



## **Application Notes for Configuring the Expand Networks Accelerator 4820 with Avaya IP Telephony through Avaya SG203 and SG208 Security Gateways - Issue 1.0**

### **Abstract**

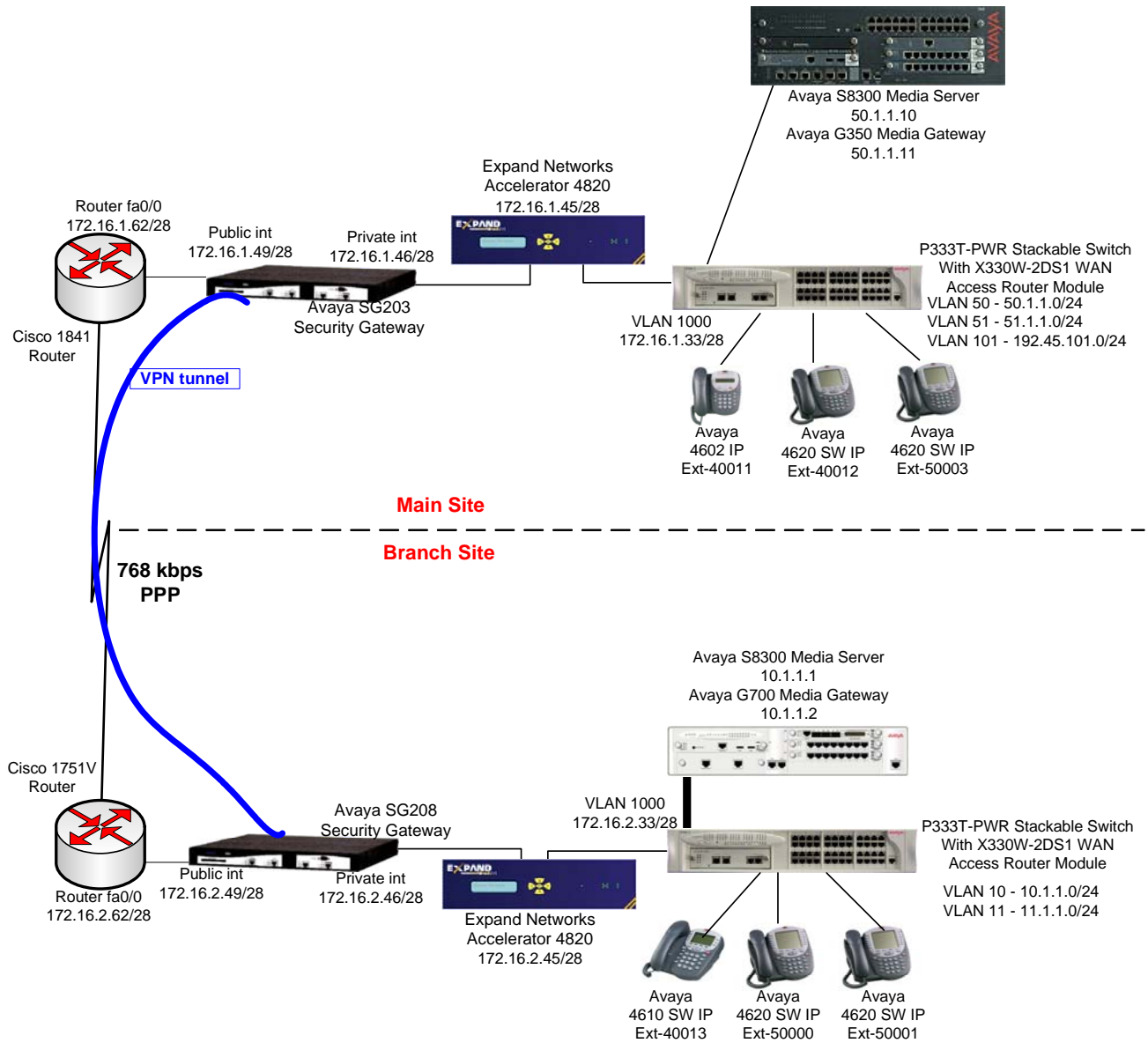
These Application Notes describe the steps for configuring the Expand Networks Accelerator 4820 to preserve WAN link bandwidth for H.323 Voice over IP (VoIP) traffic generated by Avaya IP telephones while offering data compression and acceleration. During compliance testing, H.323 phone calls traversing the WAN link were successfully established and maintained while non-VoIP competing traffic was compressed and queued according to their priority. Information in these Application Notes has been obtained through DeveloperConnection compliance testing and additional technical discussions. Testing was conducted via the DeveloperConnection Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe a compliance-tested solution comprised of Avaya Communication Managers, Avaya IP Telephones, Avaya Security Gateways and Expand Networks Accelerators. The Accelerator is a WAN optimization appliance that employs techniques such as compression, QoS, Bandwidth management, and TCP acceleration to increase capacity, applications performance and throughput, while maintaining proper prioritization for Voice over IP (VoIP) traffic going over Wide Area Network (WAN) links. Typically placed between the WAN router and LAN, the Expand Network Accelerator establishes a virtual connection between its peers and manages network traffic flow based on user-defined rules and priorities. The Expand Networks Accelerator can also set aside explicit bandwidth for VoIP traffic within the WAN link capacity to maintain the proper Quality of Service.

## 1.1. Configuration

**Figure 1** illustrates the configuration used in these Application Notes. The extension numbers beginning with the number 4 are registered with Avaya Communication Manager in the Main Site and extension numbers beginning with the number 5 are registered with Avaya Communication Manager at the Branch Site. A 768K PPP link simulating a WAN link connects the Main and Branch Site together while the Avaya Security Gateways provide the VPN tunnel over this link. An H.323 trunk routes telephone calls between the two Avaya Media Gateways.



**Figure 1: Sample Network Configuration**

## 2. Equipment and Software Validated

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

| Equipment   | Software/Firmware                                   |
|---|---|
| Avaya S8300 Media Server with G350 Avaya Media Gateway                      | Avaya Communication Manager 3.0 (R0.13x.00.0.346.0) |
| Avaya S8300 Media Server with G700 Avaya Media Gateway                      | Avaya Communication Manager 3.0 (R0.13x.00.0.346.0) |
| Avaya P333T-PWR Stackable Switch with a X330W-2DS1 WAN Access Router Module | 3.12.1  |
| Avaya SG203 Security Gateway  | 4.6.22  |
| Avaya SG208 Security Gateway  | 4.6.22  |
| Avaya 46xxSW IP Telephones (H.323)  | 1.8.2 (4602SW)<br>2.2.3 (4610SW/4620SW)             |
| Expand Networks Accelerator 4820  | 5.0(7) Build 1.45                                   |
| Cisco 1751V Router  | 12.3(13a)   |
| Cisco 1841 Router   | 12.3(8)T6   |

## 3. Avaya Communication Manager

This section highlights the important areas in Avaya Communication Manager that need to be configured. For complete documentation, see references [1] and [2]. Use the System Access Terminal (SAT) interface to perform these steps. Log in with the appropriate credentials.

### 3.1. IP Network region

Use the **change ip-network-region** command for the network region the telephone is configured for to display IP Network Region information. Note the **UDP Port Min** and **UDP Port Max** value as well as the settings for **Call Control PHB Value** and **Audio PHB Value** (DiffServ/TOS parameters). These values will be needed later when configuring the Expand Networks Accelerators.

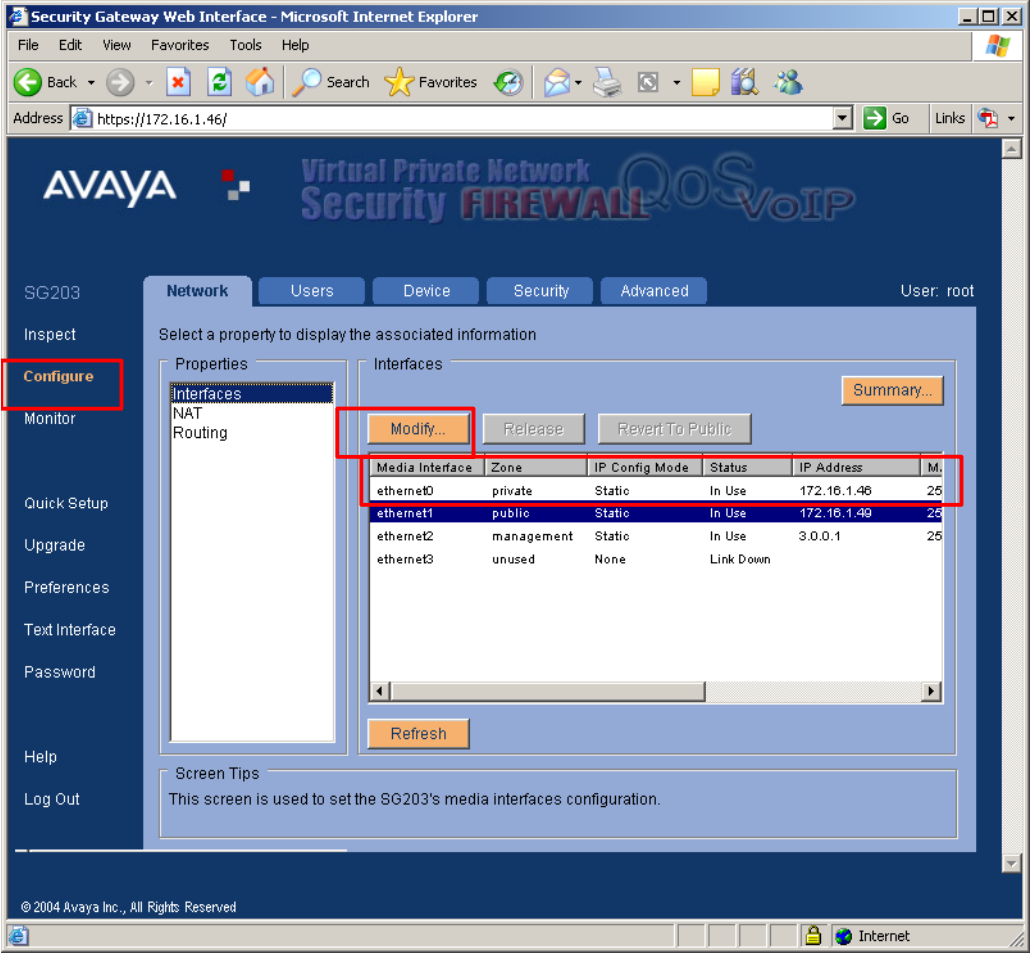
```
change ip-network-region 1                                     Page 1 of 19
                                                              IP NETWORK REGION

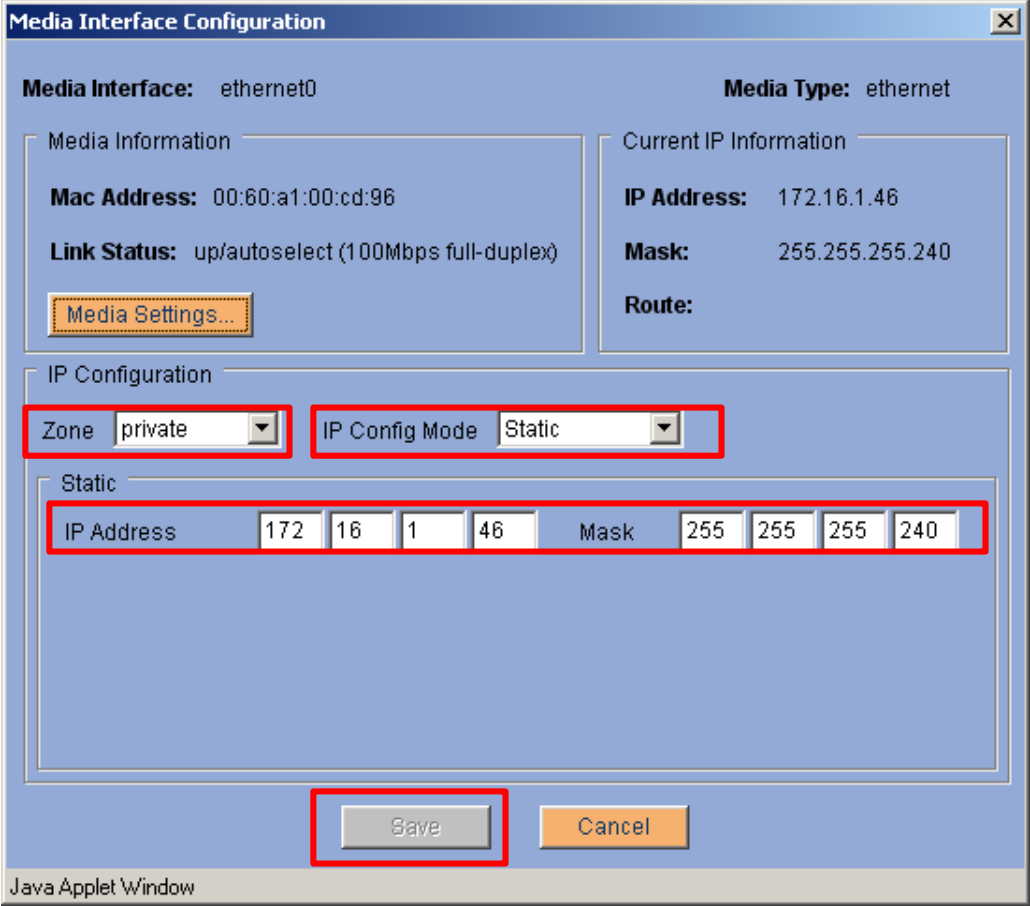
Region: 1
Location: 1          Authoritative Domain: devcon.com
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
                          Codec Set: 1          Inter-region IP-IP Direct Audio: yes
                          UDP Port Min: 2048    IP Audio Hairpinning? y
                          UDP Port Max: 3027
DIFFSERV/TOS PARAMETERS          RTCP Reporting Enabled? y
Call Control PHB Value: 34      RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46            Use Default Server Parameters? y
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

### 3.2. Avaya SG203 and SG208 Security Gateway

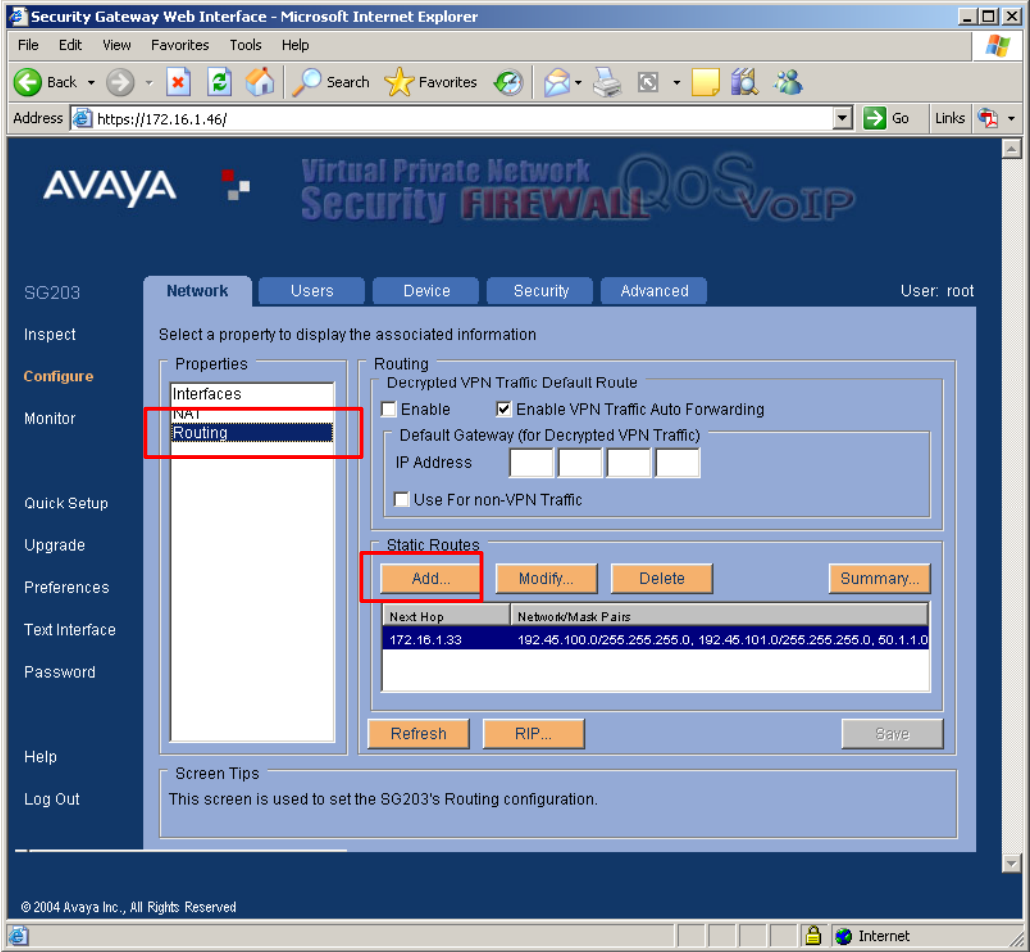
The Avaya SG203 and SG208 Security Gateways were used to establish a VPN tunnel between the Main and Branch sites. The following steps outline the configuration for the interfaces of the Avaya Security Gateways and the VPN tunnel. Refer to [3] for additional information on configuring Avaya SG203 and SG208 Security Gateways.

The steps in this section depict screen displays for the Avaya Security Gateway at the Main Site. These steps need to be repeated for the Avaya Security Gateway at the Branch Site.

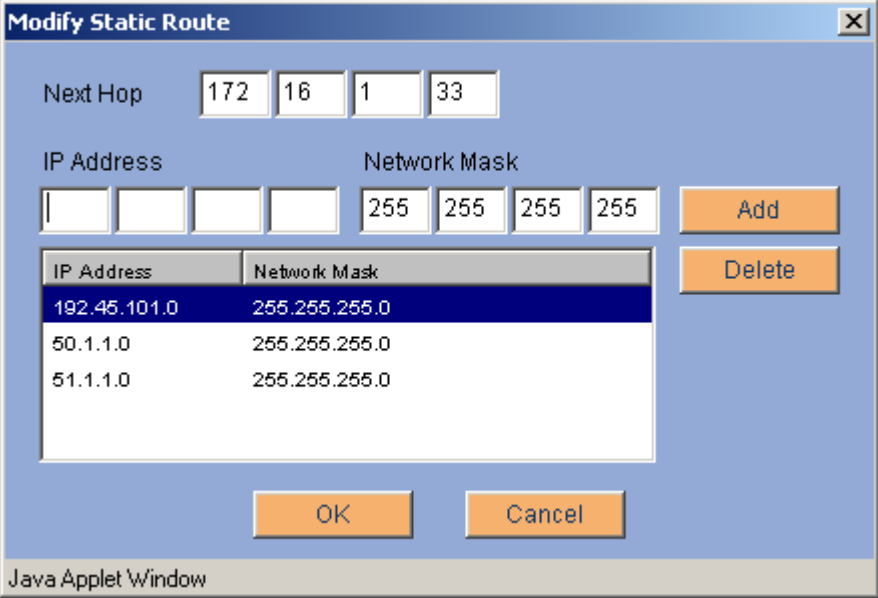
| Step            | Description   |                 |           |                |        |            |    |           |         |        |        |             |    |           |        |        |        |             |    |           |            |        |        |         |    |           |        |      |           |  |  |
|-----------------|---|-----------------|-----------|----------------|--------|------------|----|-----------|---------|--------|--------|-------------|----|-----------|--------|--------|--------|-------------|----|-----------|------------|--------|--------|---------|----|-----------|--------|------|-----------|--|--|
| 1.              | <p>Enter the URL <a href="https://IP address of the Avaya Security Gateway">https://IP address of the Avaya Security Gateway</a> to access the Avaya Security Gateway. The following screen will be displayed after successful log in. Click on <b>Configure</b> on the left and highlight <b>ethernet0</b>, and click on <b>Modify</b> to bring up the Media Interface Configuration screen.</p>  <table border="1"><thead><tr><th>Media Interface</th><th>Zone</th><th>IP Config Mode</th><th>Status</th><th>IP Address</th><th>M.</th></tr></thead><tbody><tr><td>ethernet0</td><td>private</td><td>Static</td><td>In Use</td><td>172.16.1.46</td><td>25</td></tr><tr><td>ethernet1</td><td>public</td><td>Static</td><td>In Use</td><td>172.16.1.49</td><td>25</td></tr><tr><td>ethernet2</td><td>management</td><td>Static</td><td>In Use</td><td>3.0.0.1</td><td>25</td></tr><tr><td>ethernet3</td><td>unused</td><td>None</td><td>Link Down</td><td></td><td></td></tr></tbody></table> | Media Interface | Zone      | IP Config Mode | Status | IP Address | M. | ethernet0 | private | Static | In Use | 172.16.1.46 | 25 | ethernet1 | public | Static | In Use | 172.16.1.49 | 25 | ethernet2 | management | Static | In Use | 3.0.0.1 | 25 | ethernet3 | unused | None | Link Down |  |  |
| Media Interface | Zone  | IP Config Mode  | Status    | IP Address     | M.     |            |    |           |         |        |        |             |    |           |        |        |        |             |    |           |            |        |        |         |    |           |        |      |           |  |  |
| ethernet0       | private   | Static          | In Use    | 172.16.1.46    | 25     |            |    |           |         |        |        |             |    |           |        |        |        |             |    |           |            |        |        |         |    |           |        |      |           |  |  |
| ethernet1       | public  | Static          | In Use    | 172.16.1.49    | 25     |            |    |           |         |        |        |             |    |           |        |        |        |             |    |           |            |        |        |         |    |           |        |      |           |  |  |
| ethernet2       | management  | Static          | In Use    | 3.0.0.1        | 25     |            |    |           |         |        |        |             |    |           |        |        |        |             |    |           |            |        |        |         |    |           |        |      |           |  |  |
| ethernet3       | unused  | None            | Link Down |                |        |            |    |           |         |        |        |             |    |           |        |        |        |             |    |           |            |        |        |         |    |           |        |      |           |  |  |

| Step | Description  |
|------|--|
| 2.   | <p>At the Media Interface Configuration screen for ethernet0, enter the appropriate IP address information and zone configuration. The sample network uses ethernet0 as the private side of the Security Gateway. Click <b>Save</b> to continue.</p>  <p>The screenshot shows the 'Media Interface Configuration' window for 'ethernet0'. The 'Media Type' is 'ethernet'. Under 'Media Information', the 'Mac Address' is '00:60:a1:00:cd:96' and the 'Link Status' is 'up/autoselect (100Mbps full-duplex)'. Under 'Current IP Information', the 'IP Address' is '172.16.1.46' and the 'Mask' is '255.255.255.240'. In the 'IP Configuration' section, the 'Zone' is set to 'private' and the 'IP Config Mode' is 'Static'. The 'Static' section shows the IP address '172.16.1.46' and the mask '255.255.255.240'. The 'Save' button is highlighted with a red box.</p> |

| Step                                  | Description  |
|---------------------------------------|--|
| <p data-bbox="191 163 224 197">3.</p> | <p data-bbox="277 163 1414 231">Repeats Step 2, except now highlight the <b>ethernet1</b> interface and click Modify to display the Media Interface Configuration screen for ethernet1.</p> <p data-bbox="277 273 1393 415">At the Media Interface Configuration screen for ethernet1, enter the appropriate IP address information and zone configuration. The sample network uses ethernet1 as the public side of the Security Gateway. The <b>Route</b> is the IP address of the router. Click <b>Save</b> to continue.</p> <div data-bbox="337 451 1360 1354" style="border: 1px solid black; padding: 10px;"> <p><b>Media Interface Configuration</b></p> <p><b>Media Interface:</b> ethernet1      <b>Media Type:</b> ethernet</p> <p><b>Media Information</b></p> <p><b>Mac Address:</b> 00:60:a1:00:cd:97</p> <p><b>Link Status:</b> up/autoselect (100Mbps full-duplex)</p> <p><b>Current IP Information</b></p> <p><b>IP Address:</b> 172.16.1.49</p> <p><b>Mask:</b> 255.255.255.240</p> <p><b>Route:</b> 172.16.1.62</p> <p><b>IP Configuration</b></p> <p><b>Zone:</b> public      <b>IP Config Mode:</b> Static</p> <p><b>Static</b></p> <p><b>IP Address:</b> 172 16 1 49      <b>Mask:</b> 255 255 255 240</p> <p><b>Route:</b> 172 16 1 62</p> <p><b>Save</b>      <b>Cancel</b></p> <p>Java Applet Window</p> </div> |

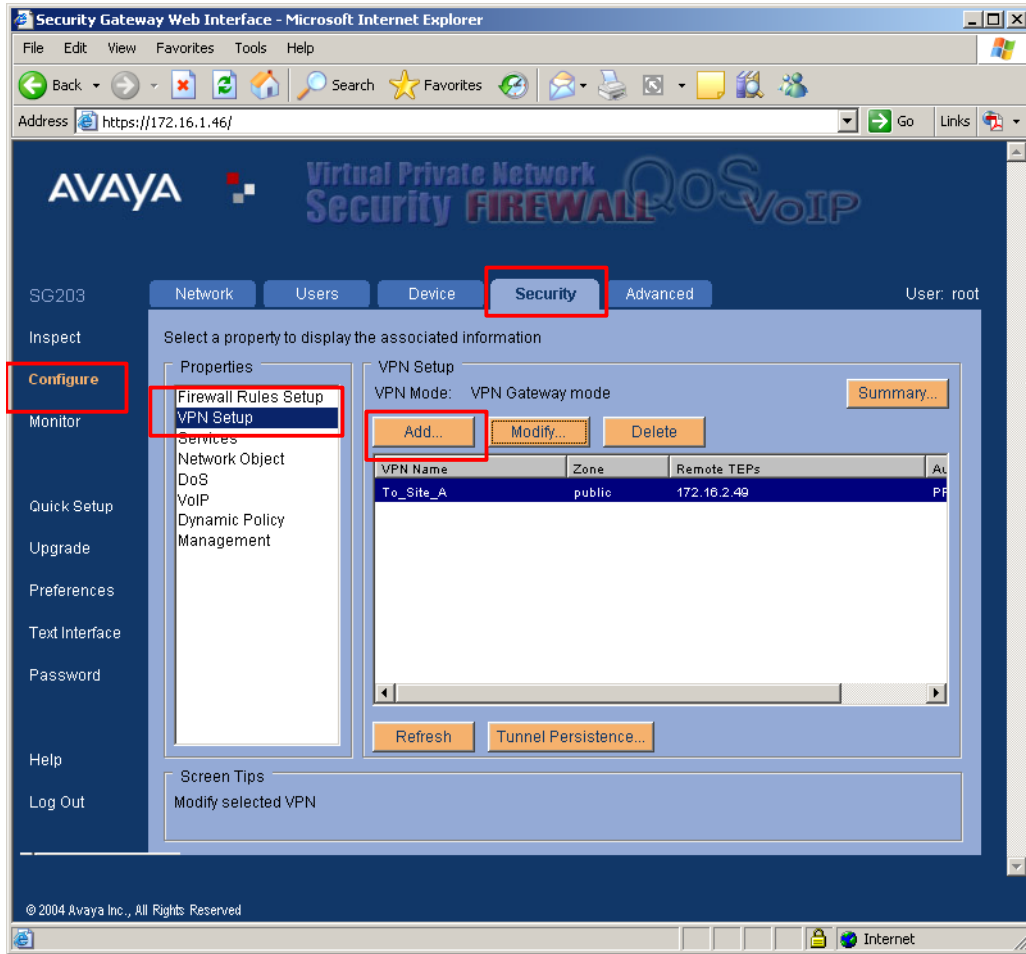
| Step        | Description  |          |                    |             |  |
|-------------|--|----------|--------------------|-------------|--|
| 4.          | <p>At the Avaya Security Gateway main menu, select <b>Routing</b> under <b>Properties</b> and click on <b>Add</b> to add a static route entry.</p>  <p>The screenshot shows the Avaya Security Gateway Web Interface in Microsoft Internet Explorer. The browser address bar shows <code>https://172.16.1.46/</code>. The interface has a dark blue header with the Avaya logo and the text "Virtual Private Network Security FIREWALL QoS VoIP". Below the header, there are tabs for "Network", "Users", "Device", "Security", and "Advanced". The "Network" tab is active, and the "Routing" option is selected in the "Properties" list on the left. The "Static Routes" section is expanded, showing a table with the following data:</p> <table border="1" data-bbox="711 869 1263 953"> <thead> <tr> <th>Next Hop</th> <th>Network/Mask Pairs</th> </tr> </thead> <tbody> <tr> <td>172.16.1.33</td> <td>192.45.100.0/255.255.255.0, 192.45.101.0/255.255.255.0, 50.1.1.0</td> </tr> </tbody> </table> <p>The "Add..." button in the "Static Routes" section is highlighted with a red box. Other buttons visible include "Modify...", "Delete", "Summary...", "Refresh", "RIP...", and "Save".</p> | Next Hop | Network/Mask Pairs | 172.16.1.33 | 192.45.100.0/255.255.255.0, 192.45.101.0/255.255.255.0, 50.1.1.0 |
| Next Hop    | Network/Mask Pairs   |          |                    |             |  |
| 172.16.1.33 | 192.45.100.0/255.255.255.0, 192.45.101.0/255.255.255.0, 50.1.1.0   |          |                    |             |  |



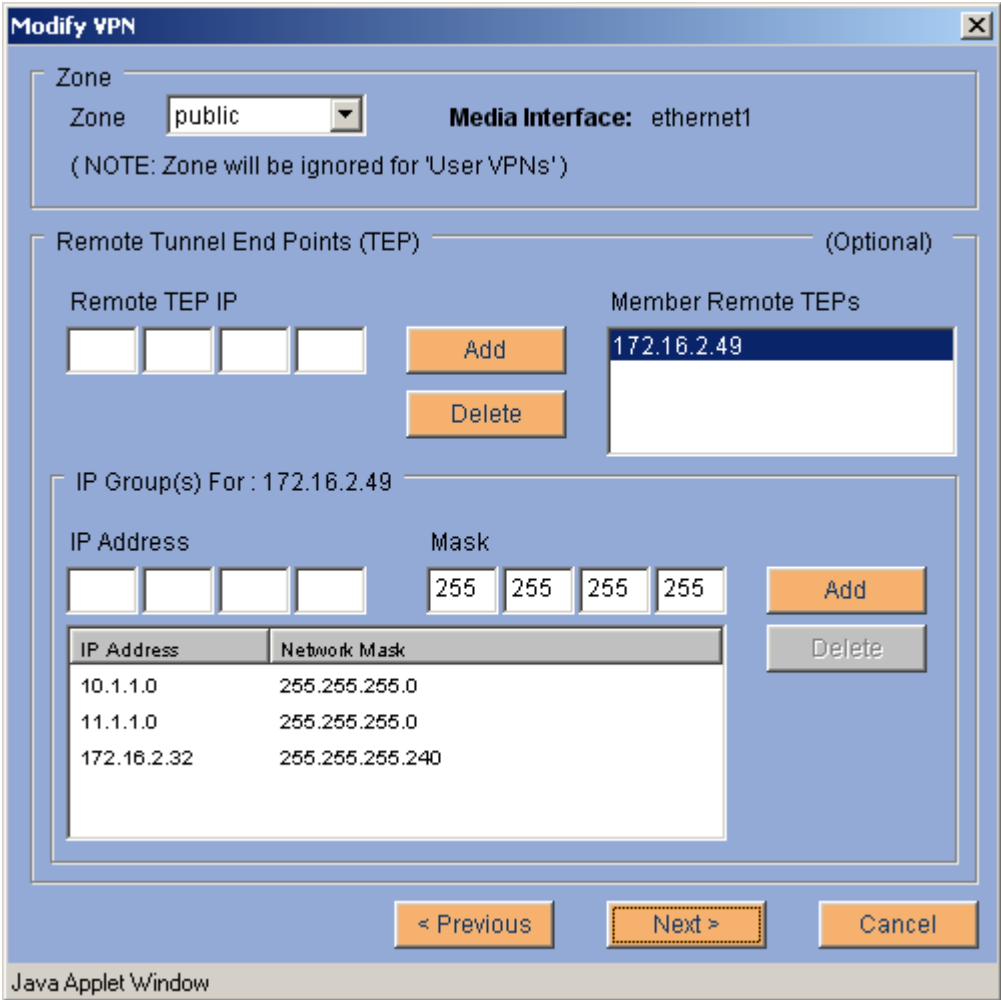
| Step | Description  |
|------|--|
| 5.   | <p>At the Modify Static Route display, enter the appropriate <b>Next Hop</b> IP address for the local IP Networks. For the Main Site, the <b>Next hop</b> IP address to reach the three local IP Networks (192.45.101.0/24, 50.1.1.0/24, and 51.1.1.0/24) is 172.16.1.33. Enter the <b>IP Address</b> information and click <b>Add</b> after each entry. Click <b>OK</b> after all the IP networks have been entered.</p>  |

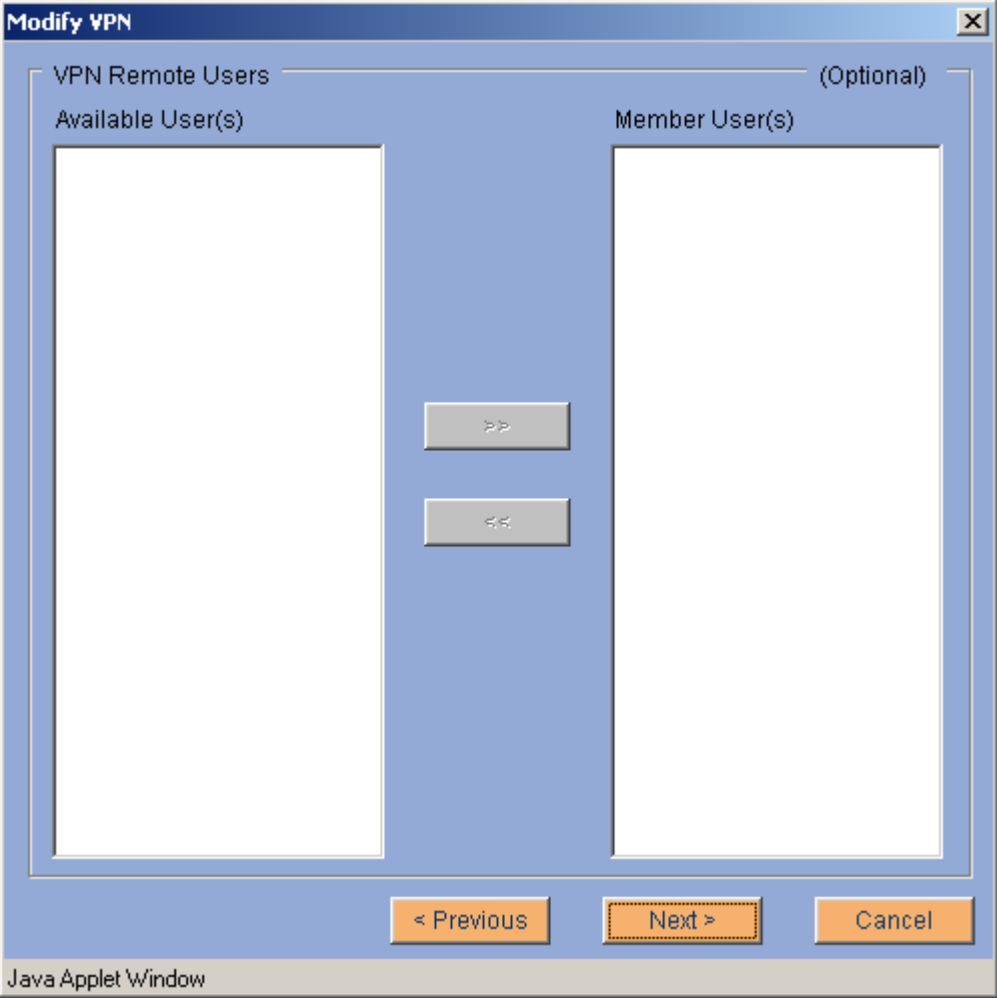
**Step** **Description**

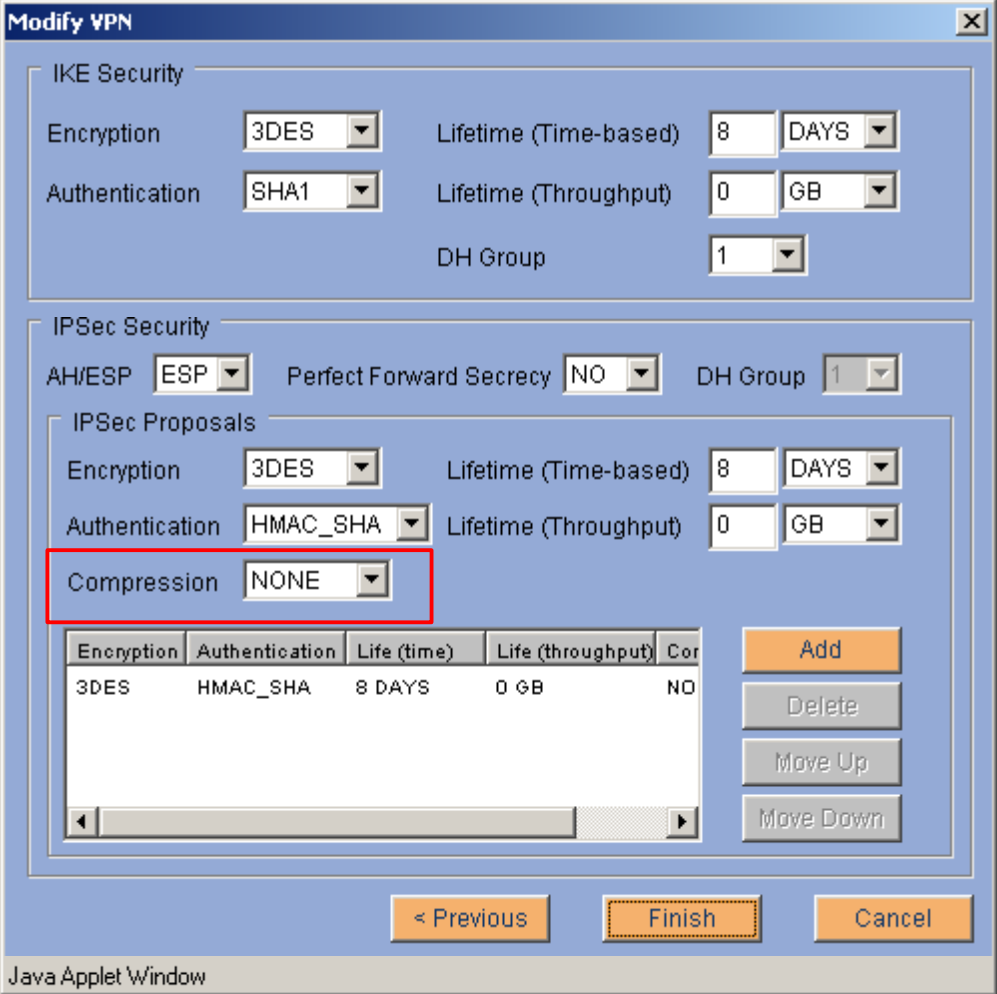
6. The next step is to configure the VPN tunnel between the two sites. Select **Configure** on the left and the **Security** tab. Highlight **VPN Setup** and click **Add** to begin configuration.



| Step | Description   |
|------|---|
| 7.   | <p>At the Modify VPN screen display, enter the following information and click <b>Next</b> to continue.</p> <p><b>VPN Name</b>                    A user-friendly name to identify the VPN connection.</p> <p><b>Preshared Secret</b>            An alphanumeric string used to establish the tunnel between the two Avaya Security Gateways. This same string needs to be entered on both Avaya Security Gateways. This string can be entered in either ASCII or Hexadecimal.</p> <p><b>Local IP Address</b>            All local IP Networks that need to be routed through the VPN tunnel. This includes the IP subnetwork that the Expand Networks Accelerator is in. For the sample network, it is 172.16.1.32 with a 255.255.255.240 mask. Click <b>Add</b> after entering each IP Network.</p> <div data-bbox="350 667 1344 1661" data-label="Image"> </div> |

| Step   | Description  |            |              |          |               |          |               |             |                 |
|--|--|------------|--------------|----------|---------------|----------|---------------|-------------|-----------------|
| <p data-bbox="191 163 224 199">8.</p> <p data-bbox="277 268 350 304"><b>Zone</b></p> <p data-bbox="277 306 496 342"><b>Remote TEP IP</b></p> <p data-bbox="277 415 444 451"><b>IP Group(s)</b></p> | <p data-bbox="277 163 1414 233">In the next Modify VPN screen, enter the following information. After completing, click <b>Next</b> to continue.</p> <p data-bbox="570 268 654 304">public</p> <p data-bbox="570 306 1403 415">This is the Public Interface of the Avaya Security Gateway at the other end that will be terminating the VPN connection. Click <b>Add</b> after entering the Remote TEP IP address.</p> <p data-bbox="570 415 1414 594">All local IP Networks that are at the other end of the VPN tunnel. This includes the IP subnet network that the Expand Networks Accelerator is in. For the sample network, it is 172.16.2.32 with a 255.255.255.240 mask. Click <b>Add</b> after entering each IP network.</p>  <p data-bbox="350 632 1344 667"><b>Modify VPN</b></p> <p data-bbox="399 695 461 720">Zone</p> <p data-bbox="415 730 461 756">Zone <input type="text" value="public"/></p> <p data-bbox="792 730 1094 756"><b>Media Interface:</b> ethernet1</p> <p data-bbox="415 779 914 804">( NOTE: Zone will be ignored for 'User VPNs' )</p> <p data-bbox="399 856 768 882">Remote Tunnel End Points (TEP)</p> <p data-bbox="1166 856 1274 882">(Optional)</p> <p data-bbox="415 915 586 940">Remote TEP IP</p> <p data-bbox="415 951 711 999"><input type="text"/></p> <p data-bbox="805 961 850 987">Add</p> <p data-bbox="792 1024 870 1050">Delete</p> <p data-bbox="954 915 1203 940">Member Remote TEPs</p> <p data-bbox="954 951 1089 976">172.16.2.49</p> <p data-bbox="415 1098 740 1123">IP Group(s) For : 172.16.2.49</p> <p data-bbox="415 1157 537 1182">IP Address</p> <p data-bbox="415 1192 711 1241"><input type="text"/></p> <p data-bbox="773 1157 837 1182">Mask</p> <p data-bbox="773 1192 1065 1241"><input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/></p> <p data-bbox="1166 1203 1211 1228">Add</p> <p data-bbox="1149 1262 1227 1287">Delete</p> <table border="1" data-bbox="415 1255 1065 1465"> <thead> <tr> <th>IP Address</th> <th>Network Mask</th> </tr> </thead> <tbody> <tr> <td>10.1.1.0</td> <td>255.255.255.0</td> </tr> <tr> <td>11.1.1.0</td> <td>255.255.255.0</td> </tr> <tr> <td>172.16.2.32</td> <td>255.255.255.240</td> </tr> </tbody> </table> <p data-bbox="760 1535 878 1560">&lt; Previous</p> <p data-bbox="992 1535 1065 1560">Next &gt;</p> <p data-bbox="1198 1535 1279 1560">Cancel</p> <p data-bbox="350 1591 557 1617">Java Applet Window</p> | IP Address | Network Mask | 10.1.1.0 | 255.255.255.0 | 11.1.1.0 | 255.255.255.0 | 172.16.2.32 | 255.255.255.240 |
| IP Address   | Network Mask   |            |              |          |               |          |               |             |                 |
| 10.1.1.0   | 255.255.255.0  |            |              |          |               |          |               |             |                 |
| 11.1.1.0   | 255.255.255.0  |            |              |          |               |          |               |             |                 |
| 172.16.2.32  | 255.255.255.240  |            |              |          |               |          |               |             |                 |

| Step | Description   |
|------|---|
| 9.   | <p>Leave everything as default (blank) and click <b>Next</b> to continue.</p>  |

| Step              | Description  |             |                   |             |                   |     |      |          |        |      |    |
|-------------------|--|-------------|-------------------|-------------|-------------------|-----|------|----------|--------|------|----|
| <p><b>10.</b></p> | <p>The last step in configuring the VPN tunnel is to select the encryption and authentication algorithm. In the sample configuration, everything is left to the default value except compression. <b>Compression</b> is set to <i>NONE</i>. Expand Networks Accelerators will be performing all the compression and bandwidth management. Click <b>Finish</b> to complete the VPN configuration.</p>  <table border="1" data-bbox="418 1003 1052 1213"> <thead> <tr> <th>Encryption</th> <th>Authentication</th> <th>Life (time)</th> <th>Life (throughput)</th> <th>Cor</th> </tr> </thead> <tbody> <tr> <td>3DES</td> <td>HMAC_SHA</td> <td>8 DAYS</td> <td>0 GB</td> <td>NO</td> </tr> </tbody> </table> | Encryption  | Authentication    | Life (time) | Life (throughput) | Cor | 3DES | HMAC_SHA | 8 DAYS | 0 GB | NO |
| Encryption        | Authentication   | Life (time) | Life (throughput) | Cor         |                   |     |      |          |        |      |    |
| 3DES              | HMAC_SHA   | 8 DAYS      | 0 GB              | NO          |                   |     |      |          |        |      |    |
| <p><b>11.</b></p> | <p>Repeat Steps 1 to 10 for the Avaya Security Gateway at the Branch Site.</p>   |             |                   |             |                   |     |      |          |        |      |    |

## 4. Expand Networks Accelerator

Configuration can be accomplished through either a Command Line Interface (CLI) or a Web Browser. The sample configuration uses the CLI. The following steps describe the configuration for the Expand Networks Accelerator located in the Main Site. Repeat all steps in this section for Accelerator located in the Branch Site, and ensure proper IP address information is used.

| Step | Description   |
|------|---|
| 1.   | <p>Enter the IP address information into the Expand Networks Accelerator using the keypad on the front of the unit. Using the <b>up/down/left/right</b> arrow keys to maneuver and change the digit in the LCD display and press the <b>ENTER</b> key accept the value. The sample configuration uses the following information for the Accelerator at the Main Site.</p> <pre> IP Address      172.16.1.45 Mask            255.255.255.240 Default Gateway 172.16.1.46           </pre>  |
| 2.   | <p>Telnet to the Expand Networks Accelerator IP address and log in using an appropriate user name and password.</p> <pre> AcceleratorOS, Accelerator 4800 Series Version v5.0(7) (Build1.45)  login:           </pre>   |
| 3.   | <p>Define a link between the two Accelerators. The destination IP address is 172.16.2.45 with a WAN bandwidth of 768kbps. Enter configuration mode by typing in <b>enable</b> and <b>configure</b>.</p> <pre> Datacenter&gt; en Datacenter# configure Datacenter(config)# wan default Datacenter(WAN)# bandwidth 768 Datacenter(WAN)# ! Datacenter(config)# interface link 1 Datacenter(LINK)# description L-172.16.2.45 Datacenter(LINK)# link destination 172.16.2.45           </pre> <p>This will limit the amount of traffic coming out from the Accelerator onto this link to no more than 768kbps.</p> |
| 4.   | <p>Enter the local IP Networks that need to be connected through the Expand Networks Accelerator.</p> <pre> Datacenter(config)# subnets Datacenter(SUBNETS)# network 50.1.1.0 255.255.255.0 advertise metric 1 Datacenter(SUBNETS)# network 51.1.1.0 255.255.255.0 advertise metric 1 Datacenter(SUBNETS)# network 192.45.101.0 255.255.255.0 advertise metric 1           </pre>   |

| Step | Description  |
|------|--|
| 5.   | <p>Define two policies for the voice traffic, one for the signaling “<i>h323-gatekeeper-stat</i>” and the other for the media “<i>avayavoip</i>” (RTP stream). The UDP port number from 2048 to 3027 was defined in Avaya Communication Manager in Section 3.1. UDP port number 1719 is the default port number used for H.323 trunk signaling between the two Media Gateways.</p> <pre>Datacenter(config)# application h323-gatekeeper-stat udp 1719 Datacenter(config)# application avayavoip udp from 2048 to 3027</pre>  |
| 6.   | <p>Define policy to prioritize the different traffic flow.</p> <p>Rule 2 was defined for traffic destined to Avaya Communication Manager (IP 10.1.1.1) at the Branch Site. This traffic is mainly for call establishment. It is set with a priority of <b>real-time</b> and a <b>Desired Bandwidth</b> of 25kbps. This 25kbps setting was tested to be adequate based on the number of stations in the sample configuration.</p> <pre>Datacenter(config)# policy-rule 2 global outbound Datacenter(RULE)# match ip dest 10.1.1.1 255.255.255.255 Datacenter(RULE)# set policy priority real-time Datacenter(RULE)# set policy rate desired 25</pre> <p>Rule 23 was defined for general VoIP traffic using the DiffServ bits. In Section 3.1, Signaling and Audio were set to use DiffServ value 34 and 46 respectively in Avaya Communication Manager. In configuring the Accelerator, these values - 34 and 46 translate to 136 and 184, respectively. See note below for details on how these values are calculated.</p> <pre>Datacenter(config)# policy-rule 23 global outbound Datacenter(RULE)# match tos bits 136 Datacenter(RULE)# match tos bits 184 Datacenter(RULE)# set policy priority real-time Datacenter(RULE)# set policy rate desired 200</pre> <p>Note: The DiffServ value of 34 in Avaya Communication Manager translates into 100010 in binary, a 6-digit number. The Accelerator calculation is based on an 8-digit number; therefore two additional zeroes must be added to the end before converting the number back to decimal. 100010 becomes 10001000, or the number 136 in decimal.</p> |
| 7.   | <p>Define a <b>decision</b> to turn off acceleration for RTP traffic. Since G.729 codec already has compression and compression may affect voice quality when using G.711 codec, compression was disabled for all voice media traffic in the sample configuration. By default, the Accelerator compresses all traffic unless compression is explicitly disabled.</p> <pre>Datacenter(config)# decision 1 Datacenter(DECISION)# match application avayavoip Datacenter(DECISION)# set accelerate disable</pre>  |



| Step | Description   |
|------|---|
| 8.   | By default, IPComp compression is enabled and there is no need to configure it. The default configuration is not listed when the “show run” command is entered into the system to list current running configuration. |
| 9.   | Repeat Steps 1 to 8 for the Expand Network Accelerator in the Branch Site. Ensure the proper IP addresses are entered, as the IP addresses may be different from what is shown above for the Main Site.               |

## 5. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the impact that the Expand Networks Accelerator has on Avaya VoIP traffic traversing the PPP link connecting the Main and Branch sites simulating a WAN. Compression and TCP acceleration were enabled for competing non-VoIP traffic while bandwidth preservation was enabled for Avaya VoIP traffic on the Accelerators.

### 5.1. General Test Approach

The general test approach was to verify that the Avaya IP telephones could successfully place and receive calls through the network infrastructure comprised of Avaya SG203 and SG208 Security Gateway and Expand Networks Accelerators through a VPN tunnel while competing with simulated non-VoIP low priority traffic and compression. Compression and Acceleration was implemented in the Expand Networks Accelerator for all non-voice traffic to maximize throughput over the WAN link.

The main objectives were to verify that:

- Calls between telephones in different sites are successfully completed and maintained with good voice quality.
- Multiple telephones calls between sites can be completed as per the Desired Bandwidth configured in the Accelerator.
- Non-VoIP traffic does not encroach upon the bandwidth reserved for voice applications.
- The solution supports G.711 and G.729 codecs.
- The solution supports DTMF.
- Layer-3 DiffServ information is preserved.

### 5.2. Test Results

The objectives in Section 5.1 were successfully verified during compliance testing. Multiple telephone calls were successfully placed and received as per bandwidth policies defined by the Expand Network Accelerators during varying levels of simulated competing traffic. Voice quality was good throughout testing regardless of traffic flow.

## 6. Verification Steps

The following steps may be used to verify the configuration:

- Ensure that all the Accelerator interfaces are reachable by using ping.
- Place and receive call from the Avaya IP telephones.
- From the Accelerator, verify the status of the Link.
- From the Accelerator, verify that the Rule is correctly configured using the “debug traffic-statistics policy-rule” command.
- From the Accelerator, verify the Application is configure correctly by using “show application” command.

## 7. Support

For technical support on the Expand Network Accelerator, contact Expand Networks, Inc. at <http://www.expand.com/CustomerSupport/Overview.html>

Email: TAC@expand.com

|               |                               |
|---------------|-------------------------------|
| North America | 1-877-4-EXPAND (877-439-7263) |
| International | +1-920-490-7337               |
| UK            | 1800559803                    |
| Netherlands   | 08000233047                   |
| France        | 0800906560                    |

## 8. Conclusion

These Application Notes have described the administration steps required to configure the Expand Networks Accelerator to interoperate with and prioritize WAN bandwidth for an Avaya VoIP solution. During compliance testing, H.323 phone calls traversing the WAN link were successfully established and maintained while sharing the link with non-VoIP traffic.

## 9. Additional References

- [1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 1, June 2005
- [2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005 Release 3.0
- [3] *Avaya Security Gateway Configuration Guide for VPNs Release 4.6*, Doc # 670-100-602, Issue 4, May 2005
- [4] *Expand Network Accelerator Configuration Guide version 5.7*

Product documentation for Avaya products may be found at  
<http://support.avaya.com>

Product documentation for Expand Networks products may be found at  
<http://www.expand.com>

---

**©2006 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).