2. Test Results

All test cases were executed and verified. The following were the observations on IP Trade from the compliance testing.
- Avaya did not interpret DMTF digits from IP Trade endpoints, so the DTMF tests only covered the IP Trade interpretation of DMTF digits from the Avaya side. During the voicemail retrieving scenario, DTMF from IP Trade side was verified.

2.3. Support

Technical support on IP Trade Voice Trading Solution can be obtained through the following:

- **Phone:** +32 494 53 41 94
- **Email:** Support@iptrade-networks.com

3. Reference Configuration

As shown in **Figure 1** below, IP Trade Voice Trading Solution consists of the Turret Support Server, Turret Proxy to Open Line Dealing Server, and IP Trade turret. During the compliance test, IP Trade turrets are registered with Session Manager.

The detailed administration of basic connectivity among Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Modular Messaging is not the focus of these Application Notes and will not be described.
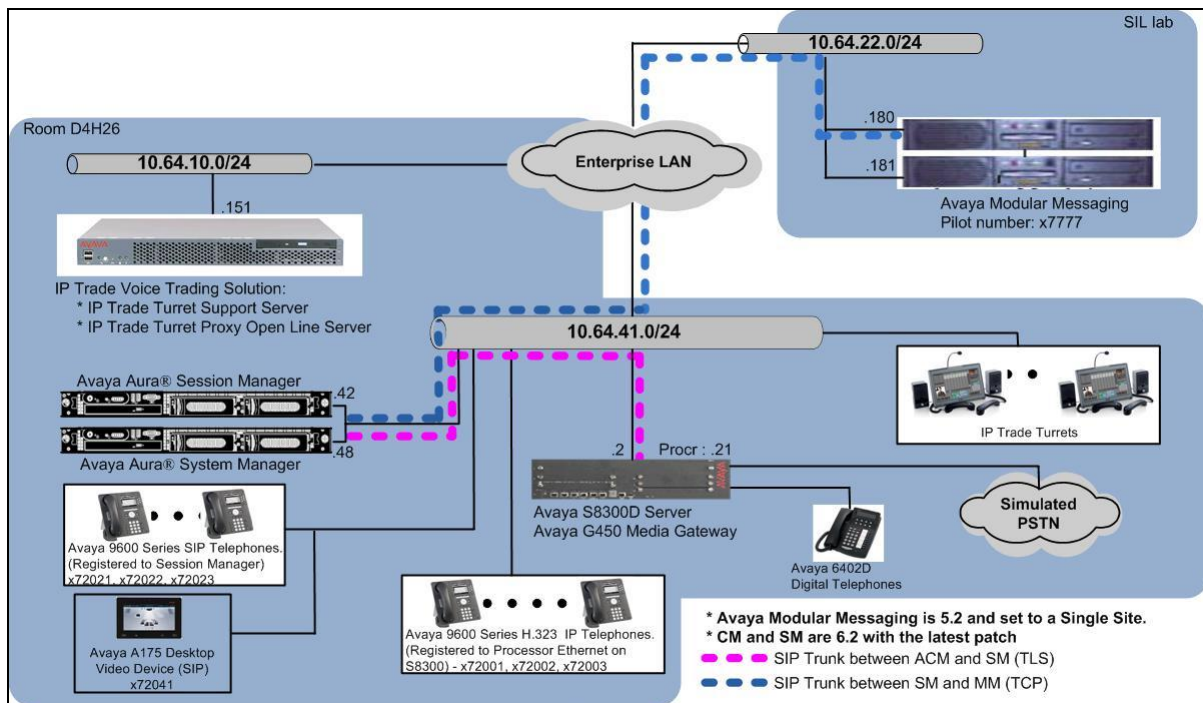

Figure 1: Test Configuration of IP Trade

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8300D Server	6.2 (R016x.02.0.823.0-20001)
Avaya Aura® Session Manager	6.2.2.0622005
Avaya Aura® System Manager	6.2.12.0

Avaya Modular Messaging
  • Messaging Storage Server
  • Messaging Application Server
	5.2 SP9 P4
	5.2 SP9 P4

Avaya A175 Desktop Video Device (SIP)	1.1.1
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 96xx IP Telephone (SIP)	2.6.8

IP Trade Voice Trading Solution
  • Turret Support Server
  • Turret Proxy to Open Line Dealing Server
  • IP Trade turret
	7.1.20852
	7.1.20843
	7.1.21096

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer public Unknown Numbering for PSTN

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

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

IP PORT CAPACITIES                                              USED
                   Maximum Administered H.323 Trunks: 4000      27
          Maximum Concurrently Registered IP Stations: 2400     3
             Maximum Administered Remote Office Trunks: 4000     0
Maximum Concurrently Registered Remote Office Stations: 2400     0
              Maximum Concurrently Registered IP eCons: 68       0
  Max Concur Registered Unauthenticated H.323 Stations: 100      0
                        Maximum Video Capable Stations: 2400     2
                  Maximum Video Capable IP Softphones: 2400      2
                     Maximum Administered SIP Trunks: 4000       70
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000     0
   Maximum Number of DS1 Boards with Echo Cancellation: 80       0
```

5.2. Administer SIP Trunk Group

Use the "add trunk-group n" command, where "n" is an available trunk group number, in this case "92". Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** "sip"
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** "tie"

```
add trunk-group 92                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 92                      Group Type: sip        CDR Reports: y
  Group Name: SM 41 42                      COR: 1     TN: 1      TAC: 1092
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                         Night Service:
Queue Length: 0
Service Type: tie                       Auth Code? n
                                                Member Assignment Method: auto
                                                         Signaling Group: 92
                                                       Number of Members: 10
```

Navigate to **Page 3**, and enter "private" for **Numbering Format**.

```
add trunk-group 92                                          Page   3 of  21
TRUNK FEATURES
         ACA Assignment? n          Measured: none
                                                        Maintenance Tests? y


                 Numbering Format: private
                                             UUI Treatment: service-provider

                                             Replace Restricted Numbers? n
                                             Replace Unavailable Numbers? n

                            Modify Tandem Calling Number: no
```

5.3. Administer SIP Signaling Group

Use the "add signaling-group n" command, where "n" is an available signaling group number, in this case "92". Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** "sip"
- **Transport Method:** "tls"
- **Near-end Node Name:** An existing C-LAN node name or procr.
- **Far-end Node Name:** The existing Session Manager node name.

- **Near-end Listen Port:** An available port for integration on Communication Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** A network region for integration with IP Trade turrets, in this case "1".
- **Far-end Domain** Set to "avaya.com"

```
add signaling-group 92                                       Page   1 of   2
                              SIGNALING GROUP

 Group Number: 92                     Group Type: sip
  IMS Enabled? n                  Transport Method: tls
       Q-SIP? n
    IP Video? y          Priority Video? n       Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM


     Near-end Node Name: procr                  Far-end Node Name: SM-1
  Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1


Far-end Domain:avaya.com
                                       Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate            RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload     Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3             IP Audio Hairpinning? n
        Enable Layer 3 Test? y           Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n     Alternate Route Timer(sec): 6
```

5.4. Administer IP Network Region

Use the "change ip-network-region n" command, where "n" is the existing far-end network region number used by the SIP signaling group from **Section 5.3**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Authoritative Domain:** "avaya.com"
- **Codec Set:** Set to "1"
- **Intra-region IP-IP Direct Audio:** "yes"
- **Inter-region IP-IP Direct Audio:** "yes"

```
change ip-network-region 1                                   Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                    Intra-region IP-IP Direct Audio: yes
     Codec Set: 1                   Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                          IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```

5.5. Administer IP Codec Set

Use the "change ip-codec-set n" command, where "n" is the codec set number from **Section 5.4**. Update the audio codec types in the **Audio Codec** fields as necessary.

Note that IP Trade supports the G.711MU and G.711A codecs. During the compliance test, G.711MU was utilized.

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

                         IP Codec Set

    Codec Set: 1

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

5.6. Administer Route Pattern

Use the "change route-pattern n" command, where "n" is an existing route pattern number to be used to reach IP Trade turrets, in this case "92". Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:**   A descriptive name.
- **Grp No:**   The SIP trunk group number from **Section 5.2**.
- **FRL:**   A level that allows access to this trunk, with 0 being least restrictive.

```
change route-pattern 92                                        Page   1 of   3
                    Pattern Number: 92  Pattern Name: no IMS SIP trk
                          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: 92   0                                                           n   user
2:                                                                  n   user

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

5.7. Administer Private Numbering

Use the "change private-numbering 0" command, to define the calling party number to send to IP Trade. Add an entry for the trunk group defined in **Section 5.2**. In the example shown below, all calls originating from a 5-digit extension beginning with 72 and routed to trunk group 92 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change private-numbering 0                              Page   1 of   2
                        NUMBERING - PRIVATE FORMAT


Ext Ext              Trk         Private          Total
Len Code             Grp(s)      Prefix           Len
5   72               92                           5       Total Administered: 10
5   72               93                           5          Maximum Entries: 540
```

5.8. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 7206x to IP Trade. Note that other methods of routing may be used. Use the "change uniform-dialplan 0" command, and add an entry to specify the use of AAR for routing digits 7206x, as shown below.

```
change uniform-dialplan 0                               Page   1 of   2
                     UNIFORM DIAL PLAN TABLE
                                                        Percent Full: 0


 Matching                    Insert              Node
 Pattern        Len Del      Digits      Net Conv Num
 7206           5   0                    aar  n
```

5.9. Administer AAR Analysis

Use the "change aar analysis 0" command, and add an entry to specify how to route calls to 7206x. In the highlighted example shown below, calls with digits 7206x will be routed using route pattern "92" from **Section 5.6**.

```
change aar analysis 0                                   Page   1 of   2
                        AAR DIGIT ANALYSIS TABLE
                             Location: all        Percent Full: 3


       Dialed          Total      Route    Call   Node  ANI
       String         Min  Max  Pattern    Type   Num   Reqd
 7206                  5    5      92       unku         n
```

5.10. Administer public Unknown Numbering for PSTN

Use the "change public-unknown-numbering 0" command, to define the calling party number to send to PSTN from IP Trade turrets. During the compliance test, the trunk group 80 was designated to go out to PSTN. In the example shown below, all calls originating from a 5-digit extension beginning with 7206 are routed to trunk group 80 will result in a 5-digit calling number.

```
change public-unknown-numbering 0                       Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext              Trk         CPN       CPN
Len Code             Grp(s)      Prefix    Len
                                                  Total Administered: 6
 5  7206             80                    5         Maximum Entries: 240
```

6. Configure Private Line Automatic Ringdown (PLAR)

This section describes the procedures for configuring Session Manager and Communication Manager to support PLAR trunks to the Financial Circuit Carrier Network.

To terminate the PLAR trunk facilities to the PSTN, a DS1 circuit pack using robbed-bit signaling must be administered. Enter "add ds1 xxyy", where "xxyy" is the Avaya Media Gateway slot where a DS1 circuit pack has been added, and enter the following values, retaining the defaults for the remaining fields:

- **Name**: Enter a descriptive name.
- **Line Coding**: Enter the line coding scheme to be used for this facility (typically, PLAR trunks use "b8zs").
- **Framing Mode**: Enter the framing mode to be used for this facility (typically, PLAR trunks use "esf" framing).
- **Signaling Mode**: Enter "robbed-bit".

```
change ds1 1a10                                              Page   1 of   2
                              DS1 CIRCUIT PACK


          Location: 01A10                            Name: IP Trade PLAR Trunk
          Bit Rate: 1.544                     Line Coding: b8zs
  Line Compensation: 1                        Framing Mode: esf
      Signaling Mode: robbed-bit




Interface Companding: mulaw
          Idle Code: 11111111






Slip Detection? n               Near-end CSU Type: other
```

6.1. Administer PLAR Trunk Group

To configure a PLAR trunk, enter "add trunk-group x", where "x" is an available trunk group to create a trunk group that will allow access to a given PLAR trunk. Enter the following values:

- **Group Type:**   Enter "tie".
- **Group Name:**   Enter a descriptive name.
- **TAC:**   Enter an available Trunk Access Code that is consistent with the provisioned dial plan. The TAC is entered at the Target in the respective TPO Place configuration.
- **Dial Access:**   Enter "y" to allow the PLAR trunk to be seized directly by the associated TPO Place, to connect with a specific remote location.
- **Incoming Destination:**   Enter the TPO Place Local extension associated with this PLAR trunk.
- **Trunk Type (in/out):**   Enter "auto/auto"

```
add trunk-group 11                                              Page   1 of  22
                              TRUNK GROUP

Group Number: 11                    Group Type: tie         CDR Reports: y
  Group Name: S8720-PRI trunk            COR: 1       TN: 1           TAC: 1011
    Direction: two-way       Outgoing Display? n Trunk Signaling Type:
 Dial Access? y              Busy Threshold: 255  Night Service:
Queue Length: 0                             Incoming Destination: 72065
   Comm Type: voice                     Auth Code? n
                                     Trunk Flash? n


Trunk Type (in/out): auto/auto
```

On **Page 2**, set the **Sig Bit Inversion** field to "A&B".

```
add trunk-group 11                                         Page   2 of  22
     Group Type: tie                 Trunk Type: auto/auto

TRUNK PARAMETERS
                                      Incoming Rotary Timeout(sec):5
    Outgoing Dial Type: tone                  Incoming Dial Type:tone
                                         Disconnect Timing(msec):500
     Digit Treatment:                                  Digits:
                                            Sig Bit Inversion: A&B
     Analog Loss Group: 9                    Digital Loss Group: 13
    Incoming Dial Tone? y
```

On **Page 6**, enter the **Port** location of the specific DS1 channel connected to the remote destination to be reached via the corresponding TPO Place. (This should be the only member of this trunk group.)

```
add trunk-group 11                                          Page   6 of  22
                              TRUNK GROUP
                           Administered Members (min/max):   1/1
GROUP MEMBER ASSIGNMENTS          Total Administered Members:   1

       Port    Code Sfx Name      Night          Mode      Type  Ans Delay
  1: 01A1001   TN464  F
```

7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Since IP Trade turrets are registered with Session Manager as SIP endpoints, this section only describes creating users.

Access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of the System Manager server. Log in using the appropriate credentials.

In the subsequent screen (not shown), select **Users → User Management** to display the **User Management** screen below. Select **Manage Users** from the left pane, and click **New** in the subsequent screen (not shown) to add a new user for the IP Trade turret solution. Users are required for the IP Trade Turret solution for the following purposes:

- Turret User Primary Extension assignment
- TPO lines linked to TPO Places for DDI Shared Lines
- TPO lines linked to TPO Places for (PLAR) private wire access to remote Financial locations

Note: IP Trade Turret Users can be configured to use only a Global Default DDI line, without any Turret User Primary Extension.

CRK; Reviewed:
SPOC: 3/7/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
14 of 41
IPTrade-SM62

When adding new SIP user, use the option to automatically generate the SIP station in Communication Manager, after adding a new SIP user. To create a new user, provide the following information:

Identity section
- **Last Name** – Enter last name of user.
- **First Name** – Enter first name of user.
- **Login Name** – Enter extension number@sip domain. The sip domain is defined as Authoritative Domain in **Section 5.3**.
- **Authentication Type** – Verify **"Basic"** is selected.
- **Password** – Enter password to be used to log into System Manager.
- **Confirm Password** – Repeat value entered above.

Communication Profile section

- **Communication Profile Password** – Type Communication profile password in this field. This password is used when registering a SIP endpoint to the SM.
- **Confirm Password** – Repeat value entered above.

Communication Profile sub-section

- **Fully Qualified Address** – Enter the extension of the user
- Click **Add** button

<u>Session Manager Profile section</u>
- **Primary Session Manager** – Select one of the Session Managers.
- **Origination Application Sequence –** Select Application Sequence defined for Communication Manager.
- **Termination Application Sequence** – Select Application Sequence defined for Communication Manager.
- **Home Location** – Select Location defined.

Endpoint Profile section
- **System** – Select Managed Element.
- **Profile Type** – Select **Endpoint**.
- **Use Existing Endpoints -** Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
- **Extension** - Enter same extension number used in this section.
- **Template** – Select template for type of SIP phone
- **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.
- **Port** – Select **IP**
- **Voice Mail Number** – Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank. This feature is not used during the compliance test.
- **Delete Endpoint on Unassign of Endpoint from User or on Delete User**– Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

Repeat above step as necessary to configure additional extension. During the compliance test, the following extensions were created:
- 72061- 72063 – (3) IP Trade Turret Users
- 72064 – Risk Dept. Line
- 72065 – Simulated Ring-down (PLAR). Refer to **Section 6.1**

CRK; Reviewed:
SPOC: 3/7/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

18 of 41
IPTrade-SM62
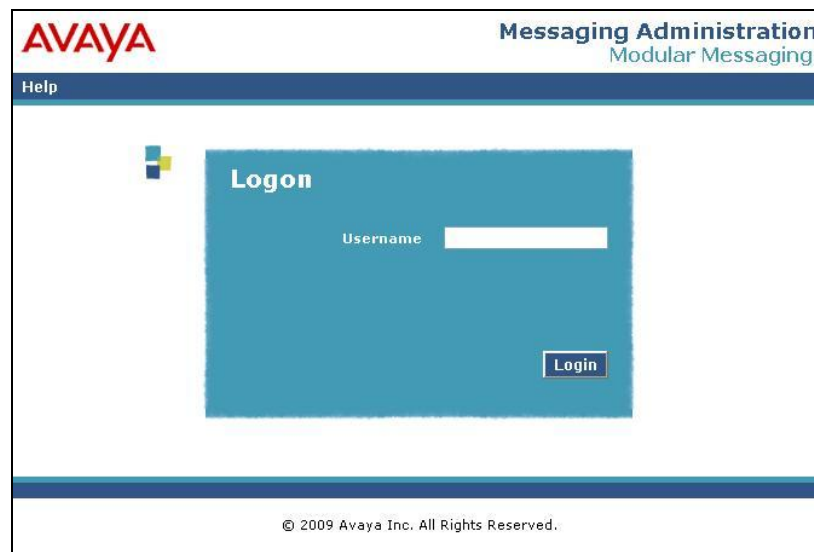
8. Configure Avaya Modular Messaging MSS

This section provides the procedures for configuring IP Trade turret users as local subscribers on Avaya Modular Messaging. The subscriber management is configured on the Messaging Storage Server (MSS) component. The configuration procedures include the following areas:

- Launch messaging administration
- Administer subscriber extension ranges
- Administer subscribers

8.1. Launch Messaging Administration

Access the MSS web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of the MSS server. The **Logon** screen is displayed. Log in using a valid user name and password. The **Password** field will appear after a value is entered into the **Username** field. The **Messaging Administration** screen appears (not shown).

8.2. Administer Subscriber Extension Ranges

Select **Messaging Administration** → **Networked Machines** from the left pane, to display the **Manage Networked Machines** screen. Select the MSS server from the table listing, and click **Edit the Selected Networked Machine** toward the bottom right of the screen.

The **Edit Networked Machine** screen is displayed. Under the **MAILBOX NUMBER RANGES** section, locate an available entry line and enter the desired starting and ending mailbox numbers to be used for the IP Trade subscribers as necessary. In the compliance testing, the existing entry covered the 7206x extensions used by the IP Trade turret users.

8.3. Administer Subscribers

Select **Messaging Administration → Subscriber Management** from the left pane, to display the **Manage Subscribers** screen. For the **Local Subscriber Mailbox Number** field toward the top of the screen, enter the first IP Trade turret user extension to add as a local subscriber, in this case "72061". Click **Add or Edit**.

The **Add Local Subscriber** screen is displayed next. Enter the desired string into the **Last Name**, **First Name**, and **Password** fields.

In the compliance testing, the same telephone extensions for the IP Trade subscribers were used for the **Mailbox Number**, **Numeric Address** fields. Select the appropriate **Class Of Service**, and retain the default values in the remaining fields.

Scroll down to the bottom of the screen and click **Save** (not shown). Repeat this section to add all IP Trade subscribers.

9. Configure IP Trade Turret Support Server

The configuration of IP Trade TSS Administration Console is typically performed by IP Trade installation technicians, and procedures are provided by an IP Trade engineer. The procedural steps are presented in these Application Notes for informational purposes.

This section describes the procedure for configuring the IP Trade TSS to create and manage User/Shared Profiles, TPO Lines and Places for DDI Lines & PLAR trunks, including FTP Settings for high level common turret settings.

From a Web browser, navigate to http://<ip-addr>/iptradenet.console, where <ip-addr> is the IP address of the TSS. After logging in with an appropriate set of credentials, the main page appears.
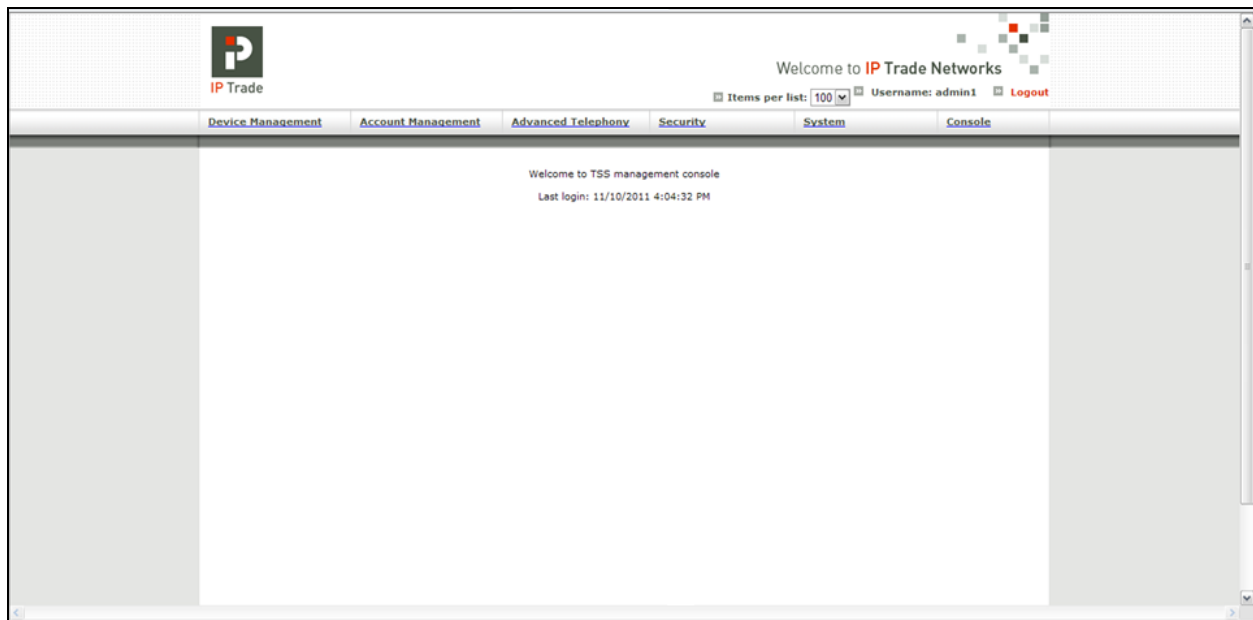
9.1. Configure FTP Settings

On the TSS administration console from the top menu bar, select **System → Settings → FTP settings** (not shown). Be sure that the version and file options are the one that will be applied to your running turret firmware. Select "SIP" on the left pane (not shown), and click the "**Basic Mode**" tab on the top menu. Provide the following:

- **SIP local domain:** Enter "avaya.com".
- **SIP Server Name:** Enter IP address of Session Manager.
- **SIP Proxy address:** Enter IP address of Session Manager.
- **SIP Connection mode:** Select "TCP" from drop down menu
- **SIP Proxy Transport:** Select "TCP" from drop down menu
- **Fast media connection on SIP Ringing state:** Select "true"
- **SIP Local IP Ports:** Enter "5060"

Click the **Update** button to update the changes.

Click the "**Expert Mode**", and provide the following:
- **Allow sip header in Register message:** Select "true" from drop down menu
- **Enable TCP on SIP stack** (not shown)**:** Select "true"
- **SIP Diversion Header Name** (not shown)**:** Enter "History-Info"

Click the **Update** button (not shown) to update the changes.

CRK; Reviewed:
SPOC: 3/7/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
25 of 41
IPTrade-SM62

9.2. Configure Turret Proxy to Open Line Dealing (TPO) Settings

Navigate to **Device Management** → **Settings** → **Basic Mode** to configure Basic TPO Cluster SIP Settings. Select SIP on the left pane, and provide the following:
- **SIP local domain:** Enter "avaya.com".
- **SIP Server Name:** Enter IP address of Session Manager.
- **SIP Proxy address:** Enter IP address of Session Manager.
- **SIP Connection mode:** Select "TCP/IP" from drop down menu
- **SIP Proxy Transport:** Select "TCP/IP" from drop down menu
- **Early media mixing:** Select "true"
- **SIP Local IP Ports:** Enter "5060"
- **Check replace header on incoming call:** Select "true"

Click the **Update** button to update the changes.

Device Management	Account Management	Advanced Telephony	Security	System	Console

Back to TPO Cluster list >

General   **Settings**   TPO Cluster   TPO Places   TPO Lines

Settings

Basic Mode   Expert Mode   Advanced Mode

	Name	Value	Description
Global	☑ SIP local domain	avaya.com	⊙
Media	☑ SIP Proxy addresses	10.64.41.42	⊙
SIP	☑ SIP Server Name	10.64.41.42	⊙
	☑ SIP Connection mode	TCP ▾	⊙
Cluster	☑ SIP Proxy Transport Type	TCP ▾	⊙
Recorder	☑ Early media mixing	◉ true ○ false	⊙
	☐ SIP Local IP Ports	5060	⊙
	☐ Use bulk registration (Cisco only)	○ true ◉ false	⊙
	☑ Check replace header on incoming call	◉ true ○ false	⊙

[Update] [Refresh]   Updated.

Navigate to **Device Management** → **Settings** → **Expert Mode** to configure Expert TPO Cluster SIP Settings. Select SIP on the left pane, and provide the following:
- **Enable TCP on SIP stack:** Select "true"
- **Add Remote party ID header on registered line:** Select "true"
- **Ringing remote party ID header:** Enter "P-Asserted-Identity"
- **Allow sip header in Register message** (not shown)**:** Select "true" from drop down menu
- **User subscription for MWI :** Select "true"

Click the **Update** button to update the changes.

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

9.3. Configure Turret Proxy to Open Line Dealing (TPO) Lines & Turret Proxy to Open Line Dealing (TPO) Places

Navigate to TPO Lines tab to add a TPO line. Provide the following information:

- **Local Extension:** Enter an extension created in **Section 7**.
- **Register:** Select "Yes".
- **SIP Display Name:** Enter a descriptive name to be used.
- **SIP Password:** Enter the password created in **Section 7**.
- **SIP Digest:** Enter the same extension created in **Section 7**.
- **SIP Domain:** Enter "avaya.com".
- **Access Point Extension:** Select "No".

Click the **Save and Go Back** button.

Repeat above step as necessary to configure additional extensions.

The following screen shows the TPO lines created during the compliance test.

Navigate to TPO Place tab and select "Add New" (not shown) to create a TPO Place. Provide the following information as shown below:

- **Name:** Enter a descriptive name to identify the TPO Place
- **Group ID:** Select the appropriate ID for the respective TPO Cluster
- **Place Type:** Select "RingdownDynamic" from the drop down.
- **VirtualSlot Extensions:** This defines the number of call appearance for the respective extension, these are called DDI Slots and are shared on the IP Trade Turrets. In this example, the TPO Place configured is for extension 72061 which will have 3 shared DDI Slots (appearances). Therefore the following was entered as shown below: 7206101 - 7206203
- **Conference Mode:** All (Default value)
- **Local Extensions:** Click on the "+ Defined Lines" to select the corresponding TPO Line that should be linked to this TPO Place. For this example, select "72061" from the list and press the "Link Selected" button.

Click the **Save and Go Back** button (not shown).

Repeat above step as necessary to configure additional TPO Places.

9.3.1. Configure Turret Proxy to Open Line Dealing (TPO) Place for Automatic Ringdown (PLAR)

Navigate to TPO Place tab and select "Add New" (not shown) to create a TPO Place. Provide the following information:

- **Name:** Enter a descriptive name to identify the TPO Place
- **Group ID:** Select the appropriate ID for the respective TPO Cluster
- **Place Type:** Select "RingdownDynamic" from the drop down.
- **VirtualSlot Extensions:** This defines the number of call appearance for the respective extension called DDI Slots shared on the IP Trade Turrets. In this example, the TPO Place configured is for extension 72065 which only requires a single appearance and is equal to the "Incoming Destination" assigned for Automatic Ring-down (PLAR) Trunk Group. [Refer to **Section 6.1**].
  - o The following was entered as shown below: 72065 – 72065**.**
  - o Enter a check mark to assign the Virtual Slot Extension as Defined Slots.
  - o Click on the "+Defined Slots" button and select the Virtual Slot Extension.
  - o Press on the "Link Selected" button to link the Defined Slot to the TPO Place.
  - o Modify the Slot Properties and assign Target: Press the "Mouse" icon as shown below by the red arrow to modify slot properties and assign the TAC in the "Target" field to the corresponding PLAR Trunk Group [Refer to **Section 6.1**]. Set the Slot Type to "Ringdown" and the other fields as shown below. Press the green check mark to save the changes.
- **Conference Mode:** All (Default value)
- **Local Extensions:** Click on the "+ Defined Lines" button and select the corresponding TPO Line that should be linked to this TPO Place. For this example, select "72065" from the list and press the "Link Selected" button.

Click the **Save and Go Back** button.

Repeat above step as necessary to configure additional TPO Places.

Note: It is recommended to add mutliple PLAR Trunks using the same TPO Place by adding mutliple Virtual Slot Extension and cooresponding Local Extensions. The following screen shows the TPO lines created during the compliance test:
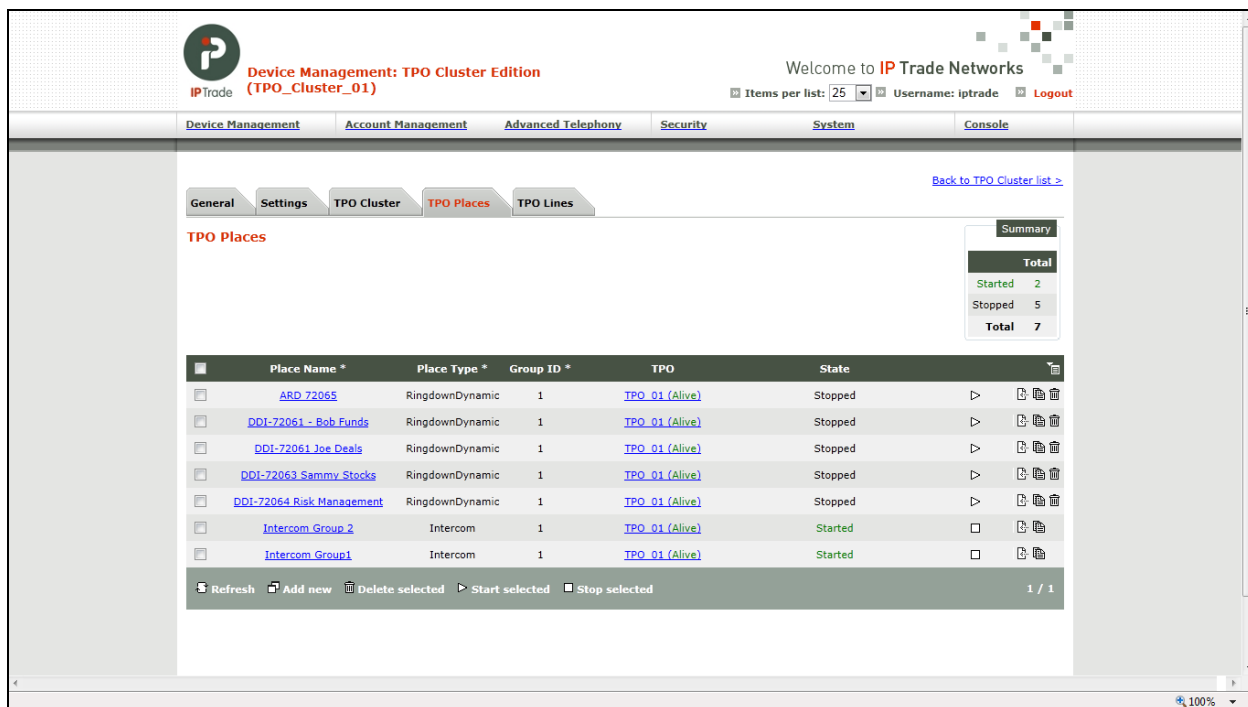
Starting the TPO Place, registers the corresponding TPO Line to Session Manager. To change the state to "Started", select the TPO Place(s) and then press "Start selected" icon.

9.4. Administer Lines in Shared Profile

These Application Notes assume that Shared Profiles are pre-configured for the respective users who are in the same Trading Group. Shared Profiles allow setting of Lines, Settings, Turret Layout settings, Shortcut Pages and Shortcuts (buttons) that are common to the users in the same Trading Group.

Navigate to "Account Management" on the top menu bar and select "Shared Profiles" (not shown). Click the Shared Profile you wish to change and then select the "Lines" tab (not shown). Click on "Add New" to assign a Line to the Shared Profile. Provide the following information as shown below:

- **Type:** Choose "DDI Shared Line" from the drop down list.
- **Subscribe to Notifications:** Must be set to "Yes" (Default value).
- **Extension:** Enter the Local Extension as defined in the corresponding TPO Place
- **TPO Group Name:** Select the name the TPO where the DDI Shared Line is hosted
- **SIP Display Name:** Enter a descriptive name for the Line.

The assignment of all other fields were set to default parameters for this line in the Shared Profile. Press "Update" to commit changes. Repeat the process above to add all Shared DDI Lines and PLAR Lines that will be part of the Shared Profile.

The following screen shows the Lines assigned to the respective Shared Profile during the compliance test:

CRK; Reviewed:
SPOC: 3/7/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
34 of 41
IPTrade-SM62

9.5. Administer Inherited Lines in the User Profile

These Application Notes assume that User Profiles are pre-configured for the respective users and are assigned to a Shared Profile for the Trader Group. Lines, Settings, Turret Layout settings, Shortcut Pages and Shortcuts (buttons) assigned in the Shared Profile are inherited values and settings in the User Profile. The User Profile allows for changes to values set in the Shared Profile for user customization.

Navigate to **Account Management → Users** and select a previously created User. Select the "Lines" tab. The Lines shown below are inherited in the User Profile from the Shared Profile.

For this example, User Profile "Bob Funds" was chosen and assigned to extension 72061 inhereted and configued in the respective Shared Profile that User "Bob Funds" is associated with. Select DDI Shared Line "Bob Funds" to change the inhereted parameter values for his Line 72061. To change the inhereted values, place a check mark to the following parameters and adjust the value as shown below:

For example:

- **In Call History:** Inherited value is "No". Change to "Yes" to record call history for this line.
- **Msg Waiting Indicator:** Inherited value is "No". Change to "Yes" to enable MWI notification for this line.

- **Global Default Line:** Inherited value is "No". Change to "Yes" to set this line as the default line for the user on his turret. If no Primary Extension is assigned, the Global Default Line becomes the Primary Extension for the turret user.

Press **Update** to commit changes.

Repeat the process in each User Profile as necessary.

The following screen from the User Profile shows the Lines that have values different than the inherited value with an asterisk "inherited *".

CRK; Reviewed:
SPOC: 3/7/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
37 of 41
IPTrade-SM62

9.6. Administer DDI Slot Buttons in Shared or User Profile

Every VirtualSlot Extension assigned to a TPO Place of a Shared DDI line (or Shared DDI Line with Slot Properties for a PLAR Line) must have its corresponding DDI slot shortcut (button) created in the Shared or User Profile. However, it is not mandatory to create each DDI slot in each user profile. User or IT administrator should create the DDI slot shortcuts (buttons) that will be effectively used by the turret user. These shortcuts(buttons) can be positioned in one of its home pages or Shortcut (button) applets. The system will automatically generate any missing DDI slot shortcuts(buttons) during line registration, but these will have no assigned ringtone. Those automatically generated shortcuts(button) are grouped in a page called "Missing DDI Slots". It is recommend to create as many DDI Slot shortcuts (buttons) as configured number of VirtualSlot Extensions.

Shortcuts(buttons) can be programmed from the TSS administration console or directly from the turret. Although not mandatory, it is advisable to have these buttons closely grouped in the same area of the screen; From the TSS administration Console, please proceed as follows to manually create DDI slot buttons (not shown):

1. Navigate to the desired User or Shared Profile to create the DDI Slots. ;
2. Go to the Shortcut tab.

 (It is assumed that a Shortcut Page is preconfigured and assigned to the Turret Layout.
3. Select the proper Shortcut Page and then click on "Add new" on the buttom of the page.
4. **Label:** Enter a descriptive label for the DDI Slot
    a.   For Example: "72061 Line 1"
5. **Type:** Select "DDI Slot" from the drop down list
6. **Phone extension:** Enter the cooresponding VirtualSlot Extension.
    a.   For this example enter "7206101"
7. Click on the "Add and Continue" to save the entry and add the next DDI Slot.

Repeat the procedure to add all necessary DDI Slots in the User or Shared Profile for Shared DDI Lines or Ringdowns (PLAR).

Note: While the system automatically creates any missing DDI slot key when the user subscribes to a line, it does not automatically remove it when the user unsubscribes or manually creates a private slot key in the user profile. Also note that removing a DDI slot key in the user profile while the user is authenticated is highly discouraged, because it would leave a slot without any key associated.

9.7. Administer Avaya Modular Messaging Pilot Extension

Navigate to Account Management → Shared Profiles (not shown) and select pre-configured Shared Profile for the Trading Group. Select the "Settings" and then "User Settings" on the left pane, and set the following as shown below:

- **Voicemail:** Set the assgined Modular Messaging Pilot Extension

Press **Update** to commit changes.

CRK; Reviewed:
SPOC: 3/7/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

39 of 41
IPTrade-SM62

10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Modular Messaging, Avaya Aura® Session Manager, and IP Trade Voice Trading Solution.

- Place a call from an IP Trade turret user to the Modular Messaging pilot number. Verify that Modular Messaging recognizes the calling party as a local subscriber.
- Place calls from an IP Trade turret to SIP, H323, and PSTN endpoints and verify that the calls are successfully established with two-way talk path.

11. Conclusion

These Application Notes describe the configuration steps required for IP Trade Voice Trading Solution 7.1 to successfully interoperate with Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2, and Avaya Modular Messaging 5.2 in a centralized messaging environment using SIP trunks. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

12. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 7.0, Release 6.2, July 2012, available at http://support.avaya.com.

2. *Administering Avaya Aura® Session Manager*, Document Number 03-603324, Release 6.2, July2012, available at http://support.avaya.com.

3. *Avaya Modular Messaging for the Avaya Message Store Server (MSS) Configuration,* Release 5.2, August 2012, available at http://support.avaya.com.

IP Trade Voice Trading Solution and Product information is available from IP Trade. Visit http://www.IPTrade-networks.com/turret.html.
For additional information or documentation, please contact your local IP Trade office. Visit http://www.iptrade-networks.com/other_inquiry.html.

CRK; Reviewed:
SPOC: 3/7/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
40 of 41
IPTrade-SM62

©2013 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.