Application Notes for Configuring a VPN for an Avaya Communication Manager and Avaya IP Office Network using the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance - Issue 1.0

Abstract

These Application Notes detail the steps for configuring a Virtual Private Network (VPN) between three sites using the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance to support an Avaya Communication Manager and Avaya IP Office network.

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

As IP telephony continues to evolve and workers become more distributed, providing solutions that deliver security, ensure quality of service (QoS) and allow remote users access corporate IP communication services becomes increasingly important. The Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance provides a secure Virtual Private Network (VPN) solution for branch offices and remote users.

The Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance provides a secure VPN and QoS solution for branch offices and remote users. Additionally, the EdgeMarc 4500 VoIP VPN Appliance provides Mean Opinion Score (MOS) call quality metrics for each call made offering management and troubleshooting capabilities.

1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network contains three sites (headquarters, branch and remote) connected together via a VPN provided by Edgewater Networks EdgeMarc 4500 VoIP VPN Appliances. The network is comprised of Avaya Communication Manager and Avaya SIP Enablement Services (SES) in the headquarters, an Avaya IP Office in the branch site, two Avaya 9630 IP telephones, one Avaya 4620SW IP Telephone, one Avaya 4625SW IP Telephone, one Avaya 5620SW IP Telephone, two Avaya 2420 Digital Telephones and three Edgewater Networks EdgeMarc 4500 VoIP VPN Appliances. Telephones in the remote site register to Avaya Communication Manager in the headquarters site. Three power-over Ethernet (PoE) switches are also present in the network. All of the IP telephones within the network are provisioned statically using the keypad present on the telephones. One computer, in the headquarters site, runs the Avaya IP Office Manager and Avaya IP Office Voice Mail Pro software applications. The same computer also runs a Syslog server where MOS scores for completed calls are directed.

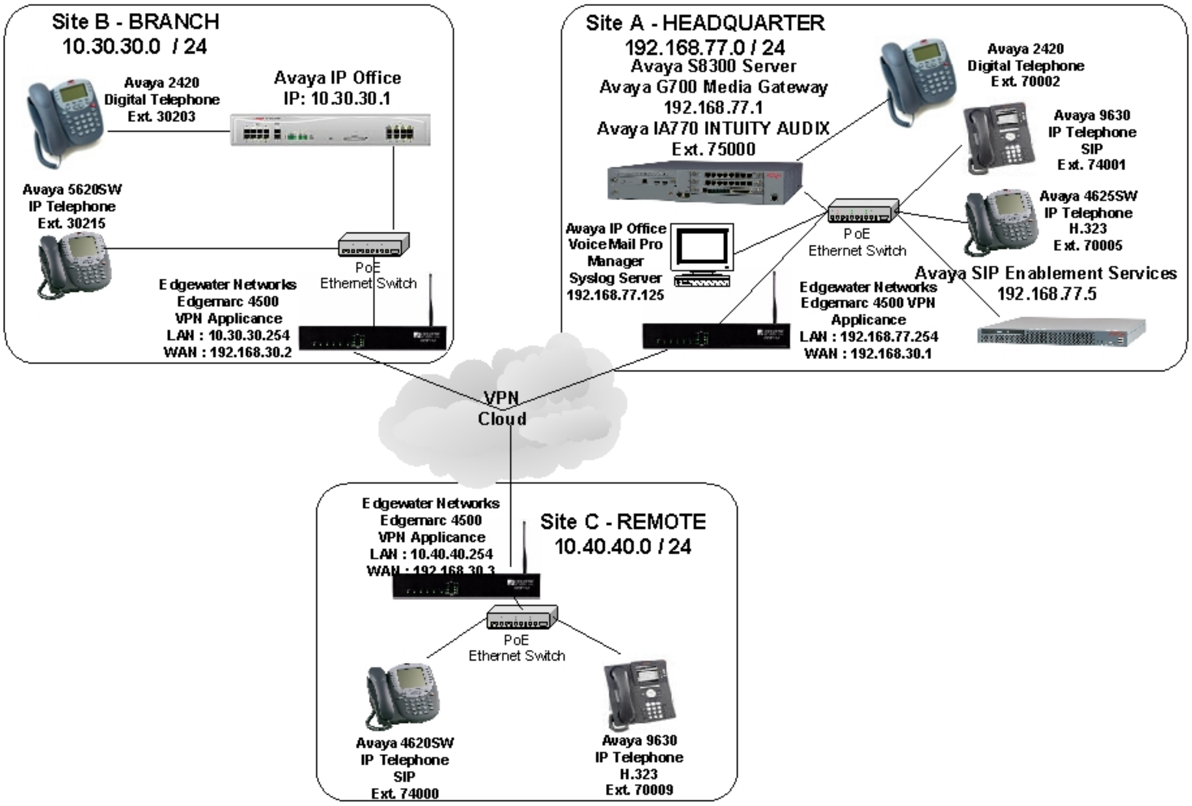


Figure 1: Sample Network Configuration

2. Equipment and Software Validated

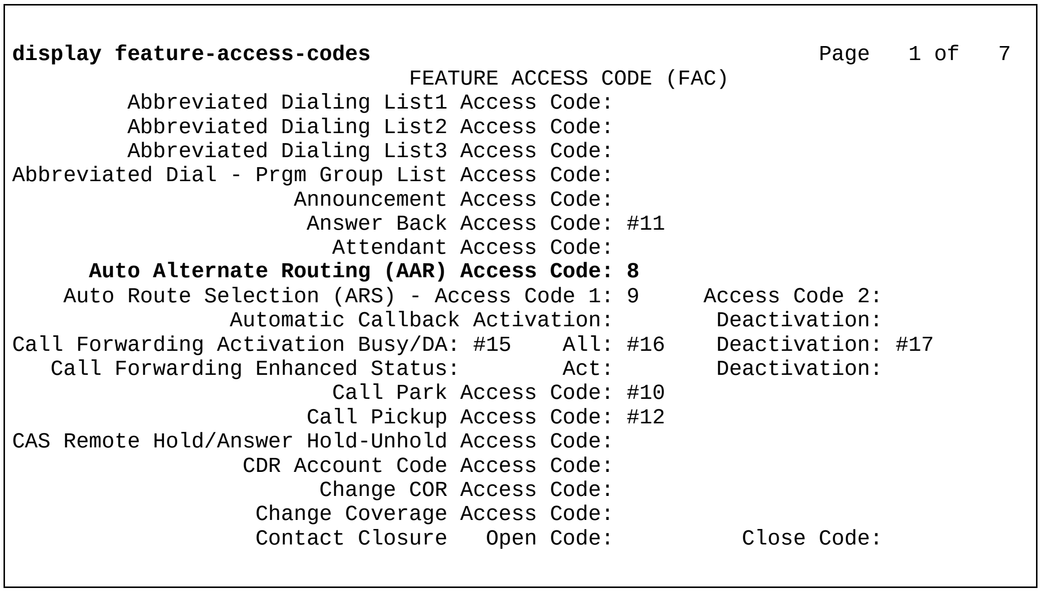
The following hardware and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Media Server	Avaya Communication Manager 4.0 (R014x.00.0.730.5)
Avaya G700 Media Gateway • MM711 Analog Media Module • MM712 DCP Media Module	26.31.0 HW04 / FW87 HW05 / FW08
Avaya SIP Enablement Services	4.0
Avaya IP Office	4.1.9
Avaya IP Office Manager	6.1.9
Avaya IP Office Voice Mail Pro	4.1
Avaya 5600 Series IP Telephones	2.3 (H.323)
Avaya 4600 Series IP Telephones	2.8.3 (H.323)
Avaya 4600 Series IP Telephones	2.2.2 (SIP)
Avaya 9600 Series IP Telephones	1.5 (H.323)
Avaya 9600 Series IP Telephones	1.0.2 (SIP)
Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance	7.9.3

3. Avaya Communication Manager Configuration

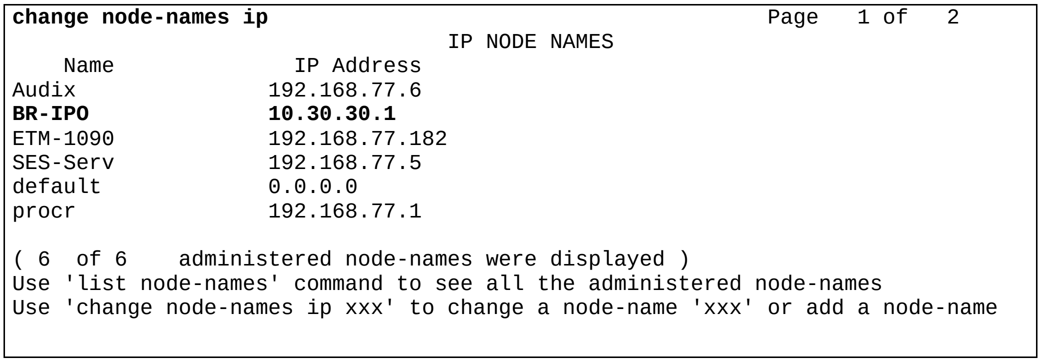
All of the telephones configured in the sample network in **Figure 1** were administered as stations or users in Avaya Communication Manager and Avaya SIP Enablement Services. SIP stations were administered as Off-PBX stations in Avaya Communication Manager. For a complete reference on how to administer these types of stations, refer to **References** [**1**,**2**]. The values for UDP parameters found under “ip-network-region” were configured to match the RTP parameters of Avaya IP Office.

Step	Description
1.	From the System Administration Terminal (SAT) interface on Avaya Communication Manager, use the “display feature-access-codes” command to obtain the access code which is used for **Auto Alternate Routing (AAR)**.



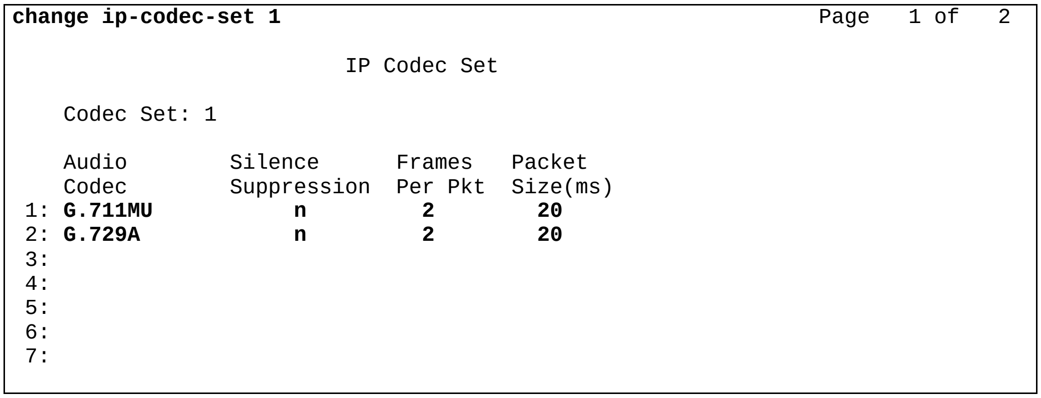
```
display feature-access-codes                                   Page   1 of   7
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code: #11
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: #15    All: #16    Deactivation: #17
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: #10
                       Call Pickup Access Code: #12
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
                   Contact Closure   Open Code:          Close Code:
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>From the SAT interface on Avaya Communication Manager, use the “change node-names ip” command to define the name and IP address of the Avaya IP Office system found in the branch site, see <b>Figure 1</b>. Enter the information displayed below and submit the changes.



<pre>
change node-names ip   Page   1 of   2
                                  IP NODE NAMES
    Name   IP Address
Audix   192.168.77.6
BR-IPO   10.30.30.1
ETM-1090   192.168.77.182
SES-Serv   192.168.77.5
default   0.0.0.0
procr   192.168.77.1

(6 of 6   administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
</pre>
</td></tr>
<tr><td>3.</td><td>From the SAT interface on Avaya Communication Manager, use the “change ip-codec set” command to specify the codecs and parameters displayed below and submit the changes.

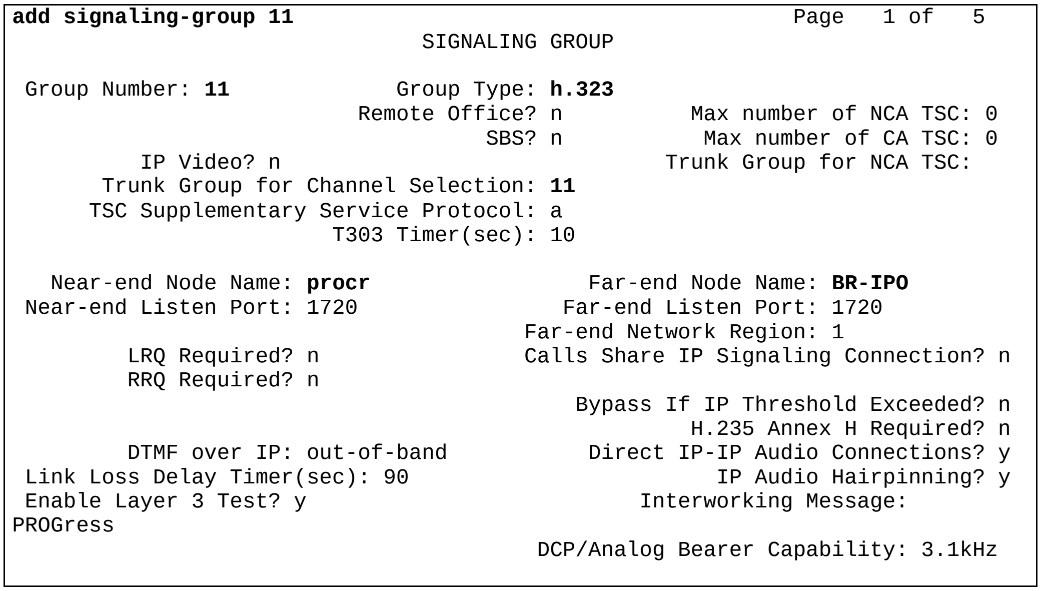


<pre>
change ip-codec-set 1   Page   1 of   2

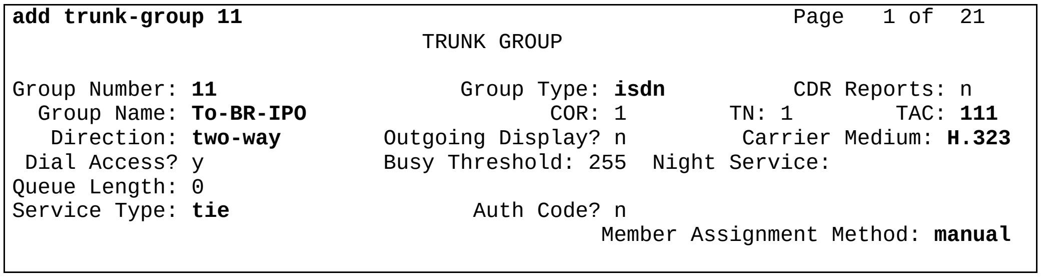
                          IP Codec Set

    Codec Set: 1

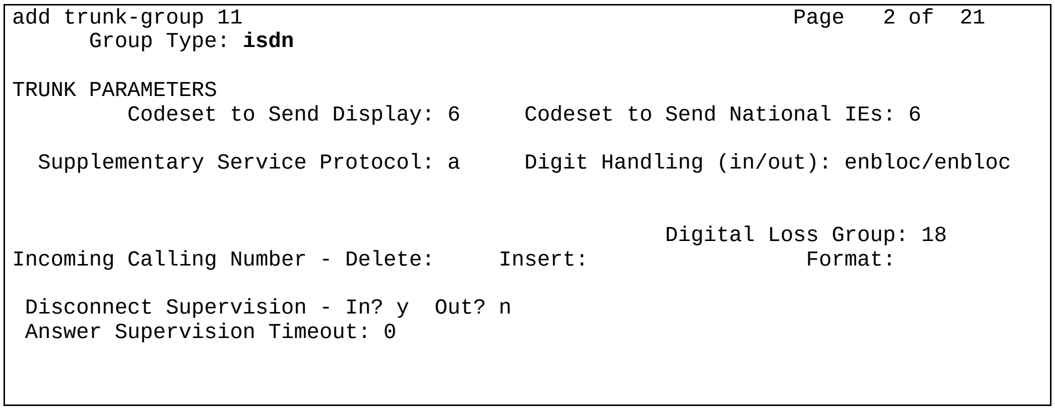
    Audio   Silence   Frames   Packet
    Codec   Suppression Per Pkt Size(ms)
 1: G.711MU   n   2   20
 2: G.729A   n   2   20
 3:
 4:
 5:
 6:
 7:
</pre>
</td></tr>
</table>

Step	Description
4.	From the SAT interface on Avaya Communication Manager, use the “add signaling-group” command to create a new signaling group. The numerical identifier used for the signaling-group can be any unused numerical value. Enter the information displayed below and then submit the changes. **Group Number** can be any unused numerical value and was set to “11”. **Group Type** was set to “h.323”. **Trunk Group for Channel Selection** can not be configured until **Step 5** is complete. The operator will have to complete **Step 5** and then use the “change signaling-group” command to configure the **Trunk Group for Channel Selection**. The value used for the **Trunk Group for Channel Selection** is the numerical identifier configured in **Step 5** for **Group Number**. **Near-end Node Name** was set to “procr”, which is an interface that belongs to Avaya Communication Manager, see **Figure 1**. **Far-end Node Name** is the node-name created in **Step 2**. The remaining parameters were left at the default values. 

```
add signaling-group 11                                       Page   1 of   5
                                SIGNALING GROUP

 Group Number: 11             Group Type: h.323
                           Remote Office? n          Max number of NCA TSC: 0
                                     SBS? n           Max number of CA TSC: 0
          IP Video? n                               Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 11
      TSC Supplementary Service Protocol: a
                         T303 Timer(sec): 10

   Near-end Node Name: procr                 Far-end Node Name: BR-IPO
 Near-end Listen Port: 1720                Far-end Listen Port: 1720
                                        Far-end Network Region: 1
         LRQ Required? n                Calls Share IP Signaling Connection? n
         RRQ Required? n
                                            Bypass If IP Threshold Exceeded? n
                                                     H.235 Annex H Required? n
         DTMF over IP: out-of-band           Direct IP-IP Audio Connections? y
 Link Loss Delay Timer(sec): 90                        IP Audio Hairpinning? y
 Enable Layer 3 Test? y                          Interworking Message:
PROGress
                                         DCP/Analog Bearer Capability: 3.1kHz
```

Step	Description
5.	From the SAT interface on Avaya Communication Manager, use the “add trunk-group” command to create a new trunk group. Enter the information displayed below. **Group Number** can be any unused numerical value and was set to “11”. **Group Type** was set to “isdn”. **Group Name** can be any descriptive text and was set to “To-BR-IPO”. **TAC** can by any unused value within the dial plan and was set to “111”. **Direction** was set to “two-way”. **Carrier Medium** was set to “H.323”. **Service Type** was set to “tie”. **Member Assignment Method** was set to “manual”. The remaining parameters were left at the default values. 

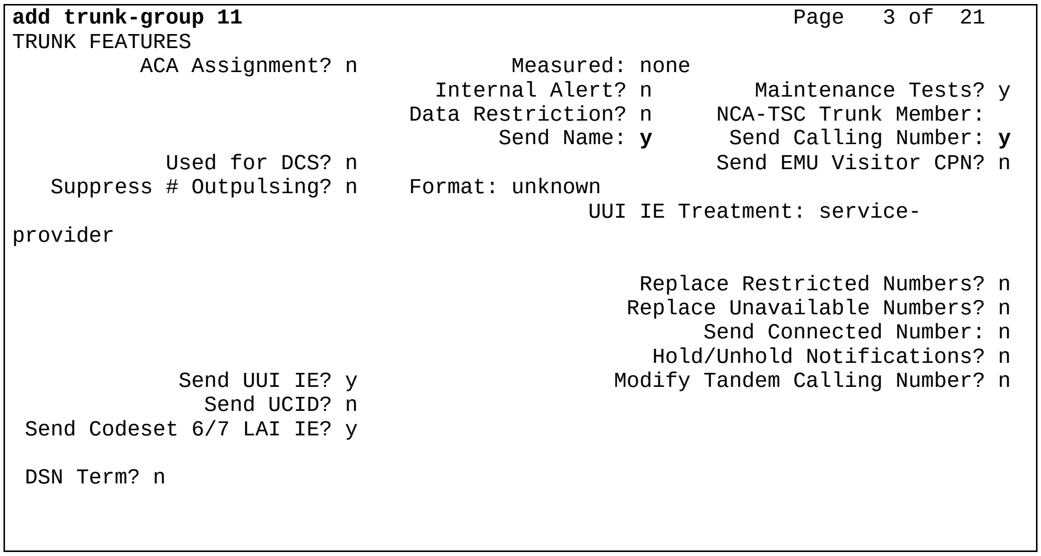
```
add trunk-group 11                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 11                  Group Type: isdn          CDR Reports: n
  Group Name: To-BR-IPO                  COR: 1        TN: 1        TAC: 111
   Direction: two-way       Outgoing Display? n         Carrier Medium: H.323
 Dial Access? y             Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                              Member Assignment Method: manual
```

6.	Navigate to page 2 on the trunk group form. Enter the information displayed below. **Group Type** was set to “isdn”. The remaining parameters were left at the default values. 

```
add trunk-group 11                                          Page   2 of  21
      Group Type: isdn

TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6

  Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc


                                                   Digital Loss Group: 18
Incoming Calling Number - Delete:     Insert:                Format:

 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>

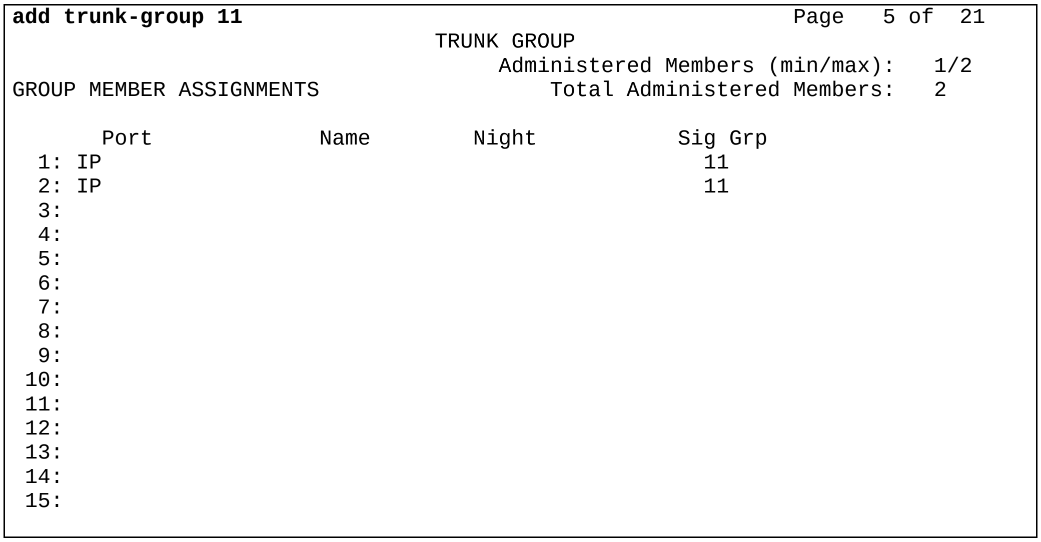
Navigate to page 3 of the trunk group form. Enter the information displayed below. **Send Name** and **Send Calling Number** were set to “y”. The remaining parameters were left at the default values.



```
add trunk-group 11                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: unknown
                                             UUI IE Treatment: service-
provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                      Send Connected Number: n
                                                   Hold/Unhold Notifications? n
             Send UUI IE? y                       Modify Tandem Calling Number? n
               Send UCID? n
 Send Codeset 6/7 LAI IE? y

 DSN Term? n
```

</td></tr>
<tr><td>8.</td><td>

Navigate to page 5 of the trunk group form. Enter the information displayed below and submit the changes. Use the keyword “IP” for each **Port** and specify the numerical identifier used for the signaling group created in **Step 4**. Configure the appropriate number of ports to match the number of trunk members on the Avaya IP Office configured in **Section 4**, **Step 6**. The remaining parameters were left at the default values.



```
add trunk-group 11                                          Page   5 of  21
                                 TRUNK GROUP
                                      Administered Members (min/max):   1/2
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:   2

       Port             Name        Night           Sig Grp
  1: IP                                               11
  2: IP                                               11
  3:
  4:
  5:
  6:
  7:
  8:
  9:
 10:
 11:
 12:
 13:
 14:
 15:
```

</td></tr>
</table>

Step **Description**

9. In this sample configuration, the branch site is using five digit extensions beginning with “3”. To allow the headquarters site to dial the branch site using AAR, modify the AAR analysis table and create a route pattern. From the SAT interface on Avaya Communication Manager, use the “change aar analysis” command. Enter the information displayed below and submit the changes. **Dialed String** was set to “3”. **Total Min** and **Total Max** were set to “5”. **Route Pattern** was set to “11” (see **Step 10**). **Call Type** was set to “aar”.

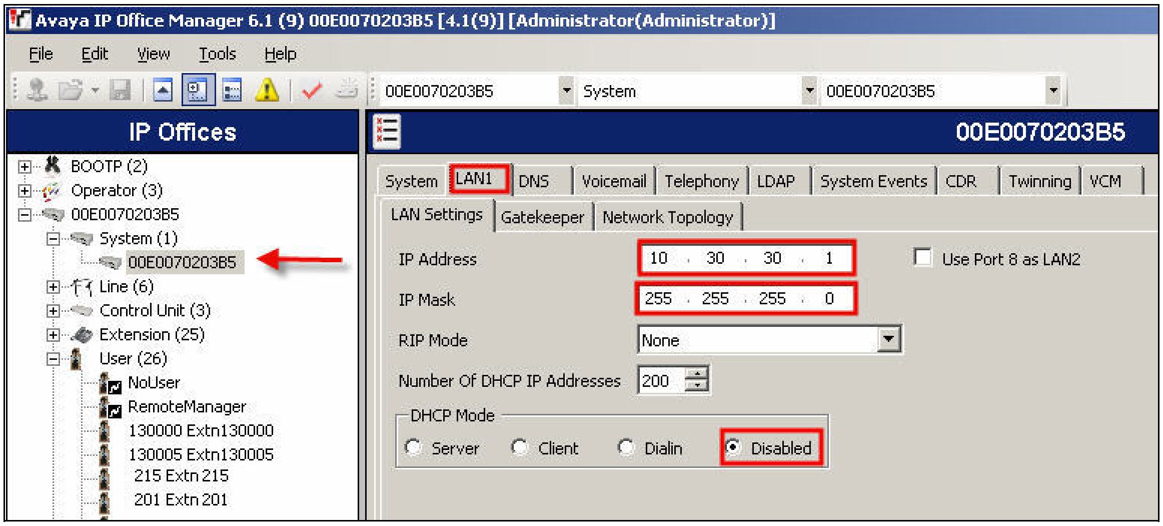
```
change aar analysis 3                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                                            Percent Full:    3

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    3                     5    5     11       aar          n
    75000                 5    5     3        aar          n
```

10. From the SAT interface on Avaya Communication Manager, use the “change route-pattern” command. Enter the information displayed below and submit the changes.
Grp No is the numerical identifier used for the **Trunk Group** configured in **Step 5**.
FRL was set to “0”. The remaining parameters were left at the default values.

```
change route-pattern 11                                        Page   1 of   3
                    Pattern Number: 11  Pattern Name:
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 11   0                                                               n   use
 2:                                                                      n   use
 3:                                                                      n   use
 4:                                                                      n   use
 5:                                                                      n   use
 6:                                                                      n   use

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

4. Avaya IP Office Configuration

Avaya IP Office is administered using the Avaya IP Office Manager Windows application. The application can be accessed by navigating to **Start→Programs→IP Office→Manager**. Appropriate logon credentials are required to gain access to the application. For information on installation and administration of Avaya IP Office software applications, refer to **References** [**3**,**4**].

Step	Description
1.	Navigate to the **LAN1** tab by clicking under the Avaya IP Office's MAC address under **System** within the navigation panel on the left side of **Avaya IP Office Manager** window. Then click **LAN1**. Enter the information displayed below and then click **OK**. The **OK** button is found on the bottom left Avaya IP Office Manager application. Configure the **IP Address** and **IP Mask** per **Figure 1**. Configure **DHCP Mode** to "Disabled". When changing tabs on Avaya IP Office Manager, the operator may be asked to save configuration changes. Confirm and save the configuration changes if prompted. 

Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4.1(9)] [Administrator(Administrator)]

00E0070203B5 – System – 00E0070203B5

LAN1 – LAN Settings

IP Address: 10 . 30 . 30 . 1

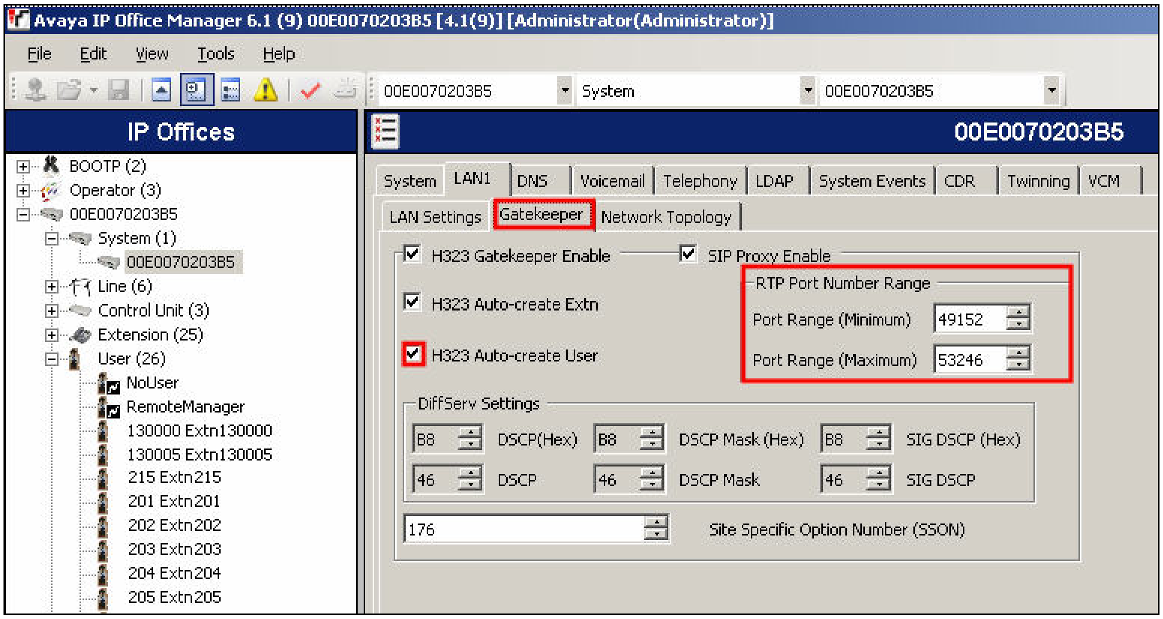
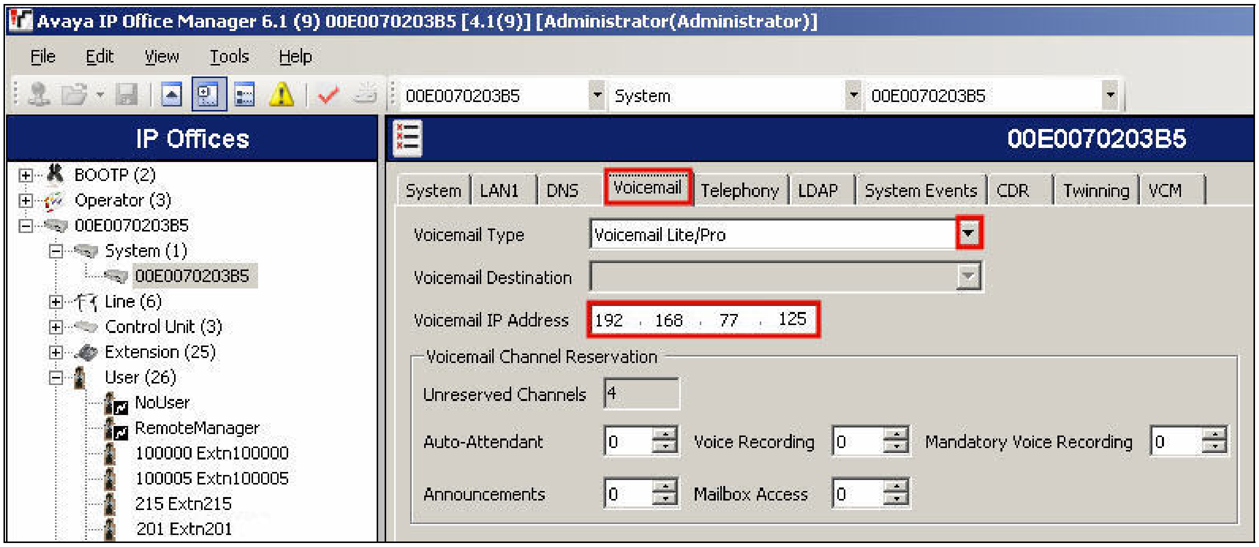
IP Mask: 255 . 255 . 255 . 0

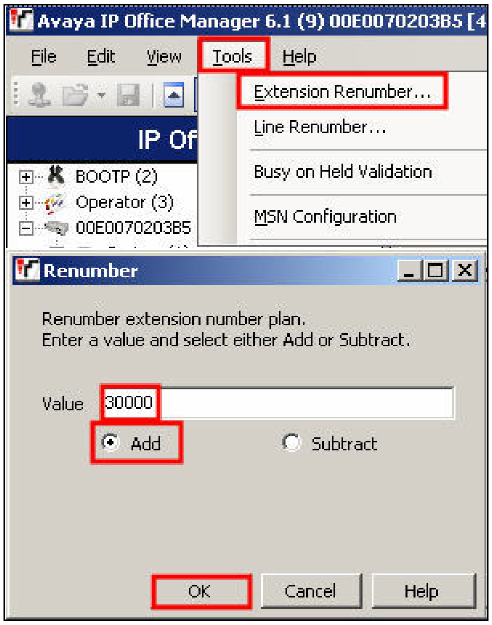
RIP Mode: None

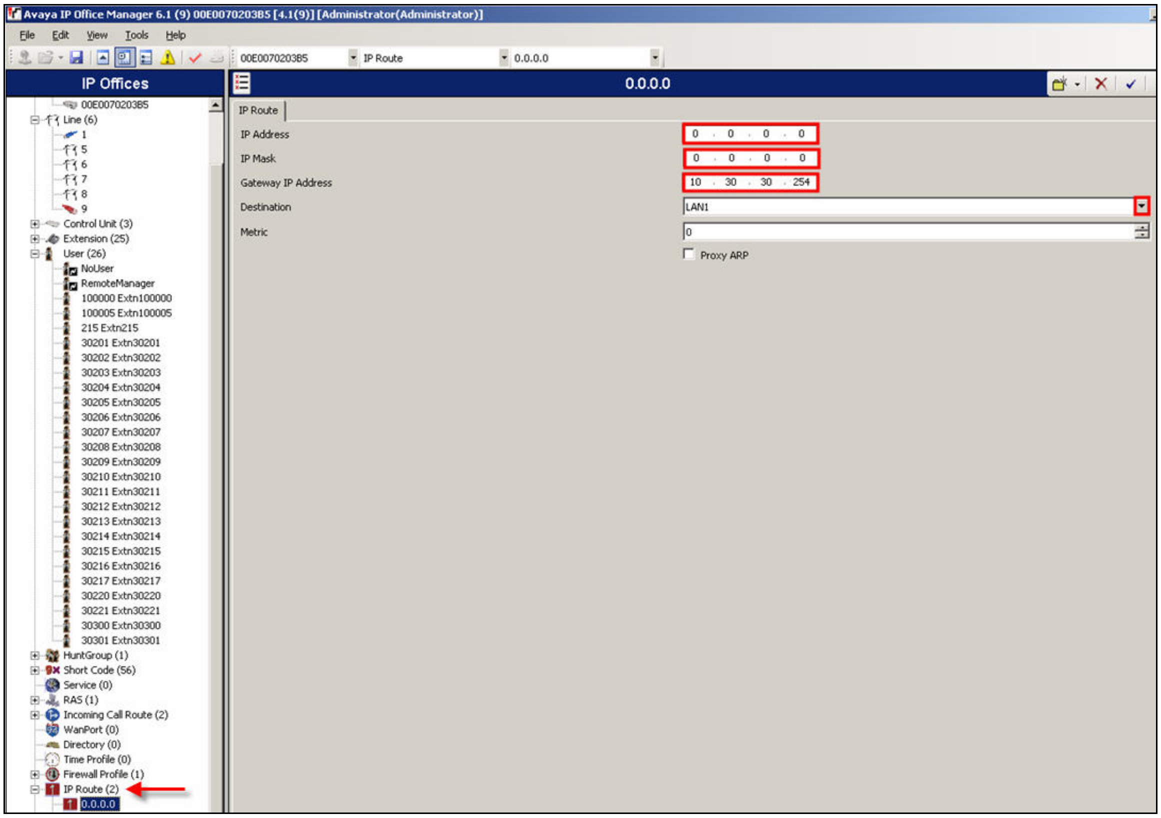
Number Of DHCP IP Addresses: 200

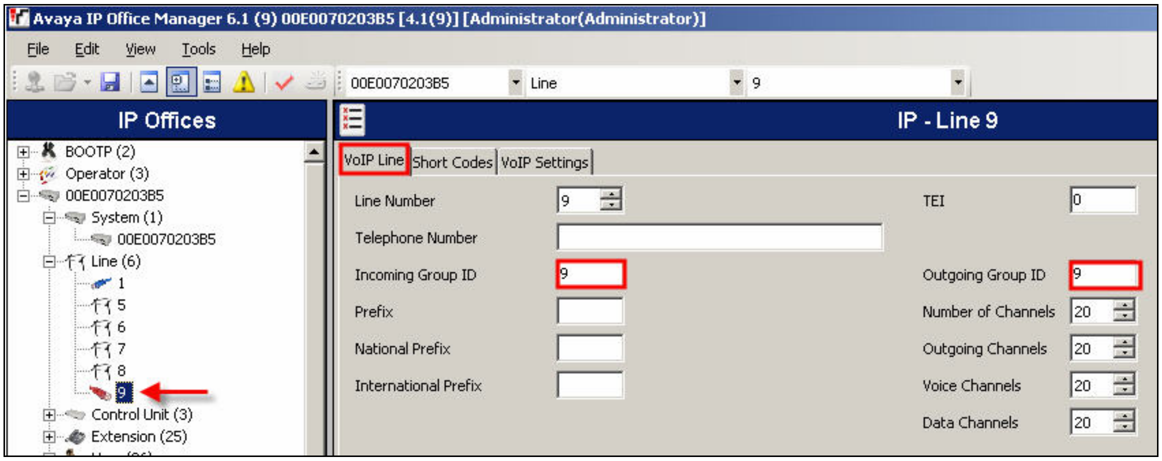
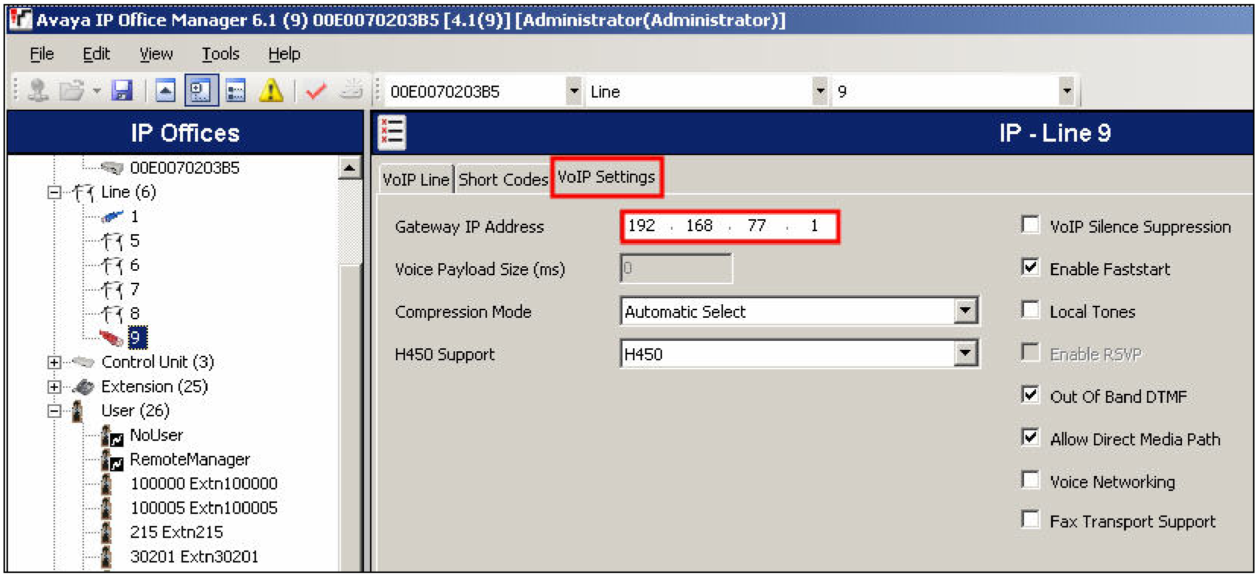
DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

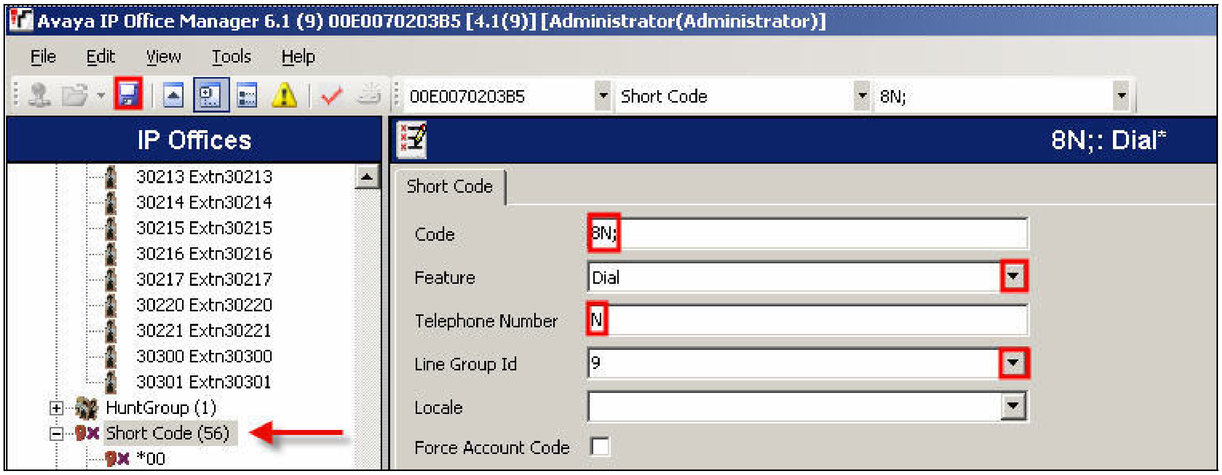
□ Use Port 8 as LAN2

Step	Description
2.	Navigate to the **Gatekeeper** tab by clicking **Gatekeeper**. Check the **H323 Auto-create User** check box. This feature allows Avaya IP Office to dynamically create **Users** and **Extensions** when a telephone registers. Make note of the **RTP Port Number Range** information. This information will need to be configured on each EdgeMarc 4500 VoIP VPN Appliance in **Section 5**, **Step 7**.  Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4.1(9)] [Administrator(Administrator)] ☑ H323 Gatekeeper Enable ☑ SIP Proxy Enable ☑ H323 Auto-create Extn ☑ H323 Auto-create User RTP Port Number Range Port Range (Minimum) 49152 Port Range (Maximum) 53246 DiffServ Settings B8 DSCP(Hex) B8 DSCP Mask (Hex) B8 SIG DSCP (Hex) 46 DSCP 46 DSCP Mask 46 SIG DSCP 176 Site Specific Option Number (SSON) File Edit View Tools Help 00E0070203B5 System 00E0070203B5 IP Offices BOOTP (2) Operator (3) 00E0070203B5 System (1) 00E0070203B5 Line (6) Control Unit (3) Extension (25) User (26) NoUser RemoteManager 130000 Extn130000 130005 Extn130005 215 Extn215 201 Extn201 202 Extn202 203 Extn203 204 Extn204 205 Extn205 00E0070203B5 System LAN1 DNS Voicemail Telephony LDAP System Events CDR Twinning VCM LAN Settings Gatekeeper Network Topology
3.	Navigate to the **Voicemail** tab by clicking **Voicemail**. Enter the information displayed below and then click **OK**. Use the drop-down list for **Voicemail Type** to select “Voicemail Lite/Pro”. **Voicemail IP Address** is the IP address assigned to the computer running Avaya IP Office Voice Mail Pro, see **Figure 1**.  Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4.1(9)] [Administrator(Administrator)] Voicemail Type: Voicemail Lite/Pro Voicemail Destination: Voicemail IP Address: 192 . 168 . 77 . 125 Voicemail Channel Reservation Unreserved Channels 4 Auto-Attendant 0 Voice Recording 0 Mandatory Voice Recording 0 Announcements 0 Mailbox Access 0 File Edit View Tools Help 00E0070203B5 System 00E0070203B5 IP Offices BOOTP (2) Operator (3) 00E0070203B5 System (1) 00E0070203B5 Line (6) Control Unit (3) Extension (25) User (26) NoUser RemoteManager 100000 Extn100000 100005 Extn100005 215 Extn215 201 Extn201 00E0070203B5 System LAN1 DNS Voicemail Telephony LDAP System Events CDR Twinning VCM

Step	Description
4.	By default, Avaya IP Office assigns extensions starting with 200. In the sample configuration, the branch site Avaya IP Office was using five digit extensions starting with “3”. To accomplish this, use the **Extension Renumber** feature by clicking **Tools** and then clicking **Extension Renumber**. Enter the information below and then click **OK**.  Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4 File Edit View Tools Help Extension Renumber... Line Renumber... Busy on Held Validation MSN Configuration IP Of BOOTP (2) Operator (3) 00E0070203B5 Renumber OK Cancel Help Renumber extension number plan. Enter a value and select either Add or Subtract. Value 30000 ● Add ○ Subtract

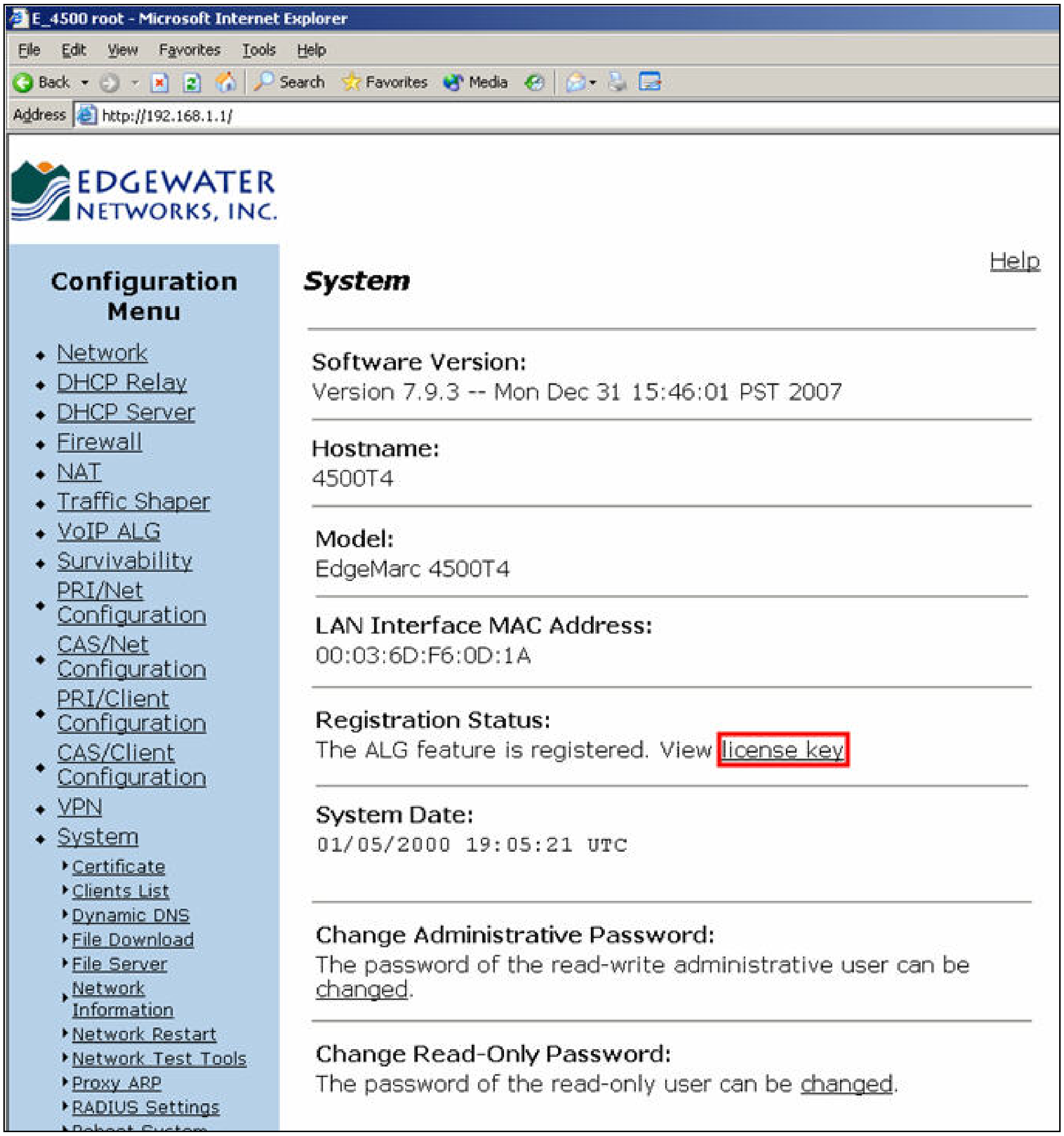
Step	Description
5.	Navigate to the **IP Route** tab by clicking **IP Route** within the navigation panel on the left side of **Avaya IP Office Manager** window. Enter the information displayed below and then click **OK**. **IP Address** and **IP Mask** are both “0.0.0.0”, indicating a default route. **Gateway IP Address** is the IP address assigned to the LAN interface on the EdgeMarc 4500 VoIP VPN Appliance within the specific site being configured. Use the drop-down list for **Destination** and select “LAN1”.  Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4.1(9)] [Administrator(Administrator)] 00E0070203B5 · IP Route · 0.0.0.0 IP Route IP Address: 0 . 0 . 0 . 0 IP Mask: 0 . 0 . 0 . 0 Gateway IP Address: 10 . 30 . 30 . 254 Destination: LAN1 Metric: 0 □ Proxy ARP File Edit View Tools Help IP Offices 00E0070203B5 Line (6) 1 5 6 7 8 9 Control Unit (3) Extension (25) User (26) NoUser RemoteManager 100000 Extn100000 100005 Extn100005 215 Extn215 30201 Extn30201 30202 Extn30202 30203 Extn30203 30204 Extn30204 30205 Extn30205 30206 Extn30206 30207 Extn30207 30208 Extn30208 30209 Extn30209 30210 Extn30210 30211 Extn30211 30212 Extn30212 30213 Extn30213 30214 Extn30214 30215 Extn30215 30216 Extn30216 30217 Extn30217 30220 Extn30220 30221 Extn30221 30300 Extn30300 30301 Extn30301 HuntGroup (1) Short Code (56) Service (0) RAS (1) Incoming Call Route (2) WanPort (0) Directory (0) Time Profile (0) Firewall Profile (1) IP Route (2) 0.0.0.0

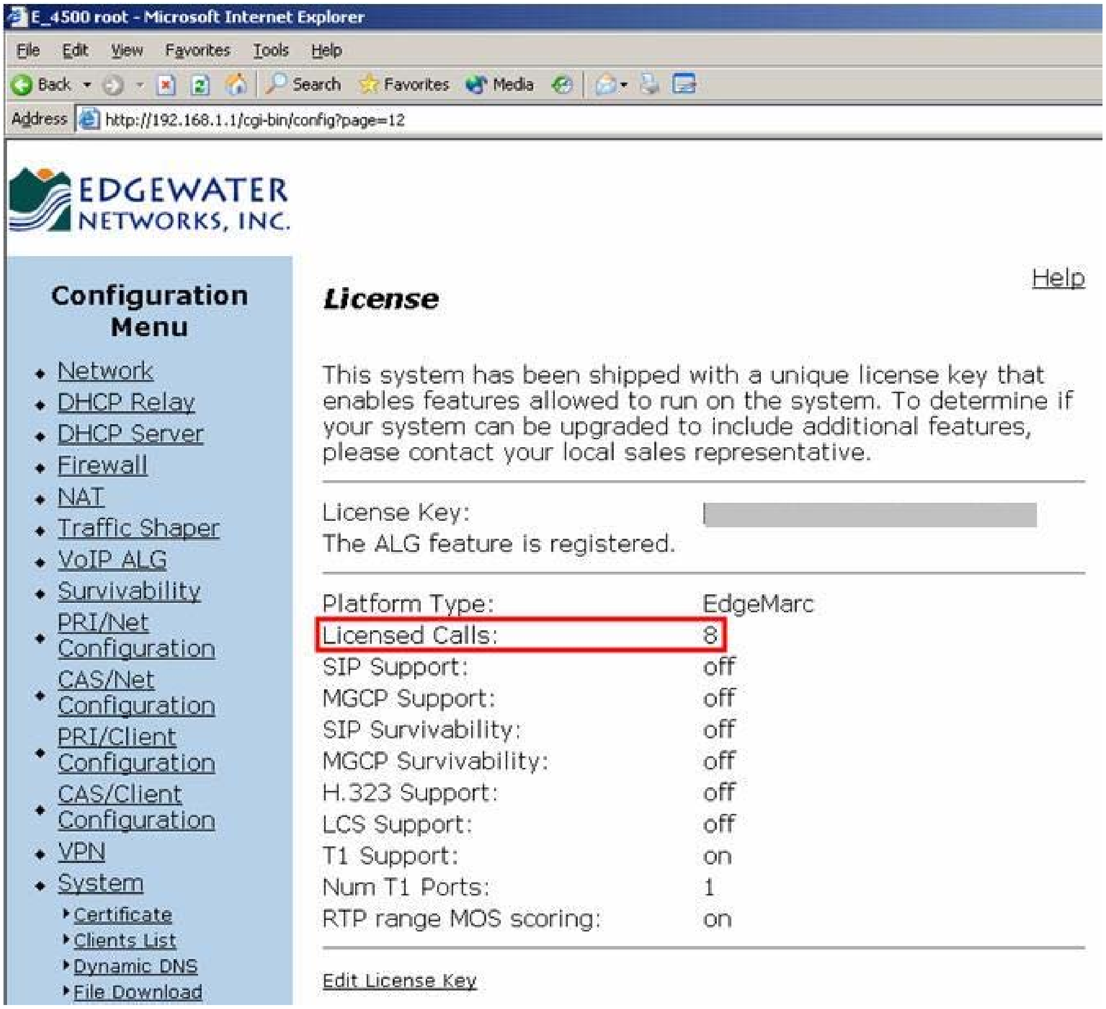
Step	Description
6.	Create a new **IP Line** by right clicking on **Line**, select **New** and then select **IP Line** (not shown). Enter the information displayed below and then click **OK**. **Line Number** will be auto-populated with the next available value. **Incoming Group ID** and **Outgoing Group ID** can be any numeric value and were set to "9" in the sample configuration.  Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4.1(9)] [Administrator(Administrator)] IP - Line 9 VoIP Line | Short Codes | VoIP Settings Line Number: 9 Telephone Number: Incoming Group ID: 9 Prefix: National Prefix: International Prefix: TEI: 0 Outgoing Group ID: 9 Number of Channels: 20 Outgoing Channels: 20 Voice Channels: 20 Data Channels: 20 File Edit View Tools Help 00E0070203B5 Line 9 IP Offices BOOTP (2) Operator (3) 00E0070203B5 System (1) 00E0070203B5 Line (6) 1 5 6 7 8 9 Control Unit (3) Extension (25)
7.	Navigate to the **VoIP Settings** tab by clicking **VoIP Settings**. Enter the information displayed below and then click **OK. Gateway IP Address** is the IP address of Avaya Communication Manager in the headquarters.  Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4.1(9)] [Administrator(Administrator)] IP - Line 9 VoIP Line | Short Codes | VoIP Settings Gateway IP Address: 192 . 168 . 77 . 1 Voice Payload Size (ms): 0 Compression Mode: Automatic Select H450 Support: H450 ☐ VoIP Silence Suppression ☑ Enable Faststart ☐ Local Tones ☐ Enable RSVP ☑ Out Of Band DTMF ☑ Allow Direct Media Path ☐ Voice Networking ☐ Fax Transport Support File Edit View Tools Help 00E0070203B5 Line 9 IP Offices 00E0070203B5 Line (6) 1 5 6 7 8 9 Control Unit (3) Extension (25) User (26) NoUser RemoteManager 100000 Extn100000 100005 Extn100005 215 Extn215 30201 Extn30201

Step	Description
8.	In order for the trunk to operate correctly a short code must be defined that uses this trunk. Right click on **Short Code** and select **New** (not shown). Enter the information displayed below, click **OK** and then click the **Save Configuration** icon, . **Code** was set to "8N". The value "8" indicates that users will need to dial "8" in order to access this short code. The value "N" indicates that dialed digits/numbers will be used. Use the drop-down list for **Feature** to select "Dial". **Telephone Number** was set to "N". Use the drop-down list for **Line Group Id** to select the **Line Number** created in **Step 6**.  Avaya IP Office Manager 6.1 (9) 00E0070203B5 [4.1(9)] [Administrator(Administrator)] 00E0070203B5 · Short Code · 8N; 8N;: Dial* Code: 8N; Feature: Dial Telephone Number: N Line Group Id: 9 Locale: Force Account Code: □

5. Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance Configuration

The initial configuration of the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance is performed via a web interface. By default, the EdgeMarc 4500 VoIP VPN Appliance will be assigned an IP address of 192.168.1.1, subnet mask of 255.255.255.0. Operators will need to configure a computer to reside in this IP network in order to access the web interface. The following URL was used to access the web interface of the EdgeMarc 4500 VoIP VPN Appliance, http://192.168.1.1. A login is required to access the web interface, for complete details on how to access the web interface of the EdgeMarc 4500 VoIP VPN Appliance refer to **References** [5,6].

Step	Description
1.	The initial login screen displays some basic system information such as software version, hostname, MAC address and other details. Click **license key**.  E_4500 root - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Media Address http://192.168.1.1/ EDGEWATER NETWORKS, INC. Configuration Menu Network DHCP Relay DHCP Server Firewall NAT Traffic Shaper VoIP ALG Survivability PRI/Net Configuration CAS/Net Configuration PRI/Client Configuration CAS/Client Configuration VPN System Certificate Clients List Dynamic DNS File Download File Server Network Information Network Restart Network Test Tools Proxy ARP RADIUS Settings Help System Software Version: Version 7.9.3 -- Mon Dec 31 15:46:01 PST 2007 Hostname: 4500T4 Model: EdgeMarc 4500T4 LAN Interface MAC Address: 00:03:6D:F6:0D:1A Registration Status: The ALG feature is registered. View license key System Date: 01/05/2000 19:05:21 UTC Change Administrative Password: The password of the read-write administrative user can be changed. Change Read-Only Password: The password of the read-only user can be changed.

Step	Description
2.	The **License** web page indicates the number of licensed calls the system is configured to support. A user with administrative privileges will need to ensure that their system has the appropriate license capacity to support the number of calls. 

License

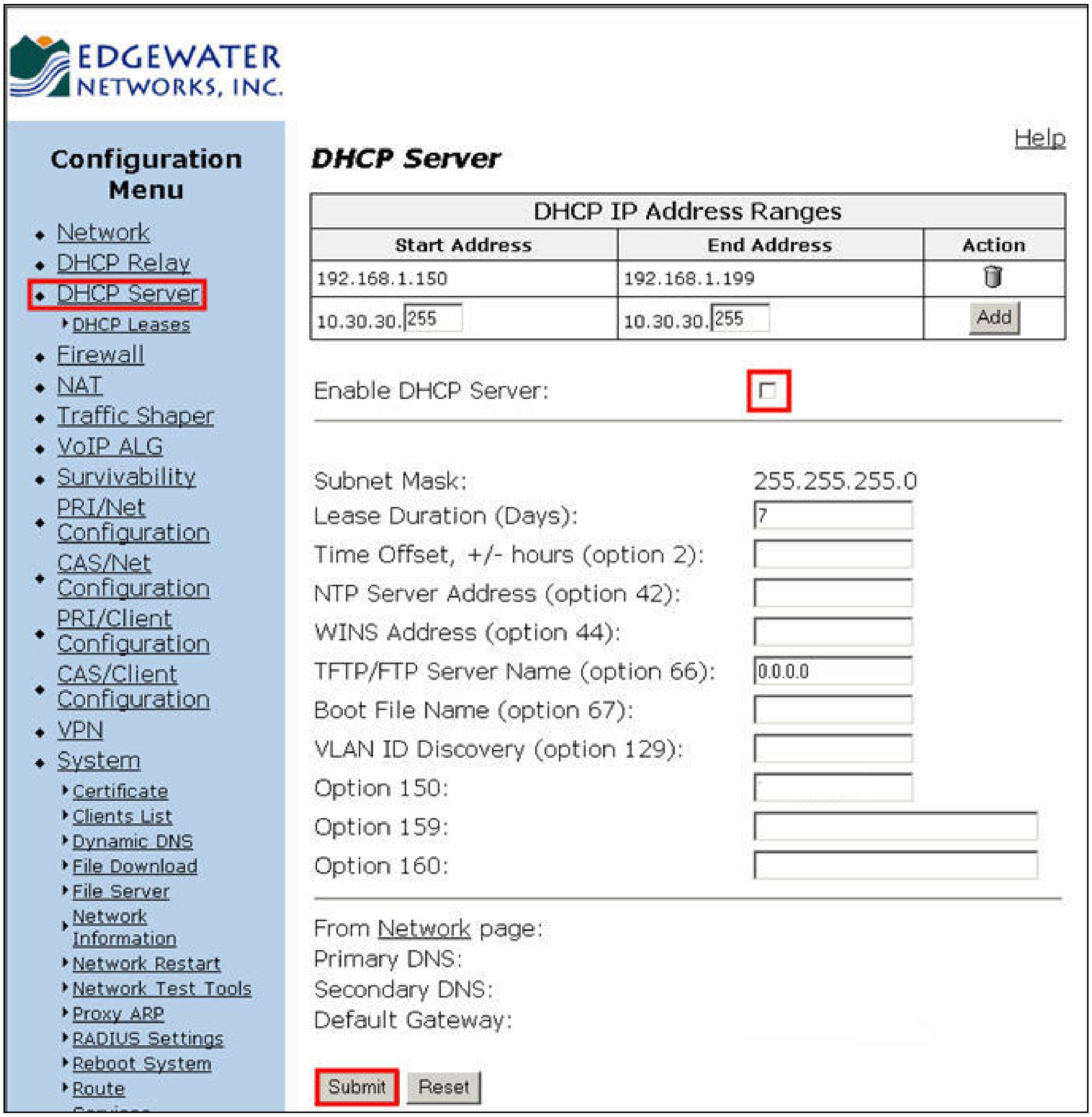
This system has been shipped with a unique license key that enables features allowed to run on the system. To determine if your system can be upgraded to include additional features, please contact your local sales representative.

License Key: [redacted]

The ALG feature is registered.

Platform Type:	EdgeMarc
Licensed Calls:	8
SIP Support:	off
MGCP Support:	off
SIP Survivability:	off
MGCP Survivability:	off
H.323 Support:	off
LCS Support:	off
T1 Support:	on
Num T1 Ports:	1
RTP range MOS scoring:	on

Edit License Key

Step	Description
3.	Navigate to the **DHCP Server** web page by clicking **DHCP Server** within the navigation panel on the left side of the web page. Ensure the **Enable DHCP Server** checkbox is not checked. 

DHCP Server

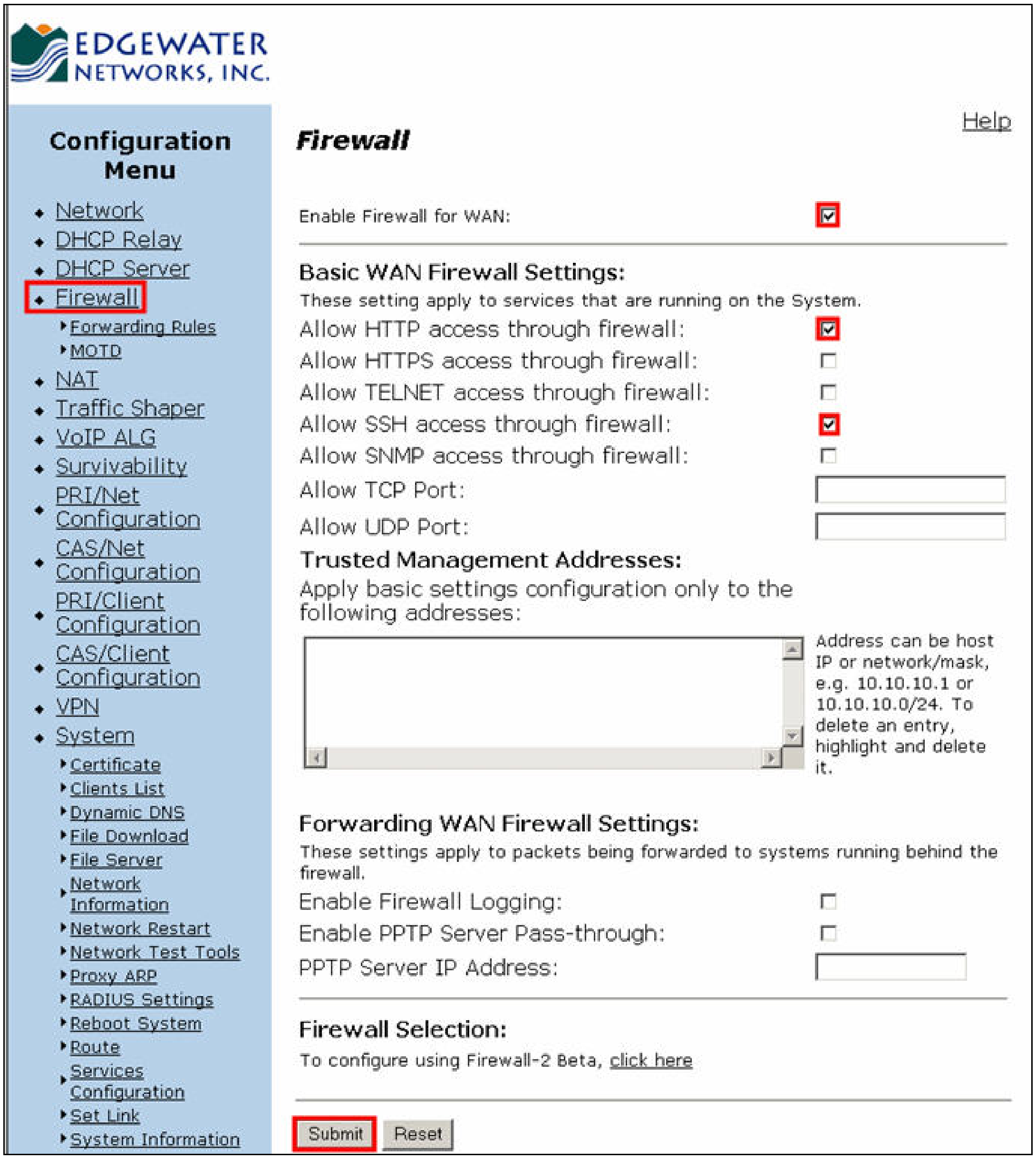
DHCP IP Address Ranges

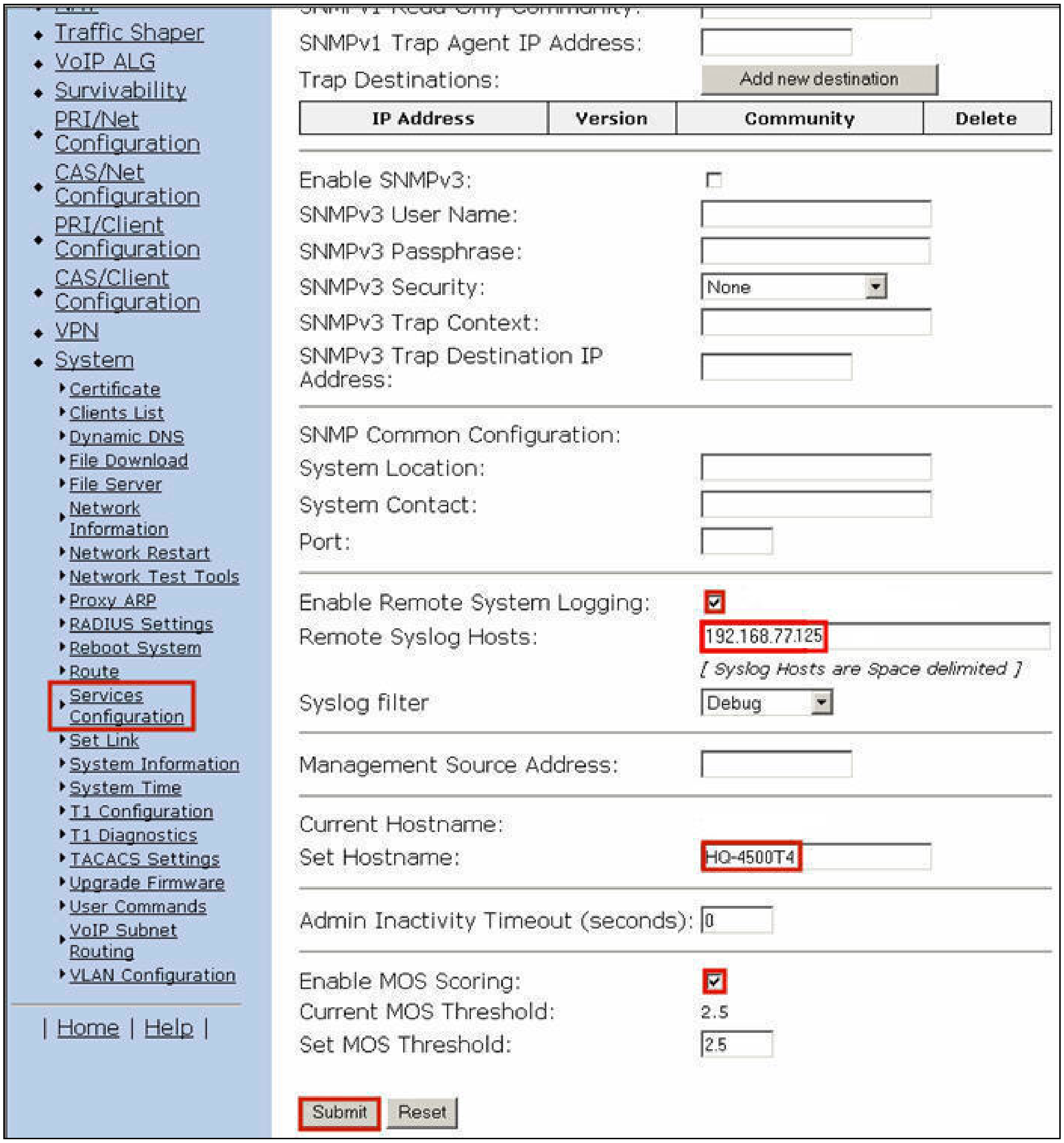
Start Address	End Address	Action
192.168.1.150	192.168.1.199	🗑
10.30.30.255	10.30.30.255	Add

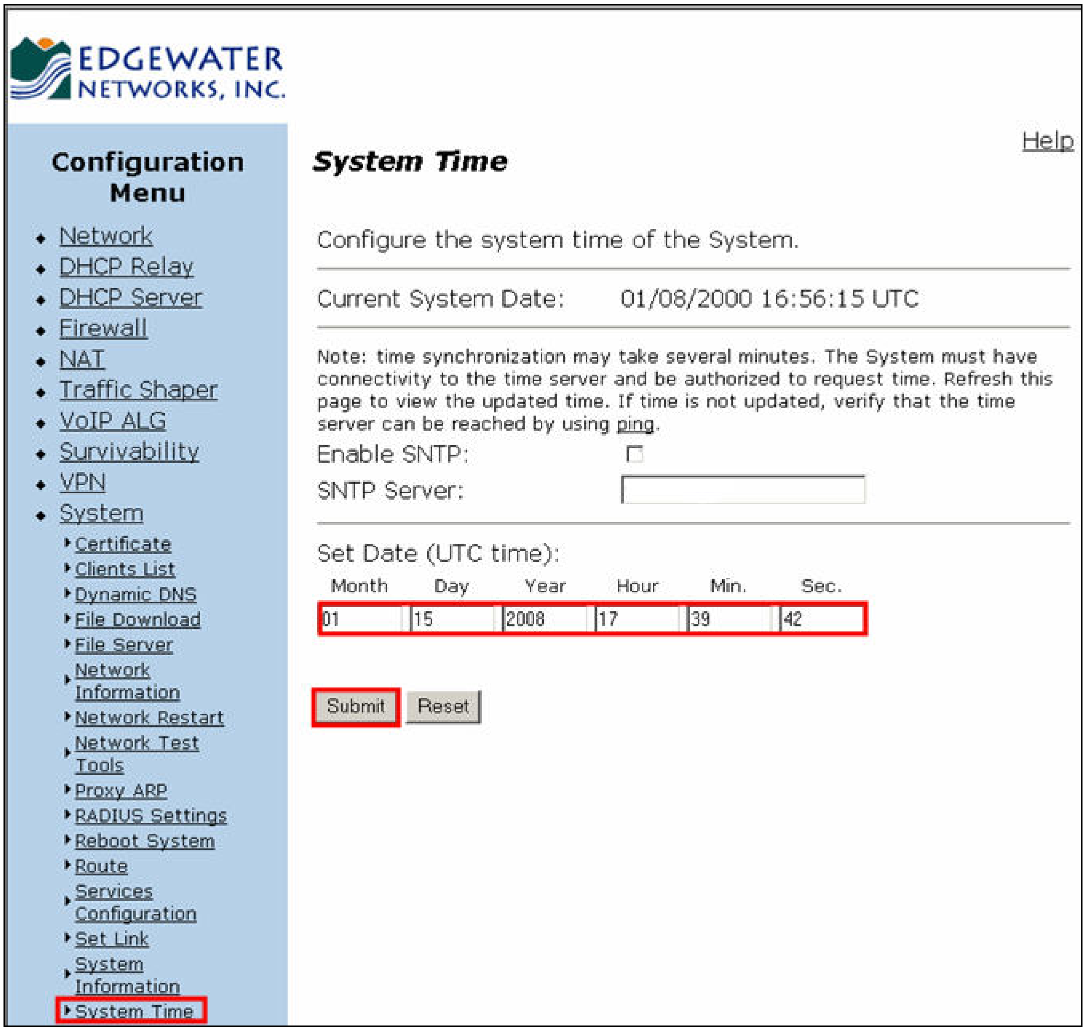
Enable DHCP Server: □

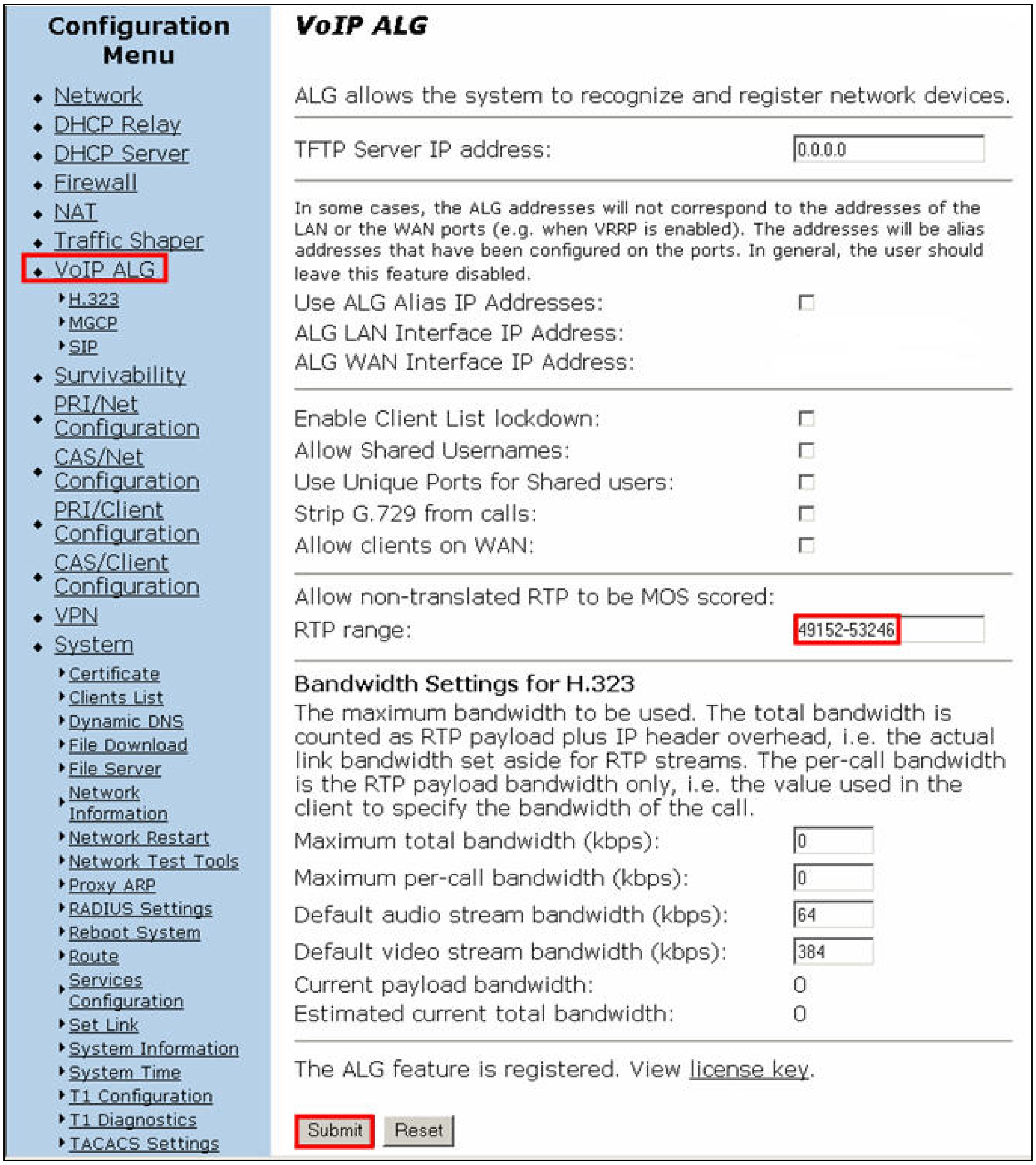
Subnet Mask:	255.255.255.0
Lease Duration (Days):	7
Time Offset, +/- hours (option 2):	
NTP Server Address (option 42):	
WINS Address (option 44):	
TFTP/FTP Server Name (option 66):	0.0.0.0
Boot File Name (option 67):	
VLAN ID Discovery (option 129):	
Option 150:	
Option 159:	
Option 160:	

From Network page:
Primary DNS:
Secondary DNS:
Default Gateway:

Step	Description
4.	Navigate to the **Firewall** web page by clicking **Firewall** within the navigation panel on the left side of the web page. Check the **Enable Firewall for WAN** check box. The remaining check boxes enable the access types from the WAN interface on the EdgeMarc 4500 VoIP VPN Appliance. In the sample configuration, HTTP and SSH were allowed from the WAN interface. For complete information on the security recommendations for the EdgeMarc 4500 VoIP VPN Appliance, refer to **Reference** [**6**]. Click **Submit**.  EDGEWATER NETWORKS, INC. Configuration Menu Network DHCP Relay DHCP Server Firewall Forwarding Rules MOTD NAT Traffic Shaper VoIP ALG Survivability PRI/Net Configuration CAS/Net Configuration PRI/Client Configuration CAS/Client Configuration VPN System Certificate Clients List Dynamic DNS File Download File Server Network Information Network Restart Network Test Tools Proxy ARP RADIUS Settings Reboot System Route Services Configuration Set Link System Information Help **Firewall** Enable Firewall for WAN: ☑ **Basic WAN Firewall Settings:** These setting apply to services that are running on the System. Allow HTTP access through firewall: ☑ Allow HTTPS access through firewall: ☐ Allow TELNET access through firewall: ☐ Allow SSH access through firewall: ☑ Allow SNMP access through firewall: ☐ Allow TCP Port: Allow UDP Port: **Trusted Management Addresses:** Apply basic settings configuration only to the following addresses: Address can be host IP or network/mask, e.g. 10.10.10.1 or 10.10.10.0/24. To delete an entry, highlight and delete it. **Forwarding WAN Firewall Settings:** These settings apply to packets being forwarded to systems running behind the firewall. Enable Firewall Logging: ☐ Enable PPTP Server Pass-through: ☐ PPTP Server IP Address: **Firewall Selection:** To configure using Firewall-2 Beta, click here Submit Reset

Step	Description
5.	Navigate to the **Services Configuration** web page by clicking **System** and then clicking **Services Configuration** within the navigation panel on the left side of the web page. The EdgeMarc 4500 VoIP VPN Appliance can provide Syslog data, which includes a MOS score for calls completed across the VPN. Check the **Enable Remote System Logging** and **Enable MOS Scoring** check boxes. **Remote Syslog Hosts** was set to “192.168.77.125”, which is the IP address of a Syslog server, see **Figure 1**. **Set Hostname** can be any alpha-numeric string that identifies the system. **Set Hostname** was set to “HQ-4500T4” in the sample configuration. Click **Submit**.  Traffic Shaper VoIP ALG Survivability PRI/Net Configuration CAS/Net Configuration PRI/Client Configuration CAS/Client Configuration VPN System Certificate Clients List Dynamic DNS File Download File Server Network Information Network Restart Network Test Tools Proxy ARP RADIUS Settings Reboot System Route Services Configuration Set Link System Information System Time T1 Configuration T1 Diagnostics TACACS Settings Upgrade Firmware User Commands VoIP Subnet Routing VLAN Configuration | Home | Help | SNMPv1 Trap Agent IP Address: Trap Destinations: Add new destination IP Address | Version | Community | Delete Enable SNMPv3: ☐ SNMPv3 User Name: SNMPv3 Passphrase: SNMPv3 Security: None SNMPv3 Trap Context: SNMPv3 Trap Destination IP Address: SNMP Common Configuration: System Location: System Contact: Port: Enable Remote System Logging: ☑ Remote Syslog Hosts: 192.168.77.125 *[Syslog Hosts are Space delimited]* Syslog filter: Debug Management Source Address: Current Hostname: Set Hostname: HQ-4500T4 Admin Inactivity Timeout (seconds): 0 Enable MOS Scoring: ☑ Current MOS Threshold: 2.5 Set MOS Threshold: 2.5 Submit Reset

Step	Description
6.	Navigate to the **System Time** web page by clicking **System Time** within the navigation panel on the left side of the web page. Configure the correct date and time. Click **Submit**.  EDGEWATER NETWORKS, INC. Configuration Menu Network DHCP Relay DHCP Server Firewall NAT Traffic Shaper VoIP ALG Survivability VPN System Certificate Clients List Dynamic DNS File Download File Server Network Information Network Restart Network Test Tools Proxy ARP RADIUS Settings Reboot System Route Services Configuration Set Link System Information System Time Help **System Time** Configure the system time of the System. Current System Date: 01/08/2000 16:56:15 UTC Note: time synchronization may take several minutes. The System must have connectivity to the time server and be authorized to request time. Refresh this page to view the updated time. If time is not updated, verify that the time server can be reached by using ping. Enable SNTP: □ SNTP Server: Set Date (UTC time): Month: 01 Day: 15 Year: 2008 Hour: 17 Min.: 39 Sec.: 42

Step	Description
7.	Navigate to the **VoIP ALG** web page by clicking **VoIP ALG** within the navigation panel on the left side of the web page. **RTP range** is set to the same value for **RTP Port Number Range** fields configured in **Section 4**, **Step 2**. Click **Submit**. 

VoIP ALG

ALG allows the system to recognize and register network devices.

TFTP Server IP address: 0.0.0.0

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports (e.g. when VRRP is enabled). The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

Use ALG Alias IP Addresses: □
ALG LAN Interface IP Address:
ALG WAN Interface IP Address:

Enable Client List lockdown: □
Allow Shared Usernames: □
Use Unique Ports for Shared users: □
Strip G.729 from calls: □
Allow clients on WAN: □

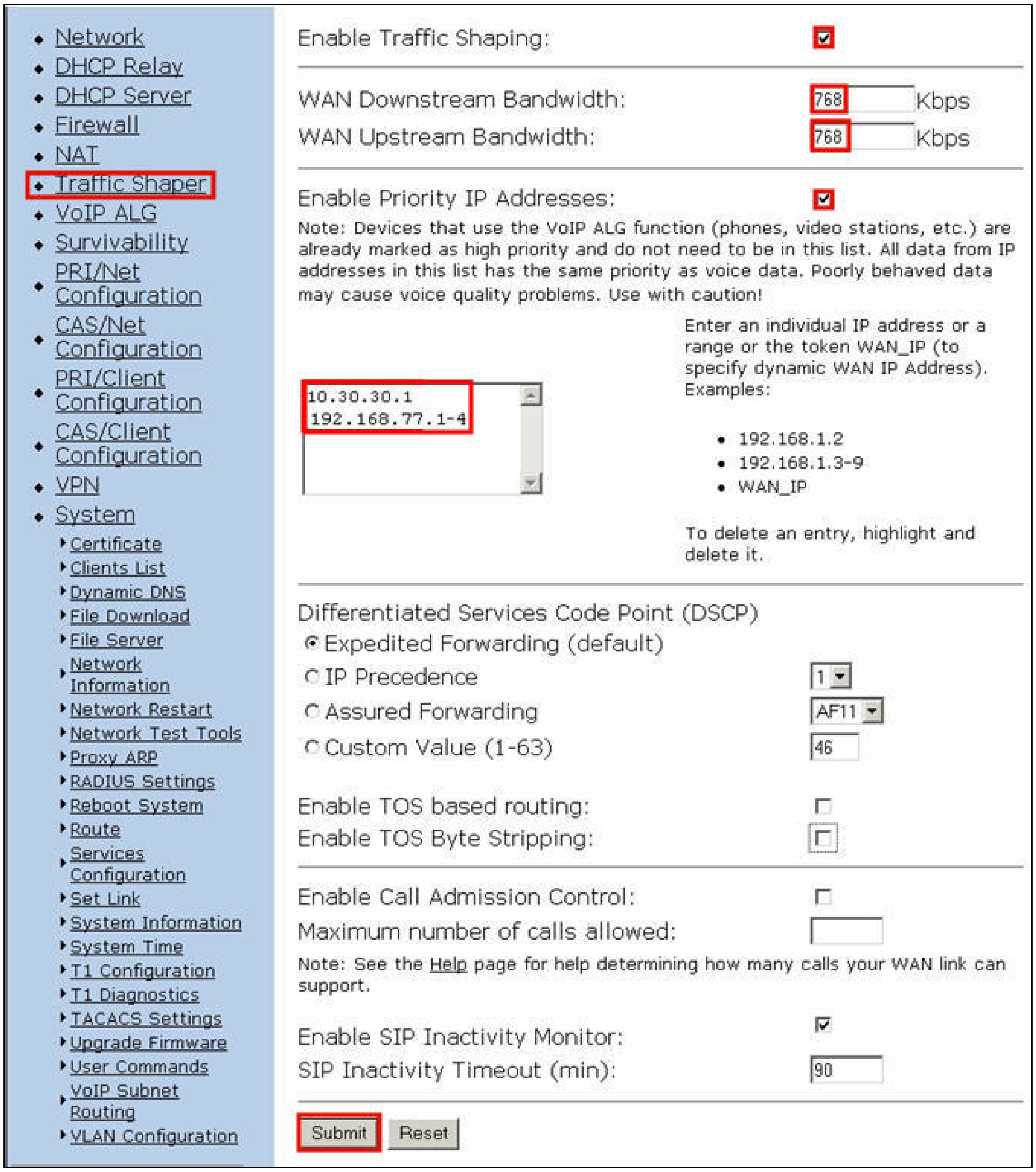
Allow non-translated RTP to be MOS scored:
RTP range: 49152-53246

Bandwidth Settings for H.323

The maximum bandwidth to be used. The total bandwidth is counted as RTP payload plus IP header overhead, i.e. the actual link bandwidth set aside for RTP streams. The per-call bandwidth is the RTP payload bandwidth only, i.e. the value used in the client to specify the bandwidth of the call.

Maximum total bandwidth (kbps): 0
Maximum per-call bandwidth (kbps): 0
Default audio stream bandwidth (kbps): 64
Default video stream bandwidth (kbps): 384
Current payload bandwidth: 0
Estimated current total bandwidth: 0

The ALG feature is registered. View license key.

Step	Description
8.	Navigate to the **Traffic Shaper** web page by clicking **Traffic Shaper** within the navigation panel on the left side of the web page. Check the **Enable Traffic Shaping** and **Enable Priority IP Addresses** check boxes. The values for **WAN Downstream Bandwidth** and **WAN Upstream Bandwidth** are applicable to the sample configuration and were set to "768". These parameters define the link speed on the WAN interface and will need to be modified for the specific installation of the EdgeMarc 4500 VoIP VPN Appliance. Enter the IP address of the Avaya IP Office and Avaya Communication Manager devices into the box found under **Enable Priority IP Addresses**. Click **Submit**. 

Enable Traffic Shaping: ☑

WAN Downstream Bandwidth: 768 Kbps

WAN Upstream Bandwidth: 768 Kbps

Enable Priority IP Addresses: ☑

Note: Devices that use the VoIP ALG function (phones, video stations, etc.) are already marked as high priority and do not need to be in this list. All data from IP addresses in this list has the same priority as voice data. Poorly behaved data may cause voice quality problems. Use with caution!

```
10.30.30.1
192.168.77.1-4
```

Enter an individual IP address or a range or the token WAN_IP (to specify dynamic WAN IP Address). Examples:

- 192.168.1.2
- 192.168.1.3-9
- WAN_IP

To delete an entry, highlight and delete it.

Differentiated Services Code Point (DSCP)

● Expedited Forwarding (default)

○ IP Precedence 1

○ Assured Forwarding AF11

○ Custom Value (1-63) 46

Enable TOS based routing: □

Enable TOS Byte Stripping: □

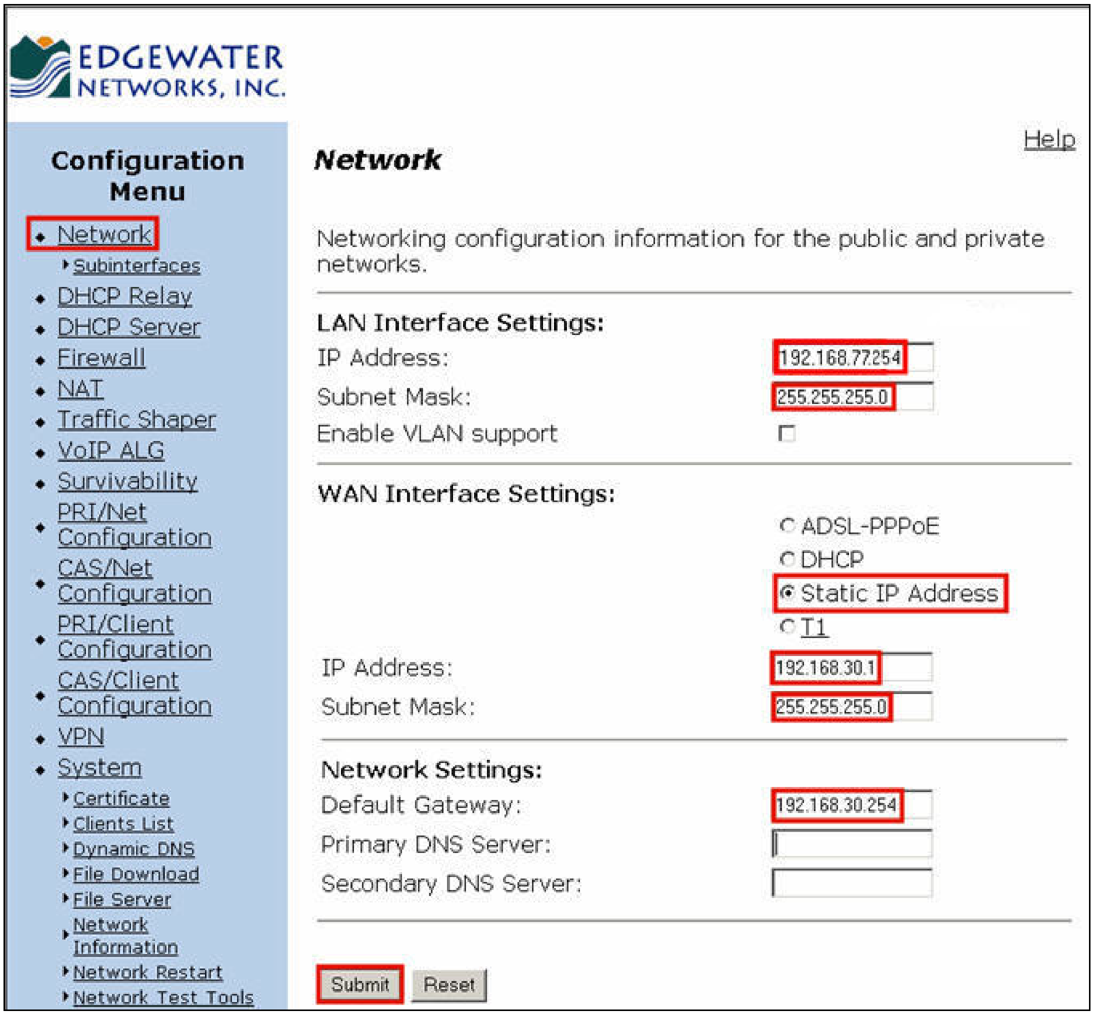
Enable Call Admission Control: □

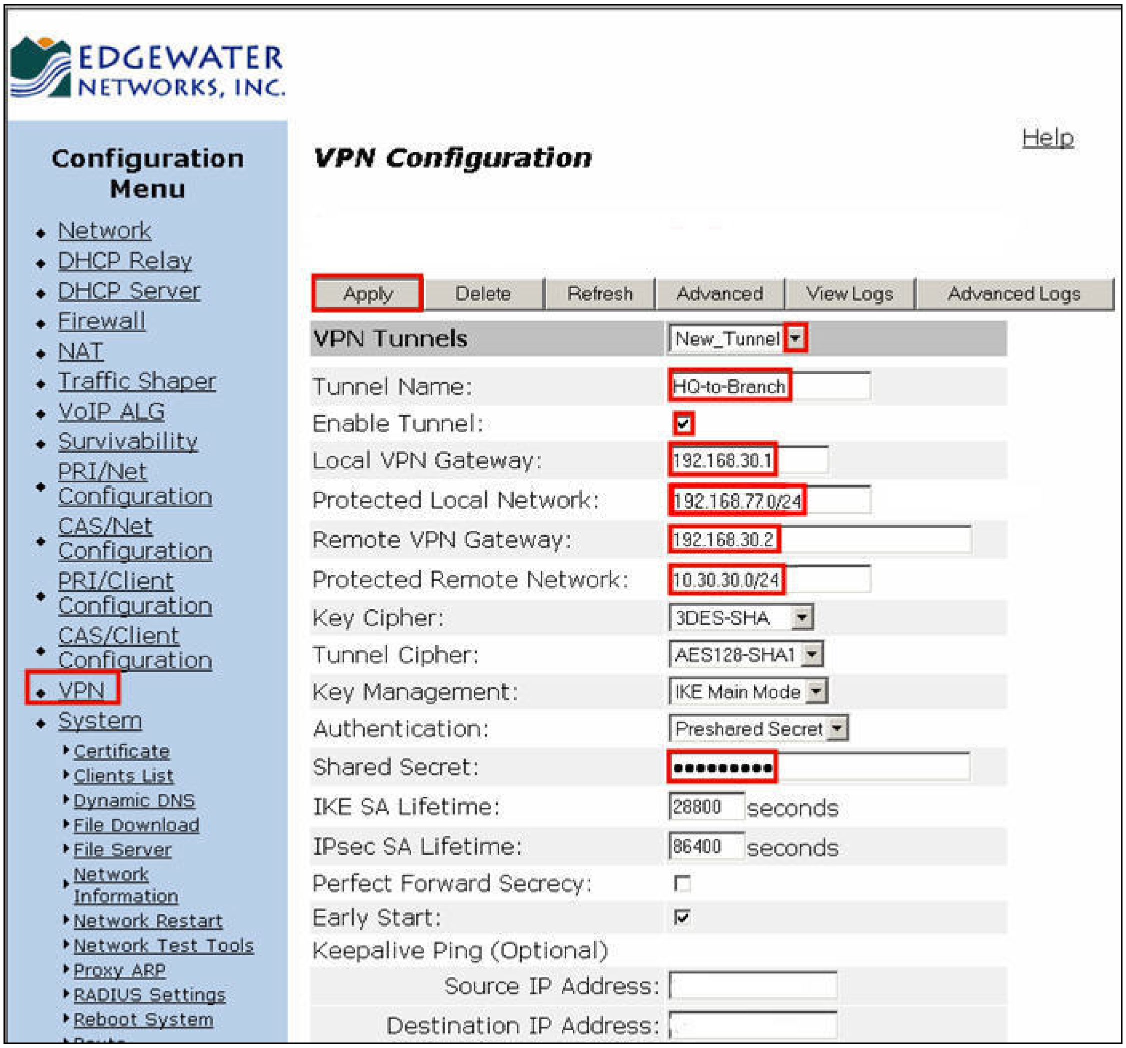
Maximum number of calls allowed:

Note: See the Help page for help determining how many calls your WAN link can support.

Enable SIP Inactivity Monitor: ☑

SIP Inactivity Timeout (min): 90

Step	Description
9.	Navigate to the **Network** web page by clicking **Network** within the navigation panel on the left side of the web page. Enter the information displayed below and then click **Submit**. Ensure that **Static IP Address** is selected for the **WAN Interface Settings**. Configure the **LAN Interface Settings** and **WAN Interface Settings** fields per **Figure 1**. **Network Settings: Default Gateway** is the IP address of the gateway on the WAN interface. Note the values used here are only applicable to the sample configuration.  EDGEWATER NETWORKS, INC. Configuration Menu Network Subinterfaces DHCP Relay DHCP Server Firewall NAT Traffic Shaper VoIP ALG Survivability PRI/Net Configuration CAS/Net Configuration PRI/Client Configuration CAS/Client Configuration VPN System Certificate Clients List Dynamic DNS File Download File Server Network Information Network Restart Network Test Tools Help **Network** Networking configuration information for the public and private networks. LAN Interface Settings: IP Address: 192.168.77.254 Subnet Mask: 255.255.255.0 Enable VLAN support ☐ WAN Interface Settings: ○ ADSL-PPPoE ○ DHCP ● Static IP Address ○ T1 IP Address: 192.168.30.1 Subnet Mask: 255.255.255.0 Network Settings: Default Gateway: 192.168.30.254 Primary DNS Server: Secondary DNS Server:

Step	Description
10.	Navigate to the **VPN Configuration** web page by clicking **VPN** within the navigation panel on the left side of the web page. Enter the information displayed below and then click **Apply**. Use the drop-down list for **VPN Tunnels** to select “New_Tunnel”. **Tunnel Name** can be any descriptive text that identifies the tunnel and “HQ-to-Branch” was used for the tunnel between the headquarters and branch sites. Check the **Enable Tunnel** check box. **Local VPN Gateway** is the IP address assigned to the **WAN Interface Settings: IP Address** configured in **Step 9**. **Protected Local Network** is the network of the **LAN Interface Settings** configured in **Step 9**. **Remote VPN Gateway** is the **WAN Interface Settings: IP Address** of the branch site EdgeMarc 4500 VoIP VPN Appliance. **Protected Remote Network** is the network of the **LAN Interface Settings** configured on the branch site EdgeMarc 4500 VoIP VPN Appliance. **Shared Secret** can be any alpha-numeric string and must match on both tunnels.  VPN Configuration VPN Tunnels: New_Tunnel Tunnel Name: HQ-to-Branch Enable Tunnel: ☑ Local VPN Gateway: 192.168.30.1 Protected Local Network: 192.168.77.0/24 Remote VPN Gateway: 192.168.30.2 Protected Remote Network: 10.30.30.0/24 Key Cipher: 3DES-SHA Tunnel Cipher: AES128-SHA1 Key Management: IKE Main Mode Authentication: Preshared Secret Shared Secret: ●●●●●●●●●● IKE SA Lifetime: 28800 seconds IPsec SA Lifetime: 86400 seconds Perfect Forward Secrecy: ☐ Early Start: ☑ Keepalive Ping (Optional) Source IP Address: Destination IP Address: EDGEWATER NETWORKS, INC. Configuration Menu Network DHCP Relay DHCP Server Firewall NAT Traffic Shaper VoIP ALG Survivability PRI/Net Configuration CAS/Net Configuration PRI/Client Configuration CAS/Client Configuration VPN System Certificate Clients List Dynamic DNS File Download File Server Network Information Network Restart Network Test Tools Proxy ARP RADIUS Settings Reboot System Help Apply Delete Refresh Advanced View Logs Advanced Logs
11.	Repeat **Step 10** and create another tunnel to the other site per **Figure 1**, modifying appropriate parameters.

Step	Description
12.	Repeat **Steps 1 – 11** for each EdgeMarc 4500 VoIP VPN Appliance in the other locations again modifying appropriate parameters per **Figure 1**.

6. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying the capability of the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance support an Avaya Communication Manager and Avaya IP Office network comprised of three sites.

6.1. General Test Approach

The general test approach was to validate proper communication across the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance when using an H.323 trunk between Avaya Communication Manager and Avaya IP Office. Additional testing verified the proper communication with a remote site, where only IP telephones were present.

6.2. Test Results

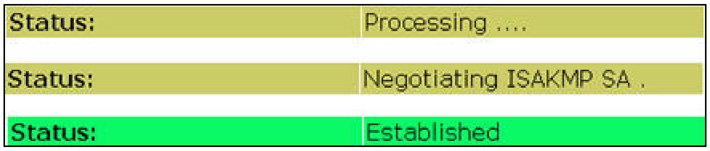
The Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance passed all test cases as listed below:

- Supporting an H.323 trunk between Avaya Communication Manager and Avaya IP Office.
- Supporting a remote site where only IP telephones were present.
- Providing priority for Avaya Communication Manager, Avaya IP Office and IP telephones when competing data traffic was passing through the VPN.
- Providing Syslog data that contained a MOS score for telephone calls completed through the VPN.
- Allowing proper operation of telephony features such as conference calls, hold/return from hold, DTMF tone interpretation, MWI, voicemail, caller ID, multiple call appearances and supporting calls with direct media between endpoints or with media centralized through the Avaya Communication Manager or Avaya IP Office system.

7. Verification Steps

The following steps can be used to ascertain the functional status of sample network.

- Verify that the VPN tunnels between each site are established. Use the **VPN Configuration** web page from **Section 5**, **Step 10** to obtain the status of the VPN tunnels. The graphic below shows the tunnel establishment process, each tunnel should show "Established".



Status:	Processing ....
Status:	Negotiating ISAKMP SA .
Status:	Established

- Verify that each tunnel has the correct Local/Remote interfaces and networks. See **Section 5**, **Step 10**.
- Place calls from site to site and verify two-way audio.
- Verify proper DTMF tone interpretation by successfully logging into voicemail.
- Access the Syslog server log and verify the receipt of Syslog data from the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance and verify that the data contains a MOS value.

8. Support

Technical support for Edgewater Networks can be obtained through the following:

- **Phone:** 1-408-351-7255
- **Email:** supportaccess@edgewaternetworks.com
- **Web:** http://www.edgewaternetworks.com

9. Conclusion

These Application Notes detail the configuration process that builds a VPN between three sites using Edgewater Networks EdgeMarc 4500 VoIP VPN appliances to support an Avaya Communication Manager and Avaya IP Office network. These Application Notes also detail the configuration process that builds an H.323 trunk between Avaya Communication Manager and Avaya IP Office.

10. Additional References

The documents references below were used for additional configuration are available at htt://support.avaya.com:

[1] *Administrator Guide for Avaya Communication Manager*, May 2006 Issue 2.1, Document Number 03-300509

[2] *Installing and Administering SIP Enablement Services*, August 2006 Issue 2.0, Document Number 03-600768

[3] *Avaya IP Office 4.0 Applications Installation and Administration*, Feb 2007 Issue 2, Document Number 15-601133

[4] *Avaya IP Office VoiceMail Pro Installation and Maintenance Guide*, Feb 2007 Issue 16, Document Number 15-601063

The Edgewater Networks, Inc references are available at http://www.edgewaternetworks.com.

[5] *EdgeMarc 4500 Series Converged Networking Router Installation Guide*, Issue 1, Document Number 100-4500-001

[6] *VoIP Operating System (VOS) for EdgeMarc User Manual*, Version 1.1, Document Number 300-VOS-001

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.