Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking between Nectar Services Corporation On Demand Voice Service and Avaya Distributed Office – Issue 1.0

Abstract

These Application Notes describe the steps for configuring SIP trunking between the Nectar Services On Demand Voice service "formerly known as AGN Networks On Demand SIP service) and an Avaya Distributed Office (Release 1.2) using various Avaya telephony endpoints.

Enterprise customers with this Avaya SIP-based solution can connect via dedicated Internet access using Nectar Services as a service provider to complete PSTN calls. This includes outbound local, long distance and international calling, inbound calling to DID numbers from most major US cities and markets, and inbound toll-free calling. This solution allows customers with a converged network to lower PSTN telecommunication costs, to easily obtain local number presence without offices in each geographic area, and to easily manage their network services using web-based tools.

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

1. Introduction

These Application Notes describe the steps for configuring SIP trunking between the Nectar Services Corporation On Demand Voice service and an Avaya Distributed Office (Release 1.2) using various Avaya telephony endpoints.

Enterprise customers using this Avaya Distributed Office IP telephony solution with Nectar Services Corporation On Demand Voice service are able to place and receive PTSN calls via a dedicated broadband Internet connection using the Session Initiation Protocol (SIP). This converged network solution is an alternative to more traditional PTSN trunks such as T1 or ISDN PRI. It allows customers to possibly reduce local and long distance costs, add and delete DID and toll-free numbers in minutes, as well as benefit from capabilities such as having local numbers from numerous area-codes easily terminate at a single location.

SIP (Session Initiation Protocol) is a standards-based communications approach designed to provide a common framework to support multimedia communication. RFC 3261 [10] is the primary specification governing this protocol. SIP manages the establishment and termination of connections and the transfer of related information such as the desired codec, calling party identity, etc. Within these Application Notes, SIP is used as the signaling protocol between the Avaya Distributed Office and the network services offered by Nectar Services Corporation.

The Nectar Services Corporation On Demand Voice family of services covered by this solution includes:

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

For the remainder of this document the entire family will simply be referred to as “On Demand Voice” service unless there is a need to differentiate among the services.

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

1.1. Typical Enterprise Customer Location

Figure 1 illustrates a typical customer location using an Avaya Distributed Office with SIP trunking to Nectar Services Corporation. This configuration includes:

- Avaya Distributed Office i120 providing the communication services for this customer location.
- Various Avaya telephones and other endpoints.
- IP routing and data network infrastructure to support IP connectivity between the enterprise location and the Nectar Services Corporation service.

For simplicity, aspects that may exist in customer configurations but are beyond the scope of these Application Notes are not addressed. Specifically,

- The initial installation and administration of the Avaya Distributed Office to provide basic telephony services is not addressed. The SIP trunking configuration described within assumes a previously configured system capable of extension to extension calling.
- The concepts presented in these Application Notes apply to both Avaya Distributed Office i120 and (the smaller) i40 configuration. However, the i40 is not specifically discussed.
- The use of analog or digital PSTN trunks in addition to SIP trunking is not discussed.
- The configuration of Avaya 9600, 4600, and 1600 Series IP telephones.
- IP Network Address Translation (NAT), firewalls, Application Layer Gateway (ALG), and/or Session Border Controller (SBC) devices may exist between the Nectar Services Corporation On Demand Voice service and the Avaya Distributed Office within a customer's communications infrastructure. While a Juniper SSG 520M[1] firewall was used to validate these Application Notes, other devices with similar functionality could be used. These devices generally must be SIP-aware and configured properly for SIP trunking to function properly. When configured correctly, they are transparent to the Avaya communications infrastructure.

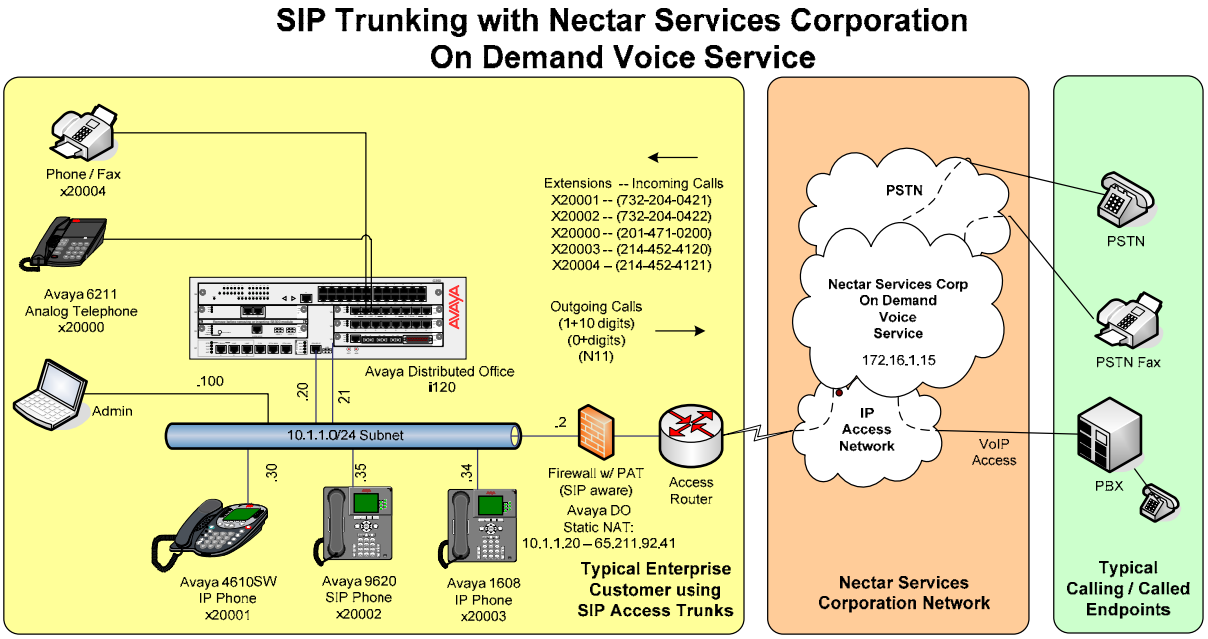

Figure 1 – Typical SIP Trunking Configuration

[1] A copy of the firewall configuration used during testing is provided in Appendix B.

Figure 2 illustrates the Network Connection information for the Avaya Distributed Office i120.

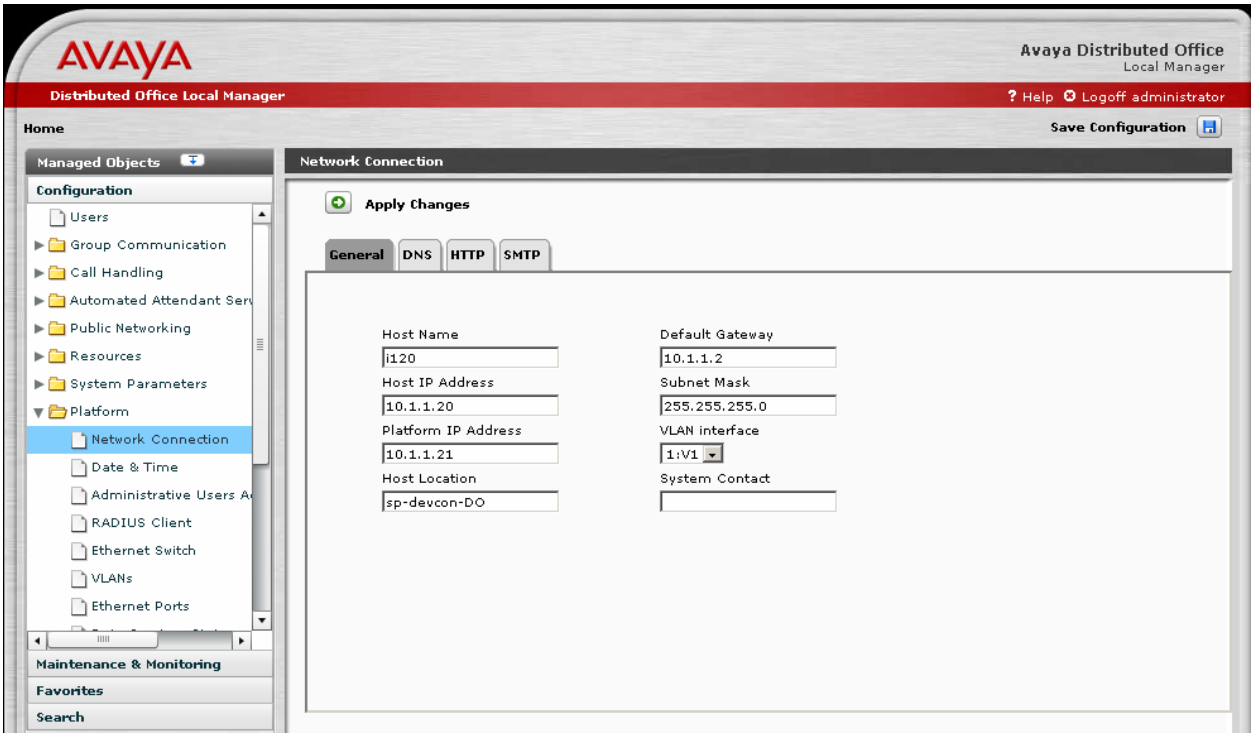

Figure 2 - Avaya Distributed Office Network Connection Assignments

It is a mandatory requirement that IP routing exist between any IP or SIP endpoints and the enterprise firewall and between the enterprise firewall and Nectar Services Corporation Border Element(s) whenever using direct media.

1.2. Nectar Services Configuration Information

These Application Notes provide **an illustrative example** of how the Avaya Distributed Office SIP trunking solution is configured with the Nectar Services Corporation On Demand Voice service.

The specific values provided below are illustrative only and must not be used for customer configurations. *Each customer must obtain the specific values for their configuration from Nectar Services Corporation during service provisioning of their On Demand Voice service.*

Nectar Services Provisioning Information	**Illustrative Values in these Application Notes**
Nectar Services Corporation Border Element IP Address(es)	172.16.1.15
G.729A, G.711MU, G.711A Codecs Supported	Yes
RFC 2833 (DTMF Event) Supported	Yes
Via Header Routing	Yes
Maximum Concurrent Calls (specified by customer during service ordering)	30
Assigned Direct Inward Dial (DID) Numbers	See **Figure 1**
DID Digits Passed in SIP Request URI (Configurable from Nectar Services Portal)	902 prefix followed by DID number
DID Digits Passed in SIP To Header	Same as Assigned DID Numbers

Table 1 – Illustrative Nectar Services Corporation Network Provisioning Information

2. Equipment and Software Validated

The following equipment and software was used during the DevConnect compliance testing with the Nectar Services Corporation On Demand Voice service.

Component	**Version**
Avaya	
Avaya Distributed Office i120	Release 1.2 (1.2.0_24.05)
Avaya 4621SW IP (H.323) Telephone	Release 2.8.8.7
Avaya 1608 IP (H.323) Telephone	Release 1.0.2
Avaya 9620 one-X™ Deskphone SIP Telephone	Release 2.0.4.0(2)
Avaya 6211 Analog Telephone	n/a
MultiTech Fax Modem	Model MT5634ZBA
Venta Fax & Voice Fax Application	Release 2.8
Nectar Services Corporation	
Nectar Services Corporation SIP Proxy	Nextone MSC v4.0c2-1

Table 2 – Equipment and Version

3. Configure Avaya Distributed Office

The Avaya Distributed Office i120 was installed and configured for basic station to station calling prior to the beginning of the configuration shown in these Application Notes. The installation and basic configuration details are outside of the scope of the SIP trunking application and not included here.

3.1. Login to Avaya Distributed Office

Using a web browser, access the Avaya Distributed Office Local Manager by entering "http://<ip-addr>/" where "<ip-addr>" is the **Host IP Address** of the Avaya Distributed Office. In these Application Notes, "http://10.1.1.20" is used.

Log in with the appropriate credentials. The Local Manager Home screen is shown.

Figure 3 - Avaya Distributed Office Local Manager Home

3.2. Add a SIP Trunk Group to the Nectar Services Corporation On Demand Voice Services

From the left hand **Configuration** menu, expand the **Public Networking** option and select **Trunk Groups**. The **Trunk Groups** screen will be displayed.

Select **Add New** to display the **Add Trunk Group** screen.

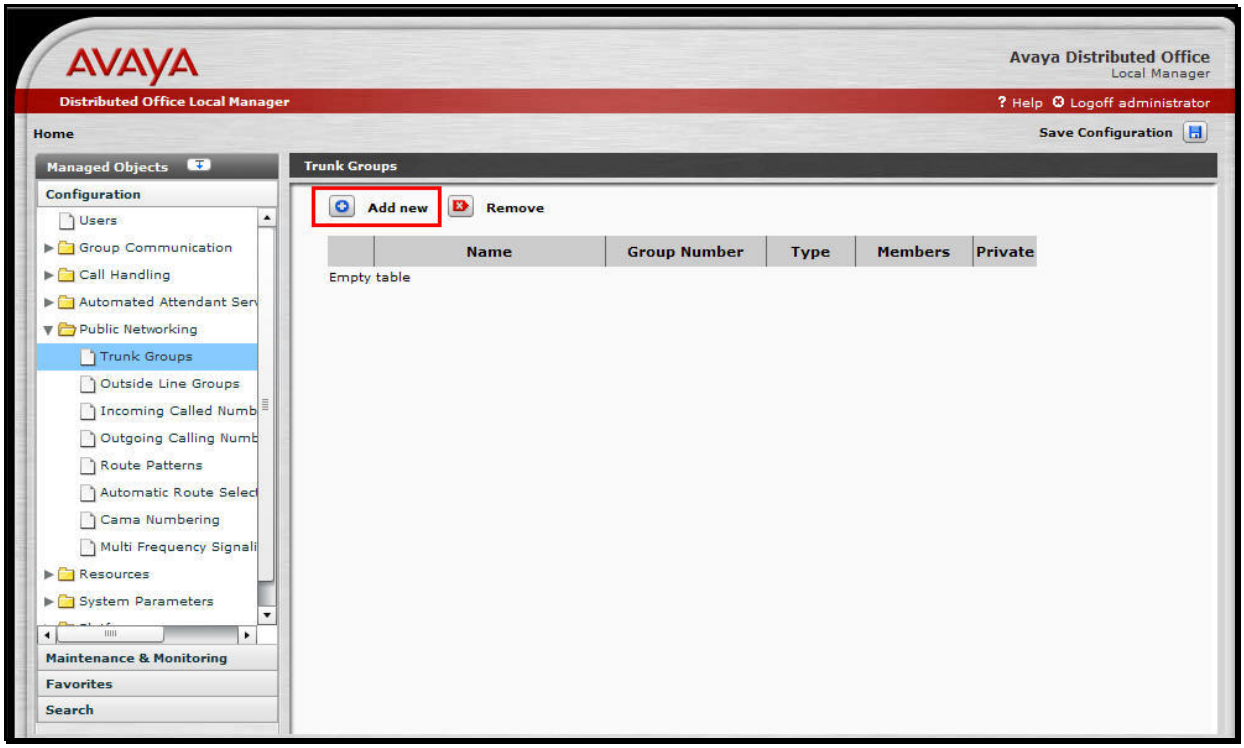

Figure 4 - Avaya Distributed Office Trunk Groups Screen

On the Add Trunk Group screen:

- Set the **Trunk Type** to "SIP".
- Enter a short text description of the trunk group (e.g., NECTAR-VOIP) in the **Native Name** field.
- The **Name (ASCII)** field will default to the Native Name field. Modify the Name if necessary to provide a corresponding ASCII version.
- Press the **Continue** button.

The Add SIP Trunk Group General Tab screen is shown.

- Select "two-way" as the **Direction** to support both incoming and outgoing calling on this trunk group.
- Press the **SIP** tab to advance to the next screen.

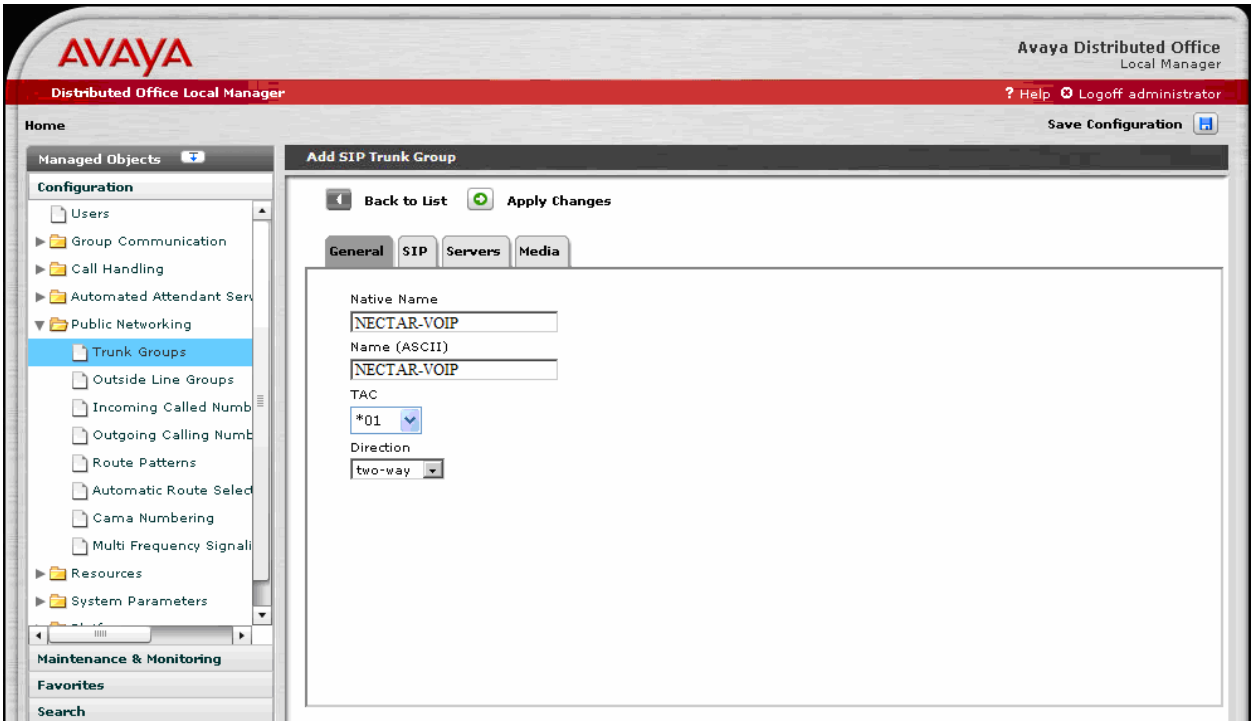

Figure 5 - Avaya Distributed Office Add SIP Trunk Group Screen – General tab

On the **SIP** tab:

- Enter a **Far-End Domain** value for the Nectar Services Corporation services.
- Enter the customer's SIP domain for the Distributed Office in the **Near-End Domain** field. In these Application Notes, "example.com" was used. It is not necessary that this domain be resolvable for the Nectar Services Corporation SIP trunking.
- Check the **Replace outgoing request-URI domain with selected server IP address** box.
- Enter "600" in the **Session Refresh Interval** field.
- The defaults shown for the **Timeout** and **Max Search Time** are used.
- Press the **Servers** tab to advance to the next screen.

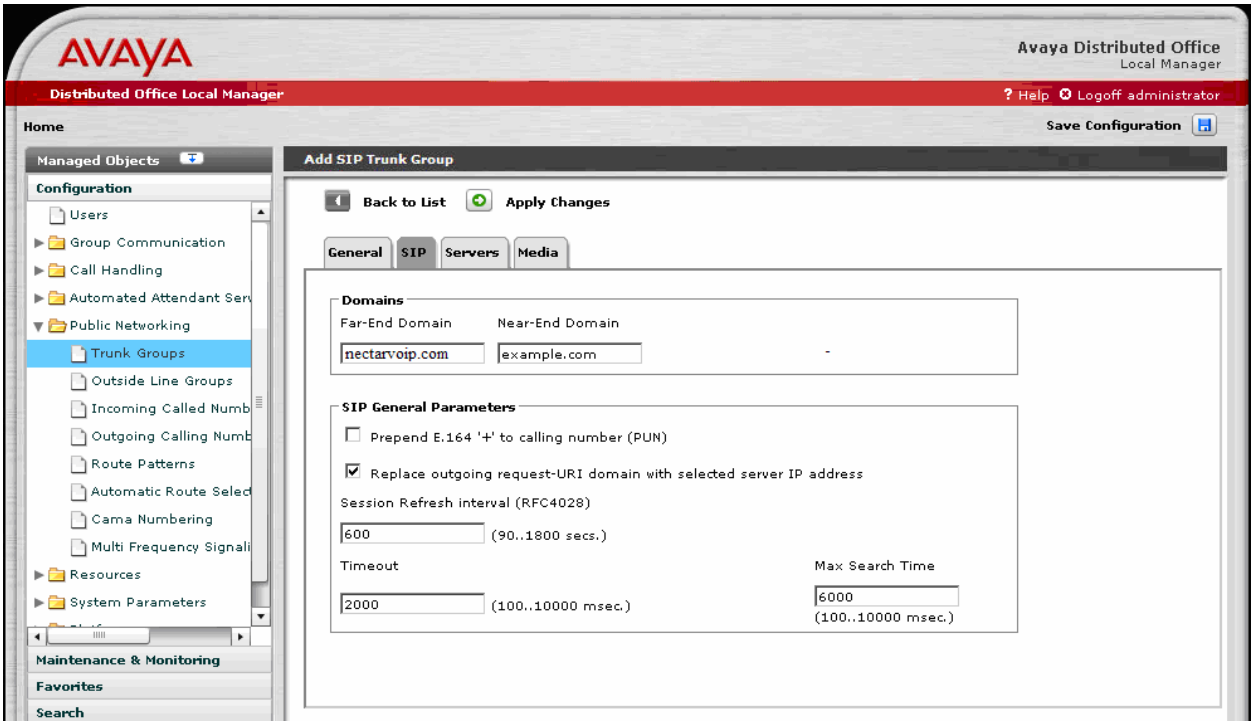

Figure 6 - Avaya Distributed Office Add SIP Trunk Group Screen – SIP Tab

On the **Servers** tab:

- Enter the IP address of the primary Nectar Services Corporation Border Element provided by Nectar in the **Address** field. In this Application Note, "172.16.1.15" is used as noted in Section 1.2. It is not necessary to specify the port since the UDP default "5060" is used.
- Select "UDP" for the **Transport** field value.
- The default **Priority** field settings shown are used.
- Press the **Media** tab to advance to the next screen.

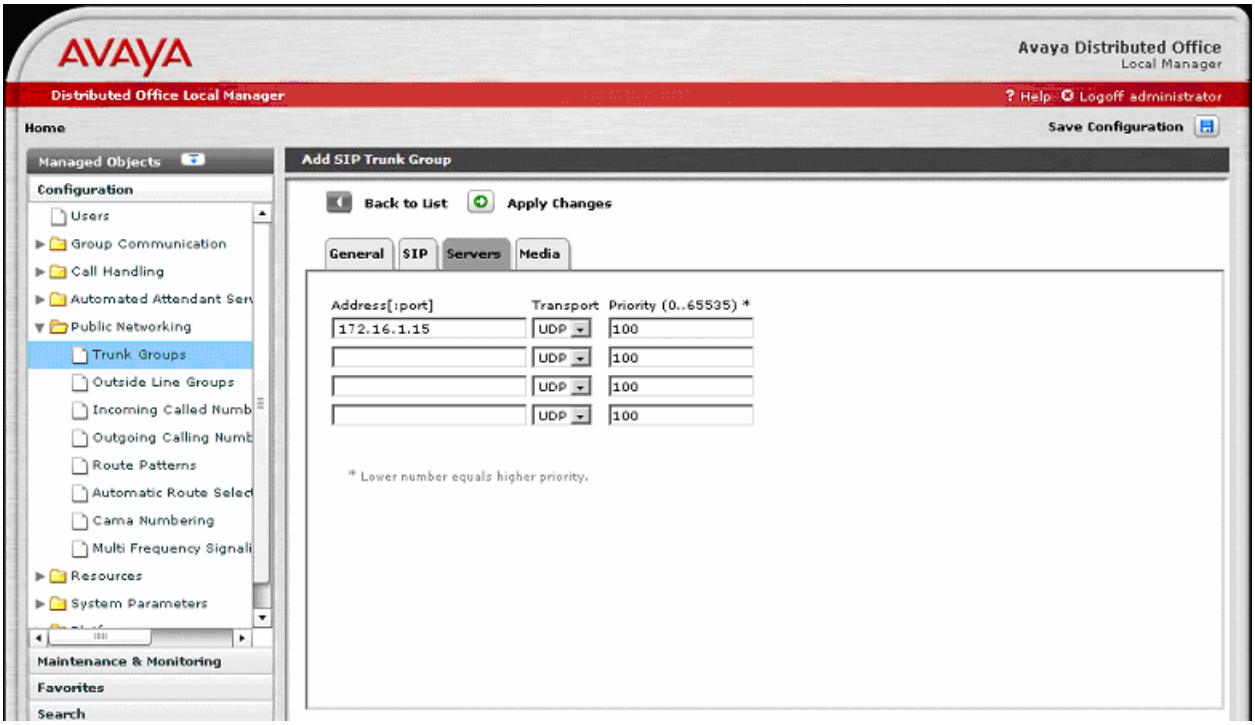

Figure 7 - Avaya Distributed Office Add SIP Trunk Group Screen – Servers Tab

On the **Media** tab:

- Set the **Telephone Events RTP Payload Type** to match the value used by the Avaya 96xx series SIP telephones. In these Application Notes "100" was used matching the Avaya 96xx series SIP telephones default.[2]
- Set the **Max Concurrent Calls** to the number of simultaneous calls supported. This value is specified by the customer when ordering the Nectar Services Corporation On Demand Voice services. It is a function of the bandwidth of the VoIP network access, codec choices and Nectar service limits.
- Check the **Direct Media** option (to allow media paths to be routed directly to IP and SIP endpoints).
- Select **Codec** row 1 to use "G.729a" to use as the preferred codec choice.
- Select Codec row 2 to use "G.711MU" as the second code choice.
- Select the "2 (20ms)" Frames per packet choice for both codecs.
- Select "t.38-standard" **Mode** with "0" **Redundancy** for fax support.

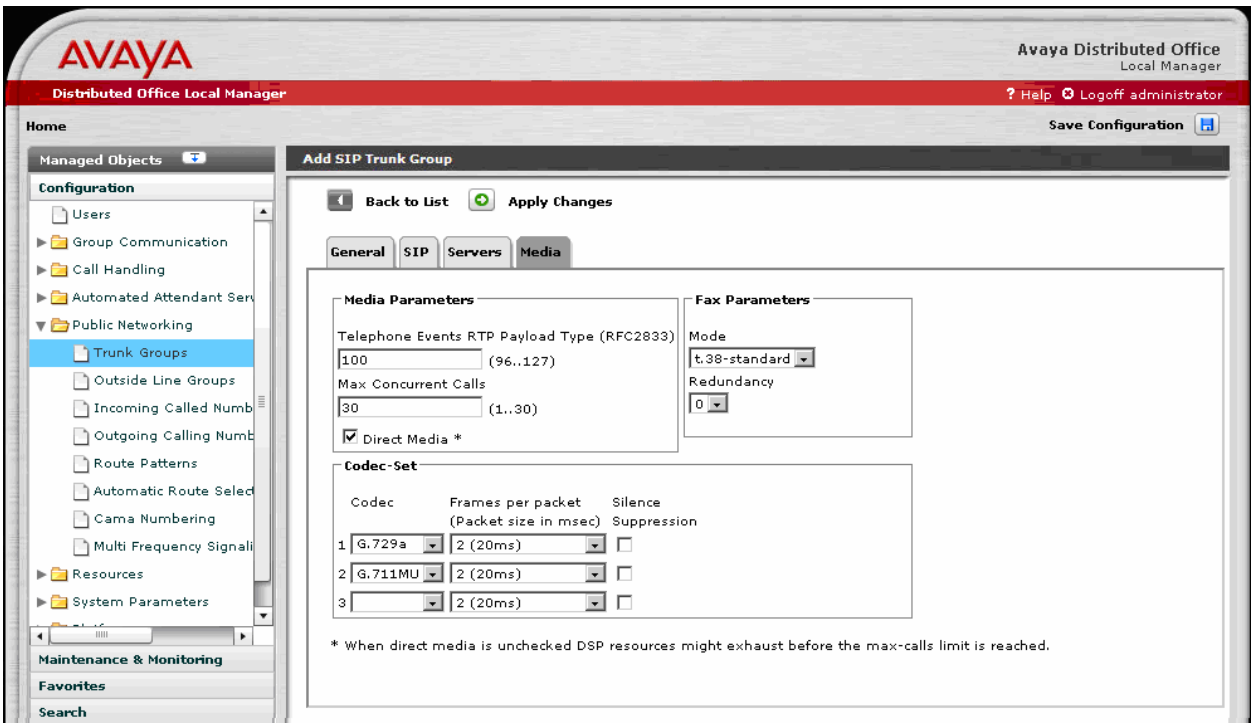

Figure 8 - Avaya Distributed Office Add SIP Trunk Group Screen – Media Tab

[2] This default value used by the 96xx telephones can be modified by changing the SET DTMF_PAYLOAD_TYPE value within the 46xxsettings.txt file used during telephone initialization. Details regarding this administration are beyond the scope of these Application Notes (but are found in Reference [8]).

Press **Apply Changes** before leaving the Add SIP Trunk Group screens.

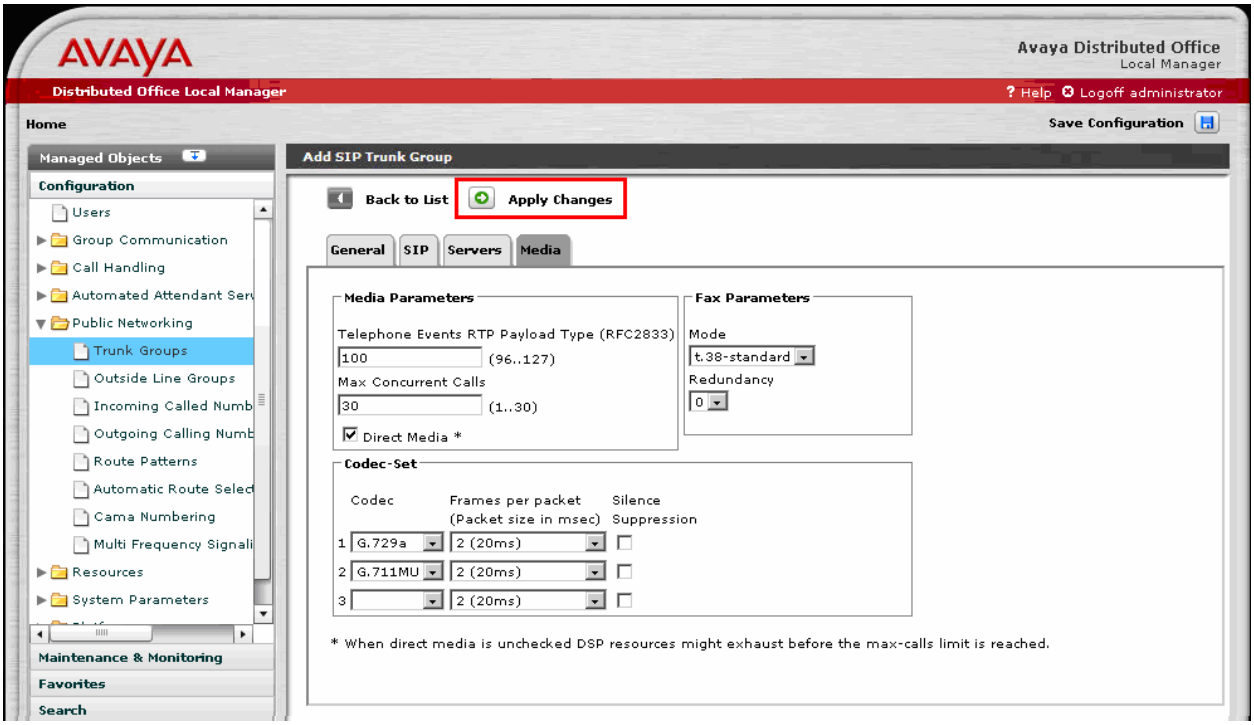

Figure 9 - Avaya Distributed Office Add SIP Trunk Group Screen – Apply Changes

3.2.1. Configure Outgoing Calling Number

The following entries determine the calling number that will be sent in the SIP From header for the corresponding extensions.

From the left hand **Configuration** menu, expand the **Public Networking** option and select **Outgoing Calling Number**. The **Outgoing Calling Number Manipulation** screen will be displayed.

- Select **Add** to display the next **Outgoing Calling Number Manipulation** listing screen.

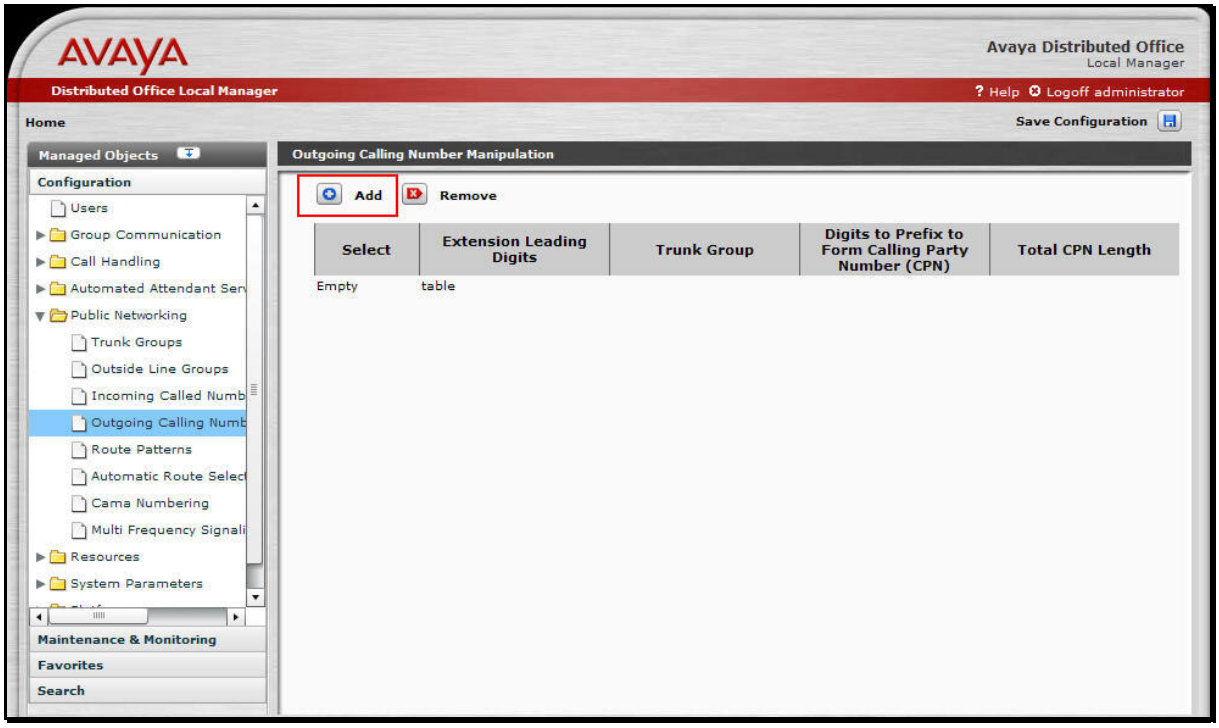

Figure 10 - Avaya Distributed Office Outgoing Calling Number Manipulation

On the **Outgoing Calling Number Manipulation** entry screen,

- Enter the **Extension Leading Digits** necessary to match the applicable range of extension numbers. In these Application Notes, each extension number was configured to map to a unique DID number.
- Select the **Trunk Group** (e.g. "NECTAR-VOIP") that this rule applies to.
- Enter the **Digits to Prefix to Form Calling Party Number**. In these Application Notes a unique 10 digit sequence corresponding to the first 10 digits of the assigned DID number was used to map to a unique enterprise extension.
- Enter the length of the calling party number in the **Total CPN Length** field. In these Application Notes "10" was used.
- Press **Apply Changes** to record the entries and return to the **Outgoing Calling Number Manipulation** summary screen.

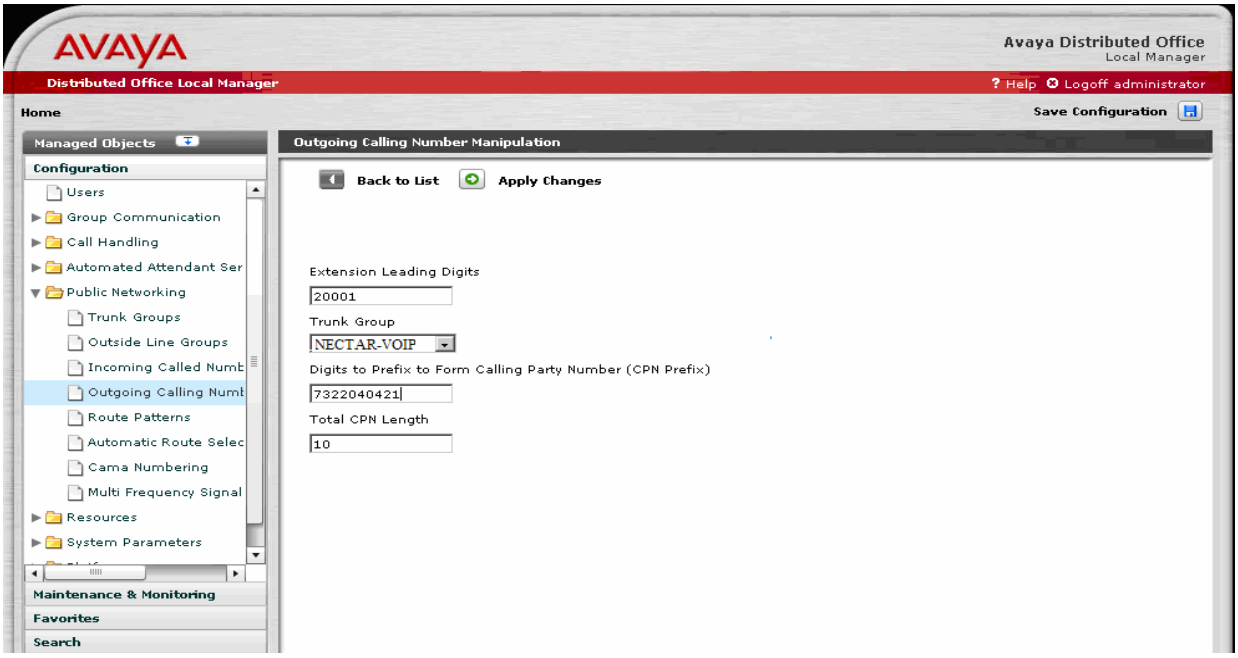

Figure 11 - Avaya Distributed Office Outgoing Calling Number Manipulation – New Entry

The **Outgoing Calling Number Manipulation** summary screen will be displayed.

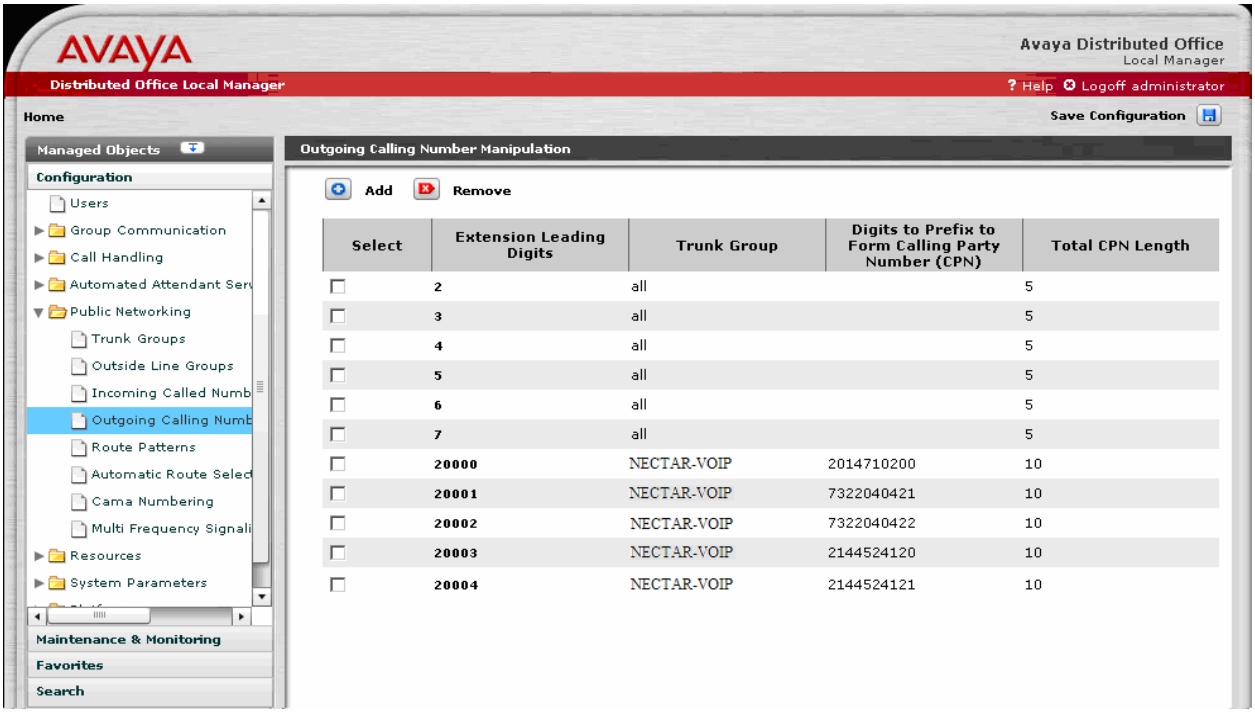

Figure 12 - Avaya Distributed Office Outgoing Calling Number Manipulation – Summary Screen

3.2.2. Configure Call Routing

3.2.2.1 Outbound Calls

The Automatic Route Selection (ARS) feature is used to choose the SIP trunk group to the Nectar Services Corporation On Demand Voice service for outgoing calls.

ARS administration begins with defining a route pattern which specifies the trunk group(s) and outbound digit manipulation rules to be used.

From the left hand **Configuration** menu, expand the **Public Networking** option and select **Route Patterns**. The **Route Patterns** summary screen will be displayed.

- Select **Add New Route Pattern** to display the **Edit Route Pattern** screen.

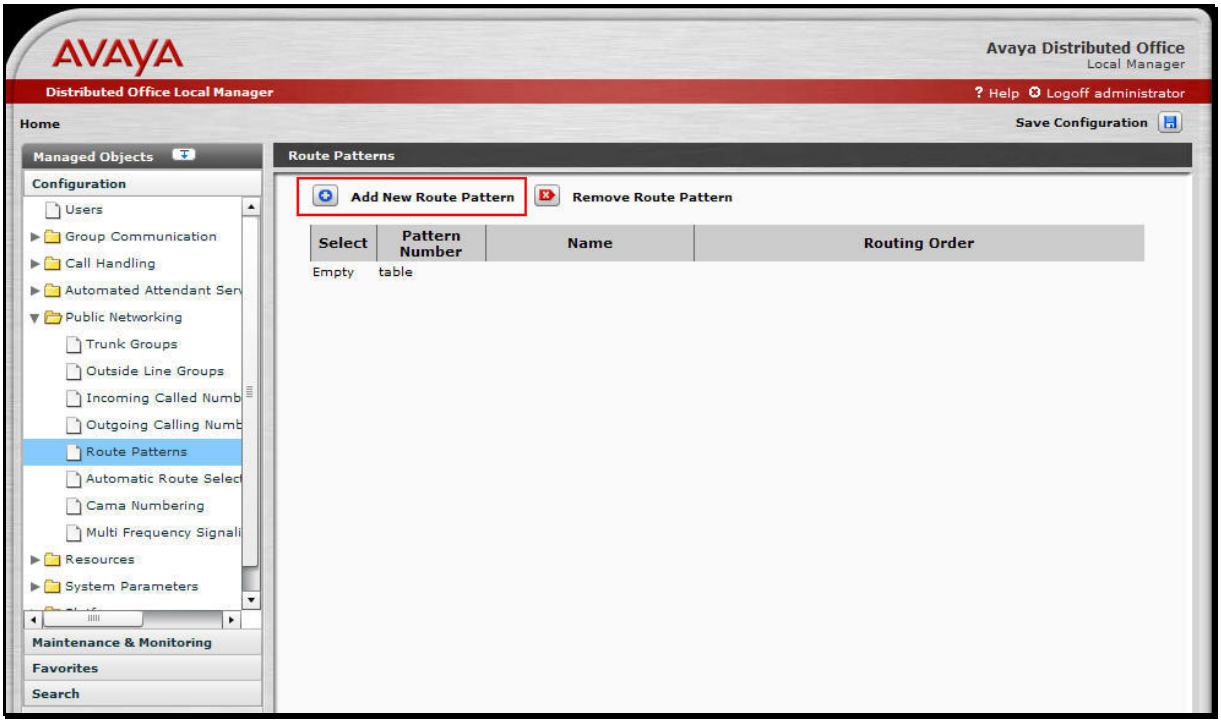

Figure 13 - Avaya Distributed Office Route Patterns

On the **Edit Route Pattern** screen,

- Select an available **Pattern Number**.
- Enter a short test description for the **Pattern Name**. In these Application Notes, "Route-A" was used.
- Select the "NECTAR-VOIP (31)" **Trunk Group** in the number "1" **Order** row. This defines the NECTAR-VOIP trunk group as the first (and only) choice trunk group within this route pattern.
- Leave the **# Digits to Delete** and **Digits to Insert** entries for row 1 blank. This means that the digits dialed at the telephone (without the digit "9" prefix used to denote an ARS routed call) will be sent in the SIP RequestURI to the Nectar Services Corporation On Demand Voice service.
- Press **Apply Changes** to record the route pattern entry and return to the **Route Patterns** screen.

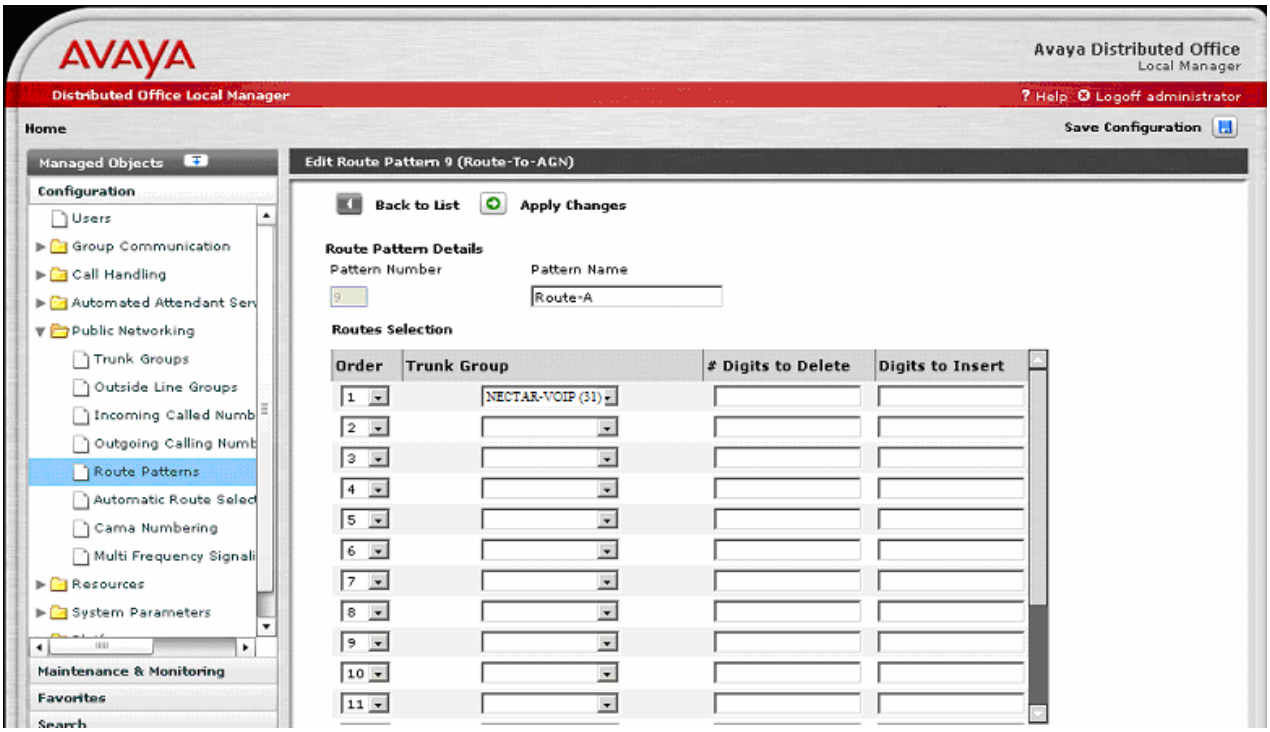

Figure 14 - Avaya Distributed Office New Route Pattern Screen

The **Route Patterns** screen is displayed.

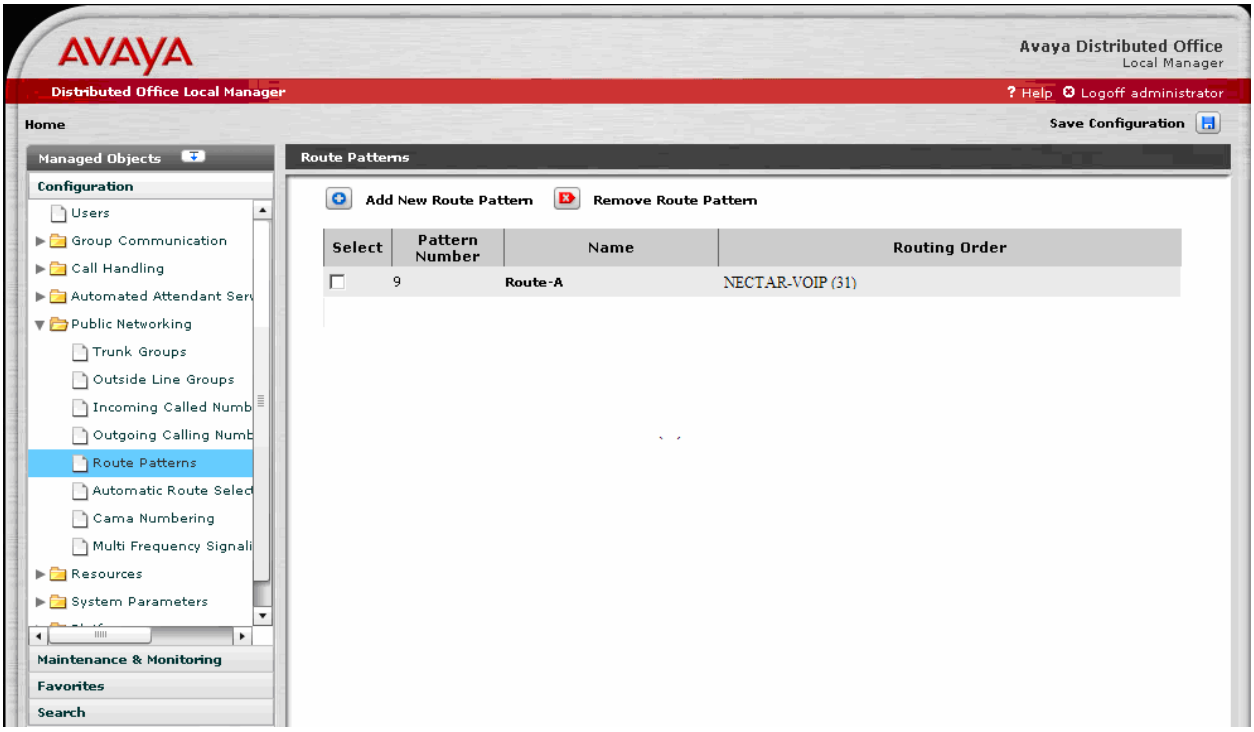

Figure 15 - Avaya Distributed Office Route Patterns – Summary Screen

The next step in ARS administration is to define dialing patterns and the corresponding route patterns and call routing privileges.

From the left hand **Configuration** menu, expand the **Public Networking** option and select **Automatic Route Selection**. The **Public Network Automatic Route Selection** screen is displayed.

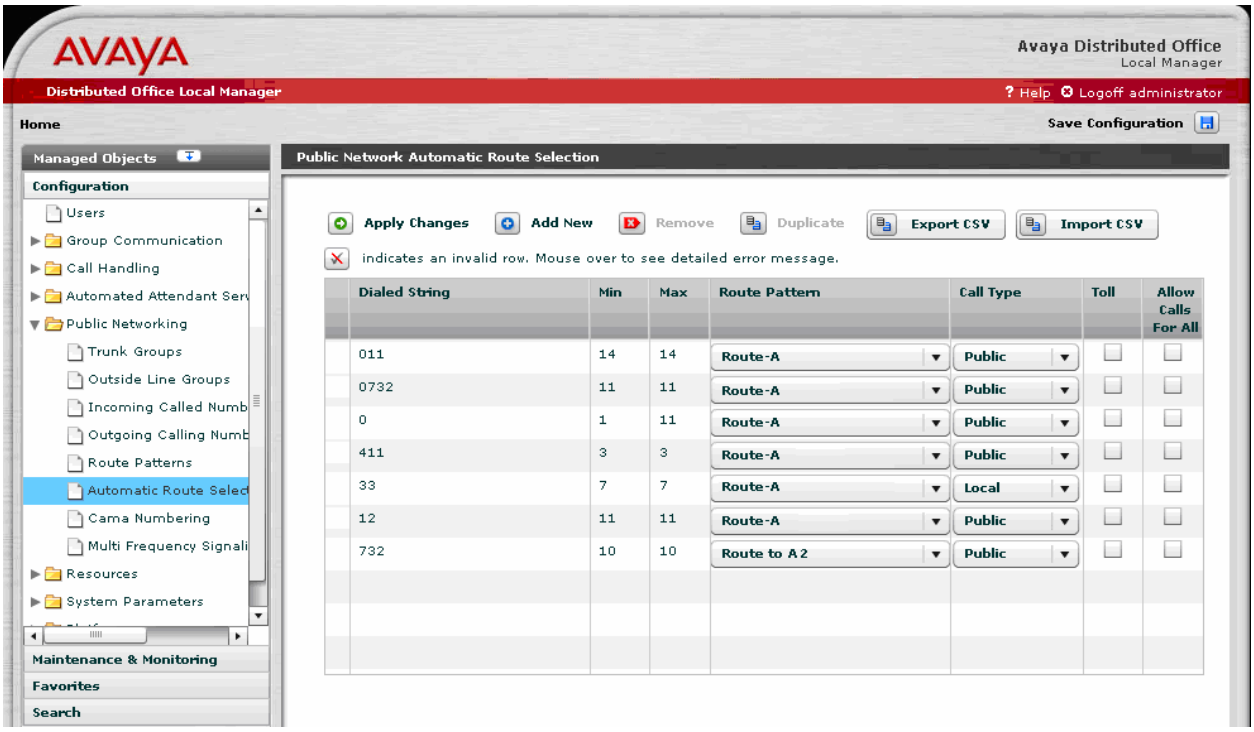

Figure 16 - Avaya Distributed Office Public Network Automatic Route Selection

The following fields are present:

- **Dialed String**: A predefined string to be matched by user-dialed numbers.
- **Min**: The minimum number of user-dialed digits to collect in order to match the dialed string.
- **Max**: The maximum number of user-dialed digits to collect in order to match the dialed string.
- **Route Pattern**: The name of the route pattern (with associated trunk groups and digit manipulation rules) to use when the **Dialed String**, **Min** and **Max** patterns are matched.
- **Call Type**: The type of call that will be placed. Choices include “deny”, “local”, “public”, “emergency” and “crisis-alert”.
- **Toll**: Specifies the extension’s privilege level necessary to place the call. Only extensions having “admin” and “high” privileges are able to place toll calls.
- **Allow Calls for All**: Specifies that any phone may place a call for this dialed pattern.

Further information can be found within the Distributed Office online-help function located on each screen.

ARS administration involves configuring the **Route Pattern**, **Call Type** and calling privileges (e.g., **Toll** and **Allow Calls for All** options) for a specific dialing pattern (e.g. the combination of **Dialed String**, **Min** and **Max**).

In these Application Notes, calls to 1-732-xxx-xxxx (where "x" is any digit) are to be routed via the Nectar Services Corporation On Demand Voice service without requiring toll calling privileges.

- Enter "1732" for the **Dialed String**.
- Enter "11" for **Min**.
- Enter "11" for **Max**.
- Select "Route-A" as the **Route Pattern**.
- Select "Public" as the **Call Type**.
- Uncheck **Toll** to allow extensions with low, medium, high and administrative user privilege levels to place 1-732-xxx-xxxx calls. (Note: the user privilege level is assigned to an extension during user administration and beyond the scope of these Application Notes.)
- Uncheck **Allow Calls for All** to prevent extensions with no privileges from being able to place 1-732-xxx-xxxx calls.

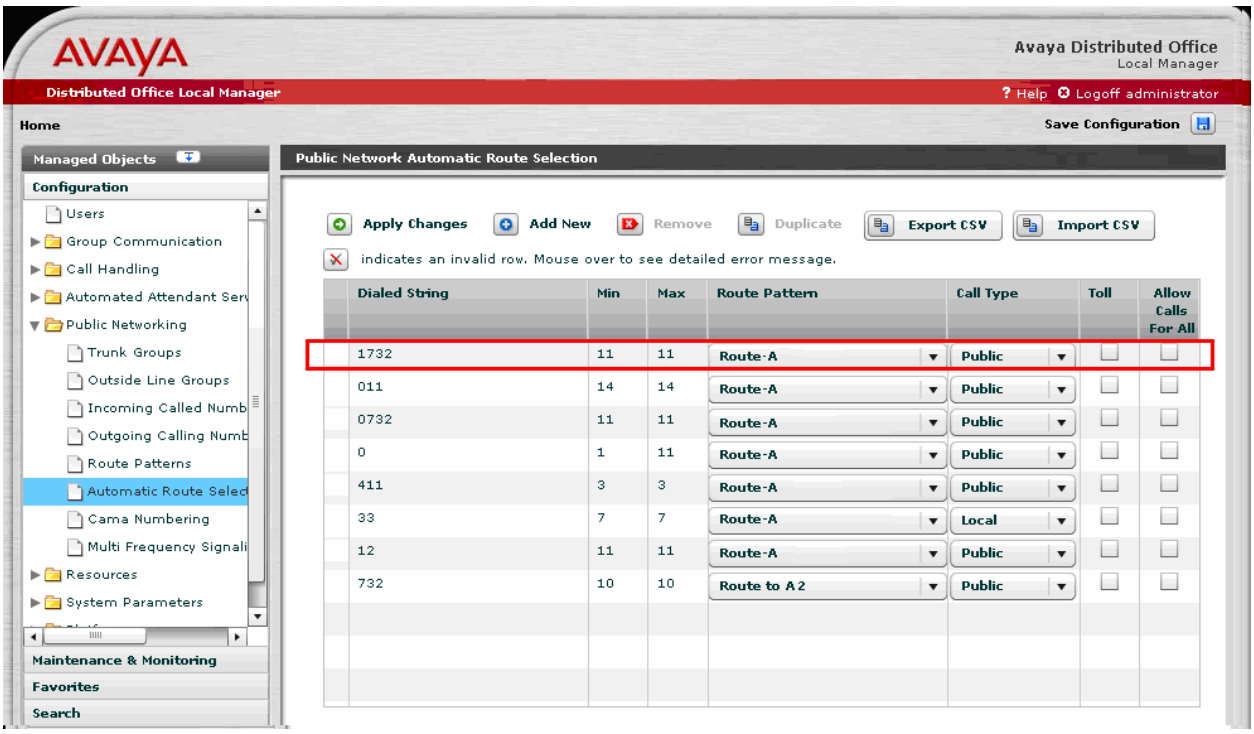

Figure 17 - Avaya Distributed Office Public Network Automatic Route Selection – Summary Screen

The figure below illustrates configuration information for a number of other dialing patterns.

After completion of the ARS entries:

- Press Apply Changes to record the ARS entries.

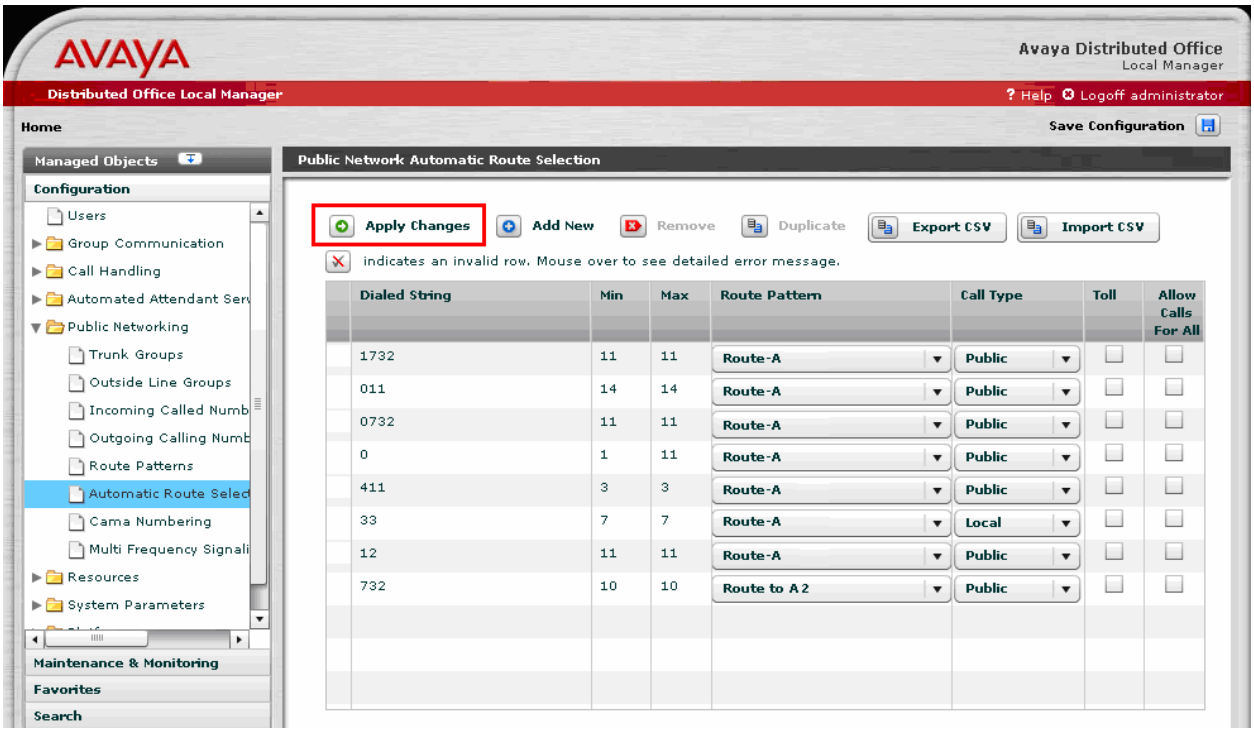

Figure 18 - Avaya Distributed Office Public Network Automatic Route Selection – Apply Changes Screen

3.2.2.2 Inbound Calls

This step configures the routing of incoming DID calls to the associated Avaya Distributed Office extensions. In these Application Notes, the incoming PSTN DID numbers listed in **Figure 1** are assigned to the extensions as shown in **Table 3**. The DNIS values were defined to be a 3-digit routing number followed by the full 11 digit North American telephone number.

Dialed PSTN Number	Digits Received (within SIP INVITE message)	Extension Assigned
1-732-204-0421	90217322040421	20001
1-732-204-0422	90217322040422	20002
1-201-471-0200	90212014710200	20000
1-214-452-4120	90212144524120	20003
1-214-452-4121	90212144524121	20004

Table 3 - Incoming DID Number Assignments

Begin the incoming DID assignments from the left hand **Configuration** menu.

- Expand the **Public Networking** option and select **Incoming Called Number Manipulation**. The **Incoming Called Number Manipulation** screen will be displayed.
- Select **Add** to display the **Add Incoming Called Number Manipulation** screen.

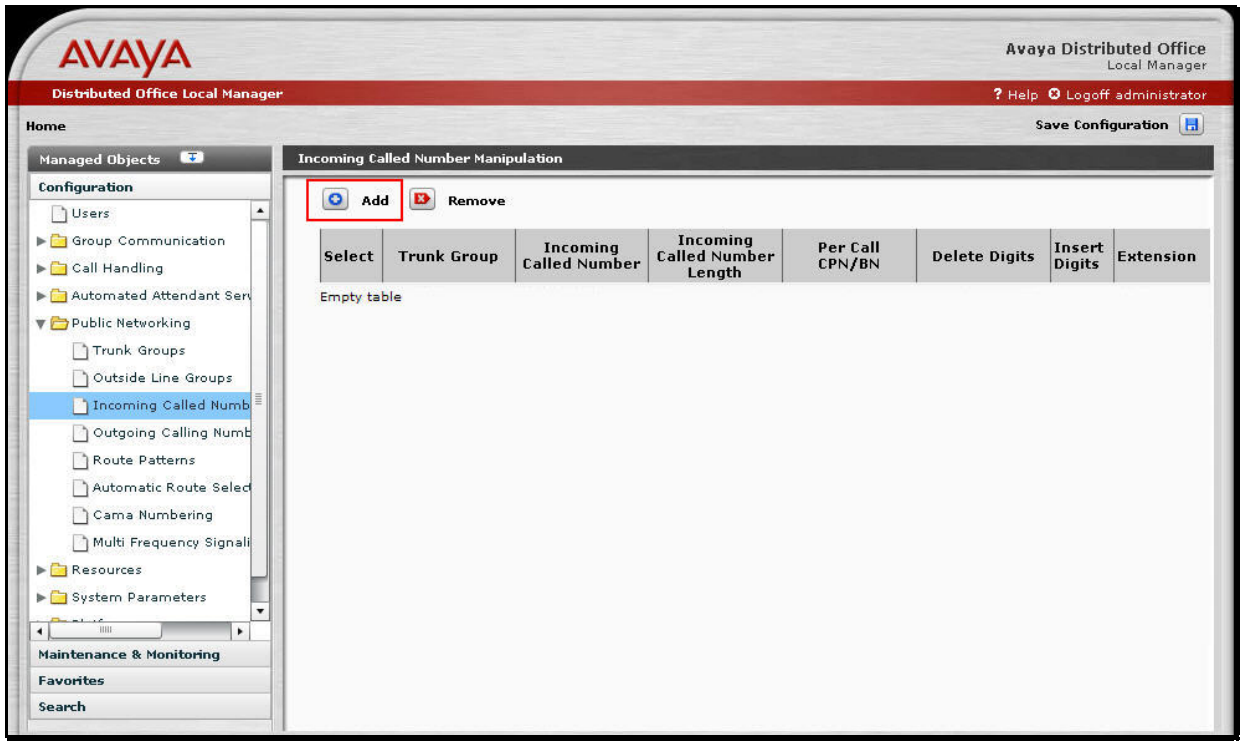

Figure 19 - Avaya Distributed Office Incoming Called Number Manipulation

From the **Add Incoming Called Number Manipulation** screen, enter the following to administer the assignments for the DID numbers:

- Select "NECTAR-VOIP" as the **Trunk Group**.
- Enter "90212014710200" as the **Called Number** digit pattern to be matched.
- Enter "14" as the **Called Number Length**. This is the total number of digits sent by Nectar Services Corporation.
- Select the **Extension** to map to the called number.
- Press **Apply Changes** to record the information entered and redisplay the **Incoming Called Number Manipulation** screen.

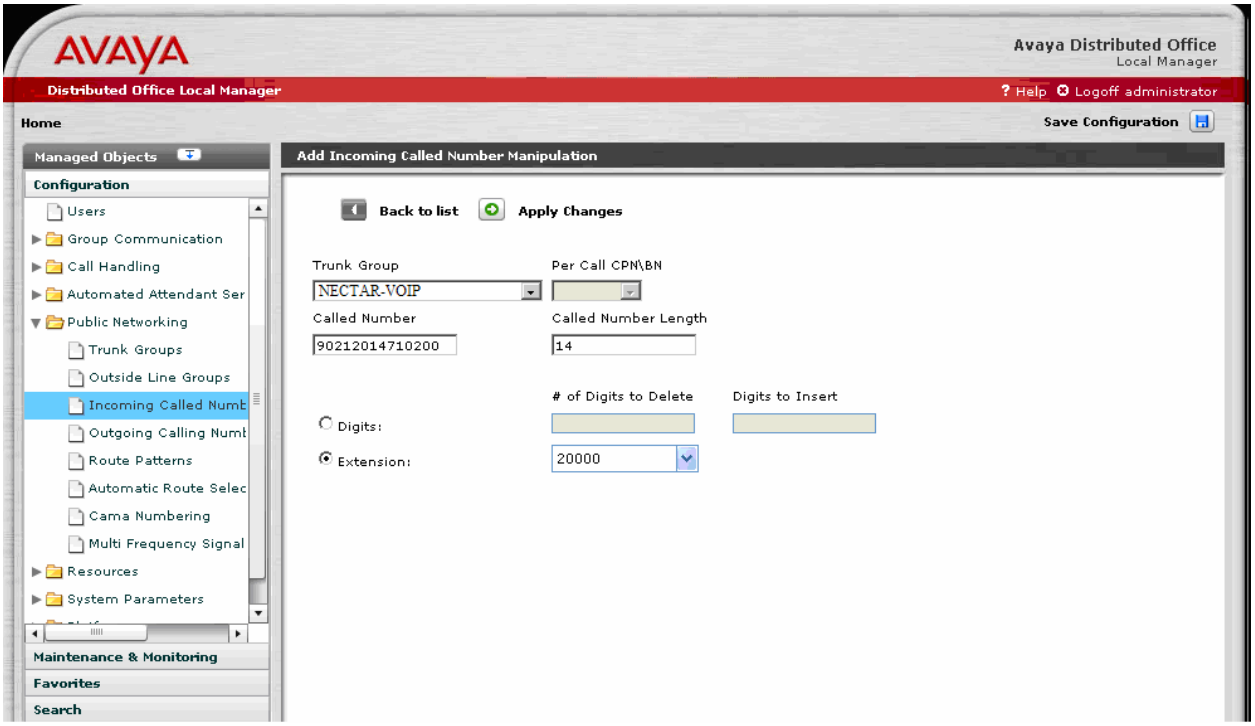

Figure 20 - Avaya Distributed Office Add Incoming Called Number Manipulation

Repeat the **Add Incoming Called Number Manipulation** process to administer the mapping for the other numbers listed in **Table 3**. After the **Apply Changes** is performed, the resulting **Incoming Called Number Manipulation** screen is shown.

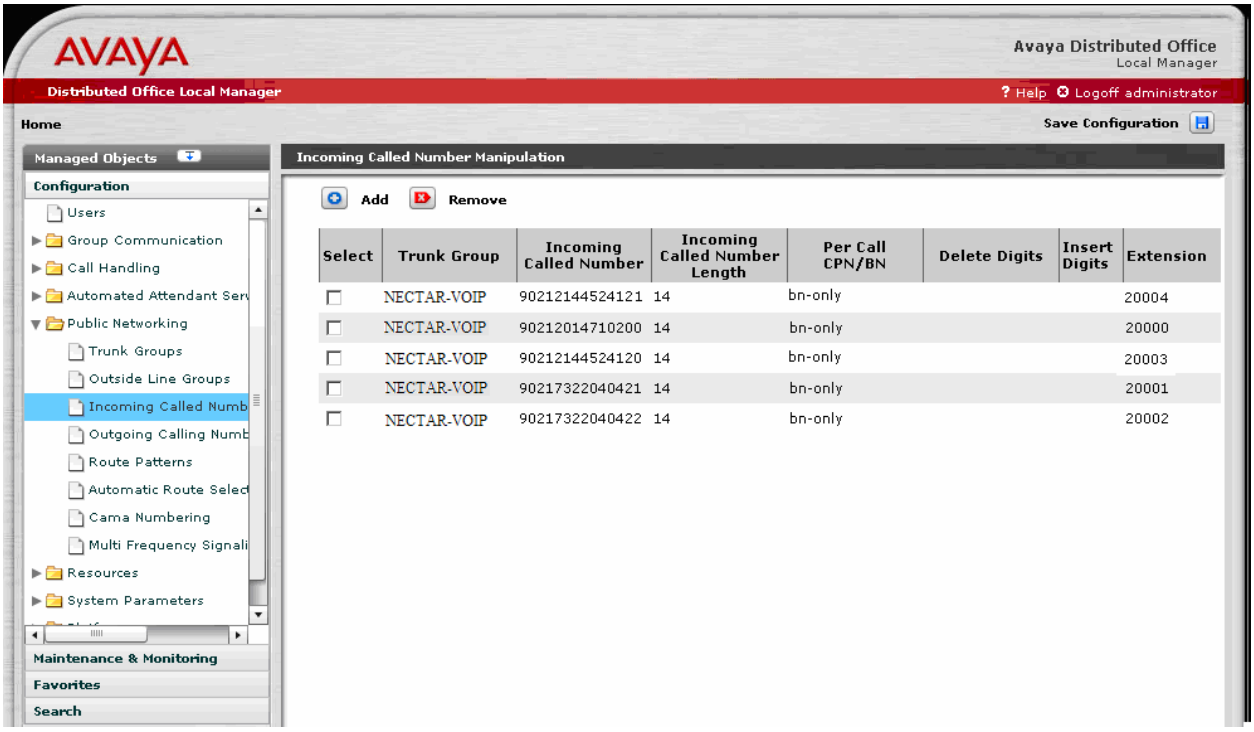

Figure 21 - Avaya Distributed Office Incoming Called Number Manipulation – Summary Screen

3.2.3. Save Avaya Distributed Office Configuration

The configuration of the Avava Distributed Office SIP trunking with the Nectar Services Corporation On Demand Voice service is now complete. Save the Avaya Distributed Office configuration (in non-volatile memory) by pressing the **Save Configuration** link found in the upper right hand corner. This prevents the administration changes from being lost upon a reboot or power failure.

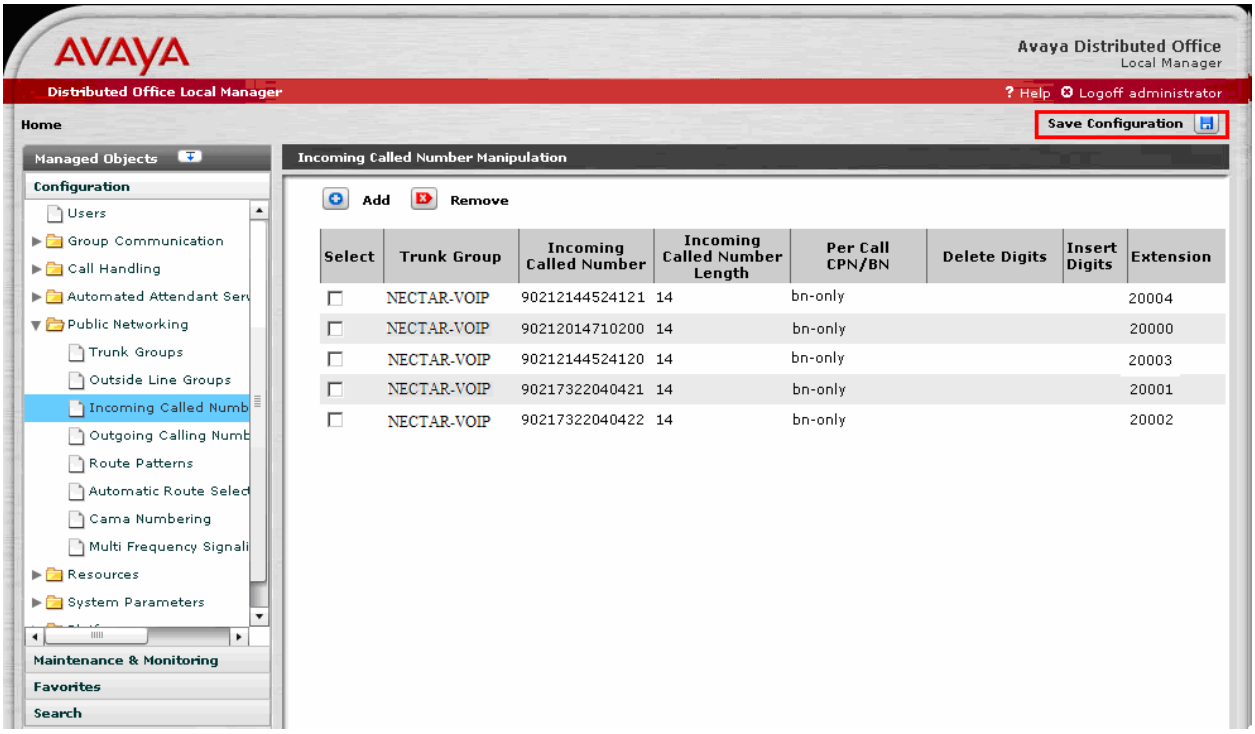

Figure 22 - Avaya Distributed Office – Save Configuration

4. Nectar Services Corporation On Demand Voice Service Configuration

In order to use the On Demand Voice service, a customer must request service using the Nectar Services Corporation sales process. The process can be started by contacting Nectar Services via the links found on their corporate web site at http://nectarnetworks.com/ and requesting information via the sales links or telephone numbers.

During the signup process, Nectar Services Corporation will require that the customer provide the public IP address used to reach the Avaya Distributed Office. Note the address used within these Application Notes is 65.211.92.41; the actual IP address will be specific to the customer implementation.

Following signup, Nectar Services Corporation will provide the following:

- Username and Password to access the customer support web site.
- IP address of the Nectar Services Corporation SIP Proxy Server.

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

Step 1: Access the Nectar Services Corporation Web Site
To begin, access the Nectar Services web site at http://my.nectarvoip.com/ as shown in **Figure 23**. Log in by entering the **Username** and **Password** provided by Nectar Services Corporation.

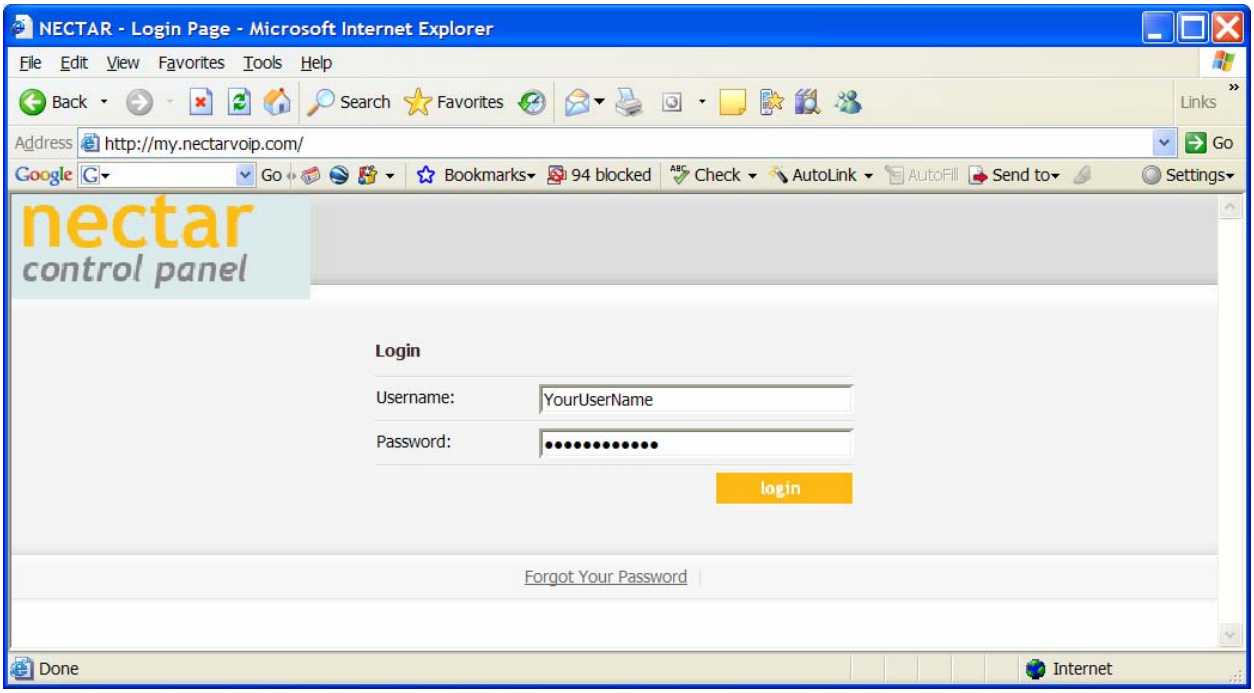

Figure 23 – Nectar Services Corporation Customer Login Screen

Step 2: Manage Addresses
Select the **Locations** tab in the horizontal navigation bar. Click on the **Manage Addresses** link found on the left hand menu followed by the **Add Address** link as shown in **Figure 24**.

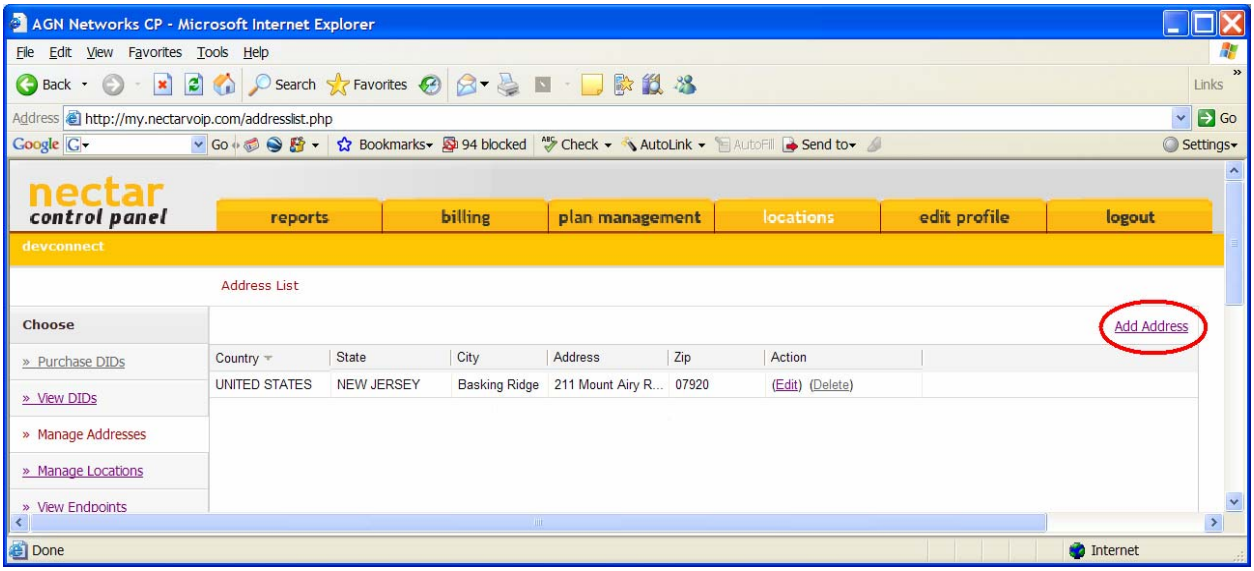

Figure 24 – Nectar Services Corporation Address List Screen

Step 3: Add a New Address
On the **Add Address** page (**Figure 25**) enter the new address information and click on **Submit**.

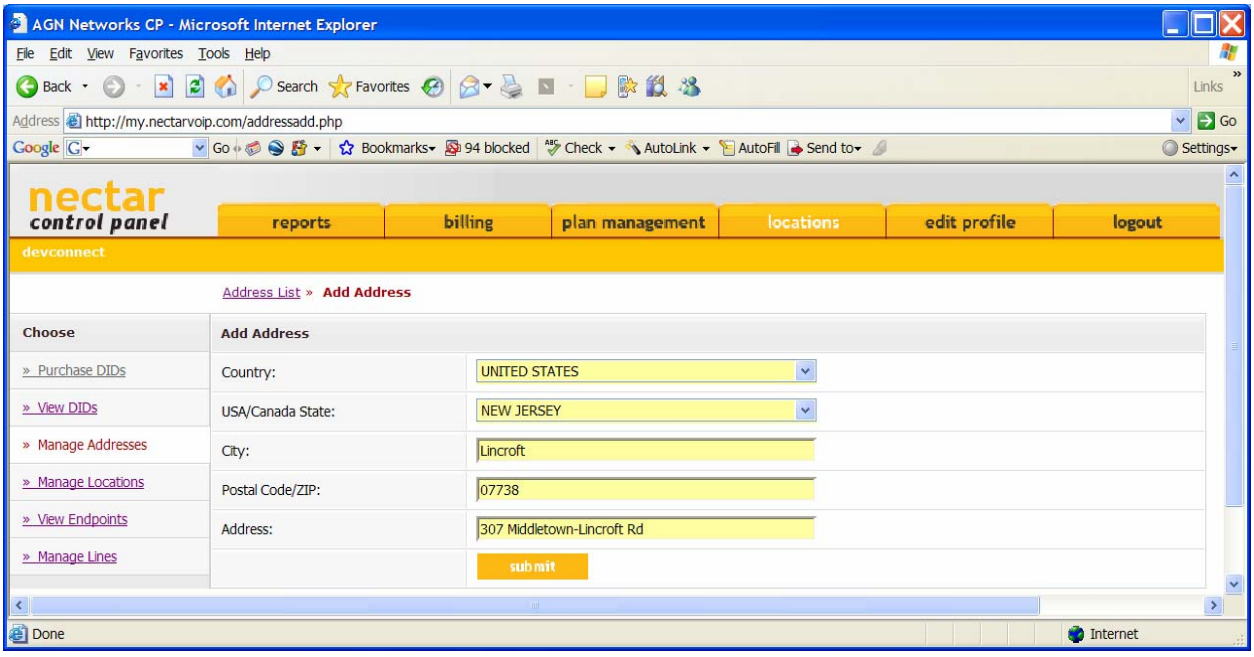

Figure 25 – Nectar Services Corporation Add Address Screen

Step 4: Purchase Telephone Lines

Select the **Locations** tab in the horizontal navigation bar. Click on the **Manage Lines** link **(Figure 26)** and enter the following:

- **Number of Lines to Purchase** – Enter the number of telephone lines to purchase.
  Lines to Disconnect – Enter the number of telephone lines to disconnect.

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

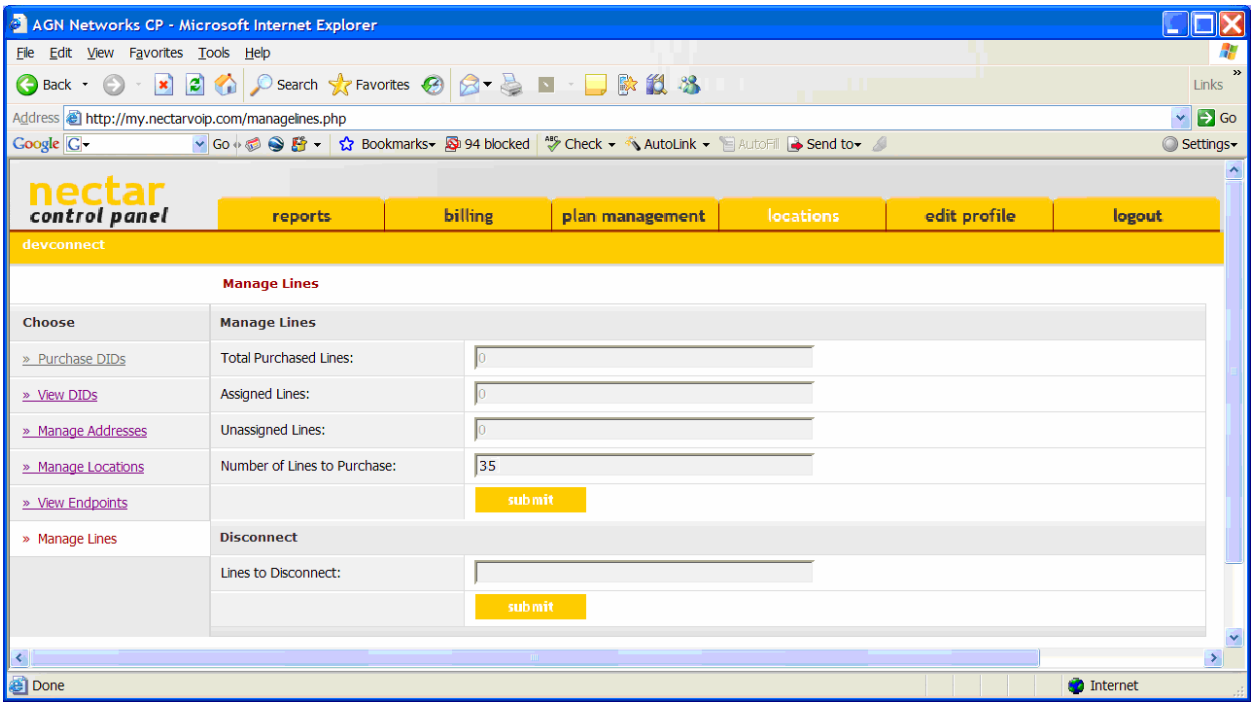

Figure 26 – Nectar Services Corporation Manage Lines Screen

Step 5: Add a New Location

Select the **Locations** tab in the horizontal navigation bar to display the **Location List** page as shown in **Figure 27**. Click on the **Add Location** link.

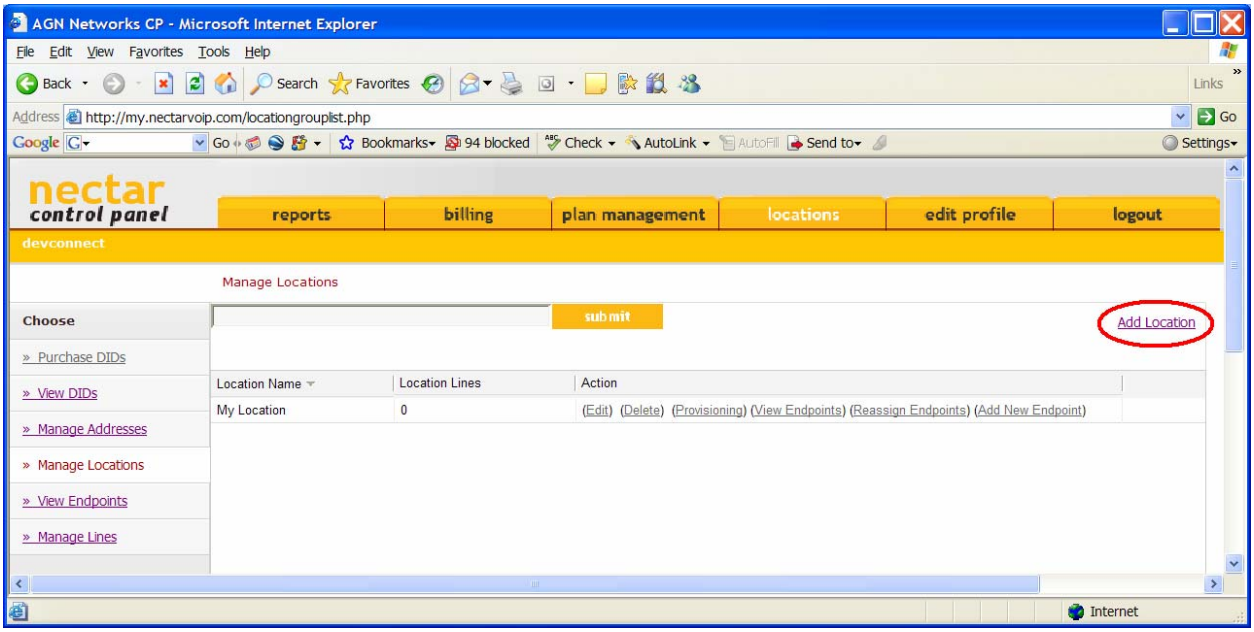

Figure 27 – Nectar Services Corporation Locations Screen

Step 6: Specify the Location Information

On the Add Location page **(Figure 28)** enter the following:

- **Location Name** – Enter an alphabetic name describing the location where the Avaya Distributed Office resides. In this example, "DevConnect Test Lab" is used as the location name.
- **Max Calls Total** – Enter the total number of calls for the location.
- **Available Lines** – Enter the number of telephone lines for the location.
- **Location Address** – Select the postal address for the location.
- **Location Reference Number** – Enter the location reference number.
- **Default Caller ID** – Enter the default caller ID for the location. This Caller ID would be used in the absence of the ANI being sent from the Avaya Distributed Office.
- **Allow CID Pass Through** – Select this field to allow Caller ID from the Avaya Distributed Office to pass through the network.

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

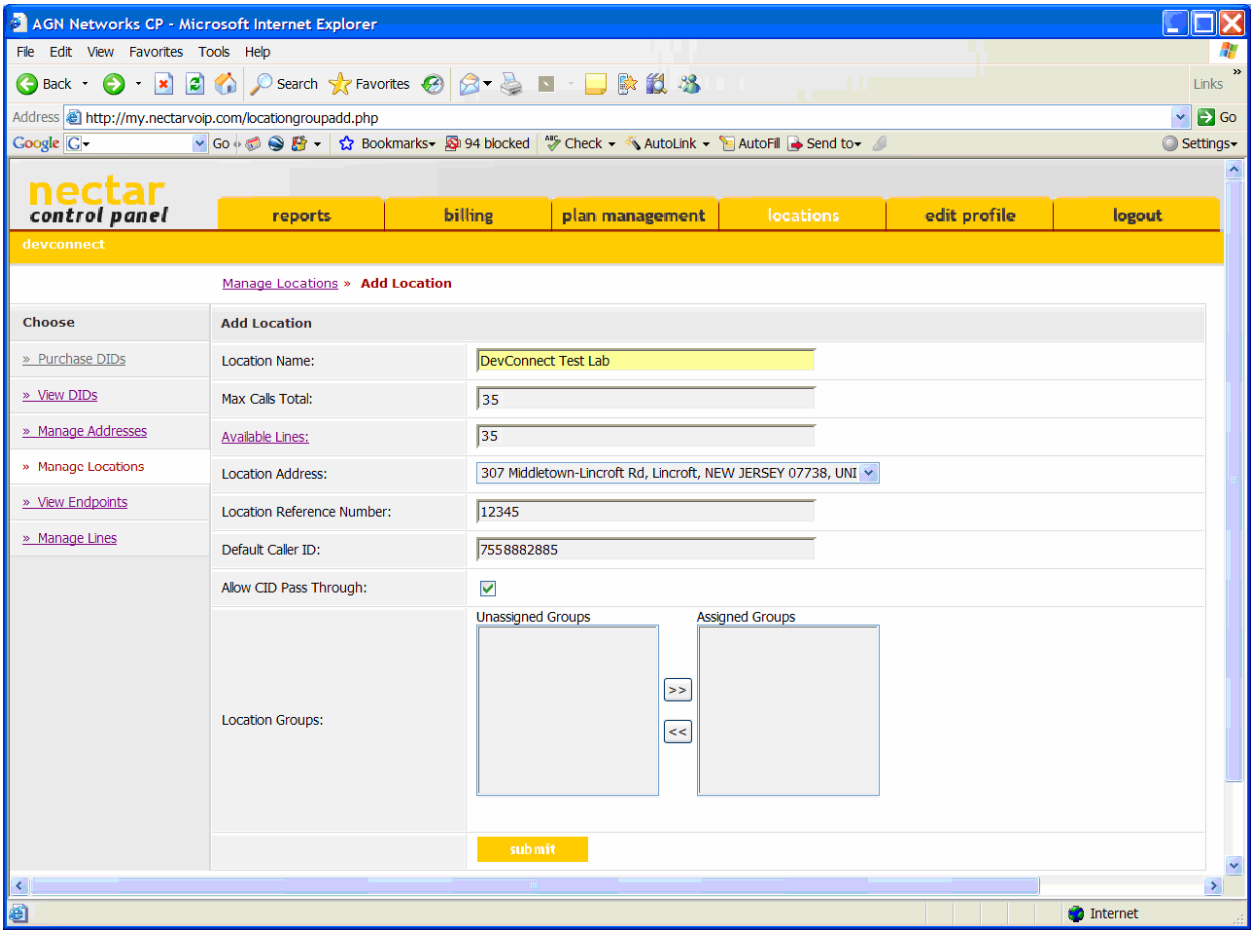

Figure 28 – Nectar Services Corporation Add Location Form

The **Manage Locations** page appears with the new list of locations. Click the **Provisioning** link associated with the provisioned location to activate the configuration.

Step 7: Manage Locations - Add Endpoint

Select the **Locations** tab in the horizontal navigation bar to display the **Manage Locations** page and click on the **Add New Endpoint** link associated with the "DevConnect Test Lab" location as shown in **Figure 29**.

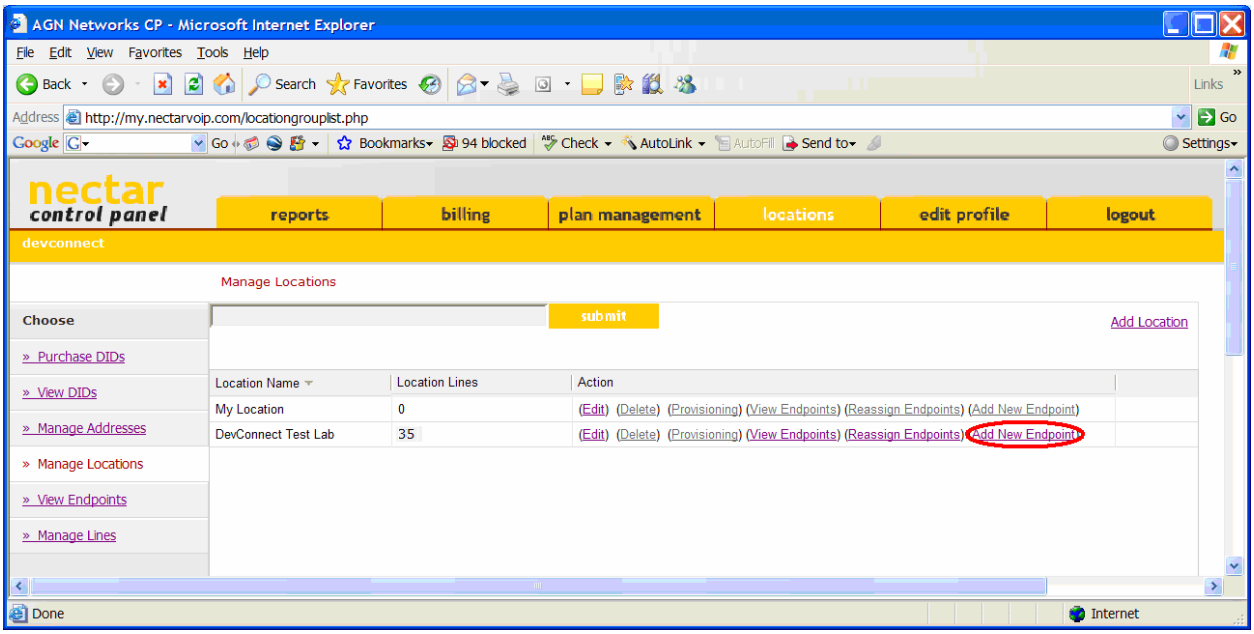

Figure 29 – Nectar Services Corporation Locations Screen

Step 8: Add Endpoint
On the **Add Endpoint** page (**Figures 30-31**), enter the relevant information associated with Avaya Distributed Office and click the **Submit** button.

Below is a description of the fields:

- **Endpoint Name** – Enter an alphabetic name describing the Avaya Distributed Office.
- **System ID** – This is the system ID associated with the endpoint that is automatically generated by the system.
- **IP Address** – Enter the public IP Address associated with the Avaya Distributed Office.
- **Signaling Port** – Enter port 5060 as per the port configured on the Avaya Distributed Office.
- **IP PBX Types** – Select "Generic SIP" for interoperability with the Avaya Distributed Office.
- **Default Caller ID** – Enter the default caller ID for the location. This Caller ID would be used in the absence of the ANI being sent from the Avaya Distributed Office.
- **Allow CID Pass Through** – Select this field to allow Caller ID from the Avaya Distributed Office to pass through the network.
- **Auth Password** – Leave the field blank for interoperability with Avaya Distributed Office.
- **Media Route** – Select this field to turn media shuffling off. Leave the field unchecked to route media directly between endpoints.
- **TCP** – Select this to field turn on TCP signaling.
- **Connection** – Select "Public" since the Avaya Distributed Office is assigned a public IP Address. The firewall NATs the public IP Address to the private IP Address assigned to the Avaya Distributed Office.
- **Choose Address –** Select the mailing address associated with the Avaya Distributed Office location.
- **Disaster Recovery Numbers (Numbers 1 through 5)** – Enter up to 5 optional disaster recovery numbers to which Nectar Services can route calls in case the Avaya Distributed Office system cannot be contacted.
- **Available Lines** – This read only field describes the number of telephone lines available to be assigned to endpoints.
- **Assigned Lines** – Enter the number of concurrent telephone lines supported by the endpoint. This number should match the number of lines configured on the Avaya Distributed Office (**Section 3.2**)

For additional information refer to the Nectar Service Portal online help.

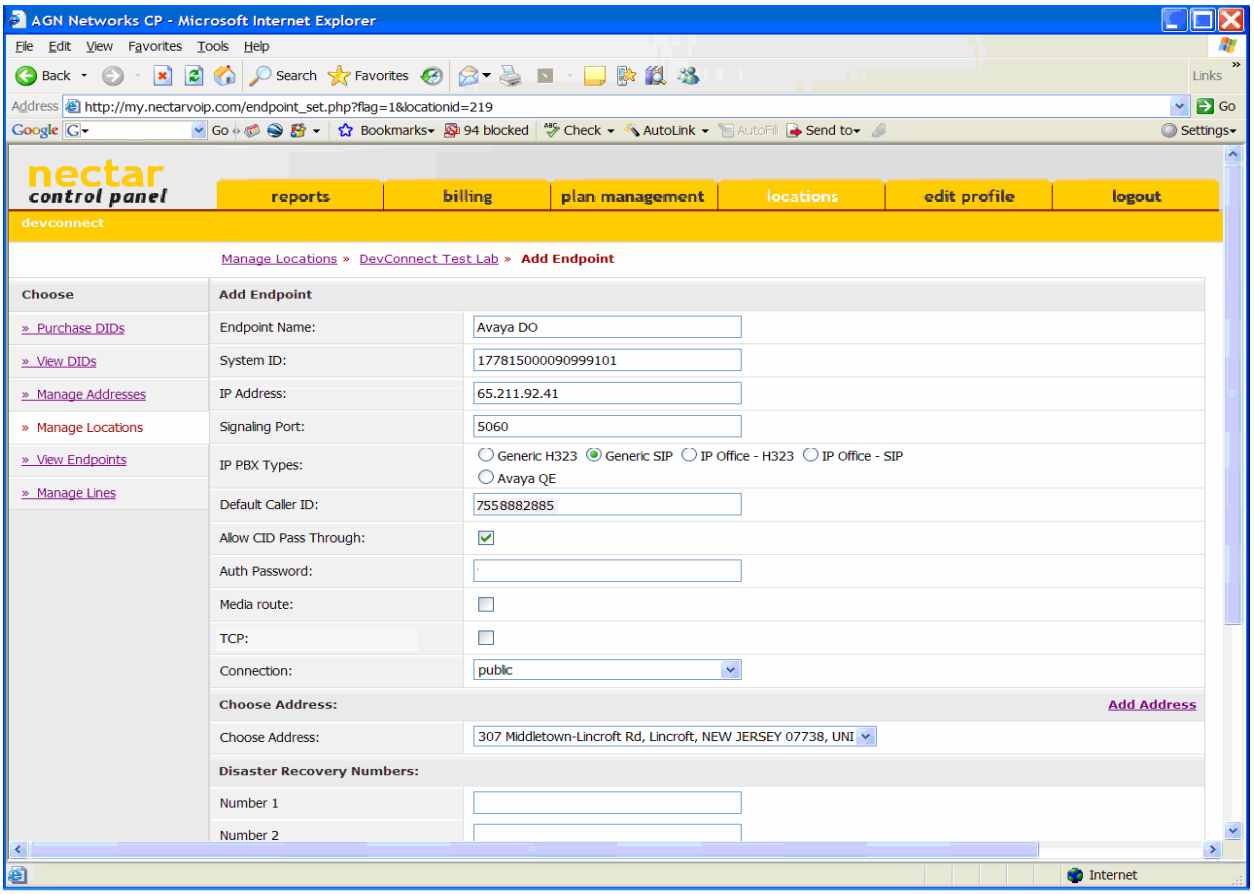

Figure 30 – Nectar Services Corporation Add Endpoint Screen – Part 1

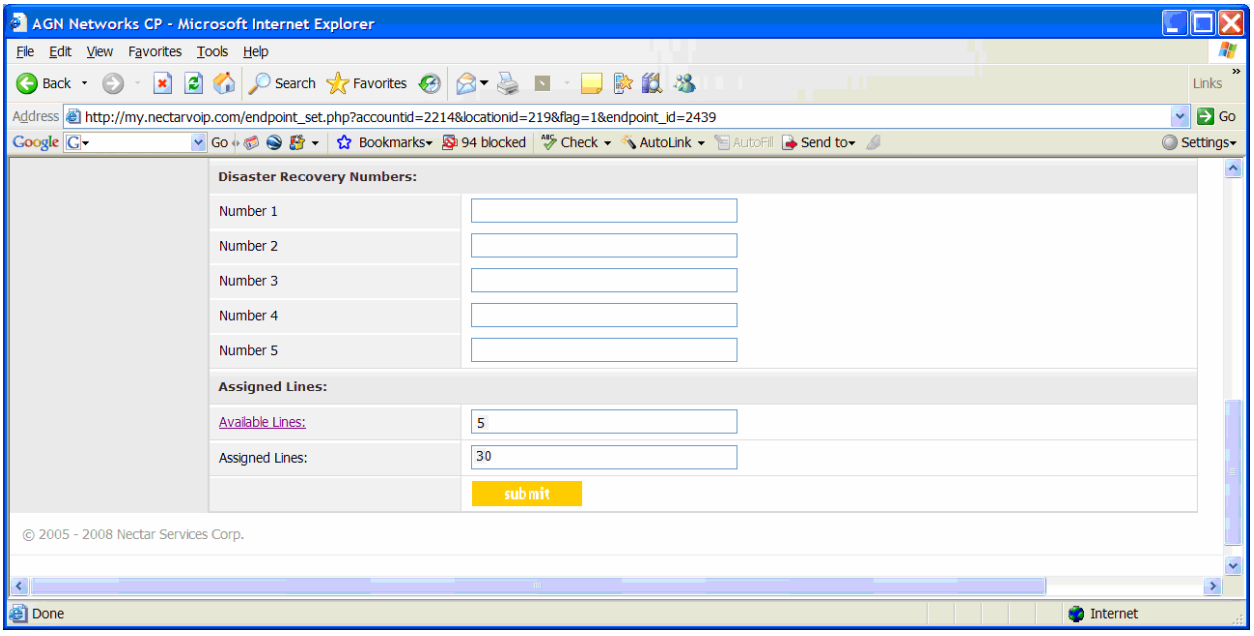

Figure 31 – Nectar Services Corporation Add Endpoint Screen – Part 2

The **Endpoints** page appears with the new list of endpoints. Click the **Provisioning** link associated with the provisioned endpoint to activate the configuration.

Step 9: Obtain DID and/or TollFree Numbers
To receive incoming calls, either DID and/or TollFree numbers must be purchased.

- From the **Locations** tab, click the **Purchase DIDs** link found on the left hand menu. The form shown in **Figure 32** appears.
- For DID numbers, select the desired **State**, **Area Codes**[3] and **City** from the drop down lists as shown.
- Enter the number of DID numbers (for that City) desired into the **Desired Quantity** field.
- Press the **Submit** button.
- Click **Yes** to indicate acceptance of additional charges in the pop-up window that may appear.

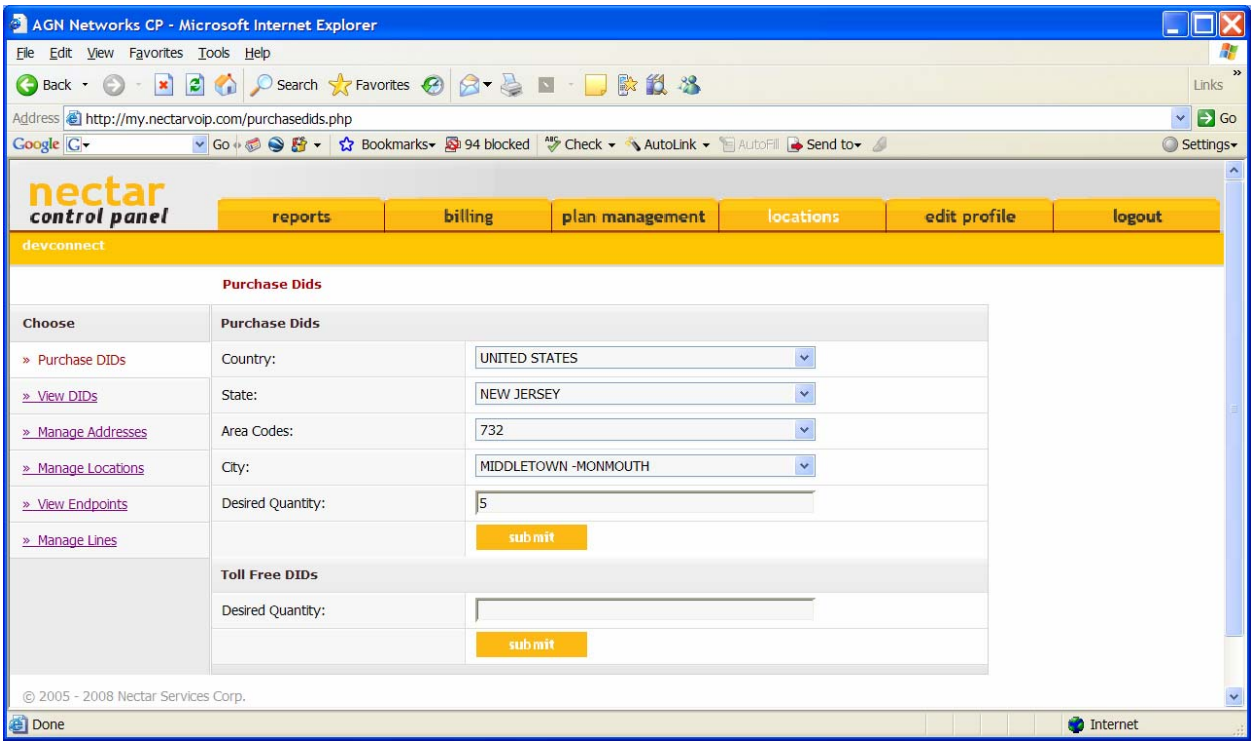

Figure 32 – Nectar Services Corporation Purchase DIDs Form

[3] DIDs starting with various area codes were used during the compliance testing. The area code shown in Figure 29 is for illustrative purposes only.

- Following the submission, use the **View DIDs** link to see the DID numbers reserved for use as shown in **Figure 33**.

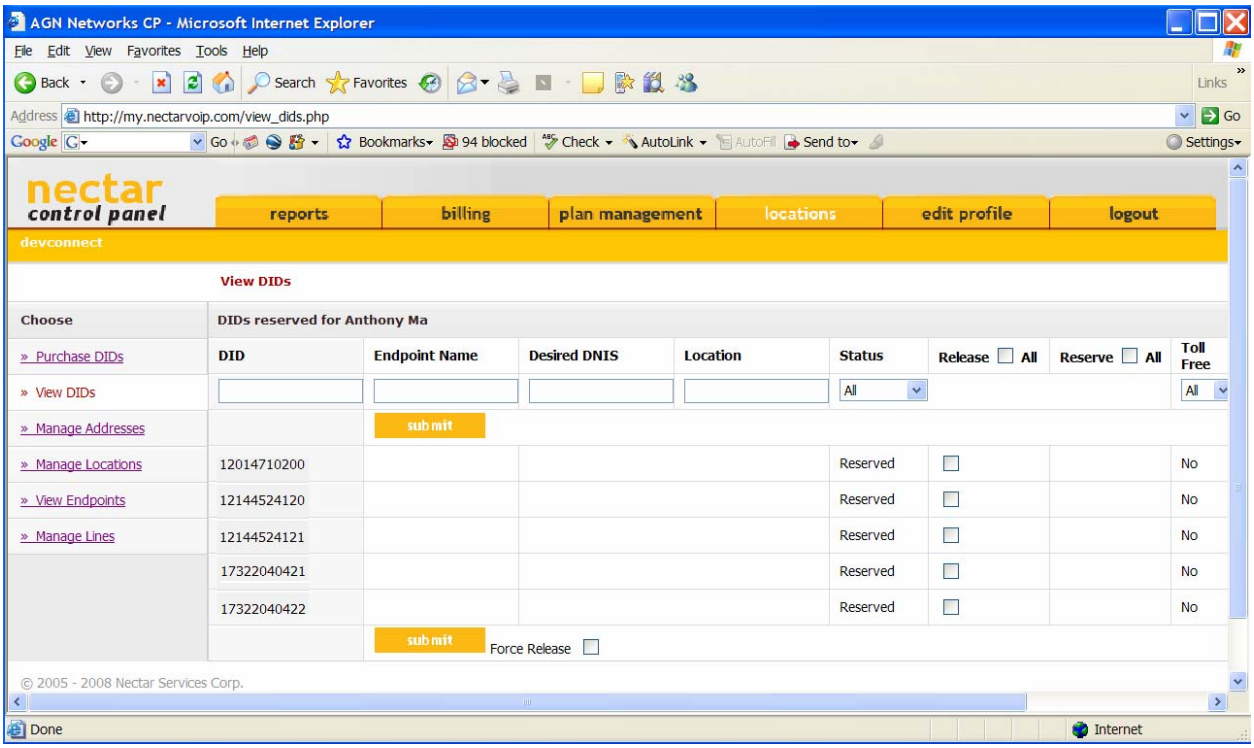

Figure 33 – Nectar Services Corporation Reserved DID Numbers

Step 10: Assign DID Numbers

The reserved DID numbers must now be assigned to the endpoints associated with the "DevConnect Test Lab" location previously defined.

- Click the **View Endpoints** link from the left menu. The **Endpoints** page **(Figure 34)** will appear.

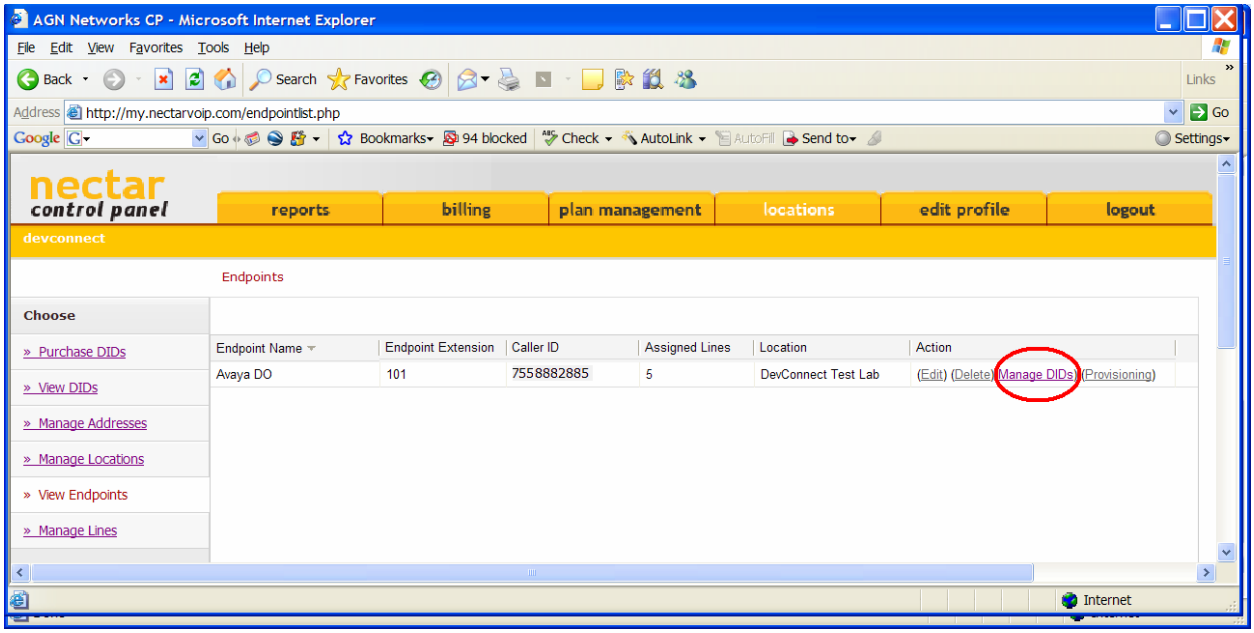

Figure 34 – Nectar Services Corporation Location Screen

- Click the **Manage DIDs** link associated with the endpoint added to the location provisioned above (i.e., DevConnect Test Lab).

The **Managed DIDs** link will open a new page.

- 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 endpoint.

Step 11: Specify the Desired DNIS Values

Finally, update the Desired DNIS values to match the routing strategy defined in Section 3.2.2.2 during the configuration of Avaya Distributed Office. 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 with default Desired DNIS values will be seen. Note that the current **Desired DNIS** values do not currently match the desired numbering strategy.
- Update each **Desired DNIS** field accordingly and press the **Submit** button. In this example, the Desired DNIS values should be "902" followed by the DID number shown in the left column.
- Verify that the correct **Desired DNIS** values are now recorded and the DID **Status** is Active as shown in **Figure 35**.

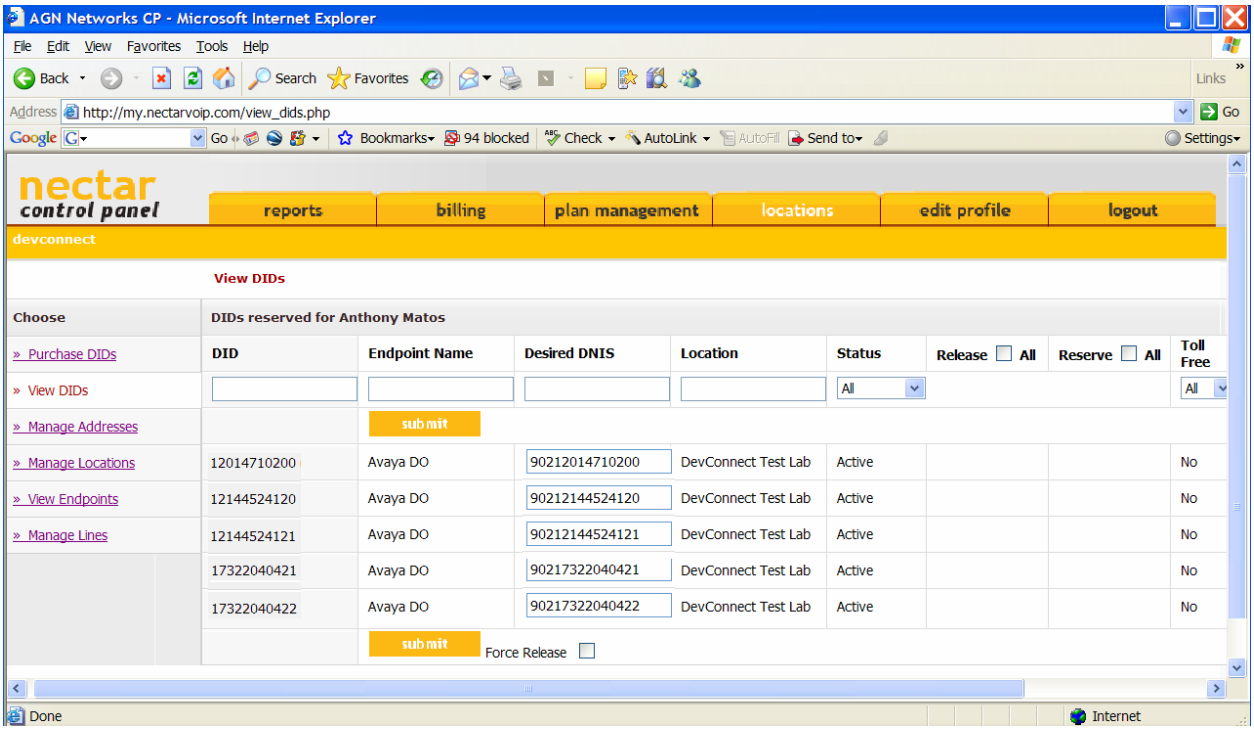

Figure 35 – Successful Update of Desired DNIS fields.

This completes the configuration within Nectar Services Corporation for inbound and outbound calling.

5. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify SIP trunking interoperability between the Nectar Services Corporation On Demand Voice services and the Avaya Distributed Office. This section covers the general test approach and the test results.

5.1. General Test Approach

Avaya Distributed Office i120 (Release 1.2) was connected using SIP trunking (via general purpose Internet services) to the Nectar Services Corporation On Demand Voice service.

The following features and functionality were covered during the SIP trunking interoperability compliance testing. All testing was successfully completed unless noted otherwise.

- Outgoing calls to PSTN telephones.
- Incoming calls to Nectar Services Corporation provided DID and Toll Free numbers from PSTN telephones.
- Calls using Avaya 4600 Series IP Telephones with the H.323 firmware configurations.
- Calls using Avaya 1600 Series IP Telephones with the H.323 firmware configurations.
- Calls using Avaya 9600 Series Telephones with the SIP firmware configurations.
- Calls using Avaya 6211 Analog telephone.
- G.729A, G.711MU, and G.711A codecs for voice calls.
- T.38 codec for fax calling.
- DTMF tone transmission using RFC 2833 with successful voice mail / IVR navigation.
- Telephone features such as hold, transfer, conference, and voice mail.
- Trunk to trunk call forwarding, transfers and EC-500 feature operation.
- Direct Media (also known as "shuffling") with IP and SIP telephones.

5.2. Test Results

Interoperability testing of the sample configuration was completed with successful results.

The following compatibility issues described in
Table **4** were observed during testing.

Item	Issue Observed
EC500 fails	Avaya Distributed Office never receives a SIP BYE message from the network when the user answers and then releases the call from the "extension to cellular" telephone.
T.38 fax only works with G.729A CODEC	Technically, Nectar Services does not support faxing, however T.38 fax worked during compliance testing when the Avaya Distributed Office system was configured to support T.38 fax with the G.729A codec. T.38 fax did not work with the G.711MU or G.711A codecs provisioned.

Table 4: Summary of Issues Identified During Interoperability Testing

6. Verification Steps

6.1. Verification Tests

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

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

- Outbound Calls – Verify that calls placed to a PSTN telephone are properly routed via the SIP trunk group(s) defined in the ARS route patterns. Verify that the talk-path exists in both directions and that calls remain stable and disconnect properly.

- Inbound DTMF Digit Navigation – Verify inbound DID calls can properly navigate the Avaya Distributed Office automated attendant function.

- Outbound DTMF Digit Navigation – Verify outbound calls can properly navigate a voice mail or interactive response system reached via a PSTN number.

6.2. Troubleshooting Tools

The Avaya Distributed Office has several troubleshooting tools that can be helpful to diagnosis SIP trunking issues.

The **Maintenance & Monitoring / Network Diagnostics** menu permits IP pings and traceroutes to be performed.

The **Maintenance & Monitoring / Telephony / Trunk Groups** menu provides:

- **Test Selected** – runs tests to verify the operation of the SIP signaling channel for the selected SIP trunk group.
- **Trace Selected** – provides a diagnostic trace of the call processing activities using the selected SIP trunk group.
- **Get Hourly Statistics** – shows the hourly traffic statistics for the selected SIP trunk group.

The **Maintenance & Monitoring / Telephony / SIP Traces** menu permits real time tracing of the SIP signaling to be displayed, captured and downloaded.

The **Configuration / Platform / Ethernet Switch** menu provides access to the **Ethernet Switch System Parameters** screen. The **Mirror Port** tab on this screen provides the ability to designate a specific Ethernet switch port to monitor (such as the connection used to reach the

Nectar Services Corporation network. This mirror port may be used with a SIP protocol analyzer such as WireShark (a.k.a., Ethereal) to monitor the SIP and RTP communications between Nectar Services Corporation service and the Avaya Distributed Office. This can be extremely valuable to support advanced troubleshooting.

7. Support

For technical support on Nectar Services Corporation On Demand Voice Service, contact support at 1-888-811-8647 or support@nectarcorp.com.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. The "Connect with Avaya" section provides the worldwide support directory. In the United States, 1-866-GO-AVAYA (1-866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on support.avaya.com) to directly access specific support and consultation services based upon their Avaya support agreements.

8. Conclusion

These Application Notes describe the steps for configuring SIP trunking between an Avaya Distributed Office (Release 1.2) and Nectar Services Corporation On Demand Voice service.

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

9. References

The Avaya Distributed Office product documentation is available at http://support.avaya.com.

[1] Avaya Distributed Office Documentation Map, 03-602021
[2] Overview of Avaya Distributed Office, 03-602024
[3] Avaya Distributed Office i120 Installation Quick Start, 03-602289
[4] Avaya Distributed Office i40 Installation Quick Start, 03-602288
[5] Feature Description for Avaya Distributed Office, 03-602027
[6] Avaya Application Solutions: IP Telephony Deployment Guide, 555-245-600
[7] 4600 Series IP Telephone LAN Administrator Guide, 555-233-507
[8] Avaya one-X™ Deskphone SIP for 9600 Series IP Telephones Administrator Guide, 16-601944

[9] Nectar Services Corporation On Demand Service Descriptions - http://nectarnetworks.com/

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

[10] RFC 3261 - *SIP (Session Initiation Protocol)*, June 2002, Proposed Standard

[11] RFC 2833 - *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, May 2000, Proposed Standard

APPENDIX A: Sample SIP INVITE Messages

This section displays the format of typical SIP INVITE messages sent between Nectar Services Corporation and the Avaya Distributed Office. These INVITE messages may be used for comparison and troubleshooting purposes. Differences in these messages may indicate that different configuration options were selected.

Sample SIP INVITE Message from the Nectar Services Corporation On Demand Voice service to the Avaya Distributed Office:

```
INVITE sip:90212014710200@65.211.92.41;user=phone SIP/2.0
Max-Forwards: 68
Session-Expires: 3600;Refresher=uac
Supported: timer
To: <sip:12014710200@172.16.1.15:5060;user=phone>
From: <sip:7328521639@172.16.1.15:5060;user=phone>;tag=SDtchr001-gK060ae642
Contact: <sip:7328521639@172.16.1.15:5060;user=phone>
Call-ID: 65957-3423571262-360180@agnnt02.avatelglobalnetworks.com
CSeq: 1 INVITE
Via: SIP/2.0/UDP 172.16.1.15:5060;branch=z9hG4bKedef97487ff38cc668d5da4236ea64ca
Content-Type: application/sdp
Content-Length: 295

v=0
o=NexTone-MSW 22472 26322 IN IP4 172.16.1.15
s=sip call
c=IN IP4 172.16.1.26
t=0 0
m=audio 36892 RTP/AVP 18 0 8 100
a=maxptime:20
a=sendrecv
a=fmtp:100 0-15
a=rtpmap:100 telephone-event/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=fmtp:18 annexb=no
a=rtpmap:18 G729/8000
```

Sample SIP INVITE Message from Avaya Distributed Office to the Nectar Services Corporation On Demand Voice service:

```
INVITE sip:17324500819@172.16.1.15;transport=udp SIP/2.0
Call-ID: 0c6f59f7243dd19c14865cee00
CSeq: 1 INVITE
From: "Analog-1" <sip:2014710200@example.com:6002>;tag=0c6f59f7243dd19b14865cee00
Record-Route: <sip:65.211.92.41:5060;lr>
Record-Route: <sip:65.211.92.41:6002;transport=tls;lr>
To: "17324500819" <sip:17324500819@nectarvoip.com>
Via: SIP/2.0/UDP 65.211.92.41:5060;branch=z9hG4bK030303363636636363378.0
Contact: "Analog-1" <sip:2014710200@65.211.92.41:6002;transport=tls>
Max-Forwards: 69
User-Agent: Avaya CM/R013w.01.2.023.0
Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS
History-Info: <sip:17324500819@nectarvoip.com>;index=1
History-Info: "17324500819" <sip:17324500819@nectarvoip.com>;index=1.1
Supported: 100rel, timer, replaces, join, histinfo
Min-SE: 1200
Session-Expires: 1200;refresher=uac
P-Asserted-Identity: "Analog-1" <sip:2014710200@example.com:6002>
Content-Type: application/sdp
Content-Length: 202

v=0
o=- 1 1 IN IP4 65.211.92.41
s=-
c=IN IP4 65.211.92.41
t=0 0
m=audio 33794 RTP/AVP 18 0 127
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:127 telephone-event/8000
```

APPENDIX B: Juniper SSG 520M Configuration

Below is a sample configuration used in **Figure 1**. The "bolded" lines are those that pertain to the ALG/NAT configuration.

```
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set alg appleichat enable
unset alg appleichat re-assembly enable
set alg sctp enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 27911
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin http redirect
set admin auth web timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Untrust"
set interface ethernet0/0 ip 10.1.1.2/24
set interface ethernet0/0 nat
unset interface vlan1 ip
set interface ethernet0/1 ip 10.10.10.15/24
set interface ethernet0/1 nat
set interface ethernet0/2 ip 65.211.92.41/27
set interface ethernet0/2 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/1 ip manageable
set interface ethernet0/2 ip manageable
set interface vlan1 manage mtrace
set interface "ethernet0/2" mip 65.211.92.41 host 10.1.1.20 netmask 255.255.255.255 vr "trust-vr"
unset flow no-tcp-seq-check
```

```
set flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set ike respond-bad-spi 1
set ike ikev2 ike-sa-soft-lifetime 60
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
set url protocol websense
exit
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "ANY" nat src permit log
set policy id 1
exit
set policy id 2 from "Untrust" to "Trust"  "Any" "MIP(65.211.92.41)" "SIP" permit log
set policy id 2
exit
set policy id 3 name "voice UDP Ports" from "Untrust" to "Trust"  "Any" "MIP(65.211.92.41)" "UDP-
ANY" permit log
set policy id 3
exit
set policy id 4 from "Untrust" to "Trust"  "Any" "Any" "ANY" deny log
set policy id 4
exit
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
unset license-key auto-update
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 0.0.0.0/0 interface ethernet0/2 gateway 65.211.92.33
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect program at devconnect@avaya.com.