Avaya Solution & Interoperability Test Lab

Application Notes for Trapeze Networks Mobility System with an Avaya IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using the Trapeze Networks Mobility System consisting of the Mobility Exchange (MX) and the Mobility Point (MP). The Trapeze Mobility Points provided network access to the Avaya Wireless IP Telephones, IP Softphone, and Phone Manager Pro, which registered with either Avaya Communication Manager or Avaya IP Office. The Avaya Voice Priority Processor (VPP) was used to support SpectraLink Voice Priority (SVP) on the Avaya Wireless IP Telephones and the Trapeze Mobility Points. An Extreme Networks Alpine 3804 Ethernet Switch interconnected all the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with Avaya wireless IP devices. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using the Trapeze Networks Mobility System consisting of the Mobility Exchange (MX) and Mobility Point (MP). Trapeze MX-20 switches and MP-252 access points were used in the compliance test. The Trapeze MPs connected Avaya 3616/3626 Wireless IP Telephones and wireless laptops running Avaya IP Softphone or Phone Manager Pro to the wired network and allowed them to register with either Avaya Communication Manager or Avaya IP Office. The Avaya Voice Priority Processor (VPP) was used to support the SpectraLink Voice Priority (SVP) Protocol on the Avaya Wireless IP Telephones and the Trapeze MPs. An Extreme Networks Alpine 3804 Ethernet Switch was used to interconnect all the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with Avaya wireless IP devices.

The MX is a wireless LAN switch that integrates with existing wired infrastructure using Layer 2 connectivity. The MX coordinates information about roaming users with other MXs in the network through tunneled communications. The MX also controls all aspects of MPs, including configuring and managing the MPs that are either directly connected to the MX or connected through the existing wired infrastructure. The MXs automatically configure the MPs, which have no local store of data. The MX-20 supports two gigabit and 20 PoE-enabled 10/100 Mbps Ethernet ports. The MX can provide power over Ethernet (PoE) to the MPs over the 10/100 Mbps Ethernet ports. The MP-252 is a dual-radio access point that supports 802.11a and 802.11b/g.

The following MX features were verified during compliance testing:

- Spanning Tree (802.1D) and Per-VLAN Spanning Tree (PVST)
- Quality of Service (QoS) based on Layer 3 and Layer 4 Application Information, such as IP DSCP Markings, Protocol Type, and UDP Port Range
- 802.1X Security and WEP Encryption
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Roaming
- SpectraLink Voice Priority (SVP)
- Power over Ethernet

Figure 1 illustrates the network configuration used to verify the Trapeze Networks solution. All of the wireless IP devices depicted in the configuration roamed among the Trapeze MPs for full mobility. The configuration also notes the ports that connected each network device to the Alpine 3804. The redundant connections between the Alpine 3804 and MX-20 switches were used to verify load-sharing groups. The connection between the two MX-20 switches was used to verify Spanning Tree (802.1D). In this configuration, there is an H.323 IP trunk between the Avaya IP Office and the Avaya S8500 Media Server with a G650 Media Gateway. However, the trunk group, signaling group, and call routing administration are not described in these Application Notes. Refer to Avaya Communication Manager documentation for details.

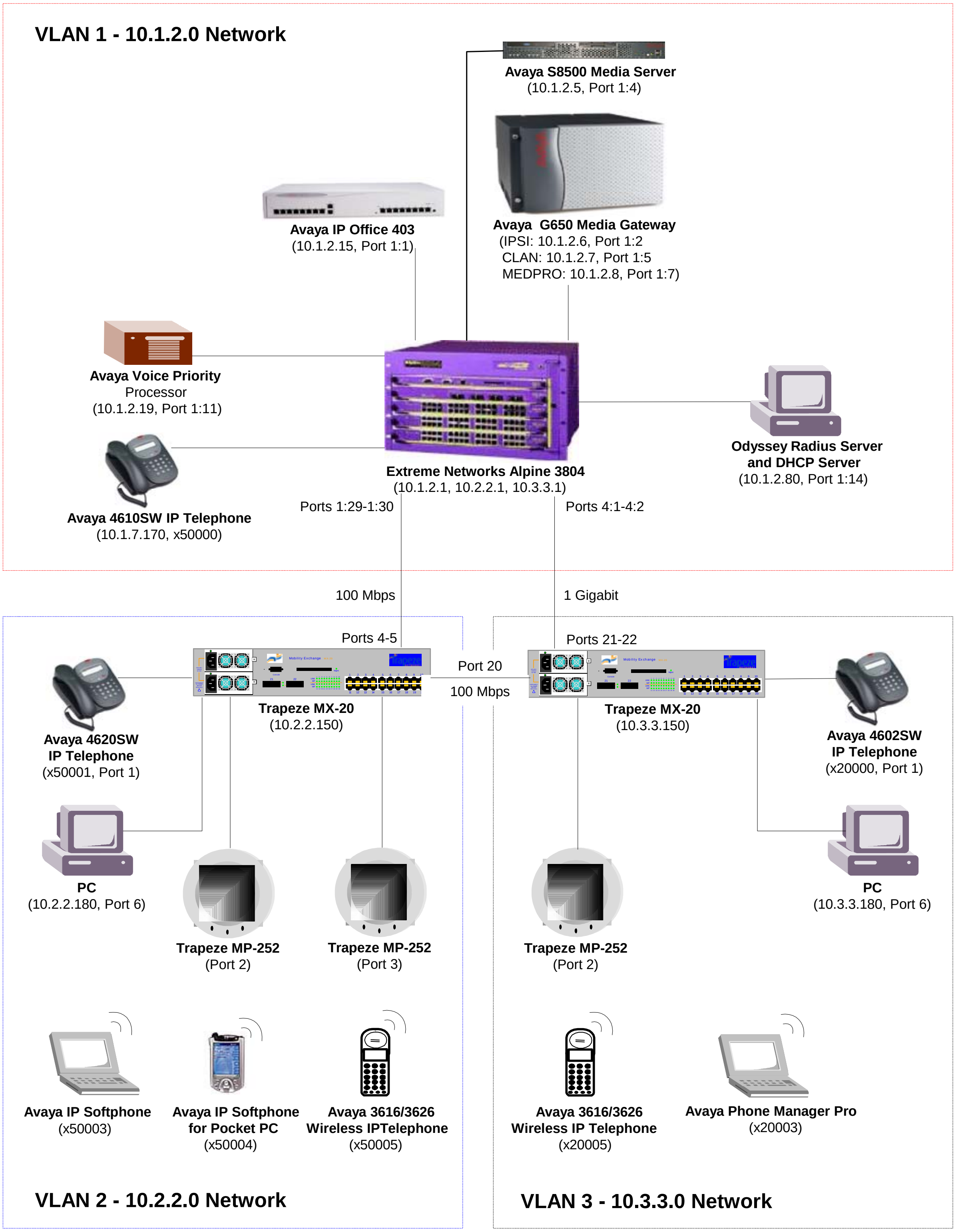


Figure 1: Avaya and Trapeze Networks Wireless LAN Configuration

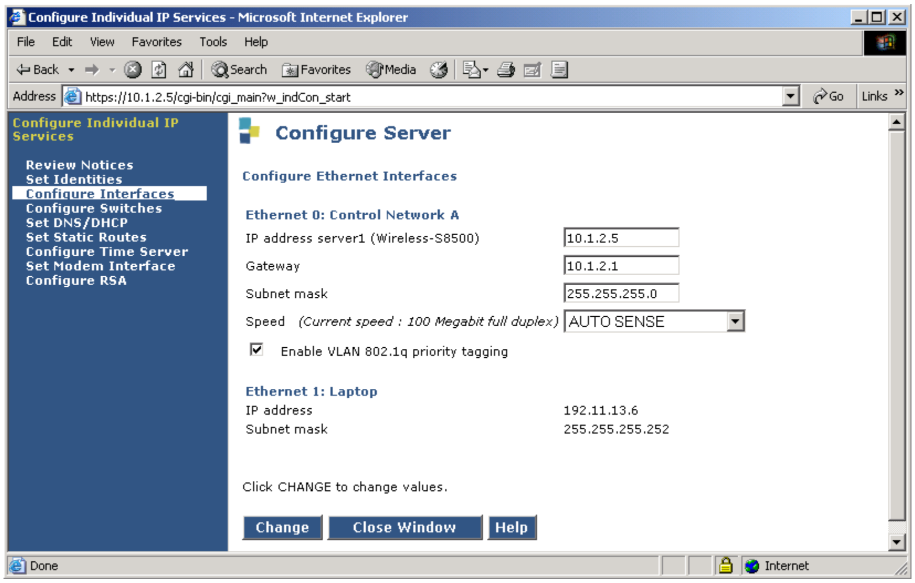
2. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Media Server with Avaya G650 Media Gateway	Communication Manager 2.1 (R012x.01.0.411.7)
Avaya IP Office 403	2.1.15
Avaya Voice Priority Processor	33/02
Avaya 4602SW IP Telephones	2.1
Avaya 3616/3626 IP Wireless Telephones	96.024
Avaya IP Softphone	5.1
Avaya IP Softphone for Pocket PC	2.3
Avaya Phone Manager Pro	2.1.7
Extreme Networks Alpine 3804 Ethernet Switch	7.2.0 Build 25
Trapeze Networks Mobility Exchange MX-20	2.1.5
Trapeze Networks Mobility Point MP-252	2.1.5
Funk Odyssey Radius Server	2.01.00.653
Funk Odyssey Client	3.03.0.119

3. Configure Avaya Communication Manager

The Avaya S8500 Media Server is configured using a web interface. To access the web interface, enter the IP address of the Services port (192.11.13.6) on the media server as the URL in a web browser. Follow the prompts and then log in. Select the **Configure Server** option to access the server configuration page and set the IP address and default gateway of the S8500 Media Server. The default gateway of the S8500 Media Server is the Alpine 3804, which has an IP address of 10.1.2.1.


Configure Individual IP Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.1.2.5/cgi-bin/cgi_main?w_indCon_start
Go Links
Configure Individual IP Services
Review Notices
Set Identities
Configure Interfaces
Configure Switches
Set DNS/DHCP
Set Static Routes
Configure Time Server
Set Modem Interface
Configure RSA
Change
Close Window
Help
Done
Internet

Configure Server

Configure Ethernet Interfaces

Ethernet 0: Control Network A

IP address server1 (Wireless-S8500): 10.1.2.5
Gateway: 10.1.2.1
Subnet mask: 255.255.255.0
Speed (*Current speed : 100 Megabit full duplex*): AUTO SENSE
☑ Enable VLAN 802.1q priority tagging

Ethernet 1: Laptop

IP address: 192.11.13.6
Subnet mask: 255.255.255.252

Click CHANGE to change values.

Figure 2: Avaya S8500 Media Server – Configure Server Form

From the System Access Terminal (SAT), enter the **change ip-network-region 1** command to configure the network region that will be assigned to the C-LAN and IP Media Processor (MEDPRO) boards in the G650 Media Gateway and to the wireless IP endpoints. IP Network Region ‘1’ specifies the codec set that will be used by the MEDPRO and wireless IP endpoints, and the UDP port range that will be used by the MEDPRO for audio. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio to be exchanged directly between IP endpoints without using MEDPRO resources. IP network region ‘1’ is assigned to the C-LAN and IP Media Processor in the **ip-interface** forms shown in **Figures 5** and **6**. The IP endpoints are also assigned to this network region automatically when they register with the S8500 Media Server via the C-LAN.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:                  Home Domain:
    Name:
                                Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS                Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                            IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 65535                      RTCP Reporting Enabled? y
                                 RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS           Use Default Server Parameters? y
 Call Control PHB Value: 34
        Audio PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 3: IP Network Region Form

On the **ip-codec-set** form, select the audio codec type to be used by the IP Media Processor and the IP endpoints in network region 1. Note that IP codec set ‘1’ was specified in IP Network Region ‘1’ in **Figure 3**. The form is accessed via the **change ip-codec-set 1** command. The default settings of the **ip-codec-set** form are shown below. However, the **Audio Codec** field may be set to *G.729* to conserve bandwidth.

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

                          IP Codec Set

    Codec Set: 1

    Audio      Silence      Frames   Packet
    Codec      Suppression  Per Pkt  Size(ms)
 1: G.711MU         n         2        20
 2:
```

Figure 4: IP Codec Set Form

Assign a default gateway and network region to the C-LAN board in location 1a02 via the **change ip-interface 1a02** form. The **Node Name** was mapped to the **IP Address** in the **Node-Names IP** form (not shown here). The default gateway is the Alpine 3804 Ethernet switch (10.1.2.1). The default gateway allows VoIP signaling packets from the C-LAN to be exchanged with the IP endpoints in other VLANs. The C-LAN was assigned to IP network region ‘1’. In the absence of an IP network map, the IP endpoints that register with this C-LAN inherit its network region. The C-LAN accepts registration and call setup requests from the IP endpoints and exchanges call setup messages with the Avaya IP Office to establish VoIP calls. There is an H.323 trunk group and signaling group configured between the Avaya S8500 Media Server and the Avaya IP Office that are not described in these Application Notes.

```
change ip-interface 1a02                                        Page   1 of   1

                                  IP INTERFACES

                  Type: C-LAN                                ETHERNET OPTIONS
                  Slot: 01A02                                       Auto? y
           Code/Suffix: TN799  D
             Node Name: CLAN-01A02
            IP Address: 10 .1  .2  .7
           Subnet Mask: 255.255.255.0
       Gateway Address: 10 .1  .2  .1
  Enable Ethernet Port? y
        Network Region: 1
                  VLAN: n

Number of CLAN Sockets Before Warning: 400
```

Figure 5: IP Interface Form for C-LAN

Assign a default gateway and IP network region to the IP Media Processor in location 1a03 via the **change ip-interface 1a03** form. The **Node Name** was mapped to the **IP Address** in the **Node-Names IP** form (not shown here). The default gateway is the Alpine 3804 Ethernet switch (10.1.2.1) and it allows VoIP media (RTP) packets to be routed to the IP endpoints in other VLANs as well as to the Avaya IP Office. The IP Media Processor was assigned to IP network region ‘1’.

```
change ip-interface 1a03                                        Page   1 of   1

                                  IP INTERFACES

                  Type: MEDPRO                               ETHERNET OPTIONS
                  Slot: 01A03                                       Auto? y
           Code/Suffix: TN2302
             Node Name: MEDPRO-01A03
            IP Address: 10 .1  .2  .8
           Subnet Mask: 255.255.255.0
       Gateway Address: 10 .1  .2  .1
  Enable Ethernet Port? y
        Network Region: 1
                  VLAN: n
```

Figure 6: IP Interface Form for IP Media Processor

Lastly, configure the stations that correspond to each of the wireless IP endpoints, including the Avaya IP Softphones and the Avaya 3616/3626 Wireless IP Telephones. The station configuration for the IP Softphone is shown in **Figure 7**. Set the **Type** field to *4620*, set the **IP Softphone** field to 'y', and specify a **Security Code**. The configuration below also applies to the Avaya IP Softphone for Pocket PC (i.e., extension 50004).

```
change station 50003                                            Page   1 of   4
                                     STATION

Extension: 50003                          Lock Messages? n          BCC: 0
     Type: 4620                           Security Code: 123456      TN: 1
     Port: S00000                       Coverage Path 1:            COR: 1
     Name: IP Softphone                 Coverage Path 2:            COS: 1
                                        Hunt-to Station:

STATION OPTIONS
              Loss Group: 19            Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 50003
            Speakerphone: 2-way                  Mute Button Enabled? y
        Display Language: english                   Expansion Module? n

 Survivable GK Node Name:                          Media Complex Ext:
                                                       IP SoftPhone? y
```

Figure 7: Station Form for IP Softphone

Figure 8 displays the station configuration for the Avaya 3616/3626 Wireless IP Telephone. Repeat this configuration for each wireless telephone.

```
change station 50005                                            Page   1 of   4
                                     STATION

Extension: 50005                          Lock Messages? n          BCC: 0
     Type: 4620                           Security Code: 123456      TN: 1
     Port: S00006                       Coverage Path 1:            COR: 1
     Name: IP Wireless Phone            Coverage Path 2:            COS: 1
                                        Hunt-to Station:

STATION OPTIONS
              Loss Group: 19            Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 50005
            Speakerphone: 2-way                  Mute Button Enabled? y
        Display Language: english                   Expansion Module? n

 Survivable GK Node Name:                          Media Complex Ext:
                                                       IP SoftPhone? n
```

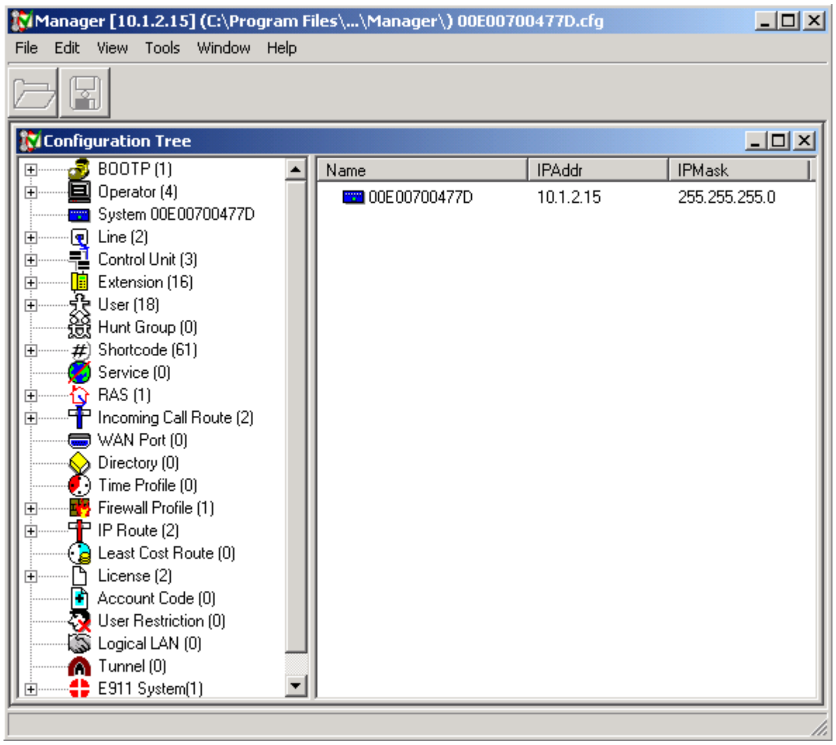
Figure 8: Station Form for the Avaya 3616/3626 Wireless IP Telephones

Note: The Dial Plan, IP Trunk, H.323 Signaling Group, and Call Routing administration are beyond the scope of these Application Notes. Refer to [1] and [2] for configuration details.

4. Configure the Avaya IP Office 403

This section describes the steps required to configure stations (i.e., Extensions and Users) for the Avaya 3616/3626 Wireless IP Telephones and the Avaya Phone Manager Pro on the Avaya IP Office. A feature license that includes *IP-Endpoints* and *Phone Manager Pro* is required in order to use the Avaya Phone Manager Pro application. The feature license is maintained on a security dongle connected to a USB or parallel port on the PC running **Avaya IP Office Manager**.

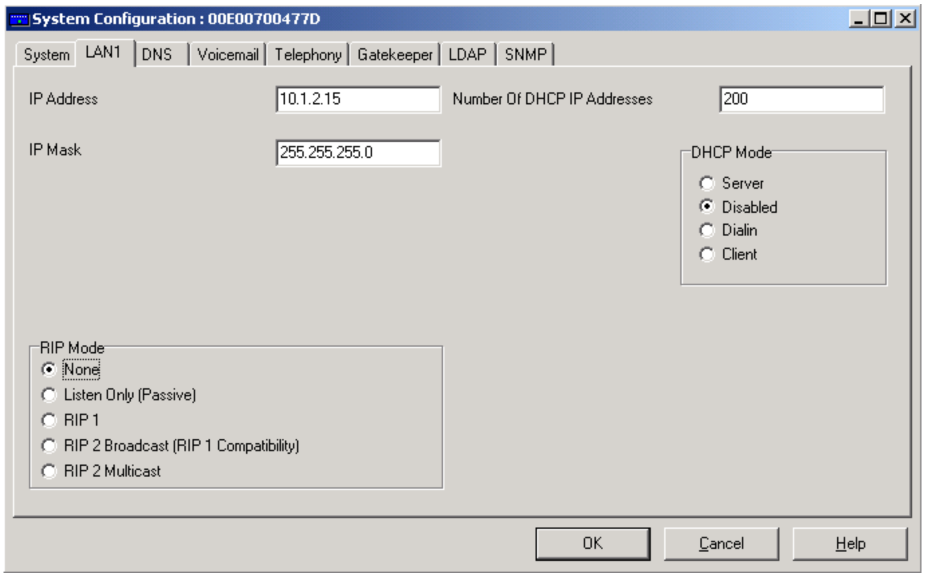
The IP Office was configured using the **Avaya IP Office Manager** application. To configure the Avaya IP Office, open the **Manager** application from a PC with IP connectivity to the IP Office. It is assumed that the IP Office has already been configured with an IP address. The **Manager** main window in **Figure 9** is displayed. All of the configuration options are selected from the tree view of the **Manager** window.



Name	IPAddr	IPMask
00E00700477D	10.1.2.15	255.255.255.0

Figure 9: Manager Main Window

To configure the IP Office with a new IP address, select the **System** option. In the **LAN1** tab, set the **IP Address** and **IP Mask** as shown in **Figure 10**. Although the integrated DHCP server in the IP Office could have been used, a separate DHCP server was used for illustrative purposes.



IP Address: 10.1.2.15

IP Mask: 255.255.255.0

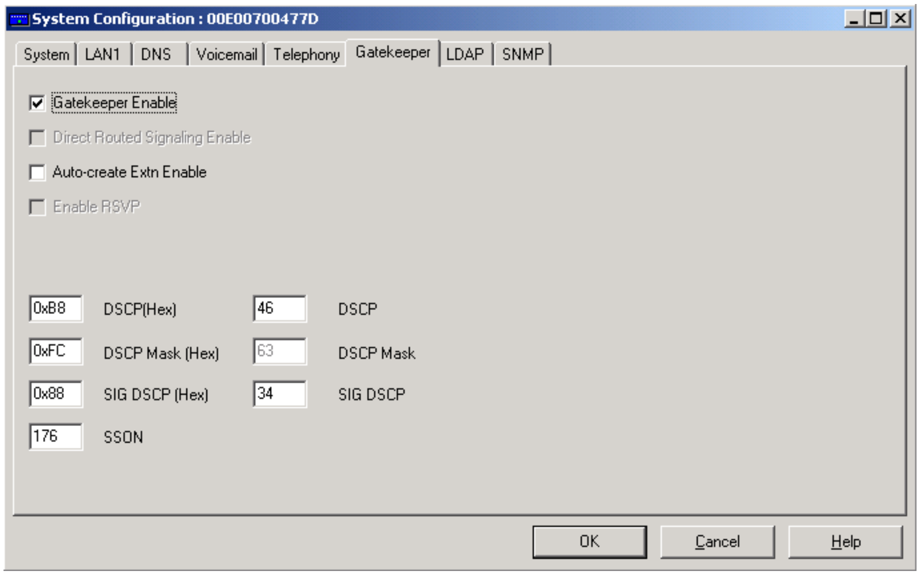
Number Of DHCP IP Addresses: 200

DHCP Mode
○ Server
● Disabled
○ Dialin
○ Client

RIP Mode
● None
○ Listen Only (Passive)
○ RIP 1
○ RIP 2 Broadcast (RIP 1 Compatibility)
○ RIP 2 Multicast

Figure 10: System Configuration – LAN1 Tab

In the **Gatekeeper** tab, select the **Gatekeeper Enable** checkbox to allow H.323 IP endpoints to register with IP Office, and set the DSCP values for audio and call signaling.

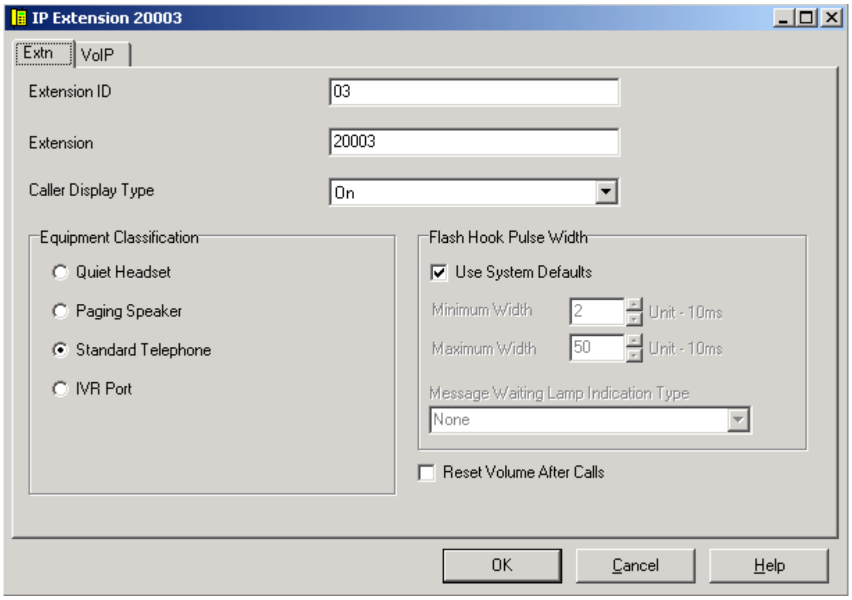


☑ Gatekeeper Enable
☐ Direct Routed Signaling Enable
☐ Auto-create Extn Enable
☐ Enable RSVP

0xB8 DSCP(Hex) 46 DSCP
0xFC DSCP Mask (Hex) 63 DSCP Mask
0x88 SIG DSCP (Hex) 34 SIG DSCP
176 SSON

Figure 11: System Configuration - Gatekeeper Tab

To configure a station on IP Office, select **Extension** from the **Manager** main window. On the right pane, use the right-mouse click and select **New** from the pop-up menu to display the **IP Extension** form shown in **Figure 12**. The **Extension** configuration shown in **Figures 12** and **13** apply to both the 3616/3626 Wireless IP telephones and the Phone Manager Pro. In the **Extn** tab, specify an **Extension ID** and **Extension** and configure the other parameters as shown in **Figure 12**. Repeat this configuration for each IP endpoint that will register with IP Office.



Extension ID: 03
Extension: 20003
Caller Display Type: On

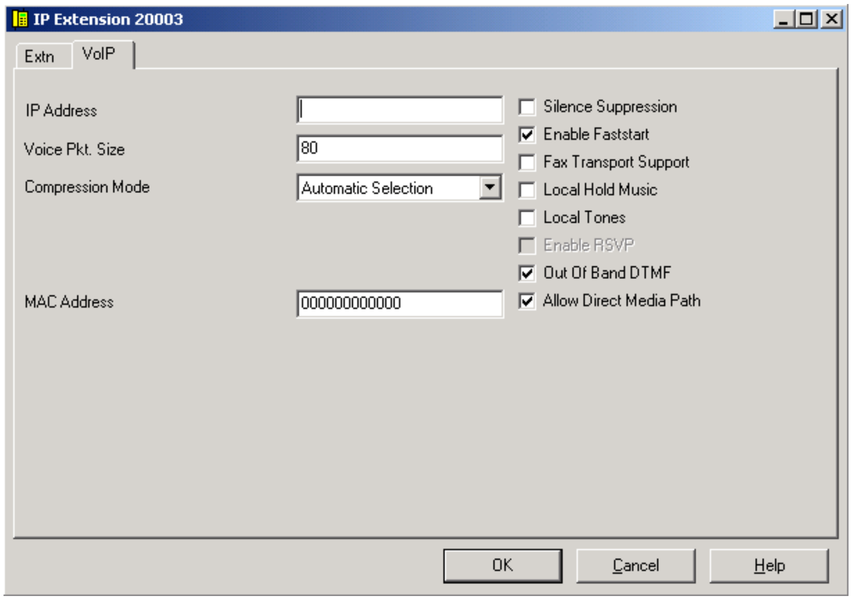
○ Quiet Headset
○ Paging Speaker
● Standard Telephone
○ IVR Port

☑ Use System Defaults
Minimum Width: 2 Unit - 10ms
Maximum Width: 50 Unit - 10ms
Message Waiting Lamp Indication Type: None

☐ Reset Volume After Calls

Figure 12: IP Extension – Extn Tab

Configure the **VoIP** tab as shown in **Figure 13**.

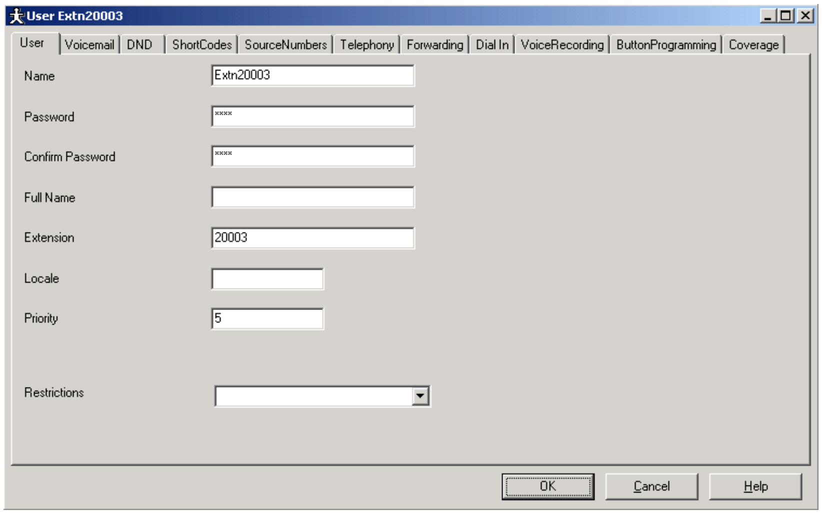


IP Address:
Voice Pkt. Size: 80
Compression Mode: Automatic Selection
MAC Address: 000000000000

☐ Silence Suppression
☑ Enable Faststart
☐ Fax Transport Support
☐ Local Hold Music
☐ Local Tones
☐ Enable RSVP
☑ Out Of Band DTMF
☑ Allow Direct Media Path

Figure 13: IP Extension – VoIP Tab

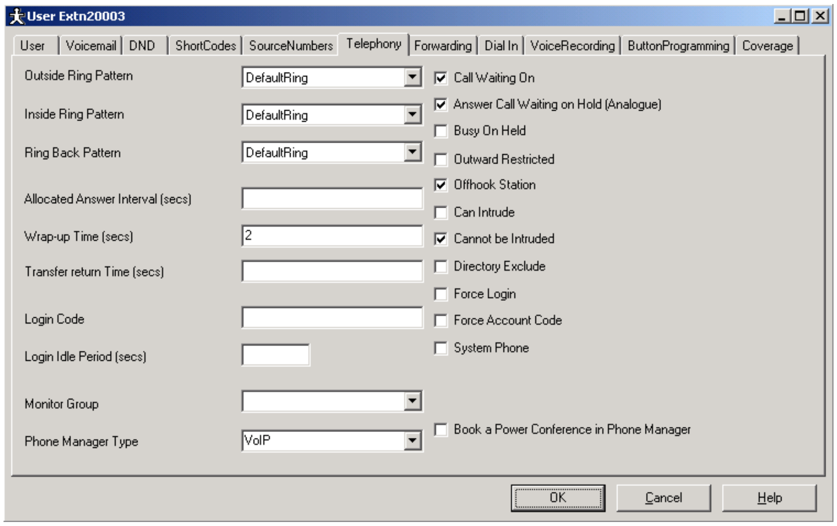
Next, select **User** from the **Manager** main window. On the right pane, use the right-mouse click and select **New** from the pop-up menu to display the **User** window shown in **Figure 14**. In the **User** tab, specify the endpoint's **Name**, **Password**, and **Extension** as shown in **Figure 14**.



Name	Extn20003
Password	****
Confirm Password	****
Full Name	
Extension	20003
Locale	
Priority	5
Restrictions	

Figure 14: User – User Tab

In the **Telephony** tab, set the **Phone Manager Type** field to *VoIP* for the Phone Manager Pro user only.



Outside Ring Pattern	DefaultRing
Inside Ring Pattern	DefaultRing
Ring Back Pattern	DefaultRing
Allocated Answer Interval (secs)	
Wrap-up Time (secs)	2
Transfer return Time (secs)	
Login Code	
Login Idle Period (secs)	
Monitor Group	
Phone Manager Type	VoIP

☑ Call Waiting On
☑ Answer Call Waiting on Hold (Analogue)
☐ Busy On Held
☐ Outward Restricted
☑ Offhook Station
☐ Can Intrude
☑ Cannot be Intruded
☐ Directory Exclude
☐ Force Login
☐ Force Account Code
☐ System Phone
☐ Book a Power Conference in Phone Manager

Figure 15: User – Telephony Tab

5. Configure the Avaya Voice Priority Processor

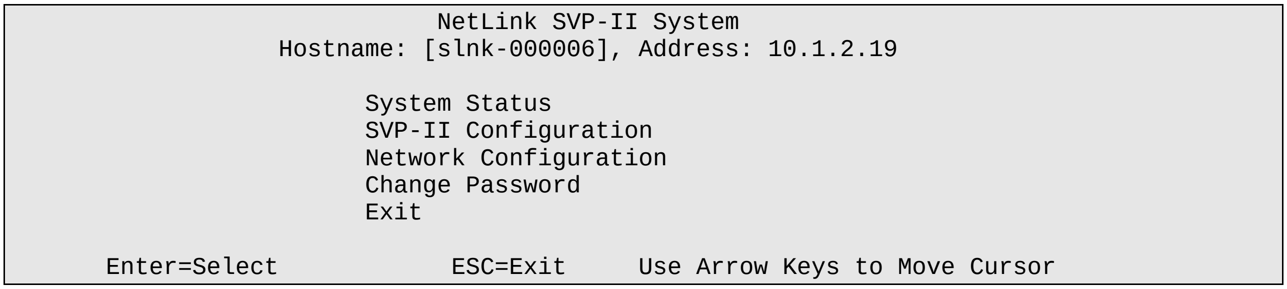
The Avaya Voice Priority Processor (VPP) utilizes SpectraLink Voice Priority (SVP) as the Quality of Service (QoS) mechanism supported by the Avaya 3616/3626 Wireless IP Telephones and the Trapeze MPs to enhance voice quality over the wireless network.

The Avaya VPP performs four major functions. First, it is a required component to utilize the 11Mbps maximum transmission speed available in the Avaya Wireless Telephones that support 802.11b. Second, it controls the maximum number of calls supported per access point. Third, SVP allows the Trapeze MPs and the Avaya Wireless IP Telephones to transmit their voice packets immediately, while other devices must wait a random backoff period as required by the 802.11 standard. This reduces jitter and delay for the voice packets. Finally, the Avaya VPP is required to serve as a “gateway” between the Avaya Wireless IP Telephones and the Avaya IP Telephony infrastructure. Since the wireless telephones support SVP, their packets are directed to the Avaya VPP so that the SVP header information can be removed before the packets are forwarded to Avaya Communication Manager.

To configure the Avaya VPP, connect a PC or laptop to the serial port of the Avaya VPP. Run a terminal emulation program with the following configuration:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Once connected, the Avaya VPP login screen is presented. Log in as *admin*. The **Avaya VPP System Menu** is displayed as shown in **Figure 16**. After configuring an IP address, a Telnet session may be used to modify the configuration.



```
                              NetLink SVP-II System
                   Hostname: [slnk-000006], Address: 10.1.2.19

                         System Status
                         SVP-II Configuration
                         Network Configuration
                         Change Password
                         Exit

      Enter=Select            ESC=Exit     Use Arrow Keys to Move Cursor
```

Figure 16: System Menu

From the **System Menu**, select **Network Configuration** to configure the IP address, subnet mask, and default gateway.

```
                              Network Configuration
                   Hostname: [slnk-000006], Address: 10.1.2.19

      Ethernet Address (fixed):      00:90:7A:00:00:06
      IP Address:                    10.1.2.19
      Hostname:                      slnk-000006
      Subnet Mask:                   255.255.255.0
      Default Gateway:               10.1.2.1
      SVP-II TFTP Download Master:   NONE
      Primary DNS Server:            NONE
      Secondary DNS Server:          NONE
      DNS Domain:                    NONE
      WINS Server:                   NONE
      Workgroup:                     WORKGROUP
      Syslog Server:                 NONE
      Maintenance Lock:              N

        Enter=Change      Esc=Exit              Use Arrow Keys to Move Cursor
```

Figure 17: Network Configuration

From the **System Menu**, select **SVP-II Configuration** to configure the **Phones per Access Point** and the **802.11 Rate** fields. In this configuration, the **802.11 Rate** was configured to *Automatic*, as shown **Figure 18**, to allow the wireless telephone to determine the rate (up to 11Mbps), as opposed to the Avaya VPP limiting the transmission rate of the wireless telephone to 1/2 Mbps. The **Phones per Access Point** field should specify the maximum number of calls supported by each Trapeze MP. Once the maximum number of calls is reached, the next 3616/3626 Wireless IP Telephone that attempts to go off-hook will try to roam to another MP within range, or will be denied with a “Net Busy” error message.

```
                              SVP-II Configuration
                   Hostname: [slnk-000006], Address: 10.1.2.19

      Phones per Access Point:       10
      802.11 Rate:                   Automatic
      SVP-II Master:                 10.1.2.19
      SVP-II Mode:                   Netlink IP
      Ethernet link:                 100mbps/full duplex
      System Locked:                 N
      Maintenance Lock:              N
      Reset System

        Enter=Change      Esc=Exit              Use Arrow Keys to Move Cursor
```

Figure 18: SVP-II Configuration

6. Configure the Extreme Networks Alpine 3804

This section covers the configuration of the Extreme Networks Alpine 3804 Ethernet switch that is relevant to the Trapeze Networks Mobility Exchange switches and Mobility Points. Specifically, the configuration related to the VLANs 2 and 3, Spanning Tree, Load-Sharing Groups, and the Ethernet ports used by the Trapeze Mobility System are covered below.

Step	Description
1.	Establish a Telnet session to the Alpine 3804 and log in as *admin*. It is assumed that an IP address has already been assigned to the Alpine 3804.

2.	Create VLANs 2 and 3 on the Alpine 3804.
	Note: The configuration of VLAN 1 is not shown in these Application Notes.
	`Alpine3804# create vlan vlan2`
	`Alpine3804# create vlan vlan3`

3.	Assign a tag to VLANs 2 and 3.
	`Alpine3804# configure vlan vlan2 tag 2`
	`Alpine3804# configure vlan vlan3 tag 3`

4.	Enable IP Forwarding on the VLAN interfaces to allow the Alpine 3804 to route between VLANs 2 and 3.
	`Alpine3804# enable ipforwarding vlan vlan2`
	`Alpine3804# enable ipforwarding vlan vlan3`

5.	Configure an IP address and subnet mask for each VLAN interface.
	`Alpine3804# configure vlan vlan2 ipaddress 10.2.2.1 255.255.255.0`
	`Alpine3804# configure vlan vlan3 ipaddress 10.3.3.1 255.255.255.0`

6.	Assign VLANs 2 and 3 to Ethernet ports 1:29 and 4:1. VLANs 2 and 3 were assigned to ports 1:29 and 4:1 as tagged to enable 802.1Q trunking to the MX-20 switches.
	`Alpine3804# configure vlan vlan2 add port 1:29,4:1 tagged`
	`Alpine3804# configure vlan vlan3 add port 1:29,4:1 tagged`

7.	Create two 2-port load-sharing groups between the Alpine 3804 and the MX-20 switches. The first 2-port load-sharing group includes ports 1:29 and 1:30 (100Mbps Ethernet ports) and the second 2-port load-sharing group includes port 4:1 and 4:2 (1 Gigabit Ethernet ports). During testing, the load-sharing groups were not configured simultaneously with STP shown in Step 8.
	`Alpine3804# configure vlan vlan2 add port 1:30,4:2 tagged`
	`Alpine3804# configure vlan vlan3 add port 1:30,4:2 tagged`
	`Alpine3804# enable sharing 1:29 grouping 1:29-1:30`
	`Alpine3804# enable sharing 4:1 grouping 4:1-4:2`

Step	Description

8.	Configure Spanning Tree Protocol (STP) on VLANs 2 and 3 with a port mode of *PVST+*. The following commands creates two STP domains: *vlan2-stp* and *vlan3-stp*. Ports 1:29 and 4:1, which connect to the MX-20 switches, are added to both STP domains. In addition, the STP priority is modified so that the Alpine 3804 becomes the root bridge. During testing, STP was not configured simultaneously with load-sharing groups shown in Step 7.
	`Alpine3804# create stpd vlan2-stp`
	`Alpine3804# configure stpd vlan2-stp add vlan vlan2`
	`Alpine3804# configure stpd vlan2-stp priority 32765`
	`Alpine3804# configure stpd vlan2-stp tag 2`
	`Alpine3804# configure stpd vlan2-stp port mode pvst-plus 1:29`
	`Alpine3804# configure stpd vlan2-stp port mode pvst-plus 4:1`
	`Alpine3804# enable vlan2-stp`
	`Alpine3804# create stpd vlan3-stp`
	`Alpine3804# configure stpd vlan3-stp add vlan vlan3`
	`Alpine3804# configure stpd vlan3-stp priority 32765`
	`Alpine3804# configure stpd vlan3-stp tag 3`
	`Alpine3804# configure stpd vlan3-stp port mode pvst-plus 1:29`
	`Alpine3804# configure stpd vlan3-stp port mode pvst-plus 4:1`
	`Alpine3804# enable vlan3-stp`

9.	Enable DHCP Relay and specify the IP address of the DHCP server. The Avaya wireless IP endpoints and the Trapeze MPs request their IP configuration from the DHCP server.
	`Alpine3804# enable bootprelay`
	`Alpine3804# configure bootprelay add 10.1.2.80`

10.	Save the configuration changes using the following command: `Alpine3804# copy running-config startup-config`

7. Configure the DHCP Server

The Avaya Wireless IP Telephones and the laptops running IP Softphone and Phone Manager Pro obtained their IP configuration, Avaya VPP IP address (Option 151), and Option 176 settings from a DHCP server. The Trapeze MPs do not require an IP address. The DHCP server was configured with two scopes that served wireless IP endpoints that register with either Avaya Communication Manager or Avaya IP Office. The following scopes were defined on the DHCP server:

```
Scope [10.2.2.0] Avaya Communication Manager
Address Pool
  Start IP Address = 10.2.2.50
  End IP Address = 10.2.2.70
Option 003 Router = 10.2.2.1
Option 151 AVPP = 10.1.2.19
Option 176 IP Telephone =
  MCIPADD=10.1.2.7,MCPORT=1719,TFTPSRVR=10.1.2.80

Scope [10.3.3.0] Avaya IP Office
Address Pool
  Start IP Address = 10.3.3.50
  End IP Address = 10.3.3.70
Option 003 Router = 10.3.3.1
Option 151 AVPP = 10.1.2.19
Option 176 IP Telephone =
  MCIPADD=10.1.2.15,MCPORT=1719,TFTPSRVR=10.1.2.80
```

8. Configure the Trapeze Mobility System

This section covers the configuration of the Trapeze Mobility System, including the MX-20 WLAN switches and the MP-252 access points. Note that the MPs download their configuration from the MX. The following configuration applies to the MX-20 in VLAN 2 with IP address 10.2.2.150.

Step	Description
1.	To perform initial configuration of the MX-20, set up a serial connection from a PC or laptop. On the PC or laptop, set up a terminal session as follows: ▪ 9600 baud ▪ 8 bits ▪ 1 stop bit ▪ No parity ▪ Hardware flow control *disabled* Log in to the MX-20 command-line interface (CLI). At the CLI prompt, enter the **enable** command to display the prompt for the enabled access level. Initially, no password is required.

Step	Description
2.	Assign a system name, IP address, and default route to the MX-20. The gateway in the default route is the Alpine 3804 Ethernet switch. In addition, configure the country code and timezone on the MX-20. The commands to enable telnet on the MX-20 are also shown below.

```
MX20-1# set system name mx20-1
MX20-1# set system ip-address 10.2.2.150
MX20-1# set ip route default 10.2.2.1 1
MX20-1# set system countrycode US
MX20-1# set timezone EST -5 0
MX20-1# set ip telnet server enable
MX20-1# set user admin password encrypted <password>
```

A Mobility Domain is a collection of MX switches that work together to support a roaming user. A user can roam across the network from one MX switch to another while maintaining the same IP address and session. Each Mobility Domain has one seed member and one or more nonseed members. Refer to [8] for additional information on Mobility Domains.

This MX switch (10.2.2.150) is configured as the seed of Mobility Domain **avaya** and the other MX switch (10.3.3.150) in the configuration is configured as a member.

```
MX20-1# set mobility-domain mode seed domain-name avaya
MX20-1# set mobility-domain member 10.3.3.150
```

Step	Description
3.	Enable Power over Ethernet (PoE) on port 1, which connects to an Avaya 4600 Series IP Telephone. By default, PoE is disabled on all other ports.

```
MX20-1# set port poe 1 enable
```

Step	Description
4.	Configure VLANs 2 and 3 and assign a VLAN name to each one. Assign an IP address to the VLAN 2 interface.

```
MX20-1# set vlan 2 name VLAN2
MX20-1# set vlan 3 name VLAN3
MX20-1# set interface 2 ip 10.2.2.150 255.255.255.0
```

Assign each VLAN to the appropriate ports according to the network configuration in **Figure 1**. VLAN 2 is assigned to ports 1 and 6 that connect to an Avaya IP telephone and PC, respectively. Ports 4 and 20 are enabled with 802.1Q trunking and are assigned to VLANs 2 and 3. These 802.1Q trunk links send packets with VLAN tags 2 and 3.

```
MX20-1# set vlan 2 port 1
MX20-1# set vlan 2 port 6
MX20-1# set vlan 2 port 4 tag 2
MX20-1# set vlan 2 port 20 tag 2
MX20-1# set vlan 3 port 4 tag 3
MX20-1# set vlan 3 port 20 tag 3
```

Step	Description

5.

The MX-20 is designed to secure network access on a per-user basis. Create a local user database for each authorized wireless device. The MAC addresses in the following example are associated with Avaya 3616/3626 Wireless IP Telephones and an Avaya IP Softphone laptop. The commands below assign each wireless device to either VLAN 2 or 3. In a large WiFi deployment, MAC users would be handled on a RADIUS server.

```
MX20-1# set mac-user 00:40:96:51:84:db attr vlan-name VLAN3
MX20-1# set mac-user 00:90:7a:01:0f:53 attr vlan-name VLAN2
MX20-1# set mac-user 00:90:7a:01:91:c8 attr vlan-name VLAN2
MX20-1# set mac-user 00:90:7a:00:f4:14 attr vlan-name VLAN3
```

If a wireless device is not associated with one of the MAC addresses in the local user database, the last-resort user will be applied and that wireless device will be assigned to VLAN 2 as indicated in the following command.

```
MX20-1# set user last-resort attr vlan-name VLAN2
```

A wireless device that uses 801.1x authentication and provides a user name of “anonymous” will be assigned to VLAN 2 according to the location policy below. This applies to the IP Softphone PC. In a typical deployment, this step is not required since a RADIUS server will usually return a VLAN assignment for all users.

```
MX20-1# set location policy permit vlan VLAN2 if user eq anonymous dap
```

6.

Create the following access lists (in the specified order) to prioritize voice packets, including H.323 call signaling and audio (RTP) packets. In this configuration, the following packets are prioritized:

- Call signaling packets with a DSCP value of 34 (precedence bits set to 4 and TOS bits set to 4) are assigned to Class of Service (COS) 7, the highest priority queue.
- Audio (RTP) packets with a DSCP value of 46 (precedence bits set to 5 and TOS bits set to 12) are assigned to COS 7, the highest priority queue.
- RTP UDP port range 2048 to 65535 is assigned to COS 7. Note that this rule is broad and can prioritize more traffic then the user intended.
- SpectraLink Voice Priority (SVP protocol 119) packets are assigned to COS 5. SVP must be assigned to COS 5.
- All other packets are permitted, but receive best-effort treatment.

Note: QoS is only enforced in the wired-to-wireless direction.

```
MX20-1# set security acl ip voice permit cos 7 ip 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255 precedence 4 tos 4
MX20-1# set security acl ip voice permit cos 7 ip 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255 precedence 5 tos 12
MX20-1# set security acl ip voice permit cos 7 udp 0.0.0.0
```

Step	Description

```
255.255.255.255 0.0.0.0 255.255.255.255 range 2048 65535
MX20-1# set security acl ip voice permit cos 5 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
MX20-1# set security acl ip voice permit 0.0.0.0 255.255.255.255
```

Commit the ACL configuration using the following command:

```
MX20-1# commit security acl voice
```

Enable the *voice* ACL on VLAN 2 in the outgoing direction (i.e., wired to wireless).

```
MX20-1# set security acl map voice vlan VLAN2 out
MX20-1# set security acl map voice vlan VLAN3 out
```

7.

Configure radio profile **avaya** with SSID **avayassid** for encrypted traffic and a WEP key as indicated by **<*wep-key*>**.

```
MX20-1# set radio-profile avaya
MX20-1# set radio-profile avaya crypto-ssid avayassid
MX20-1# set radio-profile avaya wep key-index 1 key <wep-key>
```

8.

Configure the MP-252 access points connected to ports 2 and 3 on the MX-20 using the **set port** and **set ap** commands. This includes setting the MP model, enabling PoE, and selecting the radio type. In the **set ap** command, the channel, transmit power, minimum transmit data rate, and radio profile are configured. In this example, each MP was configured with a different transmit power value, depending on its location. The MP-252 is a dual-radio access point with radio 1 supporting 802.11b/g and radio 2 supporting 802.11a (not shown below). The following commands provide the MPs on ports 2 and 3 with their configuration.

```
MX20-1# set port type ap 2 model mp-252 poe enable radiotype 11b
MX20-1# set ap 2 radio 1 channel 6 tx-power 5 min-tx-datarate 1 radio-
profile avaya mode enable
MX20-1# set port type ap 3 model mp-252 poe enable radiotype 11b
MX20-1# set ap 3 radio 1 channel 11 tx-power 7 min-tx-datarate 1
radio-profile avaya mode enable
```

9.

Enable 802.1x authentication using EAPS-TTLS and WEP encryption. To configure the MX-20 to use a RADIUS server and add the RADIUS server to a server group, use the following commands:

```
MX20-1# set radius server testLab address 10.1.2.80 key <shared-
secret>
MX20-1# set server group testLabGroup members testLab
```

The following commands reduce the amount of time that a wireless user waits to retransmit an EAP request after a failed authentication.

```
MX20-1# set dot1x quiet-period 0
```

Step | **Description**

```
MX20-1# set dot1x tx-period 1
MX20-1# set dot1x max-req 0
```

Add an authentication rule for users. Users are authenticated using EAP-TTLS to communicate with RADIUS server group **testLabGroup**. In the example below, *anonymous* refers to the user name sent by the user in the authentication request.

```
MX20-1# set authentication dot1x anonymous pass-through testLabGroup
```

The following command directs users with any MAC address to be authenticated using the local user database configured in Step 5. The ** indicates the wildcard and matches all MAC addresses.

```
MX20-1# set authentication mac ** local
```

10. Create a 2-port load-sharing group between two 100Mbps Ethernet ports 4 and 5. The VLANs assigned to port 4 in Step 4 need to be cleared before proceeding. During testing, load-sharing groups were not configured simultaneously with STP as shown in Step 11.

```
MX20-1# clear vlan 2 port 4
MX20-1# clear vlan 3 port 4
MX20-1# set port-group name group100 ports 4-5 mode on
MX20-1# set vlan 2 group100 tag 2
MX20-1# set vlan 3 group100 tag 3
```

11. Configure STP on VLANs 2 and 3. Since these VLANs are tagged on these ports, PVST+ is automatically configured. Set the priority of the MX-20 higher than the Alpine 3804 so that the Alpine 3804 becomes the root bridge.

```
MX20-1# set spantree enable vlan 2
MX20-1# set spantree enable vlan 3
MX20-1# set spantree priority 32769 vlan 2
MX20-1# set spantree priority 32769 vlan 3
```

12. Save the configuration.

```
MX20-1# save config
```

The following configuration applies to the MX-20 in VLAN 3 with IP address 10.3.3.150.

Step	Description
1.	To perform initial configuration of the MX-20, set up a serial connection from a PC or laptop. On the PC or laptop, set up a terminal session as follows: ▪ 9600 baud ▪ 8 bits ▪ 1 stop bit ▪ No parity ▪ Hardware flow control *disabled* Log in to the MX-20 command-line interface (CLI). At the CLI prompt, enter the **enable** command to display the prompt for the enabled access level. Initially, no password is required.

2.	Assign a system name, IP address, and default route to the MX-20. The gateway in the default route is the Alpine 3804 Ethernet switch. In addition, configure the country code and timezone on the MX-20. The commands to enable telnet on the MX-20 are also shown below.
	`MX20-2# set system name MX20-2`
	`MX20-2# set system ip-address 10.3.3.150`
	`MX20-2# set ip route default 10.3.3.1 1`
	`MX20-2# set system countrycode US`
	`MX20-2# set timezone EST -5 0`
	`MX20-2# set ip telnet server enable`
	`MX20-2# set user admin password encrypted <password>`
	A Mobility Domain is a collection of MX switches that work together to support a roaming user. A user can roam across the network from one MX switch to another while maintaining the same IP address and session. Each Mobility Domain has one seed member and one or more nonseed members. Refer to the Trapeze Networks documentation for additional information on Mobility Domains. The IP address of the seed member is configured below.
	`MX20-2# set mobility-domain member seed-ip 10.2.2.150`

3.	Enable Power over Ethernet (PoE) on port 1, which connects to an Avaya 4600 Series IP Telephone and two MP-252s. By default, PoE was disabled on all other ports. `MX20-2# set port poe 1 enable`

4.	Configure VLANs 2 and 3 and assign a VLAN name to each one.
	`MX20-2# set vlan 2 name VLAN2`
	`MX20-2# set vlan 3 name VLAN3`
	Assign an IP address to the VLAN 3 interface.

Step	Description

	`MX20-2# set interface 3 ip 10.3.3.150 255.255.255.0`
	Assign each VLAN to the appropriate ports according to the network configuration in **Figure 1**. VLAN 3 is assigned to ports 1 and 6 that connect to an Avaya IP telephone and PC, respectively. Ports 20 and 21 are enabled with 802.1Q trunking and are assigned to VLANs 2 and 3. These 802.1Q trunk links send packets with VLAN tags 2 and 3.
	`MX20-2# set vlan 3 port 1`
	`MX20-2# set vlan 3 port 6`
	`MX20-2# set vlan 2 port 20 tag 2`
	`MX20-2# set vlan 2 port 21 tag 2`
	`MX20-2# set vlan 3 port 20 tag 3`
	`MX20-2# set vlan 3 port 21 tag 3`

5.	The MX-20 is designed to secure network access on a per-user basis. Create a local user database for each authorized wireless device. The MAC addresses in the following example are associated with Avaya 3616/3626 Wireless IP Telephones and an Avaya IP Softphone laptop. The commands below assign each wireless device to either VLAN 2 or 3. In a large WiFi deployment, MAC users would be handled on a RADIUS server.
	`MX20-2# set mac-user 00:40:96:51:84:db attr vlan-name VLAN3`
	`MX20-2# set mac-user 00:90:7a:01:0f:53 attr vlan-name VLAN2`
	`MX20-2# set mac-user 00:90:7a:01:91:c8 attr vlan-name VLAN2`
	`MX20-2# set mac-user 00:90:7a:00:f4:14 attr vlan-name VLAN3`
	If a wireless device is not associated with one of the MAC addresses in the local user database, the *last-resort user* will be applied and that wireless device will be assigned to VLAN 3 as indicated in the following command.
	`MX20-2# set user last-resort attr vlan-name VLAN3`
	A wireless device that uses 802.1x authentication and provides a user name of “anonymous” will be assigned to VLAN 3 according to the location policy below. This applies to the IP Softphone PC. In a typical deployment, this step is not required since a RADIUS server will usually return a VLAN assignment for all users.
	`MX20-2# set location policy permit vlan VLAN3 if user eq anonymous dap`

6.	Create the following access lists (in the specified order) to prioritize voice packets, including H.323 call signaling and audio (RTP) packets. In this configuration, the following packets are prioritized: ▪ Call signaling packets with a DSCP value of 34 (precedence bits set to 4 and TOS bits set to 4) are assigned to Class of Service (COS) 7, the highest priority queue. ▪ Audio (RTP) packets with a DSCP value of 46 (precedence bits set to 5 and TOS

Step	Description

bits set to 12) are assigned to COS 7, the highest priority queue.

- RTP UDP port range 2048 to 65535 is assigned to COS 7. Note that this rule is broad and can prioritize more traffic then the user intended.
- SpectraLink Voice Priority (SVP protocol 119) packets are assigned to COS 5. SVP must be assigned to COS 5.
- All other packets are permitted, but receive best-effort treatment.

Note: QoS is only enforced in the wired-to-wireless direction.

```
MX20-2# set security acl ip voice permit cos 7 ip 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255 precedence 4 tos 4
MX20-2# set security acl ip voice permit cos 7 ip 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255 precedence 5 tos 12
MX20-2# set security acl ip voice permit cos 7 udp 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255 range 2048 65535
MX20-2# set security acl ip voice permit cos 5 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
MX20-2# set security acl ip voice permit 0.0.0.0 255.255.255.255
```

Commit the ACL configuration using the following command:

```
MX20-2# commit security acl voice
```

Enable the *voice* ACL on VLAN 2 in the outgoing direction (i.e., wired to wireless).

```
MX20-2# set security acl map voice vlan VLAN2 out
MX20-2# set security acl map voice vlan VLAN3 out
```

7.

Configure radio profile **avaya** with SSID **avayassid** for encrypted traffic and a WEP key as indicated by **<*wep-key*>**.

```
MX20-2# set radio-profile avaya
MX20-2# set radio-profile avaya crypto-ssid avayassid
MX20-2# set radio-profile avaya wep key-index 1 key <wep-key>
```

8.

Configure the MP-252 connected to port 2 on the MX-20 using the **set port** and **set ap** commands. This includes setting the MP model, enabling PoE, and selecting the radio type. In the **set ap** command, the channel, transmit power, minimum transmit data rate, and radio profile are configured. The MP-252 is a dual-radio access point with radio 1 supporting 802.11b/g and radio 2 supporting 802.11a (not shown below). The following commands provide the MP on port 2 with its configuration.

```
MX20-2# set port type ap 2 model mp-252 poe enable radiotype 11b
MX20-2# set ap 2 radio 1 channel 1 tx-power 5 min-tx-datarate 1 radio-
profile avaya mode enable
```

Step	Description

9.

Enable 802.1x authentication using EAPS-TTLS and WEP encryption. To configure the MX-20 to use a RADIUS server and add the RADIUS server to a server group, use the following commands:

```
MX20-2# set radius server testLab address 10.1.2.80 key <shared-secret>
MX20-2# set server group testLabGroup members testLab
```

The following commands reduce the amount of time that a wireless user waits to retransmit an EAP request after a failed authentication.

```
MX20-2# set dot1x quiet-period 0
MX20-2# set dot1x tx-period 1
MX20-2# set dot1x max-req 0
```

Add an authentication rule for users. Users are authenticated using EAP-TTLS to communicate with RADIUS server group **testLabGroup**. In the example below, *anonymous* refers to the user name sent by the user in the authentication request.

```
MX20-2# set authentication dot1x anonymous pass-through testLabGroup
```

The following command directs users with any MAC address to be authenticated using the local user database configured in Step 5. The ** indicates the wildcard and matches all MAC addresses.

```
MX20-2# set authentication mac ** local
```

10.

Create a 2-port load-sharing group between two Gigabit Ethernet ports 21 and 22. The VLANs assigned to port 21 in Step 4 need to be cleared before proceeding. During testing, load-sharing groups were not configured simultaneously with STP as shown in Step 11.

```
MX20-2# clear vlan 2 port 21
MX20-2# clear vlan 3 port 21
MX20-2# set port-group name group1000 ports 21-22 mode on
MX20-2# set vlan 2 group1000 tag 2
MX20-2# set vlan 3 group1000 tag 3
```

11.

Configure STP on VLANs 2 and 3. Since these VLANs are tagged on these ports, PVST+ is automatically configured. Set the priority of the MX-20 higher than the Alpine 3804 so that the Alpine 3804 becomes the root bridge.

```
MX20-2# set spantree enable vlan 2
MX20-2# set spantree enable vlan 3
MX20-2# set spantree priority 32769 vlan 2
MX20-2# set spantree priority 32769 vlan 3
```

12.

Save the configuration.

```
MX20-2# save config
```

9. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality and performance testing. Feature functionality testing verified the ability of the Trapeze Networks Mobility System to provide network access to the Avaya 3616/3626 Wireless IP Telephones, Avaya IP Softphone, and Avaya Phone Manager Pro. In addition, it was verified that Avaya 4600 Series IP Telephones and PCs could be connected to an Ethernet port on the MX-20. The emphasis of testing was on the QoS implementation in order to achieve good voice quality, Radius authentication, WEP encryption, and seamless roaming at layer-2 and layer-3.

9.1. General Test Approach

All feature functionality test cases were performed manually. The following features and functionality were verified:

- Spanning Tree (802.1D) and Per-VLAN Spanning Tree (PVST)
- Quality of Service (QoS) based on Layer 3 and Layer 4 Application Information, such as IP DSCP Markings, Protocol Type, and UDP Port Range
- 802.1X Security and WEP Encryption
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Roaming
- SpectraLink Voice Protocol (SVP)
- Power over Ethernet

Performance testing was accomplished by running a VoIP test on a traffic generator. The VoIP test generated audio (RTP) packets between two wireless clients and calculated a MOS score to quantify the voice quality. In addition, low-priority traffic was generated while empirically verifying the voice quality on an active wireless call.

9.2. Test Results

All feature functionality and performance test cases passed. The Trapeze Mobility System provided network access to the Avaya wireless IP endpoints using 802.1X Security and WEP Encryption. Good voice quality was achieved on wireless voice calls through the use of the Trapeze Networks QoS implementation. The Trapeze MPs communicated with the wireless devices using 802.11a/b/g.

Note: The Trapeze MX-20 can successfully provide Layer-2 connectivity to Avaya 4600 Series IP Telephones, including PoE. However, QoS is not enforced by the MX-20 for IP telephones connected to an MX-20 Ethernet port. That is, QoS is only enforced in the wired-to-wireless direction, not between wired devices.

10. Verification Steps

This section provides verification steps that may be performed in the field to verify that the wireless IP endpoints have connectivity to the network and that good voice quality is being provided for wireless calls. The following commands are entered on the MX-20 unless otherwise specified.

1. Check that the Avaya wireless IP endpoints have successfully registered with Avaya Communication Manager by typing the **list registered-ip-stations** command on the SAT. A sample output of the command is shown below.

```
list registered-ip-stations
                            REGISTERED IP STATIONS

Station  Set     Product    Prod  Station          Net Orig      Gatekeeper
Ext      Type    ID         Rel   IP Address       Rgn Port      IP Address
50000    4610    IP_Phone   2.100 10.1.2.170       1             10.1.2.7
50003    4620    IP_Soft    5.146 10.2.2.162       1             10.1.2.7
50005    4620    IP_Phone   1.500 10.1.2.19        1             10.1.2.7
```

2. Verify that the Avaya Wireless IP Telephones, IP Softphone, and Phone Manager Pro have connectivity to the wired network through their association with a Trapeze MP. The **show sessions** command displays the wireless devices that are associated with each MP controlled by the MX switch.

```
MX20-1# show sessions

User                         Sess  IP or MAC         VLAN                Port/
Name                           ID  Address           Name                Radio
---------------------------- ----  ----------------- --------------- ---------
00:90:7a:00:f4:14             113* 00:90:7a:00:f4:14 VLAN3                 2/1
00:90:7a:01:0f:53             115* 10.2.2.52         VLAN2                 2/1
00:90:7a:01:91:c8             110* 10.2.2.50         VLAN2                 2/1
anonymous                     109* 10.2.2.162        VLAN2                 2/1

4 sessions total
```

3. Check that the VLAN state and Ethernet port states are *Up* by using the **show vlan config** command. This command also indicates which ports are sending a VLAN tag.

```
MX20-1# show vlan config
                      Admin  VLAN  Tunl                        Port
VLAN Name             Status State Affin Port             Tag   State
---- ---------------- ------ ----- ----- ---------------- ----- -----
   1 default          Up     Down      5
   2 VLAN2            Up     Up        5
                                         1                 none Up
                                         4                    2 Up
                                         6                 none Up
                                         20                   2 Up
   3 VLAN3            Up     Up        5
                                         4                    3 Up
                                         20                   3 Up
```

4. Check the state of the Trapeze MPs connected to the MX-20 with the **show ap status** command. In the following example, two MPs were connected to ports 2 and 3, and only the first radio was enabled.

```
mx1# show ap status

Port: 2, AP model: MP-252, manufacturer: Trapeze, name: MP02
=====================================================
Link:      up, MP port 1
State:     operational, in boot: no
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                 id=0x28b10174b47f1715 ram=33554432 bytes
                 s/n=0333000398 hw_rev=A3
Uptime:    0 hours, 3 minutes, 0 seconds

Radio 1 type: 802.11b, state: configure succeed (Enabled)
      bssid1: 00:0b:0e:00:db:80
      bssid2: 00:0b:0e:00:db:82
Radio 2 type: 802.11a, state: configure succeed (Disabled)
      bssid1: 00:0b:0e:00:db:81
      bssid2: 00:0b:0e:00:db:83


Port: 3, AP model: MP-252, manufacturer: Trapeze, name: MP03
=====================================================
Link:      up, MP port 1
State:     operational, in boot: no
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                 id=0x2a00d510147f1512 ram=33554432 bytes
                 s/n=0333303069 hw_rev=A3
Uptime:    0 hours, 2 minutes, 59 seconds

Radio 1 type: 802.11b, state: configure succeed (Enabled)
      bssid1: 00:0b:0e:00:ee:c0
      bssid2: 00:0b:0e:00:ee:c2
Radio 2 type: 802.11a, state: configure succeed (Disabled)
      bssid1: 00:0b:0e:00:ee:c1
      bssid2: 00:0b:0e:00:ee:c3
```

5. Place a call between two wireless IP endpoints and verify good voice quality in both directions.

6. While there is an active wireless call, verify that packets are being filtered by the security ACLs (“hits”). The counter should increase while a call is active. To count hits for a security ACL, the **hits** option must be specified in the **set security acl** command (e.g., set security acl ip voice permit cos 7 udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 2048 65535 **hits**).

```
MX20-1# show security acl hits
ACL hit-counters

Index Counter              ACL-name
----- -------------------- --------
    0                28917 voice
```

7. Verify the STP configuration and port-state information by using the **show spantree** command.

```
MX20-1# show spantree

VLAN     2
spanning tree mode           PVST+
spanning tree type           IEEE
spanning tree enabled

Designated Root              00-04-96-00-2e-30
Designated Root Priority     32765
Designated Root Path Cost    19
Designated Root Port         4
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-00-2d-a2
Bridge ID Priority           32769
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port               VLAN       Port-State    Cost   Prio   Portfast
------------------------------------------------------------------------------
1                   2        Forwarding      19   128     Disabled
4                   2        Forwarding      19   128     Disabled
6                   2        Forwarding      19   128     Disabled
20                  2        Blocking        19   128     Disabled

VLAN     3
spanning tree mode           PVST+
spanning tree type           IEEE
spanning tree enabled

Designated Root              00-04-96-00-2e-30
Designated Root Priority     32765
Designated Root Path Cost    19
Designated Root Port         4
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-00-2d-a2
Bridge ID Priority           32769
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port               VLAN       Port-State    Cost   Prio   Portfast
------------------------------------------------------------------------------
4                   3        Forwarding      19   128     Disabled
20                  3        Blocking        19   128     Disabled
```

11. Support

For technical support on the Trapeze Mobility System, call the Trapeze Networks Technical Assistance Center (TAC) at (866) TRPZ-TAC or send email to support@trapezenetworks.com.

12. Conclusion

These Application Notes describe the configuration steps required for integrating the Trapeze Networks Mobility System with an Avaya IP Telephony infrastructure. The Trapeze MX-20 and MP-252 interoperated successfully with Avaya Communication Manager, Avaya IP Office, Avaya Voice Priority Processor, Avaya Wireless IP Telephones, Avaya IP Softphone, and Avaya Phone Manager Pro. The Trapeze MX-20 and MP-252 supported 802.11a/b/g Radio Modes, VLAN Tagging, QoS, 802.1x Security, and WEP Encryption. Seamless roaming at Layer-2 and Layer-3 was also verified. The Trapeze solution yielded good voice quality on the wireless IP telephony devices.

13. References

This section references the Avaya and Trapeze Networks product documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 8, June 2004, Document Number 555-233-504.
[2] *Administrator's Guide for Avaya Communication Manager*, Issue 8, June 2004, Document Number 555-233-506.
[3] *Avaya Voice Priority Processor*, Issue 4, May 2004, Document Number 555-301-102.
[4] *IP Office 2.1 Manager*, Issue 15c, May 2004.
[5] *Phone Manager 2.1 Installation & Maintenance*, Issue 1, April 2004.

The following Trapeze Networks product documentation is provided by Trapeze Networks. For additional product and company information, visit http://www.trapezenetworks.com.

[6] *Trapeze Mobility Point Installation Guide*, Part Number: 730-9502-0028, Revision A.
[7] *Trapeze Mobility Exchange Installation and Basic Configuration Guide*, Part Number: 730-9502-0029, Revision A.
[8] *Trapeze Mobility System Software Configuration Guide*, Part Number: 730-9502-0030, Revision A.
[9] *Trapeze System Software Command Reference*, Part Number: 730-9502-0032, Revision A.

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.