Avaya Solution & Interoperability Test Lab

Application Notes for Configuring H.323 Trunking between AGN Networks OnDemand H323 Service and an Avaya IP Telephony Solution – 1.0

Abstract

These Application Notes describe the procedure for configuring H.323 trunking between Avaya Communication Manager and the AGN Networks OnDemand H.323 service, in order to place calls to and from the Public Switched Telephone Network. The Avaya solution consisted of Avaya Communication Manager, and various Avaya digital, analog and H.323 endpoints.

Enterprise customers with this Avaya based H.323 solution can connect via a dedicated Internet connection using AGN Networks as a service provider to make and receive PSTN calls. This includes outbound local, long distance and international calling, inbound calling to DID numbers from most major US cities and inbound toll-free calling. This solution allows customers with a converged network to lower PSTN telecommunications costs, to obtain local number presence without offices in each geographic area, and to easily manage their network services using a web-based user interface.

AGN Networks is a member of the Avaya Developer*Connection* Service Provider program. Information in these Application Notes has been obtained though compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedure for configuring H.323 service between Avaya Communication Manager and AGN Networks H.323 gateway, in order to place calls to and from the Public Switched Telephone Network. The Avaya solution consists of Avaya Communication Manager and Avaya digital, analog and H.323 IP telephony endpoints.

Customers using this Avaya IP telephony solution with the AGN Networks OnDemand H.323 service are able to place and receive PSTN calls via a dedicated broadband Internet connection using the H.323 family of protocols. This converged network solution is an alternative to more traditional PSTN analog and digital trunks. It allows customers to possibly lower local and long distance costs, add and delete DID and toll-free numbers in minutes, as well as to benefit from capabilities such as having local numbers from numerous area codes easily terminated at a single location.

The AGN Networks OnDemand H.323 service covered by this solution include:

- Outbound calling to local, long distance and international locations
- Incoming Direct Inward Dialing (DID) service from most major cities in the US
- Incoming toll-free calling

Figure 1 illustrates a typical Avaya IP telephony solution at an enterprise site connected to AGN Networks OnDemand H.323 service using H.323 trunking. This is the configuration used during the Developer*Connection* compliance testing process. All IP addresses used were within the public address space. For PSTN calls to and from the Enterprise site, the Avaya Media Server exchanges H.323 signaling messages with the AGN Networks H.323 gateway which is a Nextone Multi-protocol Session Controller (MSC).

The Avaya IP telephony solution located on the enterprise site consisted of:

- Avaya S8300 Media Server installed into an Avaya G350 Media Gateway. The S8300 served as the host processor for Avaya Communication Manager.
- Avaya 9630 IP telephone configured to use the H.323 protocol.
- Avaya 4620 IP telephone configured to use the H.323 protocol.
- Avaya 6416 digital and 6211 analog telephones.

Note: Security devices, such as firewall and network address translation (NAT) devices, were not included in the tested compliance configuration show in **Figure 1**. These Application Notes focus on H.323 trunking interoperability. However, **Appendix A** shows the configuration below with a Cisco Pix 525 firewall device integrated with a typical configuration for network address translation (NAT). A subset of the main test plan was rerun with the configuration in **Appendix A**. Although all tests passed, this testing is not part of the compliance tested configuration in **Figure 1**.

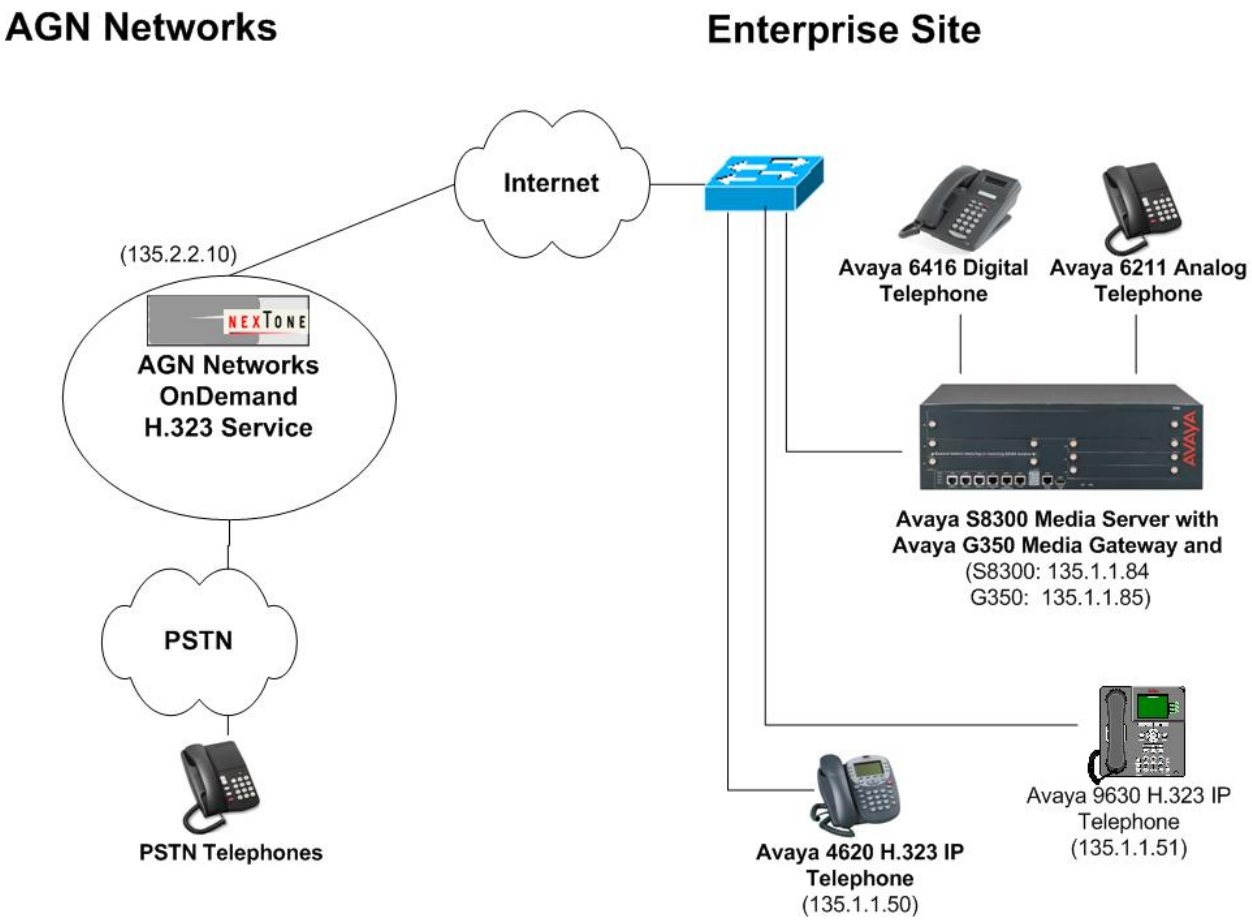

Figure 1: AGN Networks OnDemand H.323 Service Test Bed Configuration

2. Equipment and Software Validated

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

Hardware Component	Version
Avaya S8300 Media Server with an Avaya G350 Media Gateway	Communication Manager 3.1.2 R013x.01.2.632.1 Update: 01.2.632.1-12866
Avaya 4620 H.323 IP Telephones (H.323)	2.7
Avaya 9630 H.323 IP Telephones (H.323)	1.2
Avaya 6416 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
AGN Networks H.323 Gateway	Nextone MSC v4.0.c3-28

3. Configure Avaya Communication Manager

This section describes the steps for configuring H.323 trunks on Avaya Communication Manager. The H.323 trunks are established between Avaya Communication Manager and AGN Networks. These trunks will carry the H.323 signaling and RTP voice packets sent to AGN Networks.

H.323 signaling messages for all incoming calls from AGN's On Demand H.323 service are received by Avaya Communication Manager via the H.323 trunks. Incoming call treatment, such as performing incoming digit translations, may be performed as necessary. All outgoing calls to the PSTN via AGN's On Demand H.323 service are routed through Avaya Communication Manager in order to use features such as automatic route selection and class of service restrictions. Avaya Communication Manager creates the outbound H.323 signaling that is routed to AGN Networks. Note that Avaya Communication Manager acts as a H.323 proxy through which all incoming and outgoing H.323 messages flow to AGN Networks.

The dial plan for the configuration described in these Application Notes consisted of 10-digit dialing for local and long-distance calls over the PSTN. International calls (011+Country Code) were also supported. Operator calls (0), Directory Assistance calls (411) and Emergency calls (911) were not supported at the time of testing. However, Directory assistance calls (411) and Emergency calls (911) are expected to be offered in the near future. Avaya Communication Manager routed all calls using Automatic Route Selection (ARS), except for intra-switch calls.

Avaya Communication Manager configuration was performed using the System Access Terminal (SAT). The IP network properties of the Avaya S8300 Media Server were configured via its Maintenance web interface using an Internet browser (not shown here).

3.1 Configure Special Applications

Use the command **display system-parameters special-applications** and page forward to Page 4 to verify that the feature **(SA8507) - H245 Support With Other Vendors** is enabled. SA8507 must be enabled to achieve the interoperability documented in these Application Notes. If SA8507 is not enabled, contact your authorized Avaya sales representative.

```
change system-parameters special-applications                    Page   4 of   6
                              SPECIAL APPLICATIONS
     (SA8481) - Replace Calling Party Number with ASAI ANI? n
               (SA8500) - Expanded UUI Display Information? n
                 (SA8506) - Altura Interoperability (FIPN)? n
                (SA8507) - H245 Support With Other Vendors? y
                (SA8508) - Multiple Emergency Access Codes? n
 (SA8510) - NTT Mapping of ISDN Called-Party Subaddress IE? n
                      (SA8517) - Authorization Code By COR? n

   (SA8518) - Automatic Callback with Called Party Queuing? n
          (SA8520) - Hoteling Application for IP Terminals? n
  (SA8558) - Increase Automatic MWI & VuStats (S8700 only)? n

                 (SA8567) - PHS X-Station Mobility over IP? n
       (SA8569) - No Service Observing Tone Heard by Agent? n
                 (SA8573) - Call xfer via ASAI on CAS Main? n
          (SA8582) - PSA Location and Display Enhancements? n
               (SA8587) - Networked PSA via QSIG Diversion? n
                        (SA8589) - Background BSR Polling? n
     (SA8608) - Increase Crisis Alert Buttons (S8700 only)? n
                      (SA8621) - SCH Feature Enhancements? n
```

Figure 4: System-Parameters Special-Applications Form

3.2 Configure the Node Names Form

In the **IP Node Names** form, assign the node name and IP address for the AGN Networks H.323 server and the Avaya S8300 Media Server. In this case **agn-network1** and **135.2.2.10** will be used as the AGN gateway while **procr** and **135.1.1.84** are the name and IP address assigned to the S8300 Media Server.

```
change node-names ip                                             Page   1 of   1
                                  IP NODE NAMES
    Name              IP Address          Name              IP Address
agn-network1        135 . 2. 2. 10                           .   .   .
default             0  .0  .0  .0                          .   .   .
procr               135.  1. 1. 84                          .   .   .
                       .   .   .                           .   .   .
                       .   .   .                           .   .   .
 ( 6  of 6    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Figure 5: IP Node-Names Form

3.3 Configure the IP Network Region Form

The **IP Network Region** form defines the parameters associated with the H.323 trunk and signaling group. In the **IP Network Region**, configure the following settings relevant to this application:

- By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints (H.323 IP Phones), without using media resources in the Avaya G350 Media Gateway. For this solution, testing verified that calls work with **IP-IP Direct Audio** enabled and disabled, (yes/no in the form). Therefore, this feature can be enabled/disabled at the customer's discretion and based upon their specific needs.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within IP network region 1. In this configuration, this codec set will apply to calls with AGN Networks as well as any IP phone (H.323) within the enterprise.

In this case, the signaling group is assigned to the same IP network region as the G350 Media Gateway. If multiple network regions are used, Page 3 of each **IP Network Region** form must be used to specify the codec set for inter-region communications.

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name: IP Phones/Sip Trunk
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 65531
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 6: IP-Network-Region Form

3.4 Configure the IP Codec Set Form

Open the **IP Codec Set** form using the ip-codec value specified in the **IP Network Region** form (**Figure 6**) and enter the audio codec type to be used for calls routed over the H.323 trunk. The recommended settings of the **IP Codec Set** form are shown in **Figure 7.** While G.729a was tested successfully as well, AGN Networks recommends that G.711mu be used for better quality DTMF tones. Note that the **IP Codec Set** form may include multiple codecs listed in priority order to allow the codec for the call to be negotiated during call establishment.

```
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:
```

Figure 7: IP Codec Set Form Page 1

T.38 Fax mode is not supported by AGN Networks. Therefore, in order to send fax transmission via an analog POTS line using G.711mu codec, set the fields **FAX** and **Modem** to **off** as shown below in **Figure 8**:

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

                         IP Codec Set

                             Allow Direct-IP Multimedia? n


                     Mode               Redundancy
    FAX              off                 0
    Modem            off                 0
    TDD/TTY          off                 3
    Clear-channel    n                   0
```

Figure 8: IP Codec Set Form Page 2

3.5 Configure the Signaling Group

Administer a signaling group by entering **change signaling-group n,** where n is the number of the signaling group number.

- **Group Type**: Enter **h.323**.
- **Near End Node Name:** This setting depends upon which Avaya Media Server and Media Gateway is being used. Since the Avaya S8300 Media Server is being used with the G350 Media Gateway, enter **procr** as the near-end of the signaling group.
- **Far End Node Name:** Far-end is set to **agn-network1** (the IP address of AGN Network IP gateway).
- **Near End Listen Port:** Enter **1720** as the near-end listen port.
- **Far End Listen Port:** Enter **1720** as the far-end listen port.
- **Far-end Network Region:** field is set to **1**, this should match the IP Network Region form created in **Figure 6**.
- **Direct IP-IP Audio Connections** – This field can be set to **y** or **n** in order to enable/disable direct IP audio. This setting should match the setting configured in IP Network Region form created in **Figure 6**. This setting will allow Avaya IP Telephones to use the resources of the G350 media processors or forgo them and send the media stream directly to the AGN gateway.
- **DTMF over IP**: Set this field to **in-band**, the recommended setting of AGN Networks.
- **Trunk Group for Channel Selection:** This field associates a trunk group with this signaling group. Since the trunk group has not been created yet, this field will be left blank. Once the trunk group is created as described in the next section, (**Section 3.6** of this document), return to this form and add the number of the trunk group to this field, this step is detailed in **Section 3.7**.

```
add signaling-group 1                                        Page   1 of   5
                                SIGNALING GROUP

 Group Number: 1                Group Type: h.323
                              Remote Office? n          Max number of NCA TSC: 0
                                        SBS? n           Max number of CA TSC: 0
                                   IP Video? n        Trunk Group for NCA TSC:
      Trunk Group for Channel Selection:
         Supplementary Service Protocol: a          Network Call Transfer? n
                          T303 Timer(sec): 10

  Near-end Node Name: procr                   Far-end Node Name: agn-network1
Near-end Listen Port: 1720                  Far-end Listen Port: 1720
                                          Far-end Network Region: 1
        LRQ Required? n                    Calls Share IP Signaling Connection? n
        RRQ Required? n                          H245 Control Addr On FACility? n
    Media Encryption? n                      Bypass If IP Threshold Exceeded? n
                                                    H.235 Annex H Required? n
        DTMF over IP: in-band                Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? n
                                               Interworking Message: PROGress
                                          DCP/Analog Bearer Capability: 3.1kHz
```

Figure 9: Signaling Group Form

3.6 Configure the Trunk Group

Configure an H.323 IP trunk by adding a trunk group. Enter the **add trunk-group n** command, where **n** is the trunk group number. Administer the trunk group parameters, with the following settings

- **Group Type:** Enter **isdn**.
- **TAC:** Enter an available trunk access code, such as **101**.
- **Carrier Medium:** Enter **H.323**.
- **Service Type:** Enter **public** to set this as an IP tie trunk between the two servers.
- **Signaling Group:** Enter the number of the corresponding signaling group created in **Figure 9**, in this case the value is **1**.
- **Number of Members:** Add the appropriate value per the system's capabilities.

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

Group Number: 1                     Group Type: isdn          CDR Reports: y
  Group Name: AGN Networks H.323          COR: 1        TN: 1        TAC: 101
   Direction: two-way         Outgoing Display? n         Carrier Medium: H.323
 Dial Access? y                 Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: public                 Auth Code? n
                                          Member Assignment Method: auto
                                                    Signaling Group: 1
                                                  Number of Members: 10
```

Figure 10: Trunk Group Form

3.7 Associate the Signaling Group to the IP Trunk Group

Return to the signaling group created in **Section 3.5.** Use the **change signaling-group <group_number>** command to modify the group for the **Trunk Group for Channel Selection** field as shown in **Figure 11** below. Again, this value needs to match the number of the trunk group created in **Section 3.6**. In this case, the value is **1**.

```
change signaling-group 1                                        Page   1 of   5
                              SIGNALING GROUP

 Group Number: 1              Group Type: h.323
                            Remote Office? n          Max number of NCA TSC: 0
                                      SBS? n           Max number of CA TSC: 0
                                 IP Video? n        Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 1
          Supplementary Service Protocol: a          Network Call Transfer? n
                          T303 Timer(sec): 10

   Near-end Node Name: procr                  Far-end Node Name: agn-network1
 Near-end Listen Port: 1720                 Far-end Listen Port: 1720
                                          Far-end Network Region: 1
         LRQ Required? n                   Calls Share IP Signaling Connection? n
         RRQ Required? n                         H245 Control Addr On FACility? n
     Media Encryption? n                       Bypass If IP Threshold Exceeded? n
                                                        H.235 Annex H Required? n
         DTMF over IP: in-band                  Direct IP-IP Audio Connections? y
                                                          IP Audio Hairpinning? n
                                                  Interworking Message: PROGress
                                         DCP/Analog Bearer Capability: 3.1kHz
```

Figure 11: Signaling Group Form

3.8 Configure Calling Party Number Information

Use the **change public-unknown-numbering <extension_length>** command to configure the system to send the full calling party number to the far-end.

In this case, all stations with a 5-digit extension beginning with 7 should send the calling party number 732-85x-xxxx when an outbound call uses H.323 trunk group 1. This calling party number will be sent to the far-end.

```
change public-unknown-numbering 0                               Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                    Total                                 Total
Ext Ext    Trk       CPN            CPN Ext Ext    Trk       CPN            CPN
Len Code   Grp(s)    Prefix         Len Len Code   Grp(s)    Prefix         Len

 5  7      1         73285          10
```

Figure 12: Numbering Public/Unknown Format Form

3.9 Automatic Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the H.323 trunk to the AGN Networks OnDemand H.323 service to a PTSN destination.

Use the **change dialplan analysis** command to add **9** as a feature access code (**fac**).

```
change dialplan analysis                                    Page   1 of  12
                           DIAL PLAN ANALYSIS TABLE
                                                        Percent Full:    3

     Dialed  Total  Call      Dialed  Total  Call      Dialed  Total  Call
     String  Length Type      String  Length Type      String  Length Type
       1       3    dac
       7       4    ext
       8       4    ext
       9       1    fac
       *       3    fac
       #       3    fac
```

Figure 13: Change Dialplan Analysis Form

Use the **change feature-access-codes** command to specify **9** as the access code for outside dialing.

```
change feature-access-codes                                 Page   1 of   7
                            FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *03
                       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:
Call Forwarding Activation Busy/DA: *10    All: *11    Deactivation: #10
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                   CDR Account Code Access Code:
                         Change COR Access Code:
                    Change Coverage Access Code:
                    Contact Closure   Open Code:          Close Code:
                    Contact Closure  Pulse Code:
```

Figure 14: Feature Access Codes Form

Now use the **change ars analysis** command to configure the route pattern selection rule based upon the number dialed following the dialed digit "9". In this sample configuration, the PSTN numbers dialed are all in the form 1AAANNXXXXX (A= Area Code, N=[2-9], X=[0-9]). If the area code (AAA) is 732, the call is to be routed to a route pattern containing the H.323 trunk groups used for AGN Networks. Note that further administration of ARS is beyond the scope of these Application Notes but discussed in References [1] and [2].

```
change ars analysis 173                                    Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                  Location:  all           Percent Full:    3

          Dialed           Total         Route    Call   Node  ANI
          String          Min  Max      Pattern   Type   Num   Reqd
    173                   11   11         1       fnpa          n
```

Figure 15: ARS Analysis Form

Use the **change route-pattern** command to define the H.323 trunk group included in the route pattern that ARS selects. In this configuration, route pattern 1 will be used to route calls to trunk group 1 (the H.323 trunk created in **Section 3.6**).

```
change route-pattern 1                                     Page   1 of   3
                    Pattern Number: 1   Pattern Name: To 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: 1    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. Numbering LAR
    0 1 2 3 4 W     Request                                   Dgts Format
                                                           Subaddress
 1: y y y y y n  n            rest                                      none
 2: y y y y y n  n            rest                                      none
 3: y y y y y n  n            rest                                      none
 4: y y y y y n  n            rest                                      none
 5: y y y y y n  n            rest                                      none
 6: y y y y y n  n            rest                                      none
```

Figure 16: Route Pattern Form

3.10 Configure Incoming Digit Translation

This step performs the steps necessary to map incoming DID calls to the proper extension(s).

The incoming digits (specified using the AGN Networks **Desired DNIS** value shown in **Figure**) are manipulated as necessary to route calls to the proper extension on Avaya Communication Manager. Note that this step cannot be completed until the DID numbers and routing strategy defined in **Section 4** is known. Return to this step after the **Section 4** work is completed if necessary.

In the examples used in these Application Notes, the incoming DID numbers assigned by AGN Networks do not have a direct correlation to the internal extensions assigned within Avaya Communication Manager. Thus all incoming called number digits are deleted and replaced by the assigned extension number.

To create a fully mapped extension number as shown in **Figure 17**, perform the following:

- Use the **change inc-call-handling-trmt trunk-group <trunk_number>** command for the H.323 trunk group.
- For each extension, from the AGN Networks administration shown in
- **Figure** , enter the length of the incoming **Desired DNIS** value into the **Called Len** and **Del** fields, and the entire **Desired DNIS** value into the **Called Number** field. Enter the desired Avaya Communication Manager extension number into the **Insert** field.

```
change inc-call-handling-trmt trunk-group 1                    Page   1 of   3
                      INCOMING CALL HANDLING TREATMENT
 Service/       Called    Called        Del  Insert
 Feature         Len      Number
 public           14  90119087650215    14   71004
 public           14  90119087650216    14   72000
 public           14  90119087650219    14   72001
 public           14  90118776272701    14   71000
```

Figure 17: Incoming Call Handling Treatment – Full Extension Mapping

If the customer's extension numbering aligns with the DID number (i.e. the last four DID digits match the extension, it is not necessary to define an entry for each DID number. These entries might be similar to **Figure 18** where a match against the incoming routing prefix and npa/nnx could be done to route to a correlated extension.

```
change inc-call-handling-trmt trunk-group 1                    Page   1 of   3
                      INCOMING CALL HANDLING TREATMENT
 Service/       Called    Called        Del  Insert
 Feature         Len      Number
 public           14    9011908765      10
```

Figure 18: Incoming Call Handling Treatment – Simple Extension Mapping

4. AGN Networks OnDemand H.323 Service Configuration

In order to use the On Demand H.323 service, a customer must request service using the AGN Networks sales process. The process can be started by contacting AGN Networks via the links

found on their corporate web site at http://agnvoip.com and requesting information via the sales links or telephone numbers.

During the signup process, AGN Networks will require that the customer provide the public IP address used to reach the Avaya H.323 server. (Note the address used within these Application Notes is 135.1.1.84; the actual IP address will be specific to the customer implementation). Following signup, AGN Networks will provide the following:

- User name and password to access the customer support web site.
- IP address of the AGN Networks H.323 gateway.

Once this information is available, the remaining configuration is performed using a web browser with Internet access to the AGN Networks web site.

Step 1: Access the AGN Networks Web Site
To begin, access the AGN Networks web site at http://www.agnvoip.com and click on the **USER LOGIN** link in the top navigation bar as shown in **Figure 19**. The my.agnnetworks.com login page will appear.

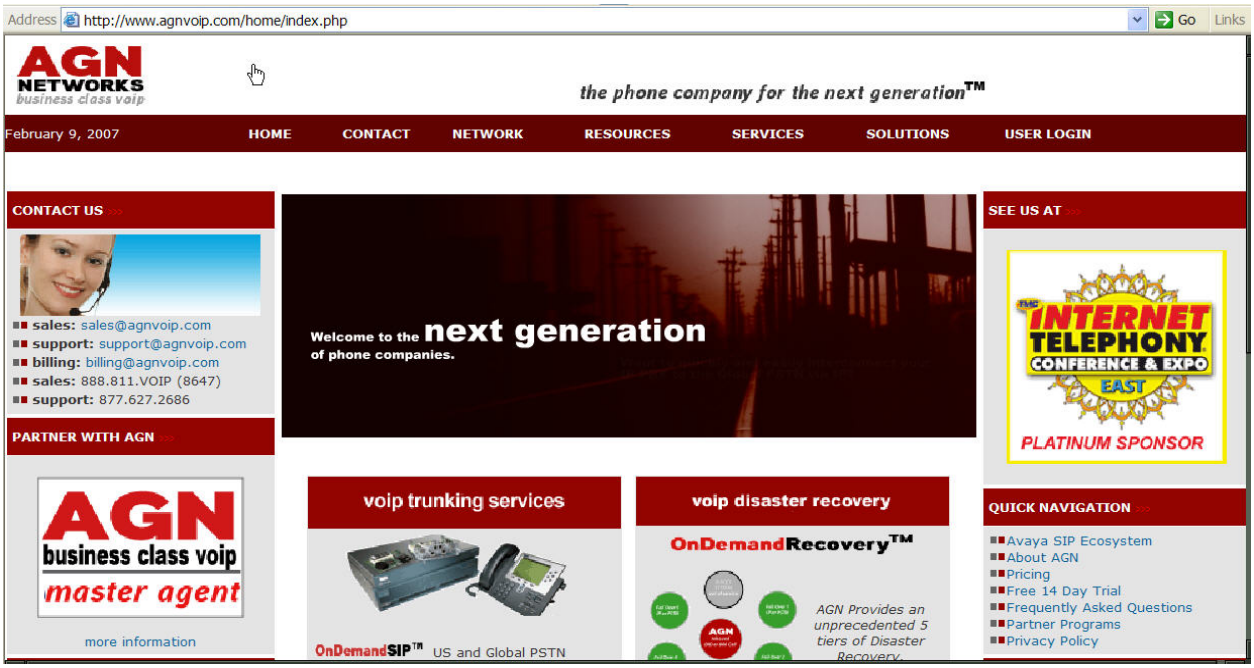

Figure 19: AGN Networks Home Page

Step 2: Log In
Log in by entering the user name and password provided by AGN Networks and then click the **Login** button as shown in **Figure 20.**

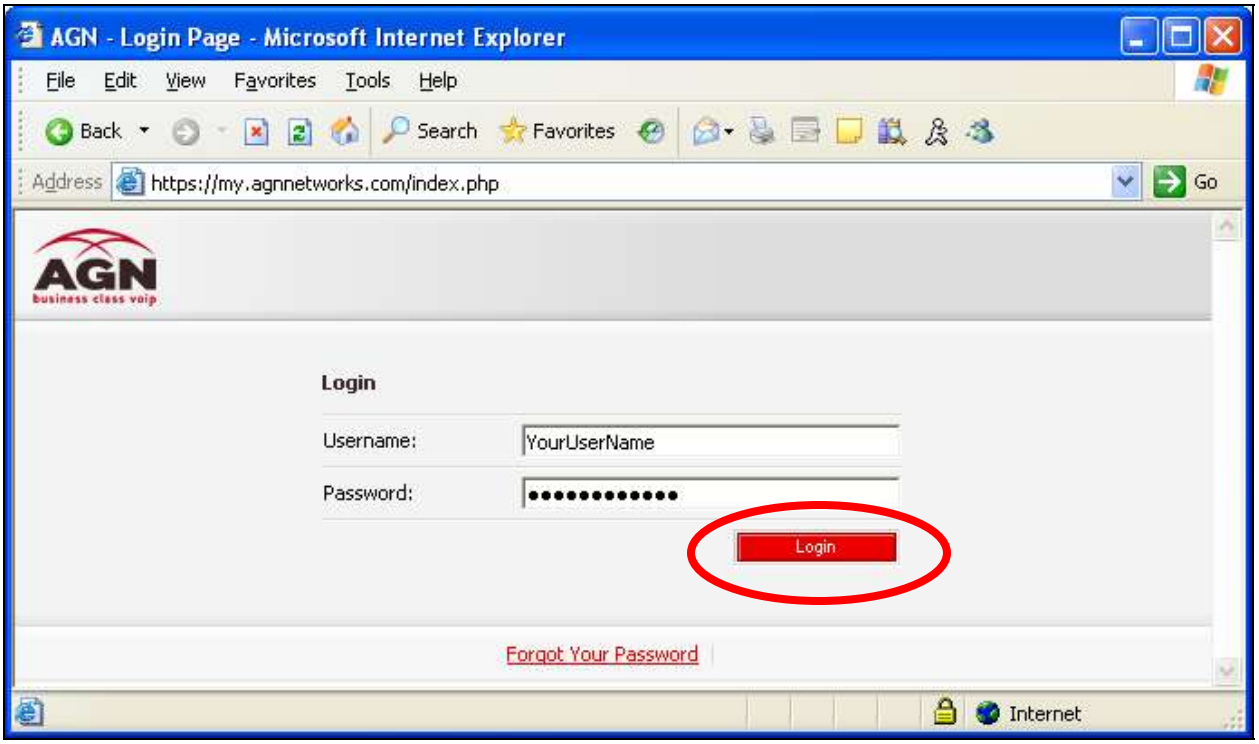

Figure 20: AGN Networks Customer Login Screen

Step 3: Add a New Location
After login, select the **Locations** tab in the horizontal navigation bar to display the **Location List** page as shown in **Figure 21.** Click on the **Add Location** link found in the left hand menu.

Figure 21: AGN Networks Locations Screen

Step 4: Specify the Location Information

On the Add Location page (**Figure 22**) enter the following:

- **Location Name** – Enter an alphabetic name describing the location that the Avaya SES supports or where the server resides. In this example, "Headquarters" is used as the location name. (Note that there should only be one location entry (corresponding to the Avaya SES) regardless of the number of customer sites served by individual Avaya Communication Managers.)
- **Extension** – Any extension number within the location. Typically this would correspond to the Listed Directory Number for the location. In this example, "70001" is entered.
- **IP Address** – The public IP address used to reach the Avaya S8300 Media Server. In this example, 135.1.1.84 is used, which is the processor for the Avaya S8300 Media Server.
- **VoIP Protocol** – Choose Generic H.323.
- **Location Address** – Enter the US postal address for the location.

Press the **Submit** button to save the information.

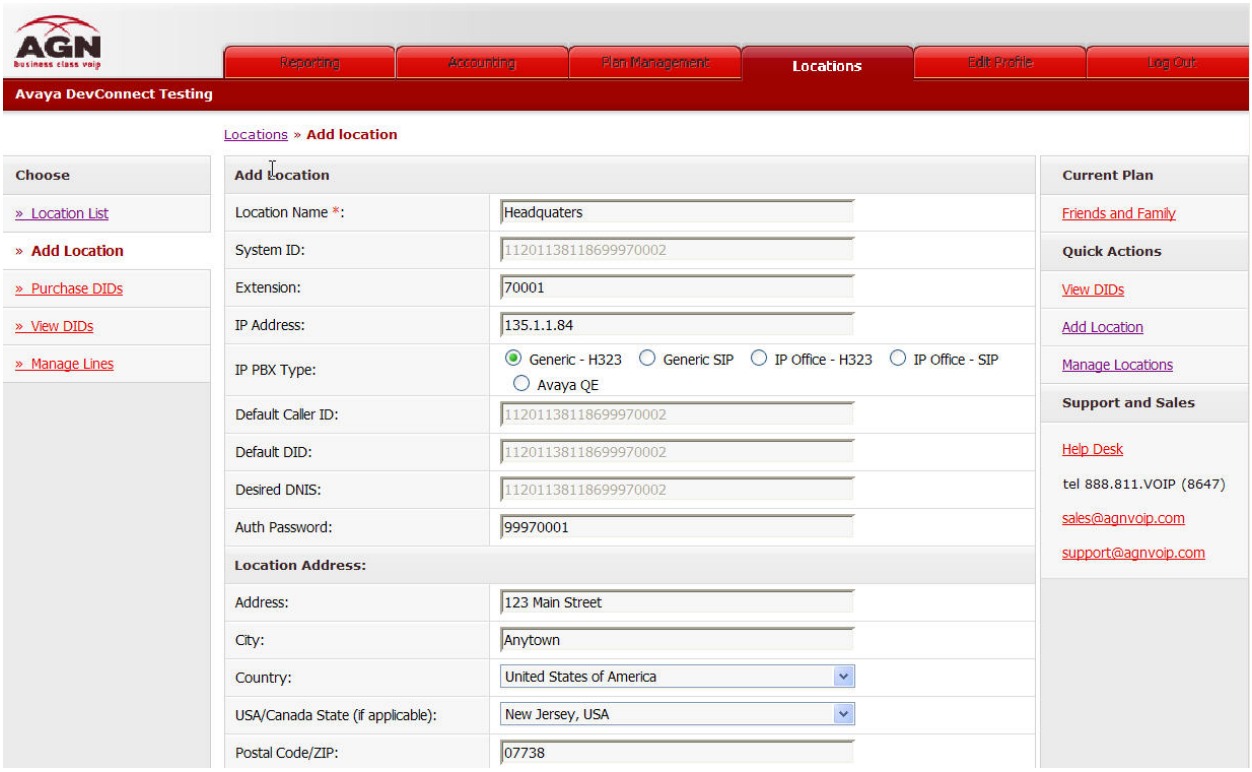

Figure 22: AGN Networks Add Location Screen

Step 5: Obtain DID and/or TollFree Numbers
To receive incoming calls, either DID and/or Toll Free numbers must be purchased.

- From the **Locations** tab, click the **Purchase DIDs** link found on the left hand menu. The form shown in **Figure 23** appears.
- Note that there are two different DID selections available, standard DID or Toll Free DID. Select the desired **Country**, **State**, **Area Codes** and **Cities** from the drop down lists as shown.
- Enter the number of DID numbers (for that City) desired into the **Desired Quantity** field corresponding to the type of DID being ordered (standard or Toll Free).
- Press the **Submit** button corresponding to the type of DID being ordered (DID or Toll Free).
- Click **Yes** to indicate acceptance of additional charges in the pop-up window that may appear.

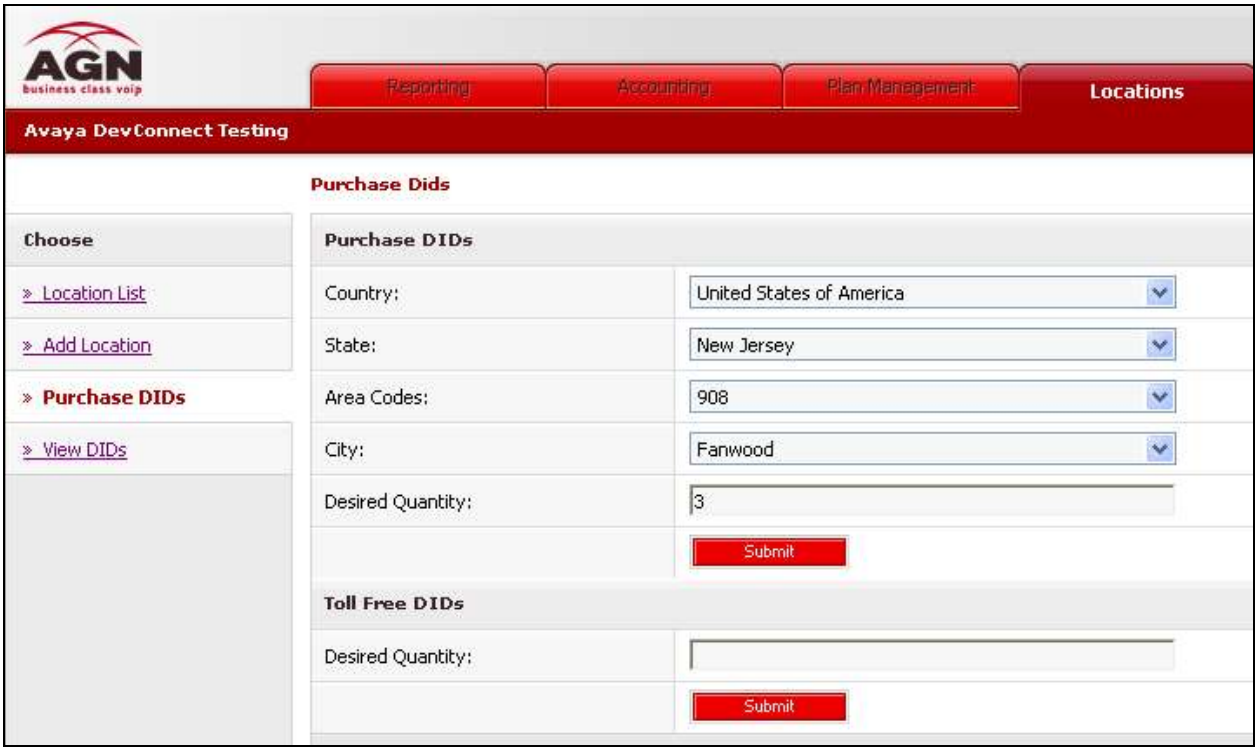

Figure 23: AGN Networks Purchase DIDs Form

- Following the submission, use the **View DIDs** link to see the DID numbers reserved for your use as shown in **Figure 24**.

Figure 24: AGN Networks Reserved DID Numbers

Step 6: Assign DID Numbers

The reserved DID numbers must now be assigned to the Headquarters location previously defined.

- Choose **Location List** from the left menu.
- Click on the link for the name of the location (i.e., Headquarters). The **Update Location** form previously completed will appear.

Figure 25: AGN Networks Location Screen

- Scroll to the bottom on that form and select the **Manage DIDs** link located just above the **Submit** button (**Figure 26**).

Figure 26: AGN Networks Location Form Manage DIDs Link

The **Managed DIDs** link will open a page as shown in **Figure 27**.

- Select one or more DID number(s) from the **Reserved DIDs** list and use the >> button to move the numbers to the **Assigned DIDs** list.
- Repeat as necessary for other DID numbers.
- Press the **Submit** button and confirm that the DIDs were successfully assigned to that location (**Figure 28**).

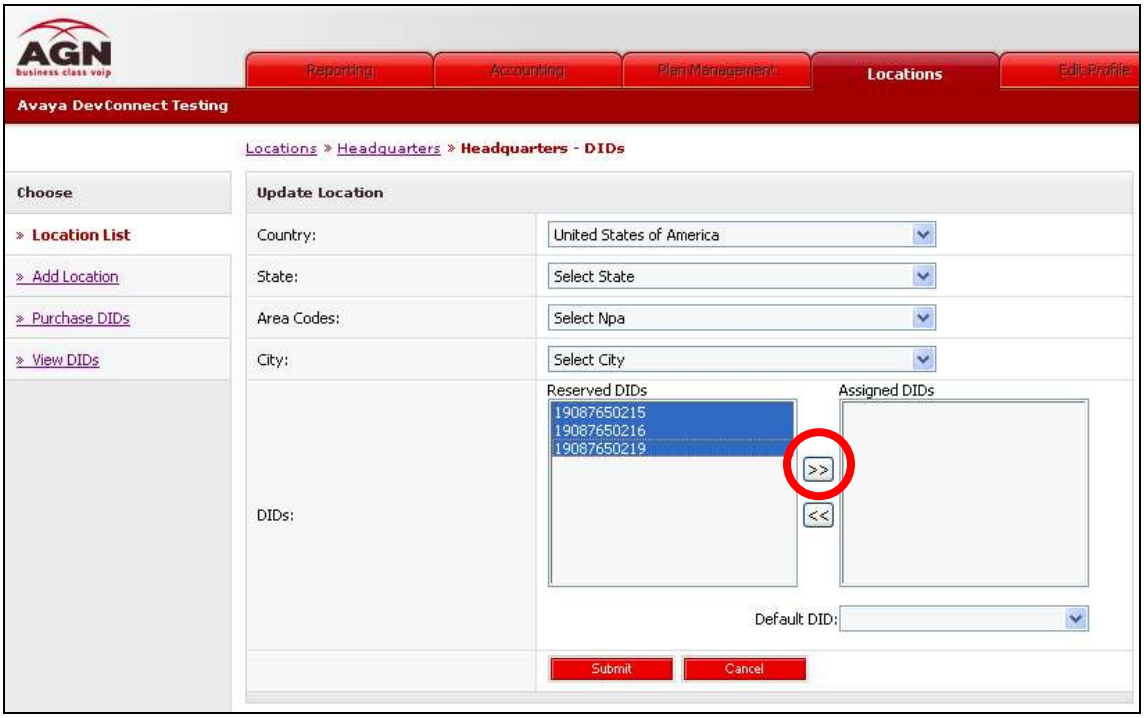

Figure 27: Assign DIDs Form

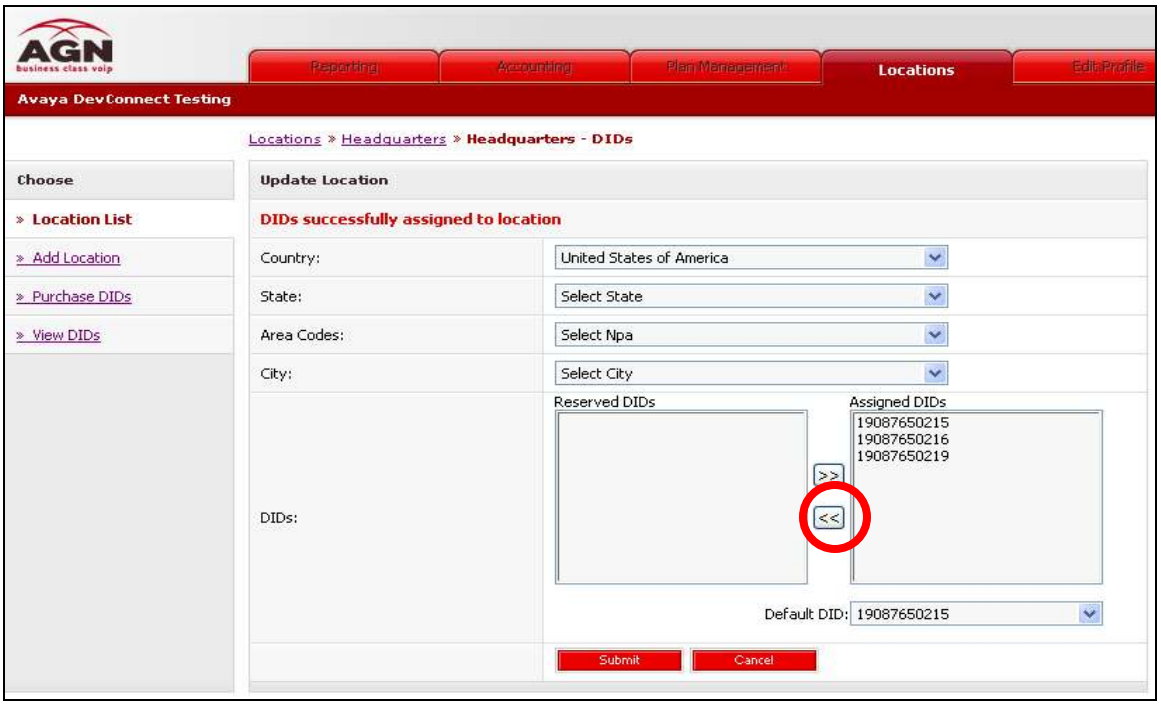

Figure 28: Successfully Assigned DIDs

Step 7: Specify the Desired DNIS Values

Finally, update the desired DNIS values to match the routing strategy defined in **Section 3** during the configuration of Avaya Communication Manager. Recall that the numbering strategy was to define the DNIS value to be a 3-digit routing number followed by the full 11 digit North American telephone number.

- Begin by choosing the **View DIDs** link found on the left hand menu of the **Locations** tab. A screen similar to **Figure 29** below will be seen. Note that the current **Desired DNIS** values do not currently match the desired numbering strategy.

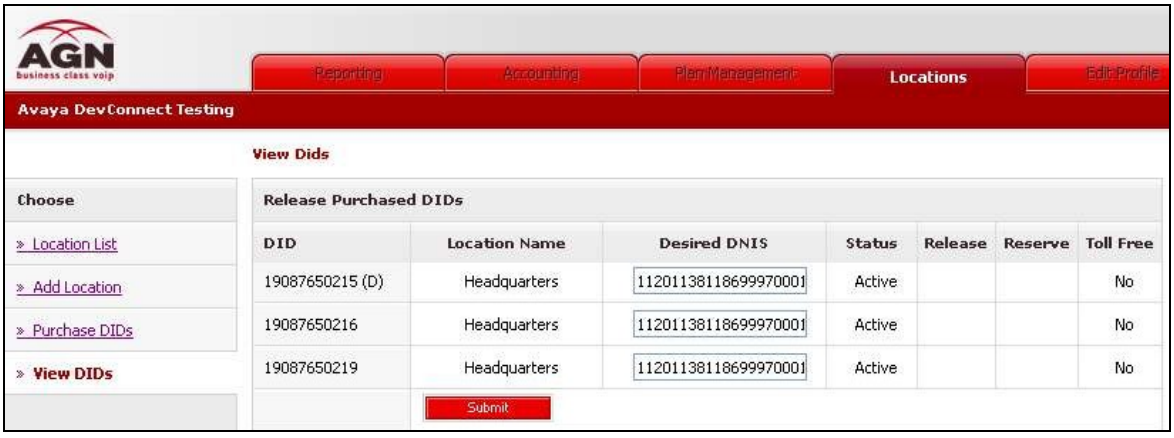

Figure 29: View DIDs Form showing Desired DNIS Values

- Update each **Desired DNIS** field accordingly and press the **Submit** button. In the test configuration, the desired DNIS values used were "901" followed by the DID number shown in the left column. The "901" is simply a prefix added in order to mark specific calls, it is not mandatory.
- Verify that the correct desired DNIS values are now recorded and the DID status is **Active** as shown in **Figure 30**.

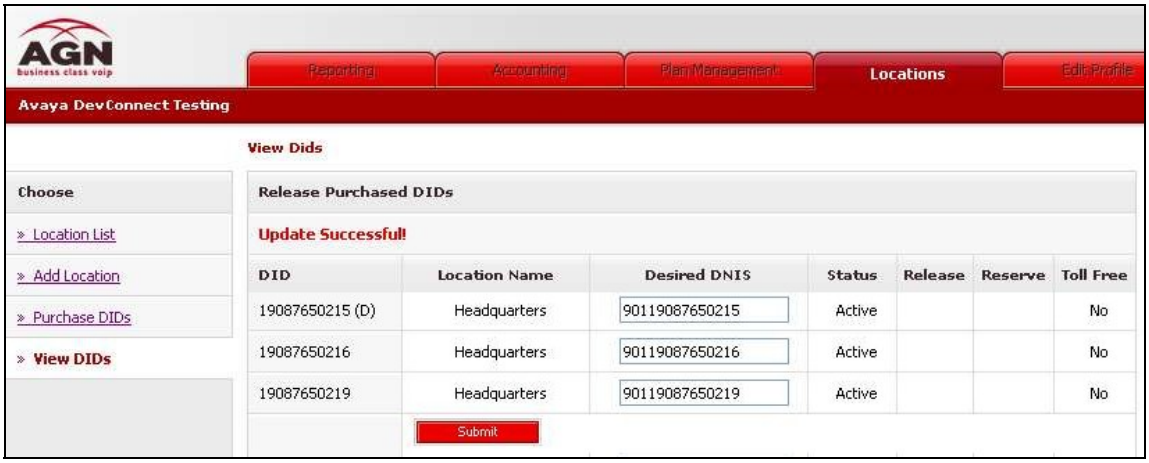

Figure 30: Successful Update of Desired DNIS fields.

This completes the configuration within AGN Networks for inbound and outbound calling.

5. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify H.323 trunking interoperability between the AGN Networks OnDemand H.323 service and an Avaya H.323 IP-based configuration. 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 telephony solution supporting H.323 trunking was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to use the commercially available On Demand H.323 services provided by AGN Networks. This allowed the enterprise site to use H.323 trunking for PTSN calling.

The following features were covered during the H.323 trunking interoperability compliance test:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by AGN Networks.
- Outgoing calls from the enterprise site to the PSTN.
- Incoming and Outgoing calls using H.323, digital and analog endpoints supported by the Avaya IP telephony solution.

- Various call types including: local, long distance, international, and toll free.
- Calls using G.711 and G.729A codecs.
- DTMF transmission using inband signaling.
- Direct IP-to-IP media (also known as "Shuffling") which allows H.323 IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.
- Fax using a standard analog line with G.711mu CODEC type. (Non T38 mode)

5.2 Test Results and Observations

All the tests outlined as the main objectives in **Section 5.1** were completed successfully. H.323 trunks, calls with and without shuffling, were successfully established. Voice, fax calls and DTMF transmission over the H.323 trunks were established with good quality.

During the testing, the following minor issues were observed:

Item	Issue Observed	Discussion / Workaround
Fax	T.38 fax mode is not yet supported for this solution.	Not Applicable
DTMF over IP	When the shuffling feature is enabled, users passing DTMF tones from a "shuffled" IP H.323 phone call out to the PSTN may experience an occasional missed tone.	The workaround can be to retransmit the tone again or to disable the shuffling feature in Avaya Communication Manager.

This section provides verification steps that may be performed in the field to verify that the H.323, digital and analog endpoints can place outbound and receive inbound PSTN through the AGN Networks services.

6. Verification Steps

1. Verify that endpoints at the enterprise site can place calls via H.323 trunks to the PSTN and that the calls remain active for more than 60 seconds.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the calls can remain active for more than 60 seconds.
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.
5. If the Direct-IP feature (a.k.a. shuffling) is enabled, verify that a call originated or terminated on an Avaya 4600/9600 Series H.323 IP Telephone has the RTP path directly between the H.323 phone and AGN Networks gateway. To determine if the call is shuffled, identify the trunk member active on the call by running the **status trunk <*group*>**, (use the trunk group created in **Section 3.6**), command using the SAT of Avaya Communication Manager. Next, run the **status trunk group/member** command and check the **Audio Connection** field. If the call is shuffled, the field should be set to *ip-direct*; otherwise, the field would be set to *ip-tdm*.

7. Support

For technical support on AGN Networks On Demand H.323 Services, contact support at 1-888-811-8647 or support@agnvoip.com.

8. Conclusion

These Application Notes describe the configuration steps required to connect an enterprise site consisting of an Avaya H.323-based telephony solution to the AGN Networks OnDemand H.323 service. H.323 trunking permits enterprise customers to reduce long distance and interconnection costs by using broadband Internet access to support PSTN telephony. In addition, customers can benefit from additional features such as web-based provisioning, virtual DID numbers and online reports available as part of the On Demand H.323 service.

9. Additional 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] *Administrator Guide for Avaya Communication Manager*, May 2006, Issue 2.1, Document Number 03-300509.
[2] *Feature Description and Implementation for Avaya Communication Manager*, Issue 4, Document Number 555-245-205.
[3] *4600 Series IP Telephone R2.7 LAN Administrator Guide*, November 2006, Document Number 555-233-507.
[4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 1.2*, January 2007, Document Number 16-300698.

Additional information about the AGN Network Services is available at http://www.agnvoip.com/avayah323.

APPENDIX A: Integrating Network and Port Address Translation (NAT/PAT) Functionality

Overview

The purpose of the compliance testing described above in the main portion of this document was to certify that AGN Networks OnDemand H.323 service was interoperable with an Avaya based H.323 telephony solution. Therefore, compliance testing was performed using publicly routable IP addresses **without** the presence of a security device running Network Address Translation (NAT) and Port Address Translation (PAT) functionalities.

It is, however, recognized that most if not all real world enterprise applications of this solution will indeed include the use of NAT/PAT functionalities for security purposes. Therefore, the purpose of this Appendix is to describe the concepts involved with the integration of NAT/PAT functionalities with the solution described above. A basic subset of the main test plan was rerun against the configuration in this appendix. Tests included incoming/outgoing PSTN calls, shuffling, and Avaya Telephone features such as Hold, Transfer and Forwarding. While these tests passed, this testing is NOT to be confused with the compliance testing in the main portion of this document.

There are two primary reasons for using NAT and PAT functionality. The first one is security. Using public addresses for critical network elements such as PBXs, switches and IP endpoints leaves them vulnerable to malicious attacks that can cripple the network and stop service. The second reason is the cost and flexibility related to the use of IP address space. Obtaining public IP addresses for all endpoints in a network can be expensive.

Using NAT/PAT can allow the critical elements of the network to be protected from malicious attack while additionally allowing the use of one public IP address for up to 65536 internal hosts.

For the scope of the discussion in this Appendix, the 10.1.1.0 255.255.255.0 will be defined as the Private IP Network while 135.1.1.0 255.255.255.0 will be defined as the public IP Network.

For the specific solution discussed in this document, both Network and Port Address Translation will be used in order to apply the security and IP address space benefits discussed above. Within the Avaya based H.323 telephony solution, there are two different categories of network elements that need to be able to communicate to the outside world in order for a phone call to be established, the signaling element which is the Avaya S8300 Media Server, and secondly additional IP media endpoints such as the Avaya IP Telephones and the Avaya G350 Media Gateway.

Signaling Network Element

Since signaling is required between the AGN Networks H.323 gateway and the Avaya S8300 Media Server in order to establish calls, it is necessary for the Avaya S8300 Media Server to have a publicly routable dedicated IP address. In order to protect the Avaya S8300 Media Server, Network Address Translation will be used to hide the real internal IP address of the server.

The Internal IP address of the S8300 will be 10.1.1.84 while the public IP address will be 135.1.1.84. For outgoing communication destined for the AGN Networks H.323 gateway, Network Address Translation in the Firewall device will examine the IP packets coming from the S8300 and replace the internal IP source address of 10.1.1.84 with the external IP address of 135.1.1.84. Conversely, for incoming communication from the AGN Networks H.323 gateway, the Firewall device will receive the IP packets, examine the header and replace the public destination IP address of 135.1.1.84 with the private IP address of 10.1.1.84.

Media Gateway and IP Phone Network Elements

These elements will need to send and receive the media stream (RTP) to and from the PSTN endpoint of the call. When shuffling, (also known as Direct IP), is disabled, the G350 Media Gateway will be sending and receiving the RTP media stream. When shuffling is enabled the Avaya IP phones themselves will directly send and receive the RTP stream.

For the application described above, these elements do not need to each have unique publicly routable IP addresses. Because of this, Port Address Translation can be used instead of Network Address Translation. PAT translates both the IP and port fields (TCP or UDP) -- wherever those values belong to an internal host. Port numbers on packets coming from the external network, rather than destination IP addresses, are used to identify and designate traffic to different computers on the inside network. By doing this, PAT can allow one public IP address to be used to represent multiple IP hosts on the inside network. For this configuration, the public IP address of 135.1.1.85 will be used to represent traffic flows coming from the Avaya G350 Media Gateway as well as the Avaya IP Telephones. When either the Avaya G350 Media Gateway or the Avaya IP Telephones are sending and receiving an RTP stream, the Firewall device will replace the internal IP address on the 10.1.1.x network with the public IP address of 135.1.1.85 and then use the UDP port numbers to route the traffic.

Configuration

Below is a table showing the NAT/PAT IP mappings that will be performed by the Firewall device discussed above:

Network Element	Private IP Address	Public IP Address
Avaya S8300 Media Server (NAT)	10.1.1.84	135.1.1.84 255.255.255.255
All Additional IP Endpoints (PAT)	10.1.1.x /24	135.1.1.85 255.255.255.255

Figure 27 below shows a high level network diagram including the Firewall device.

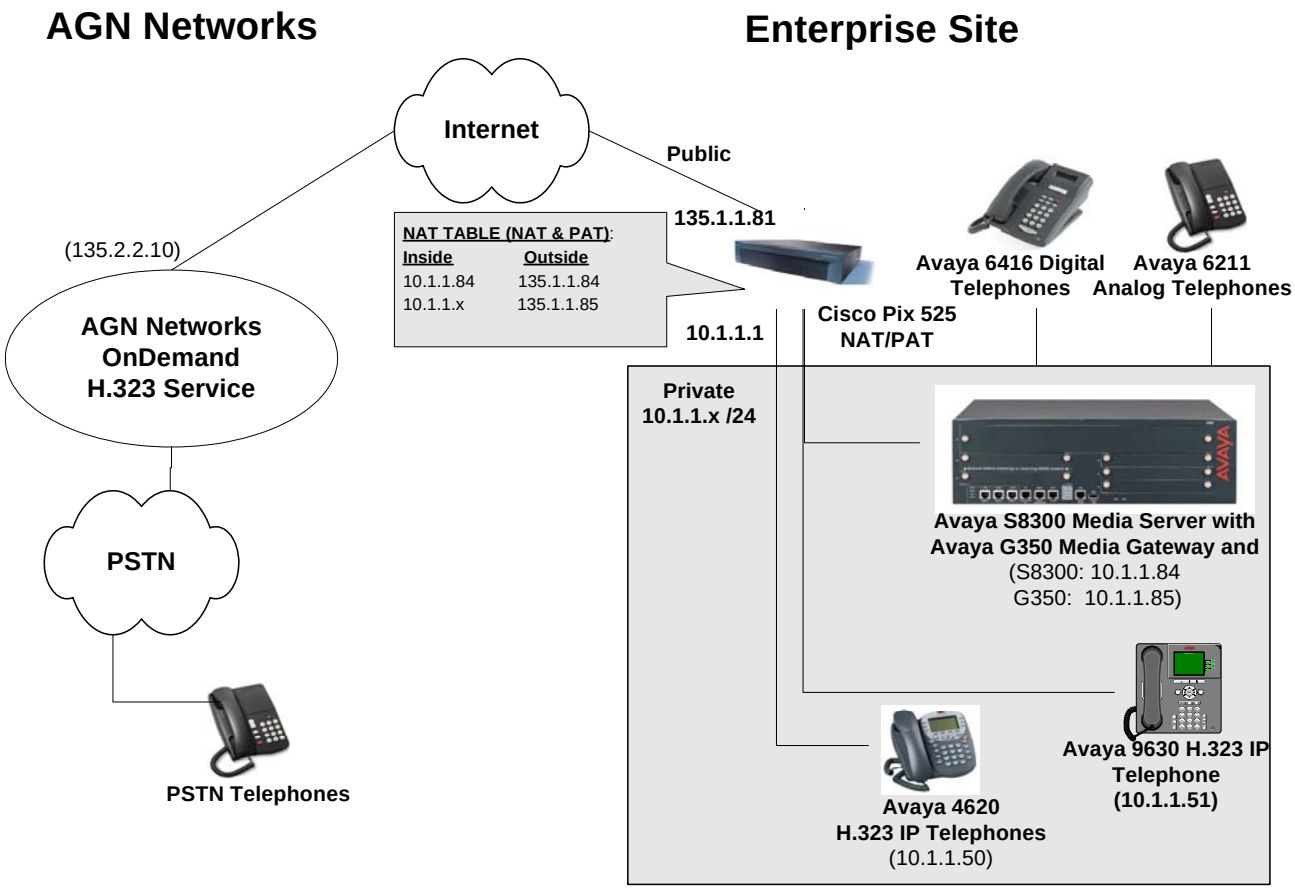

Figure 31: Network Diagram with Integrated Firewall Device performing NAT/PAT

For this exercise, a Cisco Pix 525, was used to perform the NAT/PAT functions. Below is a table displaying the key attributes of the Cisco:

Cisco Pix 525	
Software	Cisco PIX Firewall Version 6.3(5)
CPU	Pentium III 600 Mhz
Memory	256 MB RAM
License	Unrestricted

Below are the configuration steps used to setup the NAT and PAT functionalities on this device after logging into the Cisco Pix with appropriate privileges:

Enter the configuration terminal interface: "**conf t"**.

Step 1: Enable and Name the interfaces to be used for inside and outside networks and assign the associated security levels for each, 0 = least trusted; 100 = most trusted.

- **"interface ethernet0 100full"**
- **"interface ethernet1 100full"**
- **"nameif ethernet0 outside security0"**
- **"nameif ethernet1 inside security100"**

Step 2: Configure the outside and inside IP addresses and mask of the Pix device itself.

- **"ip address outside 135.1.1.81 255.255.255.0"**
- **"ip address inside 10.1.1.1 255.255.255.0"**

Step 3: Configure the Avaya S8300 Media Server's private and public IP addresses by using the static NAT command. The "0 65535" values are the port range that can be used.

- **"static (inside,outside) 135.1.1.84 10.1.1.84 netmask 255.255.255.255 0 65535"**

Step 4: Define the routable PAT address to be used for outbound connections, this will be used by the Avaya G350 Media Gateway as well as the Avaya IP telephones.

- **"global (outside) 1 135.1.1.85 netmask 255.255.255.255"**

Step 5: Define the IP PAT endpoints, (Avaya G350 Media Gateway and Avaya IP Telephones), that will use the routable address defined in **Step 4**. The "0 65535" values are the port range that can be used. The addresses below represent the two Avaya IP Telephones and the address of the Avaya G350 Media Gateway. Each additional phone would need to be added with the command below.

- **"nat (inside) 1 10.1.1.50 255.255.255.255 0 65535"**
- **"nat (inside) 1 10.1.1.51 255.255.255.255 0 65535"**
- **"nat (inside) 1 10.1.1.85 255.255.255.255 0 65535"**

Step 6: Define the access list that permits specific types of traffic through the interfaces.

- **"access-list acl_in permit tcp any any"**
- **"access-list acl_in permit udp any any"**

Step 7: Bind the access list to the outside interface by use of the access-group command. Note that access lists only need to be applied for interfaces of less "trusted security" are trying to access interfaces of a higher "trusted security". In this case, since the outside interface was set to a security of 0 in step 1, it will need the access list to "permit" it to communicate via tcp in this case to the inside interface. This command essentially allows signaling traffic from AGN networks to reach the Avaya S8300 Media Server.

- **"access-group acl_in in interface outside"**

Step 8: Add the default route, in this case 135.1.1.65 is a default router not shown in **Figure 31**.

- **"route outside 0.0.0.0 0.0.0.0 135.1.1.65 1"**

Step 9: Confirm that the fixup command for H323 trunking is enabled. (Typically, this is enabled by default) This allows the Pix to find embedded private IP addresses not in the header of the packet to be changed to the public PAT or NAT "ed" address.

- Use the **"show running command"** to search for the following **"fixup protocol h323 h225 1720".** If it is not present, you must enter the command in order for this solution to work properly.

Verification:

See **Section 6** of the main document.

During various calls placed in the verification steps, use the "show xlat" command on the Cisco Pix. This command will show the NAT and PAT translations taking place, for example, you might have an output similar to this:

"devcon-pix(config)# show xlat
14 in use, 23 most used
PAT Global 135.1.1.85(1038) Local 10.1.1.85(2056)
PAT Global 135.1.1.85(1034) Local 10.1.1.51(0)
PAT Global 135.1.1.85(1026) Local 10.1.1.85(2050)
PAT Global 135.1.1.85(1042) Local 10.1.1.85(2054)
PAT Global 135.1.1.85(1039) Local 10.1.1.85(2057)
PAT Global 135.1.1.85(1027) Local 10.1.1.85(2051)
PAT Global 135.1.1.85(1043) Local 10.1.1.85(2055)
Global 135.1.1.84 Local 10.1.1.84"

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 Developer*Connection* Program at devconnect@avaya.com.