Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking between XO Communications XO SIP Service and Avaya Communication Manager Branch Edition – Issue 1.0

Abstract

These Application Notes describe the steps for configuring SIP trunking between XO Communications XO SIP Service and Avaya Communication Manager Branch Edition (formerly known as Distributed Office) using various Avaya telephony endpoints.

Enterprise customers with this Avaya SIP-based solution can connect via dedicated Internet access using XO Communications 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.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps for configuring SIP trunking between XO Communications XO SIP Service and Avaya Communication Manager Branch Edition (formerly known as Distributed Office) using various Avaya telephony endpoints.

Enterprise customers using this Avaya Communication Manager Branch Edition telephony solution with XO Communications XO SIP 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 Communication Manager Branch Edition and the network services offered by XO Communications.

The XO Communications 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 “XO SIP Service” unless there is a need to differentiate among the services.

1.1. Interoperability Compliance Testing

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

- Outgoing calls from the Avaya IP network to the PSTN routed through the XO VoIP network.
- Incoming calls using DID and Toll Free numbers from the PSTN routed through the XO VoIP network to the Avaya IP network.
- 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.729B, and G.711MU codecs for voice calls.
- T.38 codec for fax calling.
- DTMF tone transmission using RFC 2833.
- 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.

1.2. Support

For technical support on XO Communications XO SIP Service, contact the XO Customer Care at (800) 421-3872 or via the web at

http://www.xo.com/forms/Campaign/Care/ContactCustomerCare/ContactCustomerCare.aspx

2. Reference Configuration

Figure 1 illustrates a typical customer location using an Avaya Communication Manager Branch Edition with SIP trunking to XO Communications. This configuration includes:

- Avaya Communication Manager Branch Edition 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 XO SIP 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 Communication Manager Branch Edition 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 Communication Manager Branch Edition 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 XO Communications service and the Avaya Communication Manager Branch Edition 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.

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

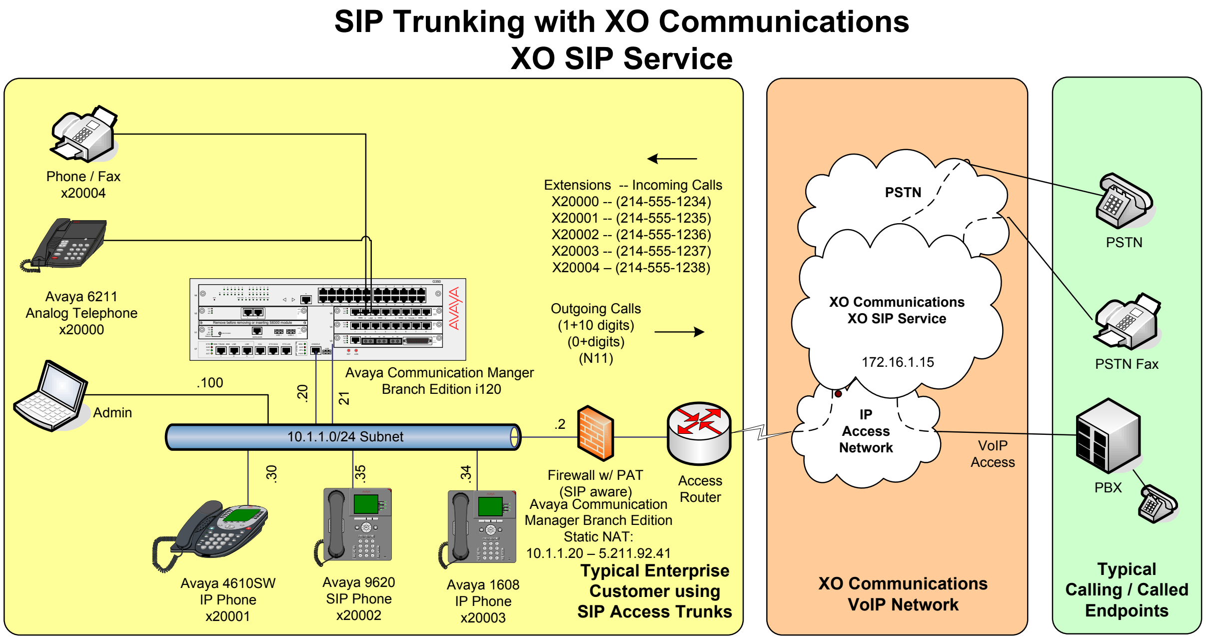

Figure 1 – Typical SIP Trunking Configuration

Figure 2 illustrates the Network Connection information for the Avaya Communication Manager Branch Edition i120.

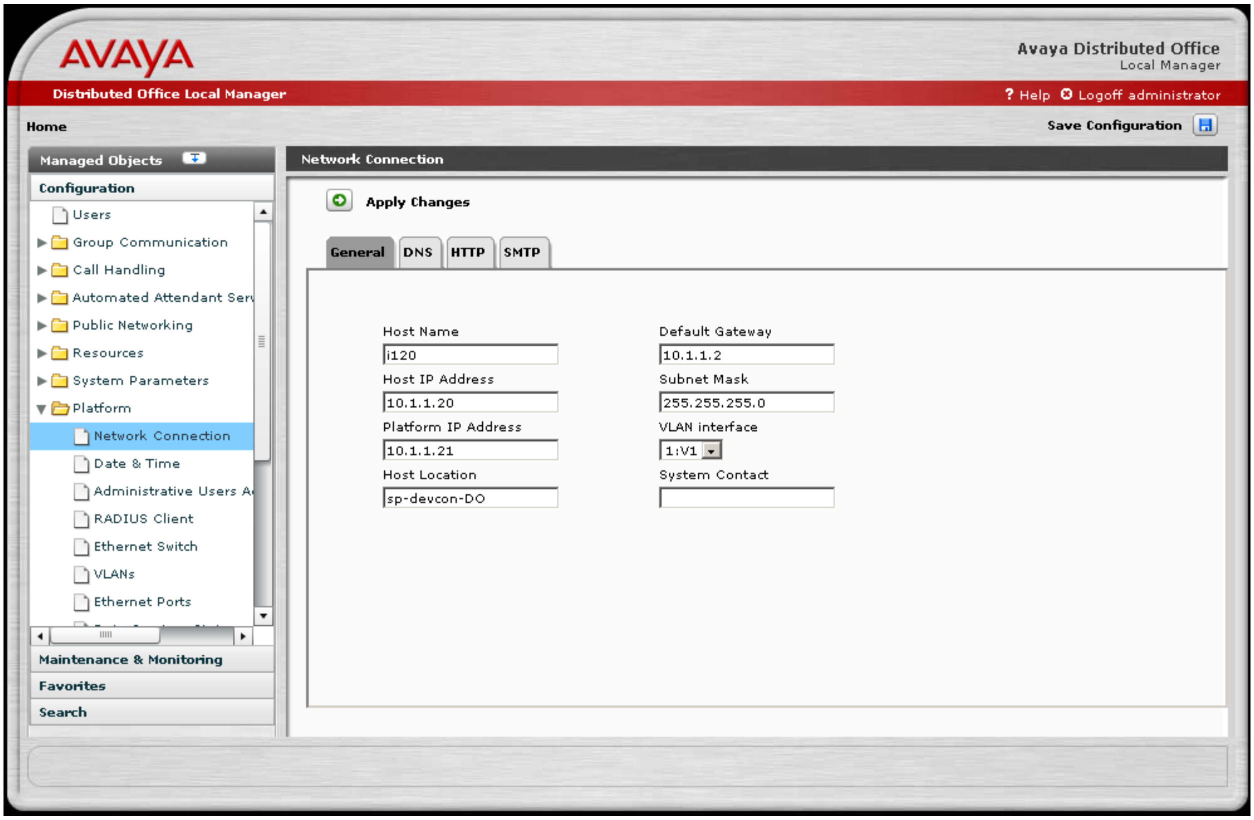

Figure 2 - Network Connection Assignments

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 XO Communications Border Element(s) whenever using direct media.

These Application Notes provide **an illustrative example** of how the Avaya Communication Manager Branch Edition SIP trunking solution is configured with the XO Communications XO SIP Service. The XO VoIP network consists of Broadsoft BroadWorks VoIP Applications Platform, Sonus Networks Network Border Switch (NBS), Sonus Networks PSX Routing Servers, and a Sonus Networks GSX Gateway. The Sonus NBS exchanges SIP signaling messages with the Avaya Communications Manager Branch Edition gateway. In this configuration, the IP address of the Sonus NBS is 172.16.1.15.

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 XO Communications during service provisioning of their XO SIP Service.*

XO Communications Services Provisioning Information	Illustrative Values in these Application Notes
G.729A, G.729B, G.711MU 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 XO Communications)	Yes
DID Digits Passed in SIP To Header	Same as Assigned DID Numbers

Table 1 – Illustrative XO Communications Network Provisioning Information

3. Equipment and Software Validated

The following equipment and software was used during the DevConnect compliance testing with the XO Communications XO SIP Service.

Component	Version
Avaya	
Avaya Communications Manger Branch Edition 120	Release 1.2 (1.2.1_02.01)
Avaya 4610SW IP (H.323) Telephone	Release 2.9
Avaya 1608 IP (H.323) Telephone	Release 1.0.30
Avaya 9620 one-X™ Deskphone SIP Telephone	Release 2.0.5
Avaya 6211 Analog Telephone	n/a
MultiTech Fax Modem	Model MT5634ZBA
Avaya IP Softphone	Release 6.01.89 (with Service Pack5)
XO Communications	
Sonus Networks Network Border Switch (NBS) Sonus Networks PSX Routing Server[2]	06.04.06 S005 06.04.03 R000
Sonus Networks GSX Gateway Sonus Networks PSX Routing Server[3]	06.04.12 R000 06.04.11 R000
Broadsoft BroadWorks VoIP Applications Platform including: • Broadsoft Application Server (AS) • Broadsoft Network Server (NS) • Broadsoft Media Server (MS)	Release 14 Rel_14.sp7_1.112 Rel_14.sp4_1.165 Rel_14.sp4_1.165

Table 2 – Equipment and Version

[2] This Sonus PSX was paired with the Sonus NBS.
[3] This Sonus PSX was paired with the Sonus GSX.

4. Configure the Avaya i120 Switch

The Avaya Communication Manager Branch Edition 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.

4.1. Log in to Avaya Communication Manager Branch Edition

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

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

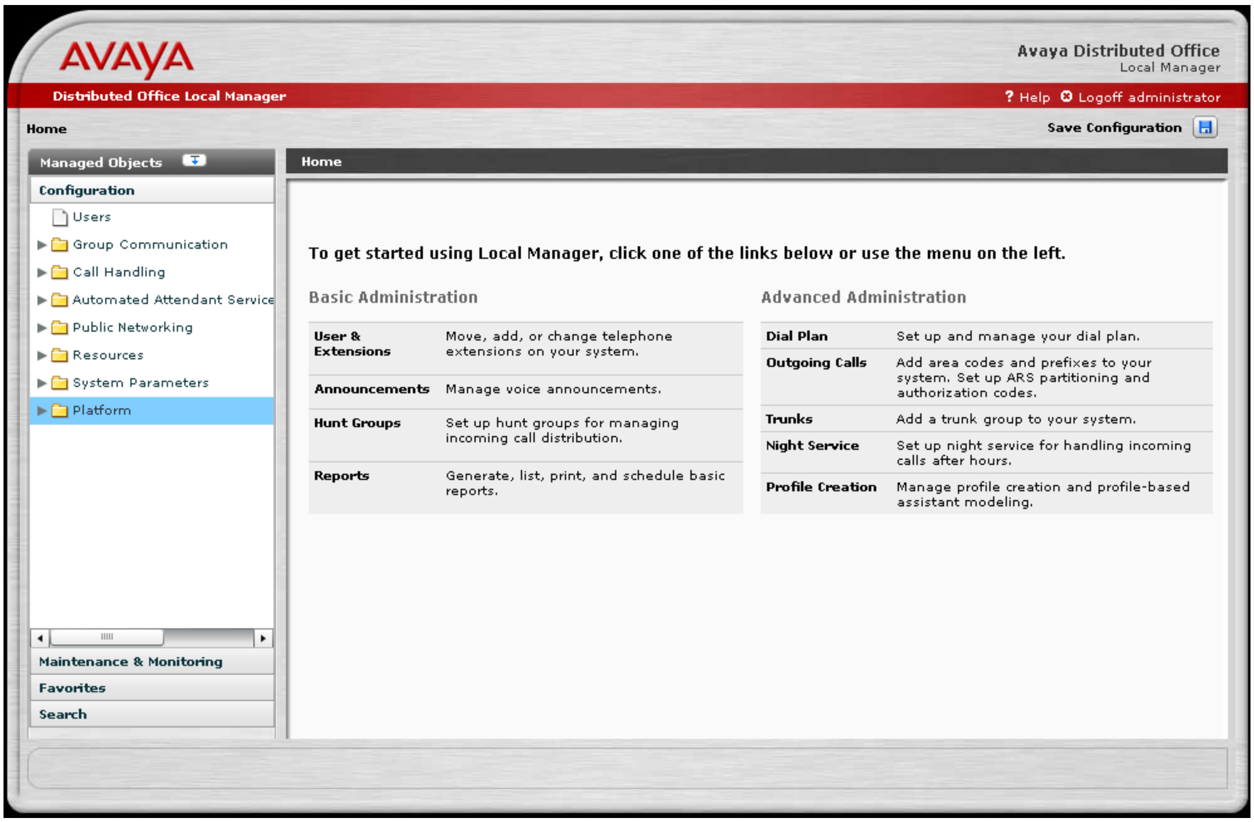

Figure 3 - Local Manager Home

4.2. Add a SIP Trunk Group to the XO SIP Service

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.

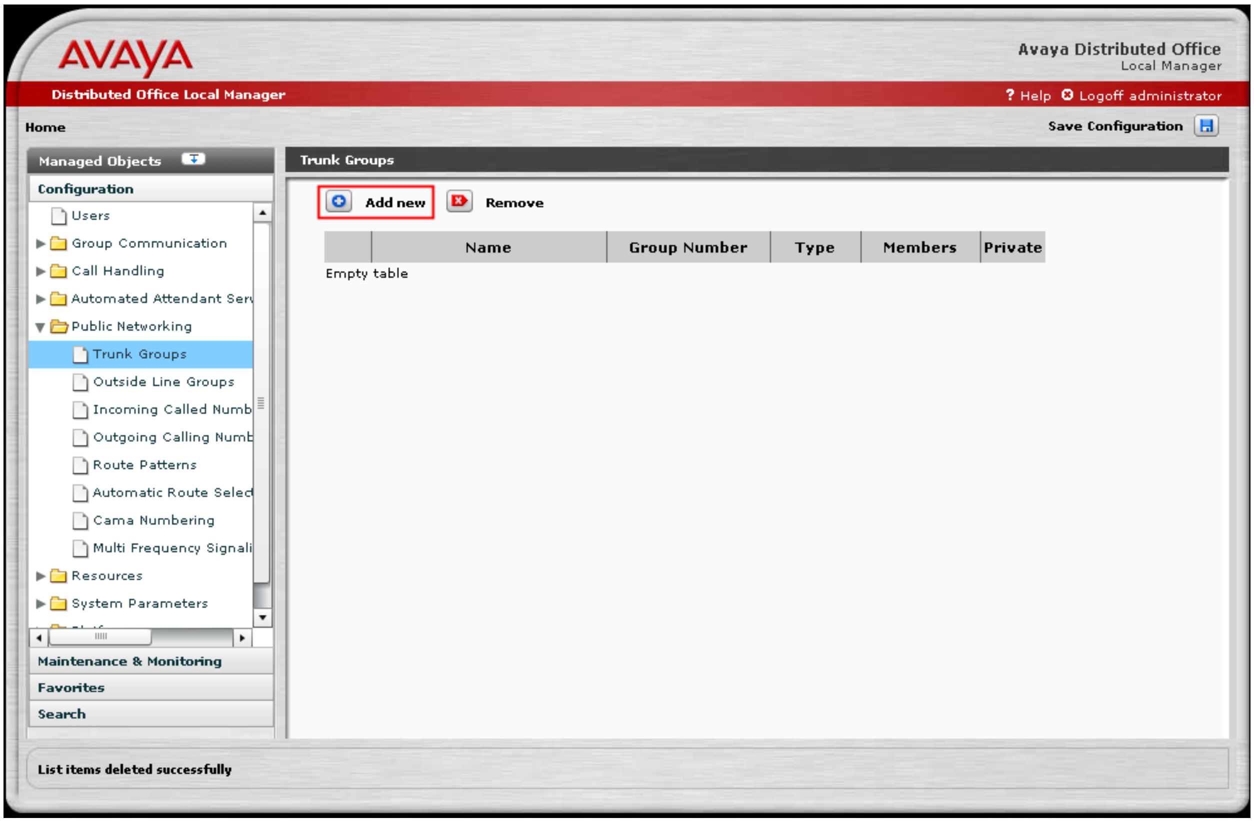

Figure 4 - Trunk Groups Screen

On the **Add Trunk Group** screen:

- Set the **Trunk Type** to "SIP".
- Enter a short text description of the trunk group (e.g., XO-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.

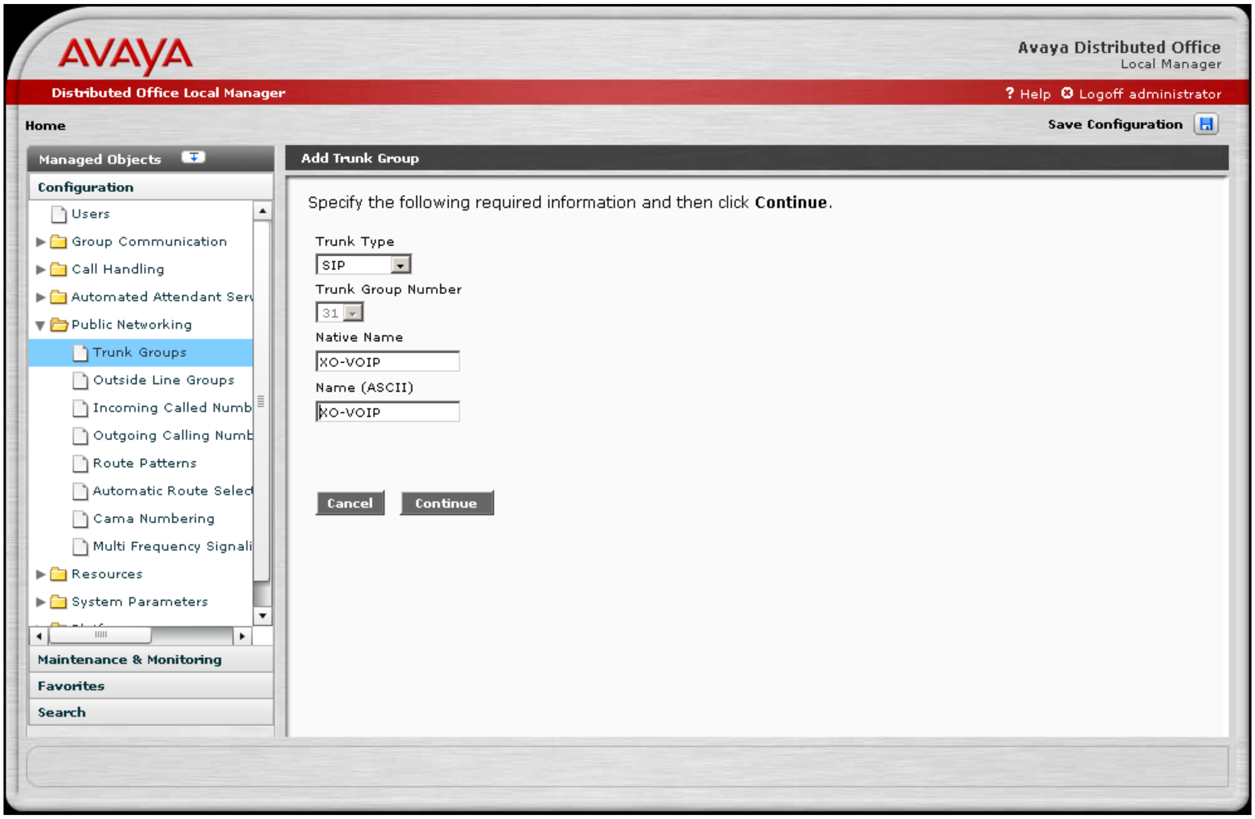

Figure 5 - Add Trunk Group Screen

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.

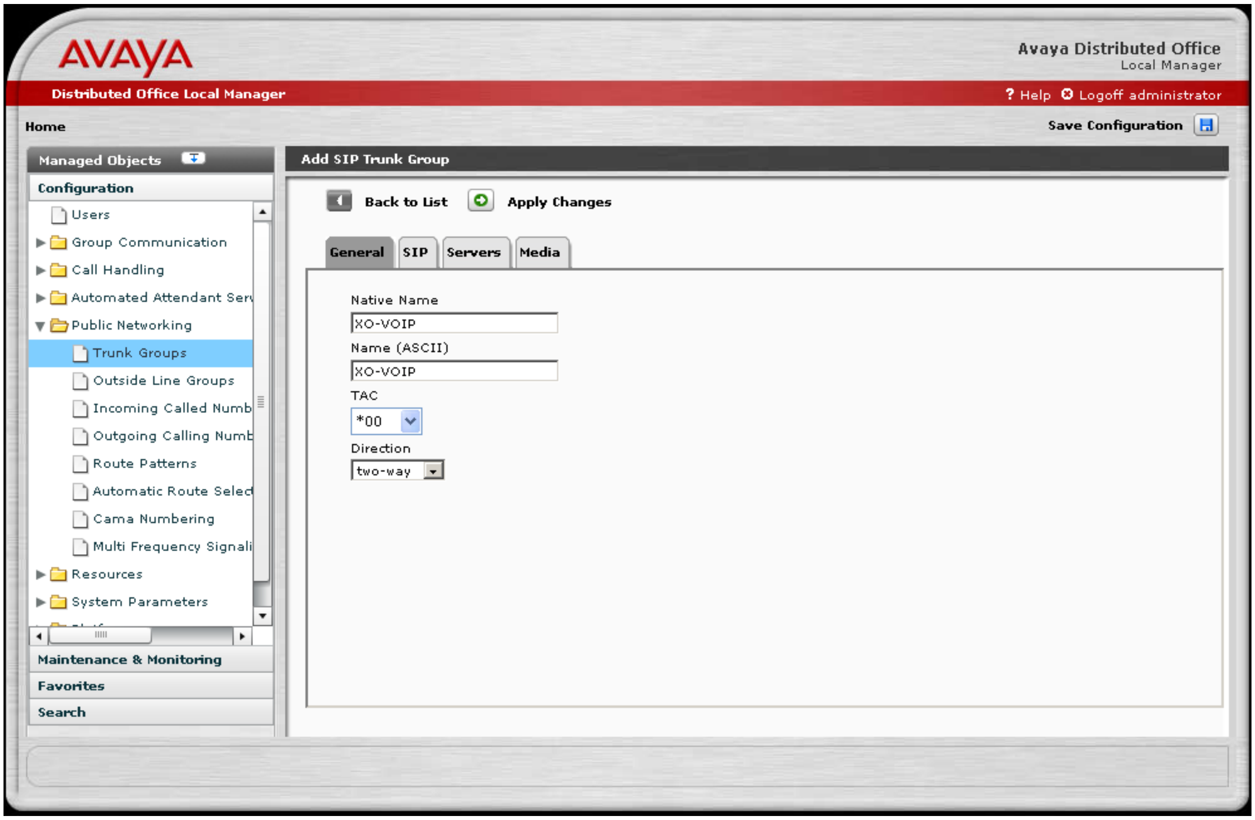

Figure 6 - Add SIP Trunk Group Screen – General tab

On the **SIP** tab:

- Enter a **Far-End Domain** value for the XO SIP Service.
- 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 XO SIP Services.
- Check the **Replace outgoing request-URI domain with selected server IP address** box.
- The defaults shown for the **Timeout, Max Search Time,** and **Session Refresh Interval** are used.
- Press the **Servers** tab to advance to the next screen.

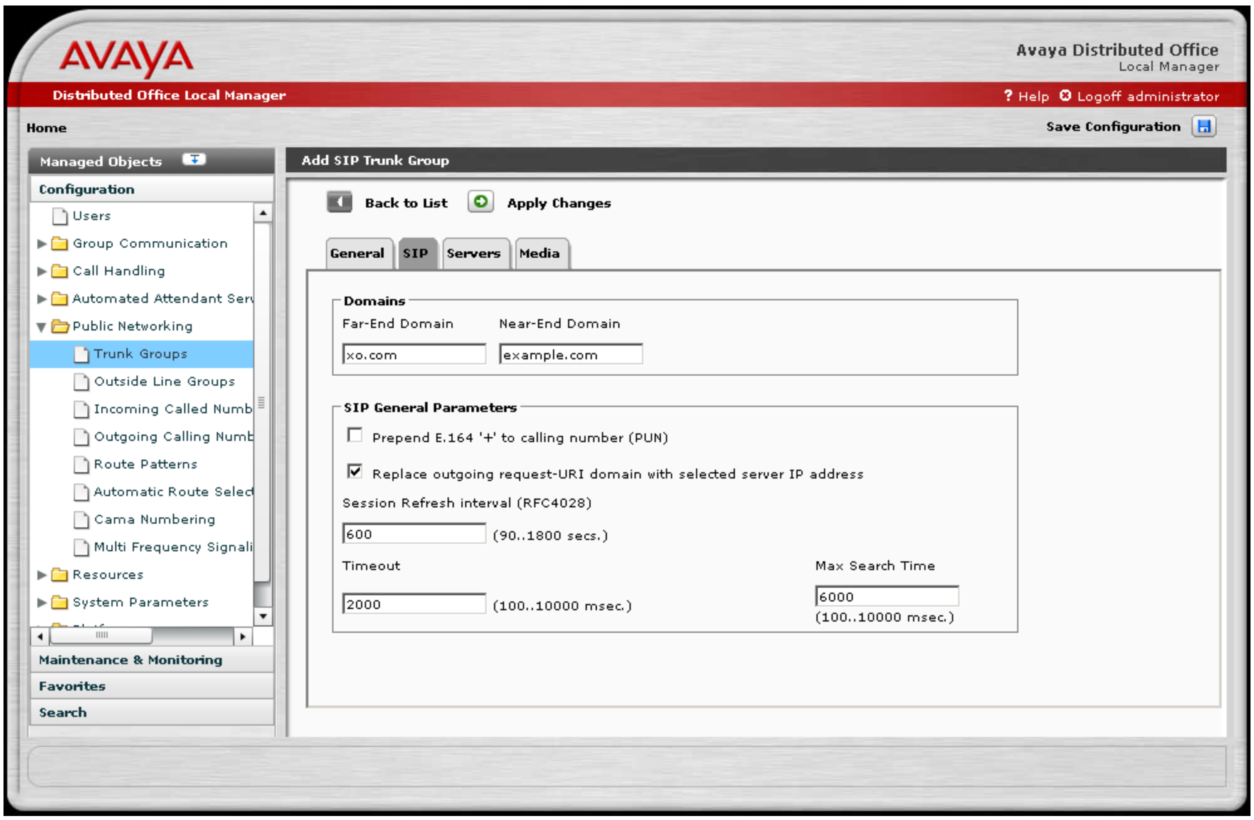

Figure 7 - Add SIP Trunk Group Screen – SIP Tab

On the **Servers** tab:

- Enter the IP address of the primary XO SIP Service Border Element provided by XO Communications in the **Address** field. In these Application Notes, "172.16.1.15" is used as noted in Section 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.

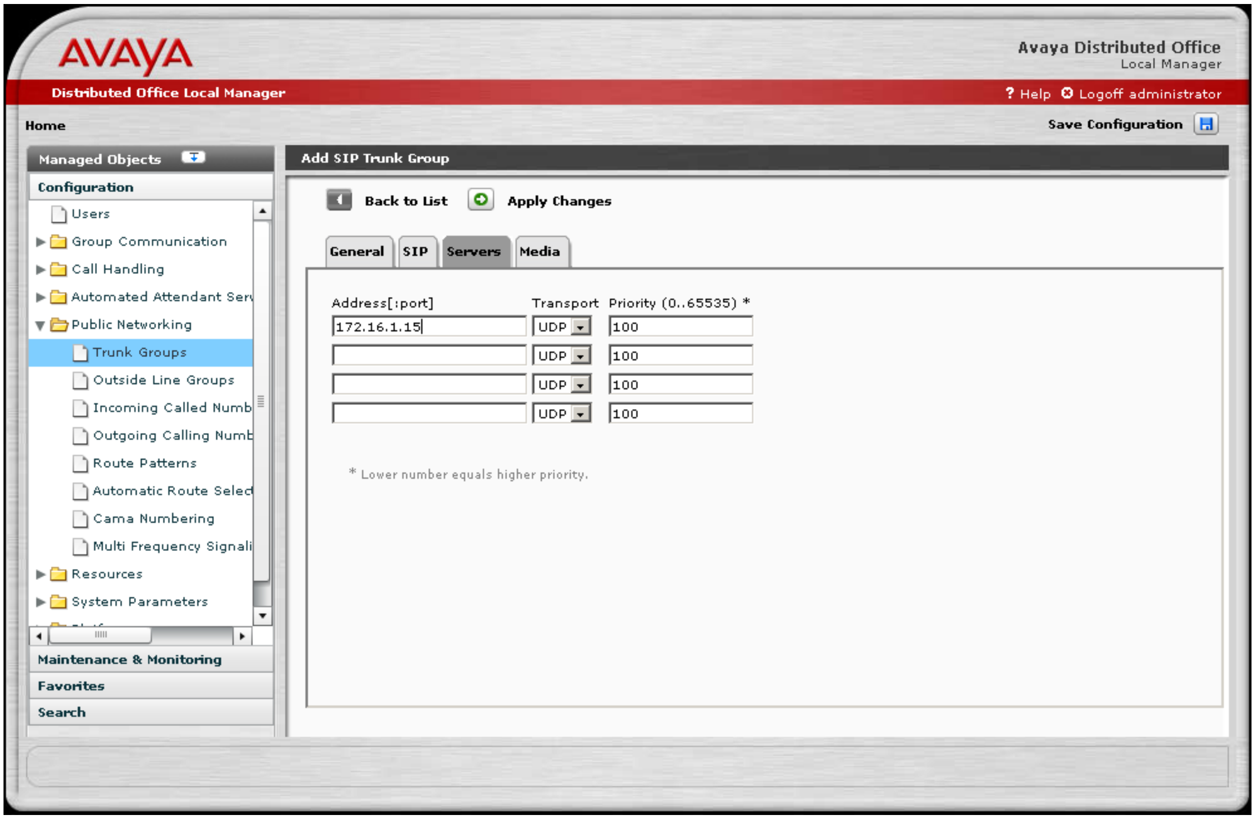

Figure 8 - Add SIP Trunk Group Screen – Servers Tab

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.[4]
- Set the **Max Concurrent Calls** to the number of simultaneous calls supported. This value is specified by the customer when ordering the XO Communications XO SIP Service. It is a function of the bandwidth of the VoIP network access, codec choices and XO SIP 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 Parameters.

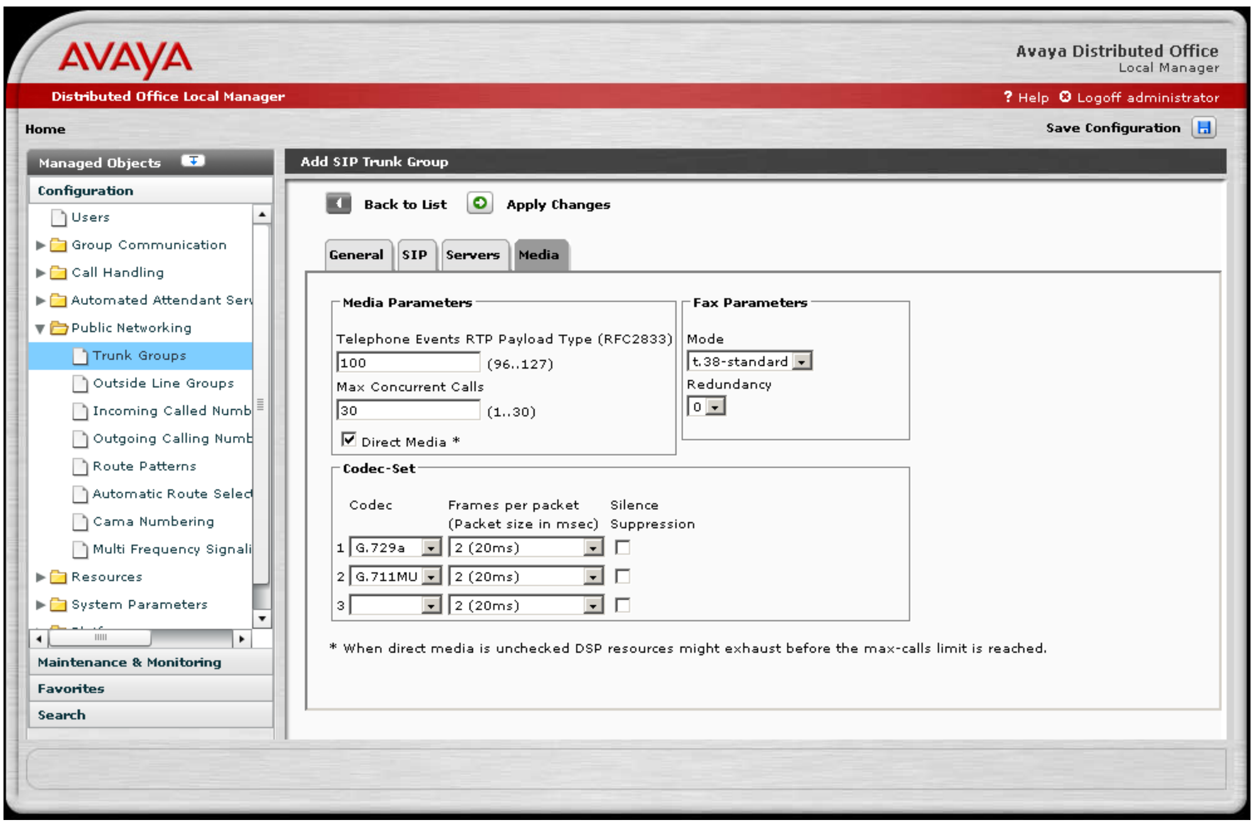

Figure 9 - Add SIP Trunk Group Screen – Media Tab

---

[4] 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.

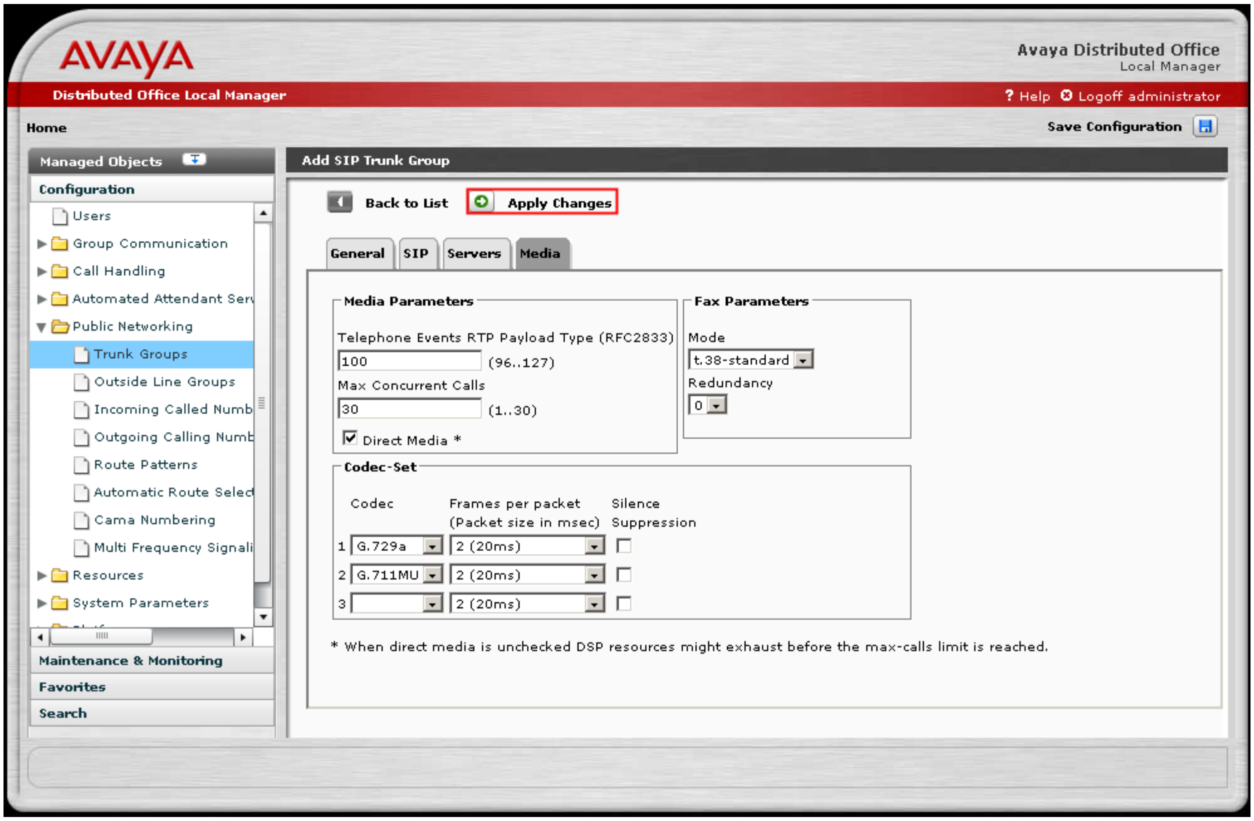

Figure 10 - Add SIP Trunk Group Screen – Apply Changes

4.2.1. 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.

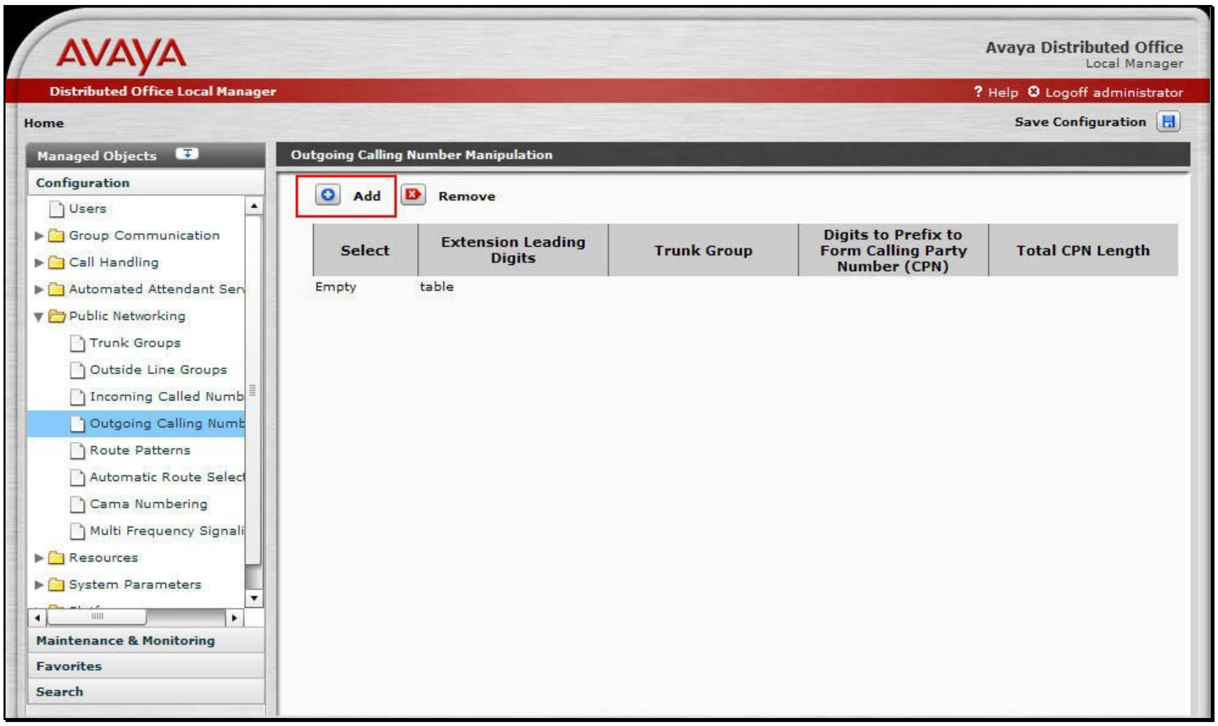

Figure 11 - Outgoing Calling Number Manipulation

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. "XO-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.

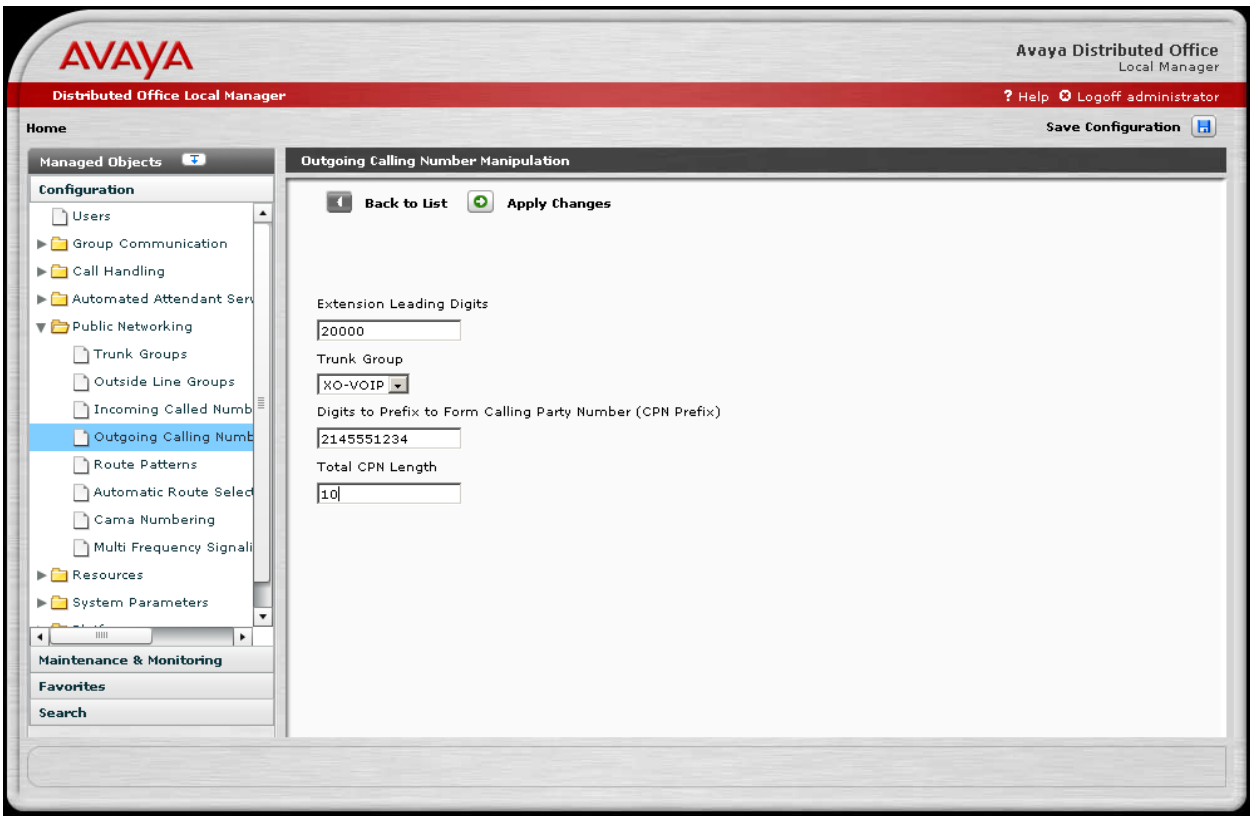

Figure 12 - Outgoing Calling Number Manipulation – New Entry

Repeat the **Outgoing Calling Number Manipulation Add** process to administer the calling numbers that will be sent in the SIP From header for the remaining stations. The **Outgoing Calling Number Manipulation** summary screen will be displayed.

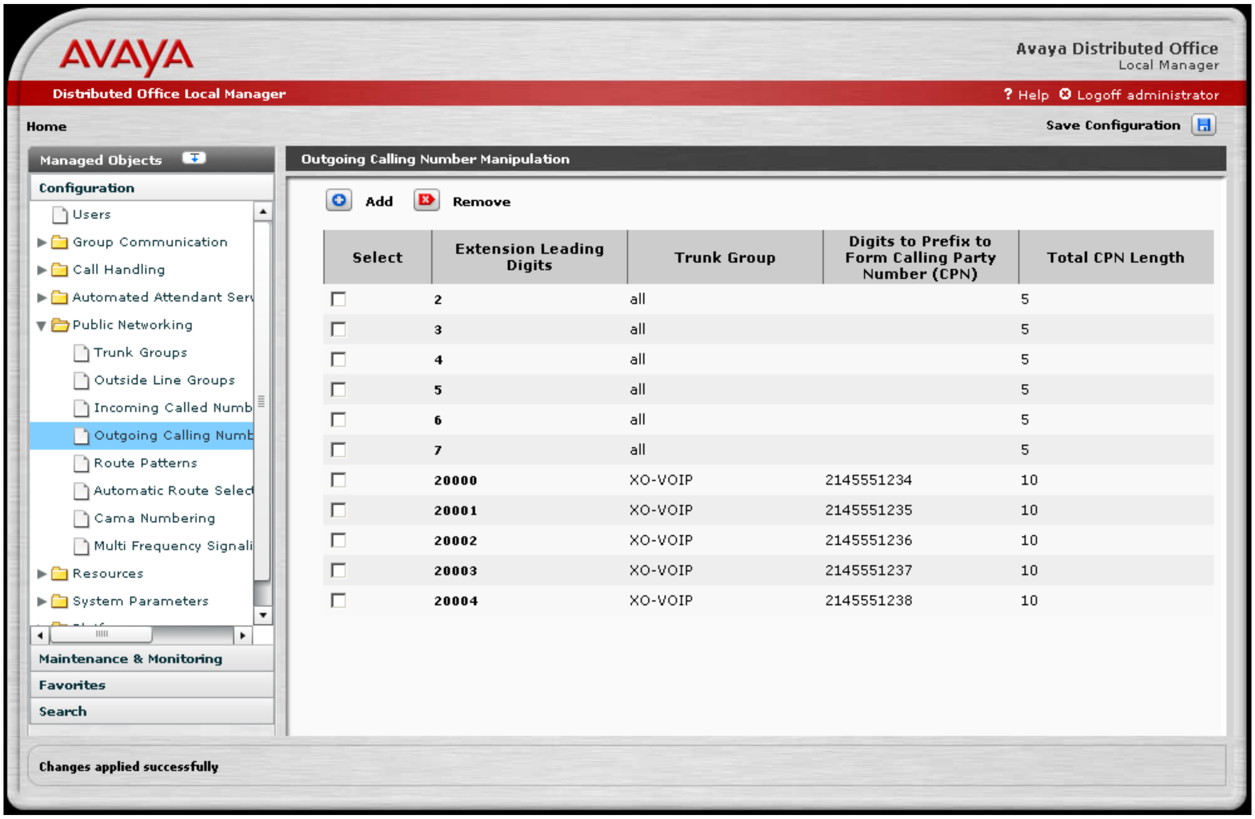

Figure 13 - Outgoing Calling Number Manipulation – Summary Screen

4.2.2. Configure Call Routing

4.2.2.1 Outbound Calls

The Automatic Route Selection (ARS) feature is used to choose the SIP trunk group to the XO SIP 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.

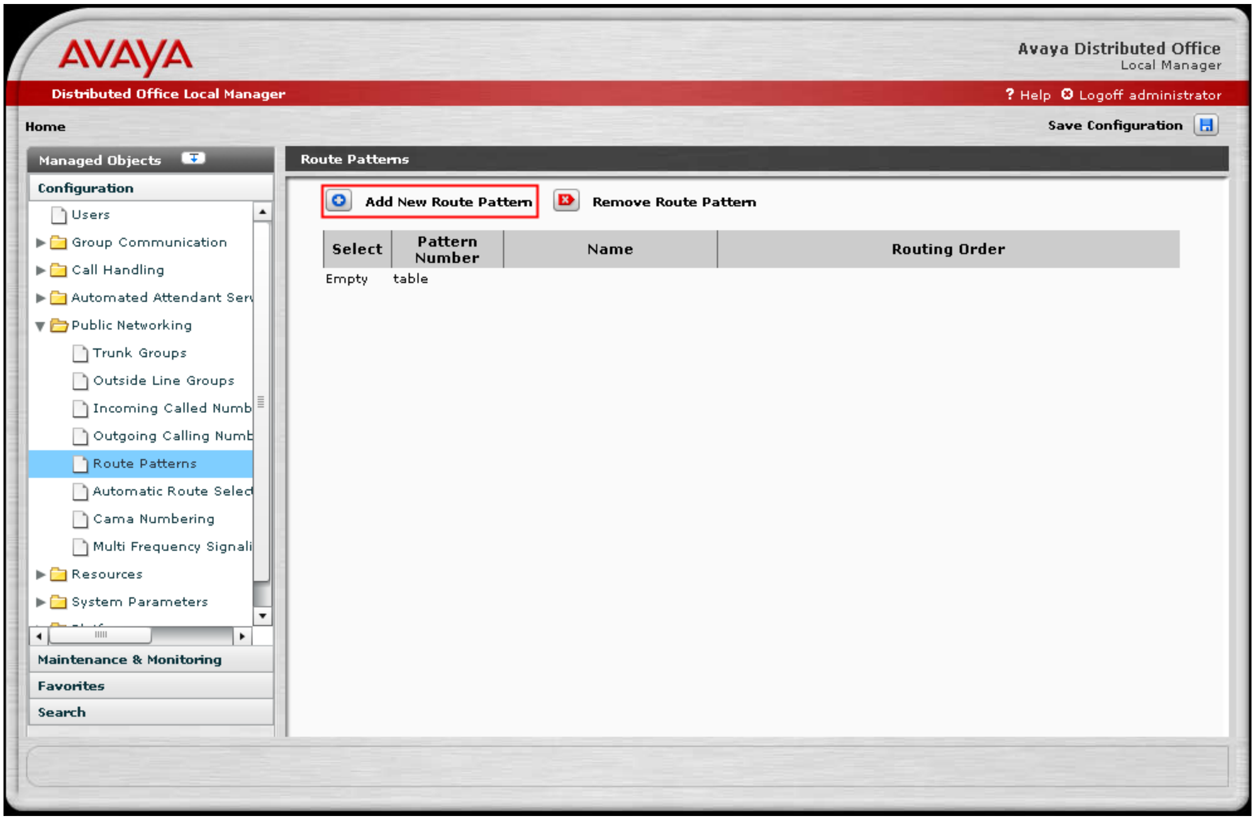

Figure 14 - Add New Route Patterns

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 to XO" was used.
- Select the "XO-VOIP (31)" **Trunk Group** in the number "1" **Order** row. This defines the XO-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 XO Communications XO SIP Service.
- Press **Apply Changes** to record the route pattern entry and return to the **Route Patterns** screen.

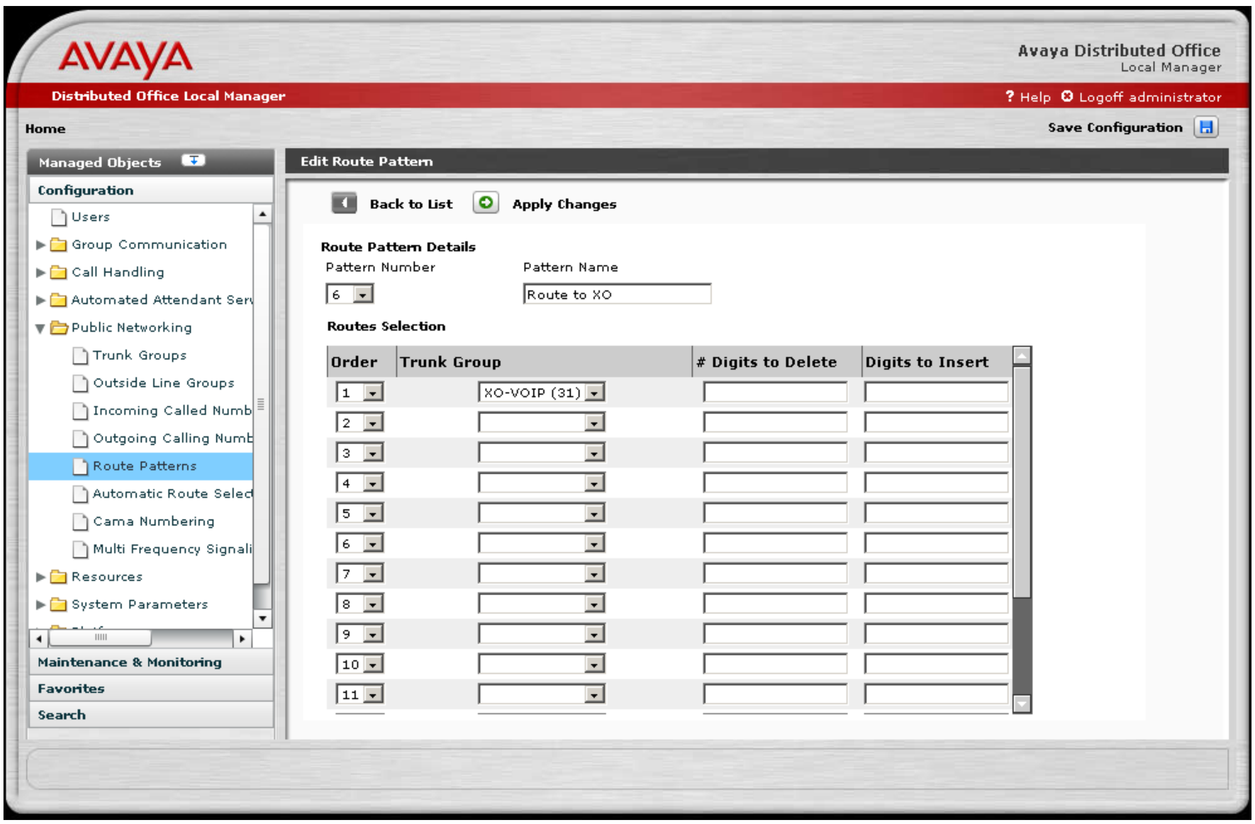

Figure 15 - New Route Pattern Screen

The **Route Patterns** screen is displayed.

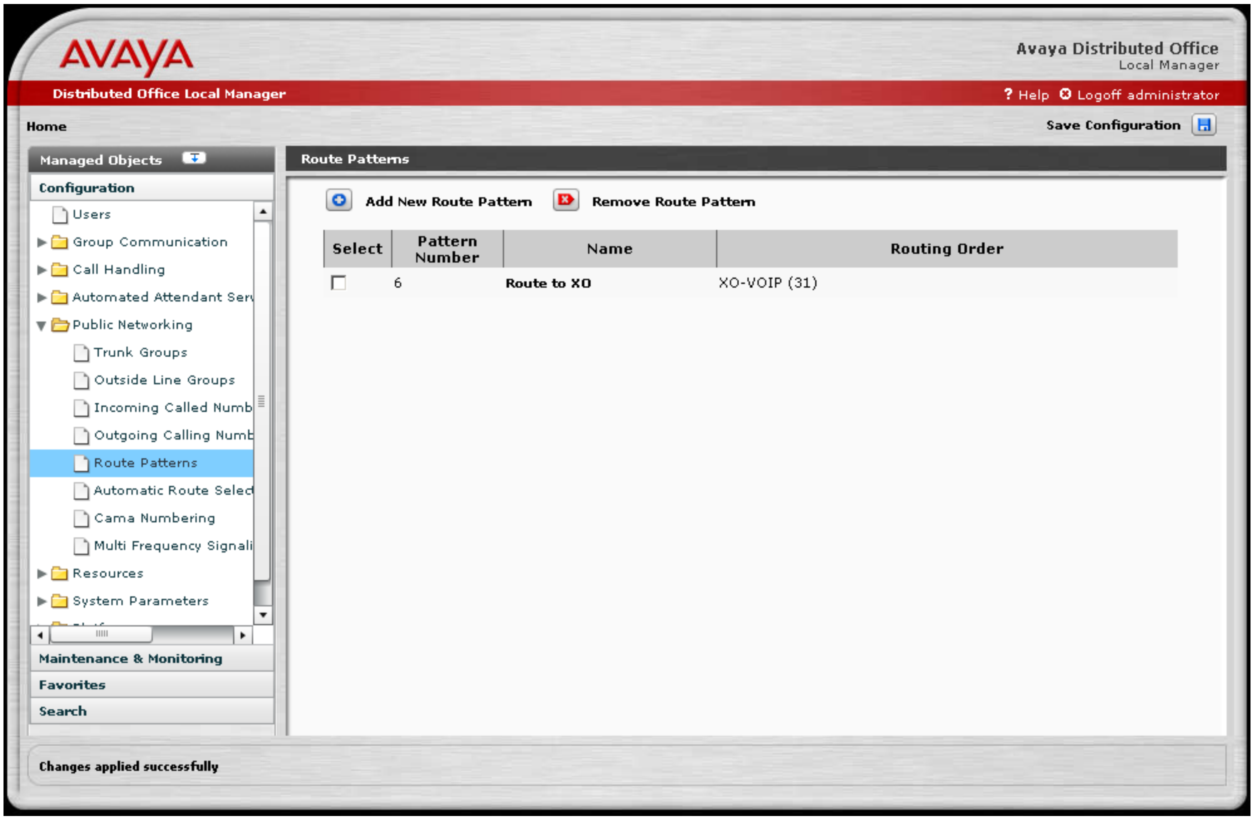

Figure 16 - Route Patterns – Summary Screen

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.

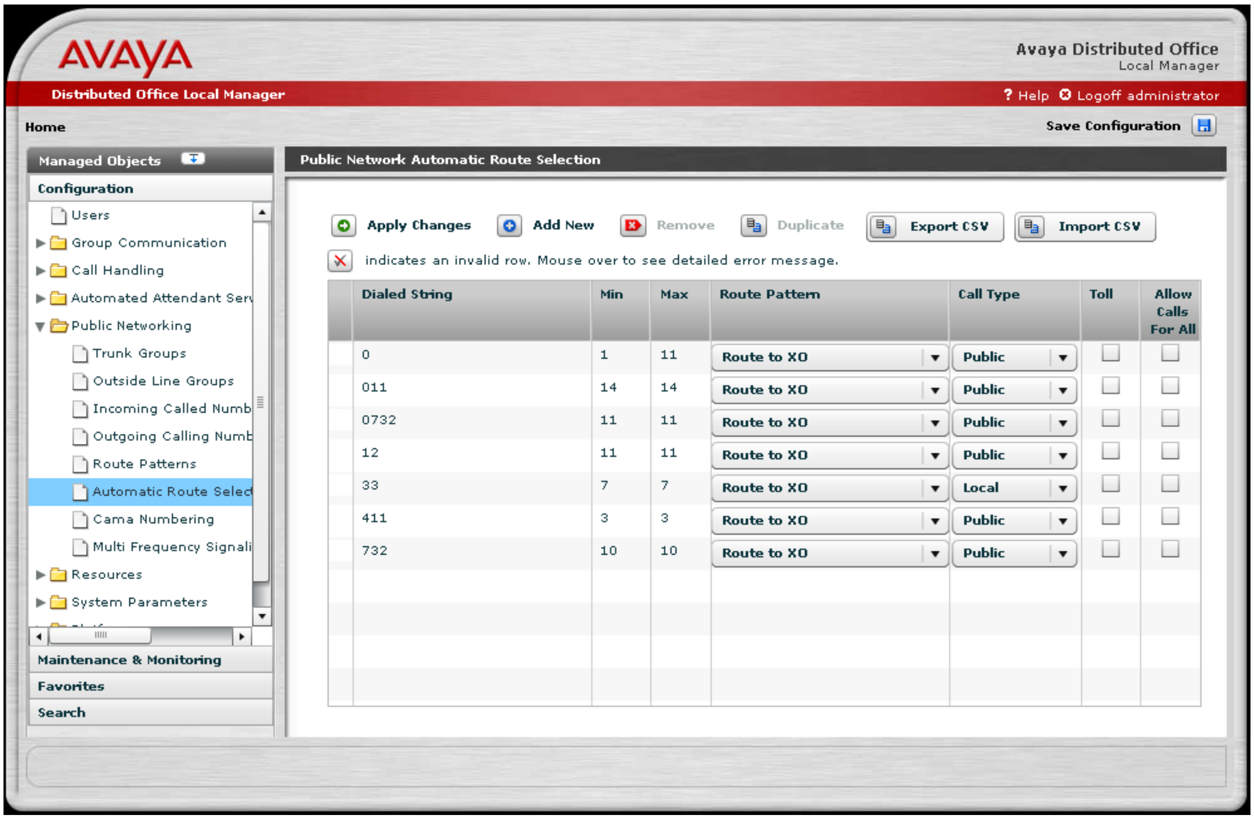

Figure 17 - Public Network Automatic Route Selection

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 Avaya Communication Manager Branch Edition 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 XO Communications XO SIP Service without requiring toll calling privileges.

- Enter "1732" for the **Dialed String**.
- Enter "11" for **Min**.
- Enter "11" for **Max**.
- Select "Route to XO" 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.

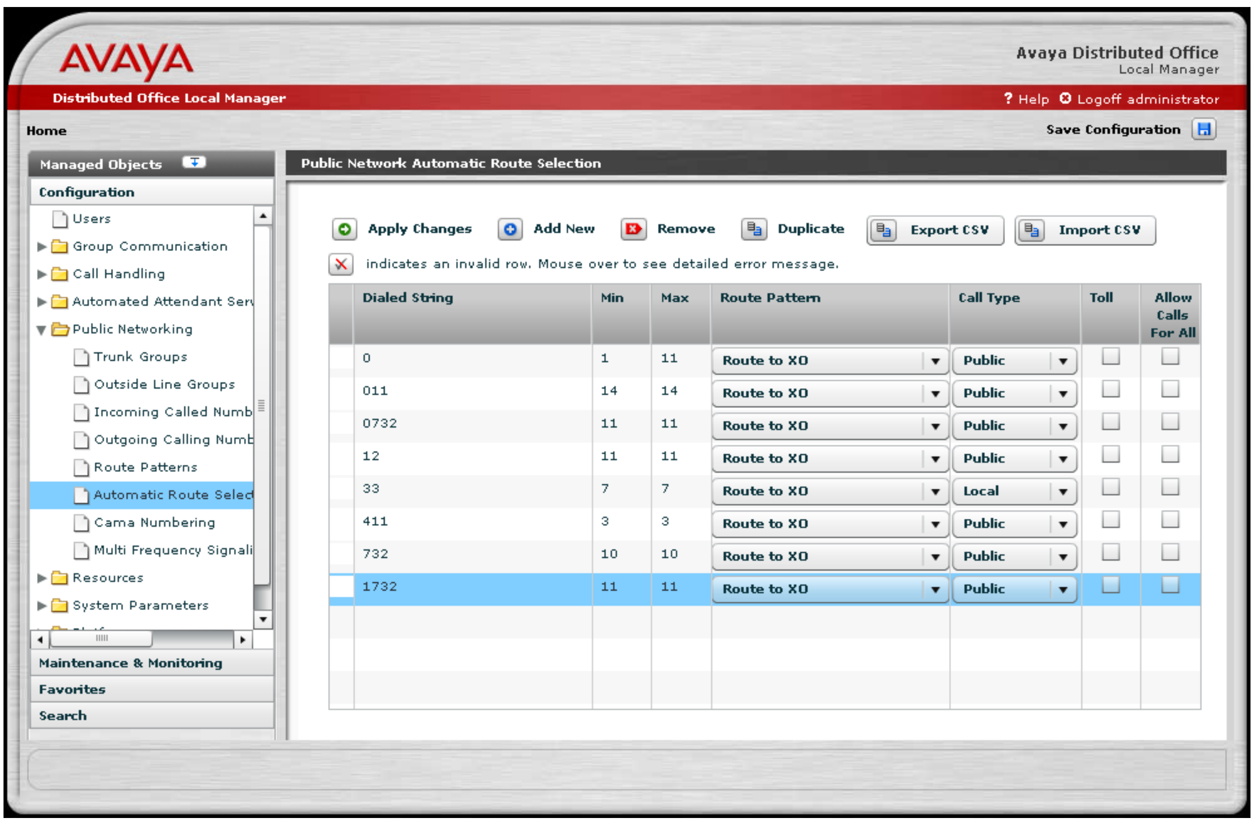

Figure 18 - Public Network Automatic Route Selection – Summary Screen

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.

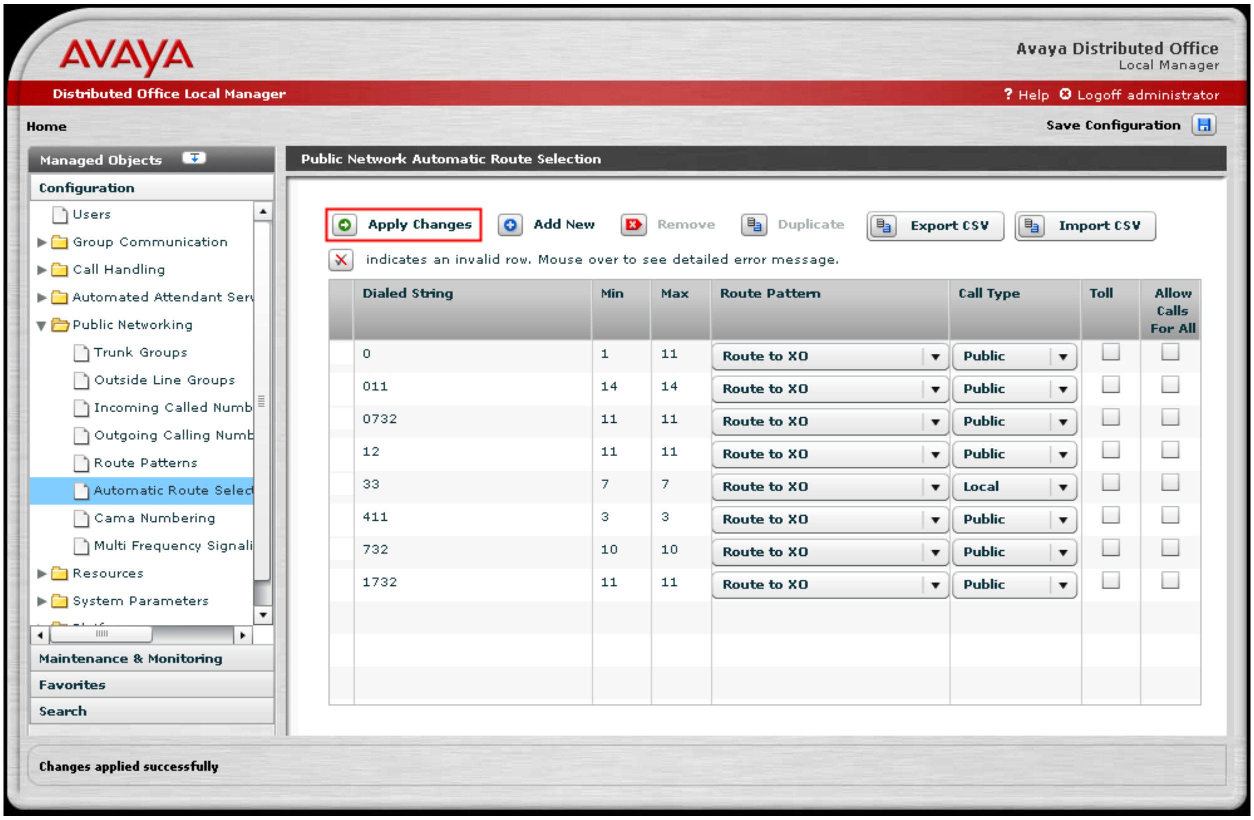

Figure 19 - Public Network Automatic Route Selection – Apply Changes Screen

4.2.2.2 Inbound Calls

This step configures the routing of incoming DID calls to the associated Avaya Communication Manager Branch Edition extensions. In these Application Notes, the incoming PSTN DID numbers listed in **Figure 1** are assigned to the extensions as shown in **Table 3**.

Dialed PSTN Number	Digits Received (within SIP INVITE message)	Extension Assigned
1-214-555-1234	2145551234	20000
1-214-555-1235	2145551235	20001
1-214-555-1236	2145551236	20002
1-214-555-1237	2145551237	20003
1-214-555-1238	2145551238	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.

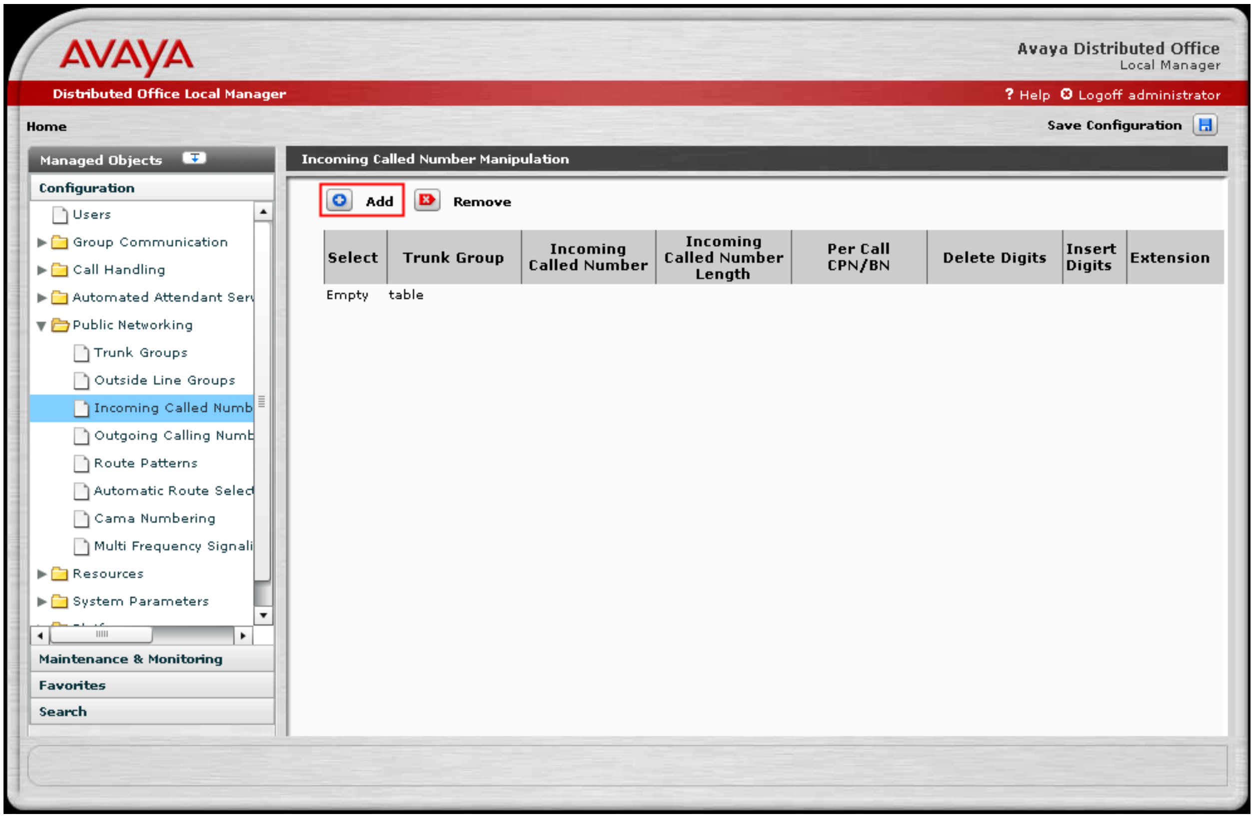

Figure 20 - Incoming Called Number Manipulation

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

- Select "XO-VOIP" as the **Trunk Group**.
- Enter "2145551234" as the **Called Number** digit pattern to be matched.
- Enter "10" as the **Called Number Length**. This is the total number of digits sent by XO Communications.
- 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.

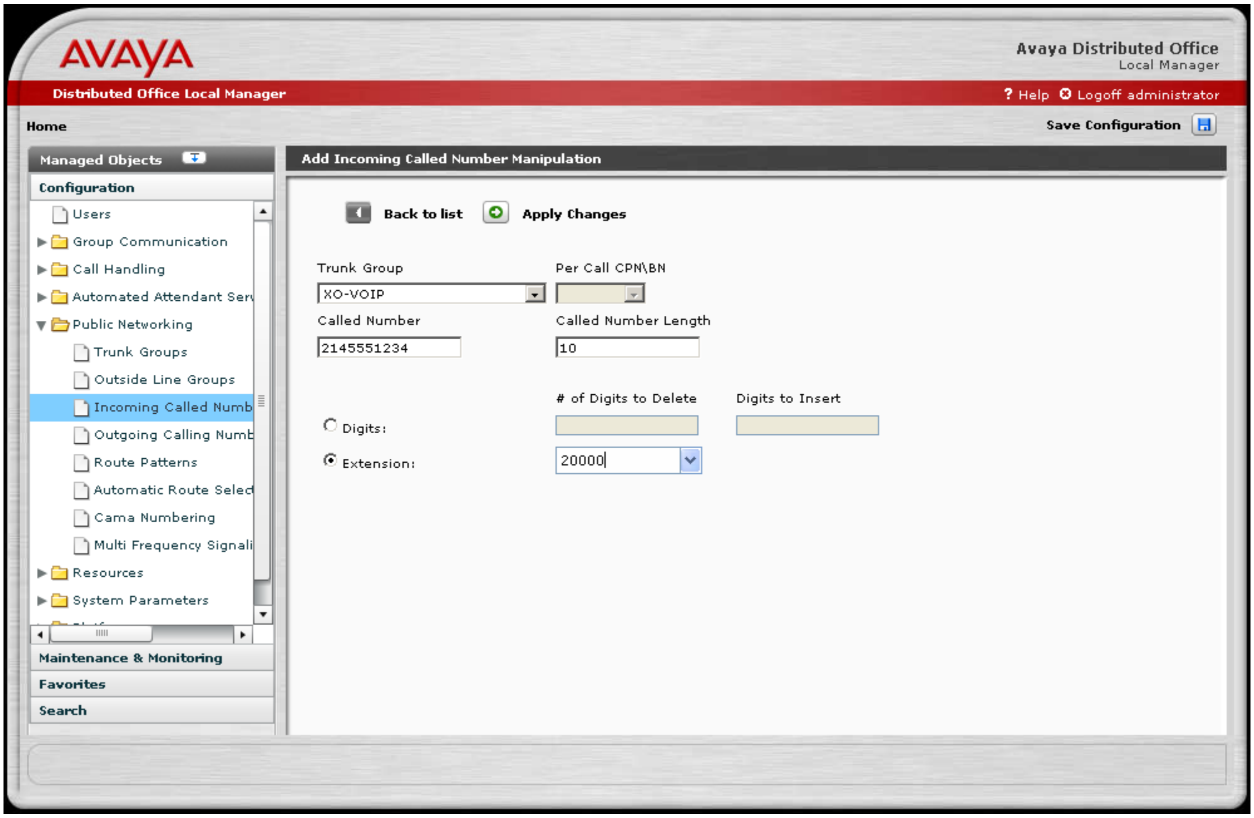

Figure 21 - Add Incoming Called Number Manipulation

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.

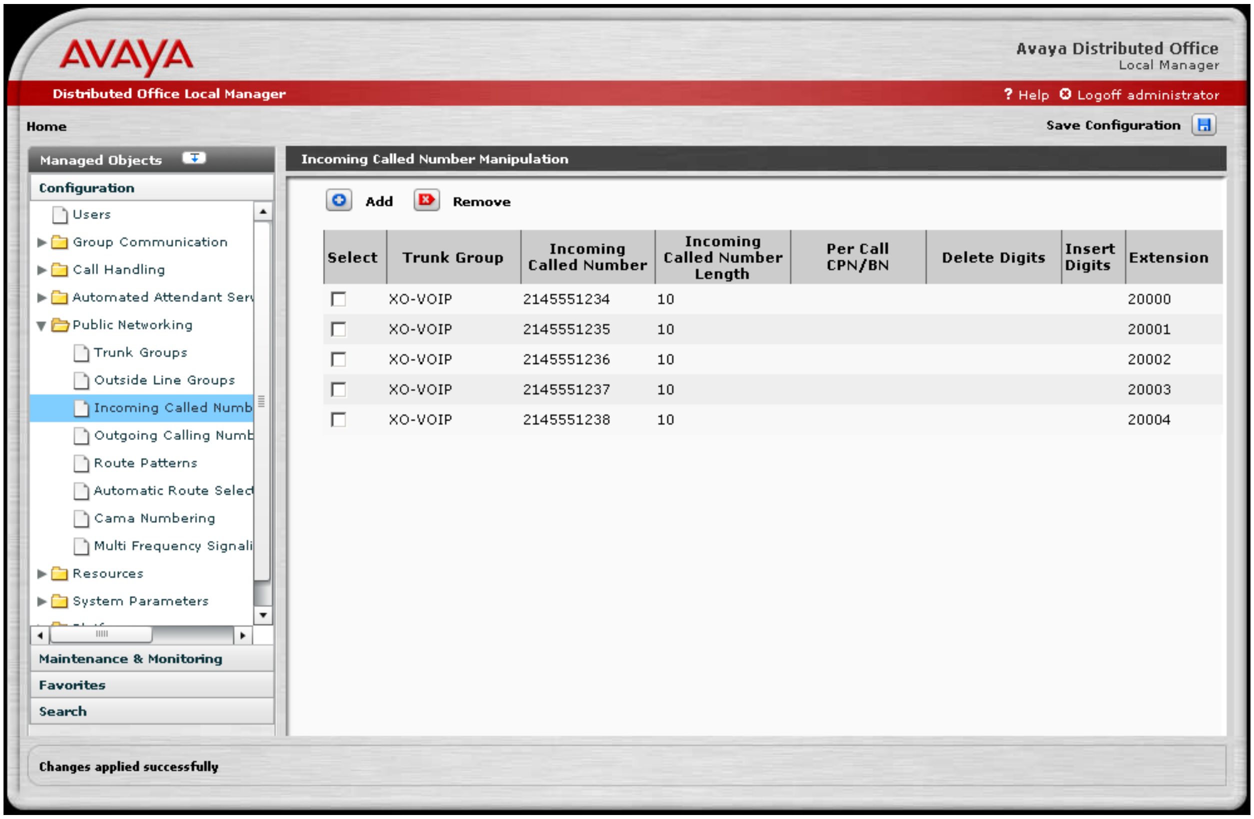

Figure 22 - Incoming Called Number Manipulation – Summary Screen

4.2.3. Save Avaya Communication Manager Branch Edition Configuration

The configuration of the Avaya Communication Manager Branch Edition SIP trunking with the XO Communications XO SIP Service is now complete. Save the Avaya Communication Manager Branch Edition 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.

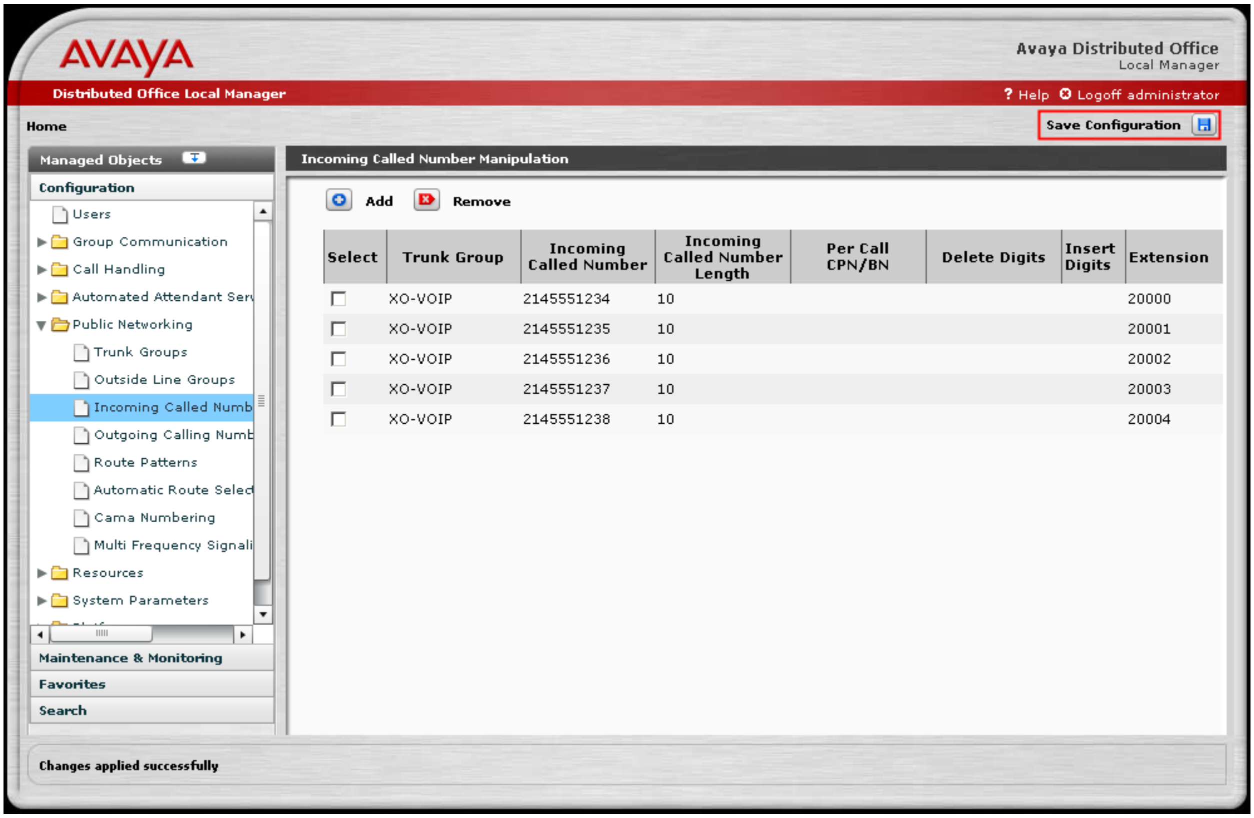

Figure 23 - Save Configuration

5. Configure the XO Communications XO SIP Service

In order to use the XO SIP Service, a customer must request service using the XO Communications sales process. The process can be started by contacting XO Communications via their corporate web site at http://www.xo.com/ or by contacting a XO Communications sales representative.

The following table contains the configuration information, coordinated with XO, which was used during the interoperability compliance testing to verify the XO SIP Service.

Feature	Test Configuration
Codec(s) Required: • G.711 mu-law • G.729A and G.729B • RFC2833 DTMF (required)	The network configuration described in these Application Notes was tested with the codecs (payload types) listed in the left column. Note: RFC2833 is required for shuffling SIP calls.
Define Dial Plan	10 digit dialing, directory assistance, toll-free, international, operator, and collect calls were supported by the test configuration.
Listed Directory Numbers provided by XO	Listed directory numbers should be assigned to the endpoints at the enterprise site. This allows calls to be delivered from the PSTN. In this configuration, listed directory numbers beginning with area code 214 were assigned to the SIP, H.323, digital, and analog endpoints in the enterprise network. In addition, these DID numbers will be sent as the CPN to the XO VoIP network for authentication.
XO provides Proxy IP Address	The IP address of the Sonus Networks NBS in the XO VoIP network was 172.16.1.15.
Avaya provides IP address of Avaya Communication Manager Branch Edition	The IP address of the Avaya Communication Manager Branch Edition gateway IP address was 5.111.92.41. XO used this IP address for routing calls to the listed directory numbers assigned to the enterprise site.
SIP Transport Protocol and Port	SIP signaling was transported between Avaya Communication Manager Branch Edition and XO using UDP and port 5060.

6. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify SIP trunking interoperability between the XO Communications XO SIP Service and the Avaya Communication Manager Branch Edition. This section covers the general test approach and the test results.

Avaya Communication Manager Branch Edition i120 (Release 1.2) was connected using SIP trunking (via general purpose Internet services) to the XO Communications XO SIP Service. The general test approach included the following:

- 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 Communication Manager Branch Edition voice mail menus.

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

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

The following compatibility issues were observed during testing:

- **Call Forwarding Off-Net**. The incoming PSTN call delivered to an Avaya telephone with Call Forwarding enabled to an off-net PSTN phone will be denied by the XO SIP Service because it won't be able to authenticate the calling number of the PSTN user sent by Avaya. In this case, the call will not be forwarded and the PSTN caller will hear "busy" tone. If the call originates from a local Avaya telephone, this issue does not occur because the XO SIP Service can authenticate the local Avaya user, if a DID number has been assigned to the user.
- **EC500**. The EC500 feature (i.e. Extension to Cellular) applies to a user who can be reached at their Avaya desk phone or a cellular phone over the PSTN by dialing a single DID number. When a call is made to this DID number from the PSTN, the desk phone and cellular phone should ring simultaneously allowing the user to answer the call on either phone depending on their location. However, in this configuration, when an incoming PSTN call arrives to an Avaya desk phone with EC500 enabled, the outgoing EC500 call to the user's cellular phone over the PSTN is denied by the XO VoIP network. The outgoing call is denied because Avaya sends out the calling number of the PSTN user, which is unknown to the XO VoIP network and can't be authenticated. In this case, only the Avaya desk phone will ring since the outgoing EC500 call was denied. If the call originates from a local Avaya telephone, this issue does not occur because the XO VoIP network can authenticate the local Avaya user, if a DID number has been assigned to the user.
  A second problem was found when dialing from a mobile phone to an extension on the same Avaya Communication Manager Branch Edition. The display on the called station showed the mobile phone calling party number rather than the associated desk phone calling party number. This results in not being able to use service codes from the mobile phone.
- **IP Softphone Telecommuter Mode**. Avaya Communication Manager Branch Edition does not support IP Softphone Telecommuter mode using SIP trunks.
- **T.38 fax requires G.711MU to be listed in the Codec-Set for the SIP trunk group**. For outgoing Fax calls, XO SIP service will transition the call from a non-G711.MU encoded call (e.g. G.729a) to G.711MU and then to T.38.
- **Avaya Communication Manager Branch Edition does not support diversion headers.** This results in the PSTN calling party ID to not appear to the called stations when either transferred or forwarded to another PSTN phone via the SIP trunk.

7. Verification Steps

7.1. Verification Tests

Configuration verification was performed with use of ping to confirm network connectivity between the Avaya Communication Manager Branch Edition and the XO VoIP network. Once verified, an initial incoming and outgoing call were completed prior to testing and reviewed with use of a SIP protocol analyzer.

7.2. Troubleshooting Tools

The Avaya Communication Manager Branch Edition 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 XO Communications VoIP 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 XO Communications XO SIP Service and the Avaya Communication Manager Branch Edition. This can be extremely valuable to support advanced troubleshooting.

8. Conclusion

These Application Notes describe the steps for configuring SIP trunking between an Avaya Communication Manager Branch Edition (Release 1.2) and XO Communications XO SIP 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. Additional References

The Avaya Communication Manager Branch Edition product documentation is available at http://support.avaya.com.

[1] Avaya Distributed Office Documentation Map Release 1.2, Issue 2, June 2008, 03-602021
[2] Overview of Avaya Distributed Office, Issue 2, June 2008, 03-602024
[3] Avaya Distributed Office i120 Installation Quick Start, Issue 2, June 2008, 03-602289
[4] Avaya Distributed Office i40 Installation Quick Start, Issue 2, June2008, 03-602288
[5] Feature Description for Avaya Distributed Office Release 1.2, Issue 2, June 2008, 03-602027
[6] Avaya Application Solutions: IP Telephony Deployment Guide, Issue 6, January 2008, 555-245-600
[7] 4600 Series IP Telephone LAN Administrator Guide, Issue 8, July 2008, 555-233-507
[8] Avaya one-X™ Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.0, Issue 2, December 2007, 16-601944

[9] XO Communications XO SIP Service Descriptions - http://www.xo.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 XO Communications and Avaya Communication Manager Branch Edition. 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 from Avaya Communication Branch Edition to XO Communications:

```
Session Initiation Protocol
    Request-Line: INVITE sip:17325550819@172.16.1.15;transport=udp SIP/2.0
        Method: INVITE
        [Resent Packet: False]
    Message Header
        Call-ID: 80627ea61bd8dd1695495d1aca00
        CSeq: 1 INVITE
            Sequence Number: 1
            Method: INVITE
        From: "Richard"
<sip:2145551234@example.com:6002>;tag=80627ea61bd8dd1685495d1aca00
            SIP Display info: "Richard"
            SIP from address: sip:2145551234@example.com:6002
            SIP tag: 80627ea61bd8dd1685495d1aca00
        Record-Route: <sip:5.211.92.41:5060;lr>
        Record-Route: <sip:5.211.92.41:6002;transport=tls;lr>
        To: "17325550819" <sip:17325550819@xo.com>
            SIP Display info: "17325550819"
            SIP to address: sip:17325550819@xo.com
        Via: SIP/2.0/UDP
5.211.92.41:5060;branch=z9hG4bK83838303030363636322d4.0
            Transport: UDP
            Sent-by Address: 5.211.92.41
            Sent-by port: 5060
            Branch: z9hG4bK83838303030363636322d4.0
        Contact: "Richard" <sip:2145551234@5.211.92.41:6002;transport=tls>
            Contact Binding: "Richard"
<sip:2145551234@5.211.92.41:6002;transport=tls>
                URI: "Richard"
<sip:2145551234@5.211.92.41:6002;transport=tls>
                    SIP Display info: "Richard"
                    SIP contact address: sip:2145551234@5.211.92.41:6002
        Max-Forwards: 69
        User-Agent: Avaya CM/R013w.01.2.024.0
        Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER,
OPTIONS
        History-Info: <sip:17325550819@xo.com>;index=1
        History-Info: "17325550819" <sip:17325550819@xo.com>;index=1.1
        Supported: 100rel, timer, replaces, join, histinfo
        Min-SE: 1200
        Session-Expires: 1200;refresher=uac
        P-Asserted-Identity: "Richard" <sip:2145551234@example.com:6002>
        Content-Type: application/sdp
```

```
        Content-Length: 155
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): - 1 1 IN IP4 5.211.92.41
                Owner Username: -
                Session ID: 1
                Session Version: 1
                Owner Network Type: IN
                Owner Address Type: IP4
                Owner Address: 5.211.92.41
            Session Name (s): -
            Connection Information (c): IN IP4 5.211.92.41
                Connection Network Type: IN
                Connection Address Type: IP4
                Connection Address: 5.211.92.41
            Time Description, active time (t): 0 0
                Session Start Time: 0
                Session Stop Time: 0
            Media Description, name and address (m): audio 34060 RTP/AVP 0
100
                Media Type: audio
                Media Port: 34060
                Media Proto: RTP/AVP
                Media Format: ITU-T G.711 PCMU
                Media Format: 100
            Media Attribute (a): rtpmap:0 PCMU/8000
                Media Attribute Fieldname: rtpmap
                Media Format: 0
                MIME Type: PCMU
            Media Attribute (a): rtpmap:100 telephone-event/8000
                Media Attribute Fieldname: rtpmap
                Media Format: 100
                MIME Type: telephone-event
```

Sample SIP INVITE Message from XO Communications to Avaya Communications Branch Manager:

```
Session Initiation Protocol
    Request-Line: INVITE sip:2145551235@5.211.92.41:5060 SIP/2.0
        Method: INVITE
        [Resent Packet: False]
    Message Header
        Via: SIP/2.0/UDP 172.16.1.15:5060;branch=z9hG4bK02B62f07cd64616b4e8
            Transport: UDP
            Sent-by Address: 172.16.1.15
            Sent-by port: 5060
            Branch: z9hG4bK02B62f07cd64616b4e8
        From: "AVAYA INC      " <sip:7324500819@172.16.1.15:5060;pstn-
params=9084818088;otg=STS_BW1_DIGIUM_INT>;tag=gK02144c10
            SIP Display info: "AVAYA INC      "
            SIP from address: sip:7324500819@172.16.1.15:5060
            SIP tag: gK02144c10
        To: <sip:2145551235@5.211.92.41:5060>
            SIP to address: sip:2145551235@5.211.92.41:5060
        Call-ID: 486722135_1897@172.16.1.15
        CSeq: 22096 INVITE
            Sequence Number: 22096
            Method: INVITE
        Max-Forwards: 70
        Allow:
INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,PRACK,UPDATE,OPTIO
NS
        Accept: application/sdp, application/isup, application/dtmf,
application/dtmf-relay,  multipart/mixed
        Contact: <sip:172.16.1.15:5060>
            Contact Binding: <sip:172.16.1.15:5060>
                URI: <sip:172.16.1.15:5060>
                    SIP contact address: sip:172.16.1.15:5060
        P-Preferred-Identity: "AVAYA INC      "
<sip:7324500819@172.16.1.15:5060>
        Supported: timer,100rel
        Session-Expires: 1800
        Min-SE: 90
        Content-Length:  242
        Content-Disposition: session; handling=required
        Content-Type: application/sdp
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): Sonus_UAC 17533 31076 IN IP4
172.16.1.15
                Owner Username: Sonus_UAC
                Session ID: 17533
                Session Version: 31076
                Owner Network Type: IN
                Owner Address Type: IP4
                Owner Address: 172.16.1.15
            Session Name (s): SIP Media Capabilities
            Connection Information (c): IN IP4 172.16.1.13
                Connection Network Type: IN
```

```
            Connection Address Type: IP4
            Connection Address: 172.16.1.13
        Time Description, active time (t): 0 0
            Session Start Time: 0
            Session Stop Time: 0
        Media Description, name and address (m): audio 11822 RTP/AVP 0
101
            Media Type: audio
            Media Port: 11822
            Media Proto: RTP/AVP
            Media Format: ITU-T G.711 PCMU
            Media Format: 101
        Media Attribute (a): rtpmap:0 PCMU/8000
            Media Attribute Fieldname: rtpmap
            Media Format: 0
            MIME Type: PCMU
        Media Attribute (a): rtpmap:101 telephone-event/8000
            Media Attribute Fieldname: rtpmap
            Media Format: 101
            MIME Type: telephone-event
        Media Attribute (a): fmtp:101 0-15
            Media Attribute Fieldname: fmtp
            Media Format: 101 [telephone-event]
            Media format specific parameters: 0-15
        Media Attribute (a): sendrecv
        Media Attribute (a): maxptime:20
            Media Attribute Fieldname: maxptime
            Media Attribute Value: 20
```

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 5.211.92.41/27
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 5.211.92.41 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(5.211.92.41)" "SIP" permit log
set policy id 2
exit
set policy id 3 name "voice UDP Ports" from "Untrust" to "Trust"  "Any" "MIP(5.211.92.41)" "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 5.211.92.33
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.