Avaya Solution & Interoperability Test Lab

Application Notes for Meru Networks Wireless LAN 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 Meru Networks Wireless LAN System consisting of a Controller managing multiple Access Points. Avaya Wireless IP Telephones, IP Softphone, and Phone Manager Pro gained network access through the Meru Access Points and 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 Meru Access Points. An Extreme Networks Alpine 3804 Ethernet Switch interconnected all of the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with the Avaya wireless IP endpoints. 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 Meru Networks Wireless LAN System consisting of the Controller managing multiple Access Points. The Meru Networks Controller 1100 and Access Point 100 were used for testing. The Meru APs connected the Avaya 3616/3626 Wireless IP Telephones and the mobile laptops running Avaya IP Softphone and Phone Manager Pro to the wired network. The Avaya wireless IP telephones registered with either Avaya Communication Manager or Avaya IP Office, and Avaya IP Softphone and Avaya Phone Manager Pro registered with Avaya Communication Manager and Avaya IP Office, respectively. The Avaya Voice Priority Processor (VPP) was used to support the SpectraLink Voice Priority (SVP) Protocol on the Avaya Wireless IP Telephones and the Meru Access Points. An Extreme Networks Alpine 3804 Ethernet Switch was used to interconnect all of the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with the Avaya wireless IP endpoints.

The compliance testing verified the following features supported by the Meru Wireless LAN System:

- Layer-2 and Layer-3 Connectivity
- 802.1X Security and WEP Encryption
- Quality of Service (QoS) based on Priority Queuing and Reserved Bandwidth
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Seamless Roaming
- SpectraLink Voice Priority (SVP)
- IEEE 802.11b
- Dynamic IP Addressing using DHCP

Figure 1 illustrates the wireless LAN (WLAN) configuration used to verify the Meru Networks solution. All of the wireless IP devices depicted in the configuration roamed between the Meru APs for full mobility. Note that IP addresses for the Meru APs in VLAN 2 are not shown because they communicate with the Meru Controller, in the same subnet, at Layer-2 using MAC addresses only. The Meru AP in VLAN 3 communicates with the Controller at Layer-3 using IP addresses. The configuration also notes the port that connected each network device to the Alpine 3804. 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.

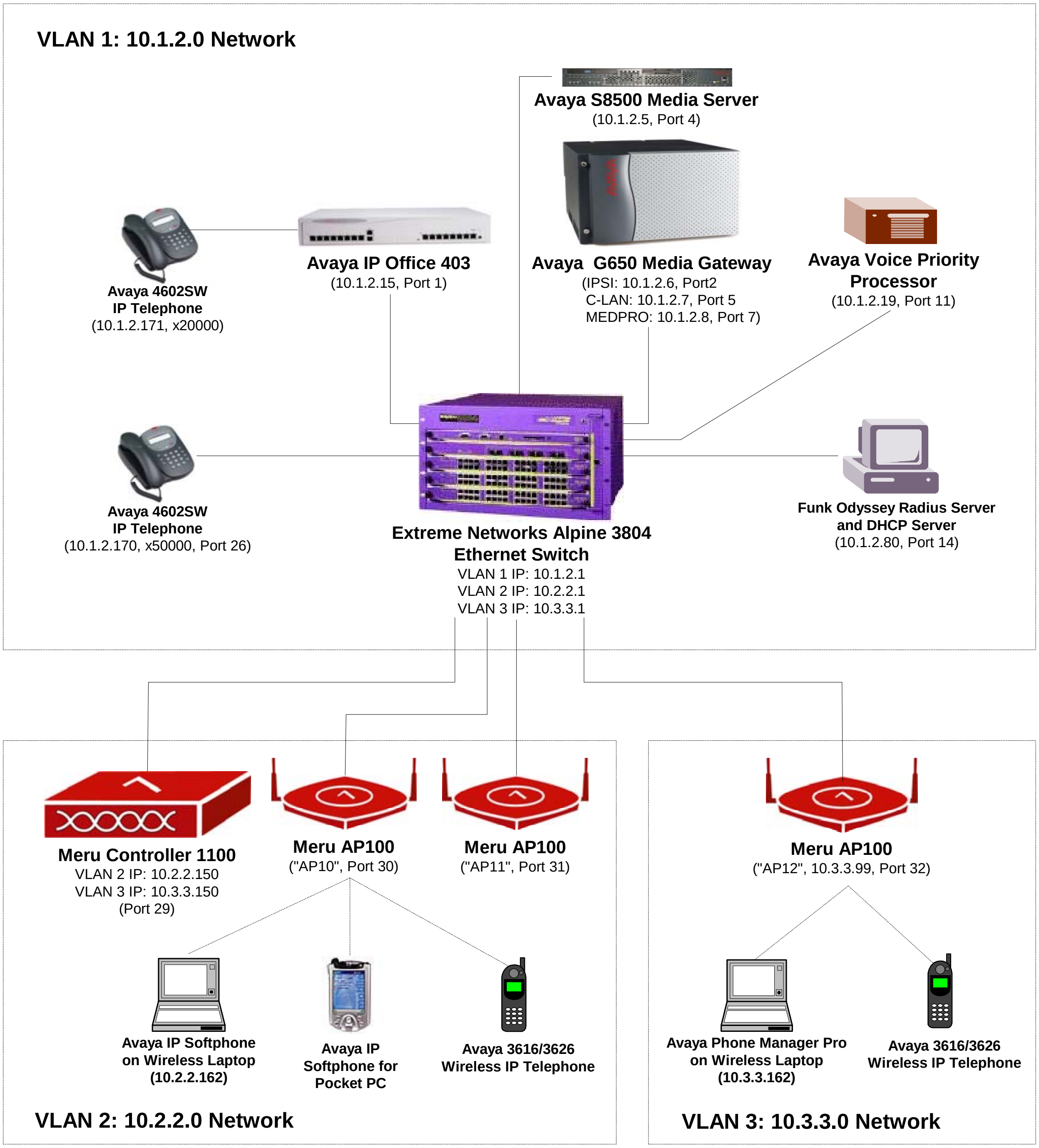


Figure 1: Avaya and Meru Networks Wireless LAN Configuration

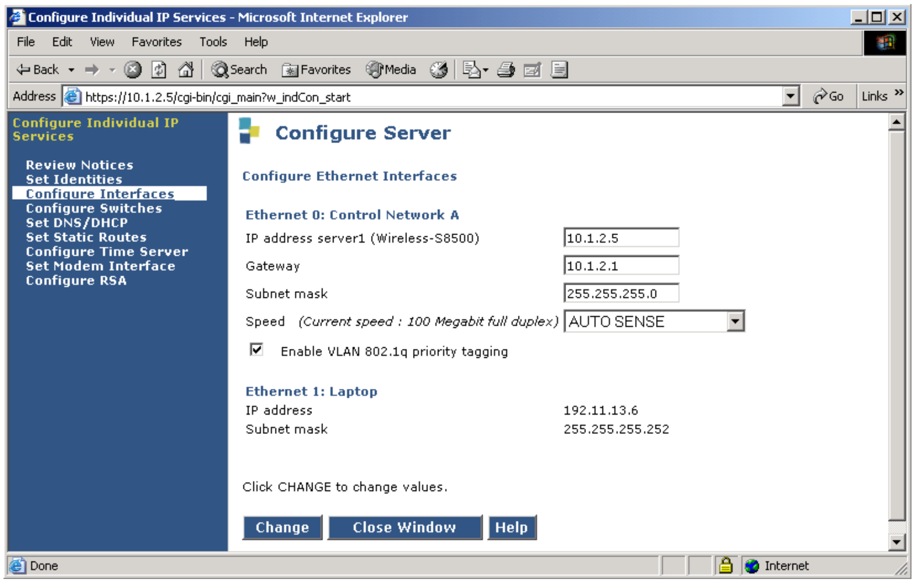
2. Equipment and Software Validated

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
Meru Networks Controller 1100	2.0.2-31-Avaya_Build
Meru Networks Access Point 100	2.0.2-31-Avaya_Build
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.



https://10.1.2.5/cgi-bin/cgi_main?w_indCon_start

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

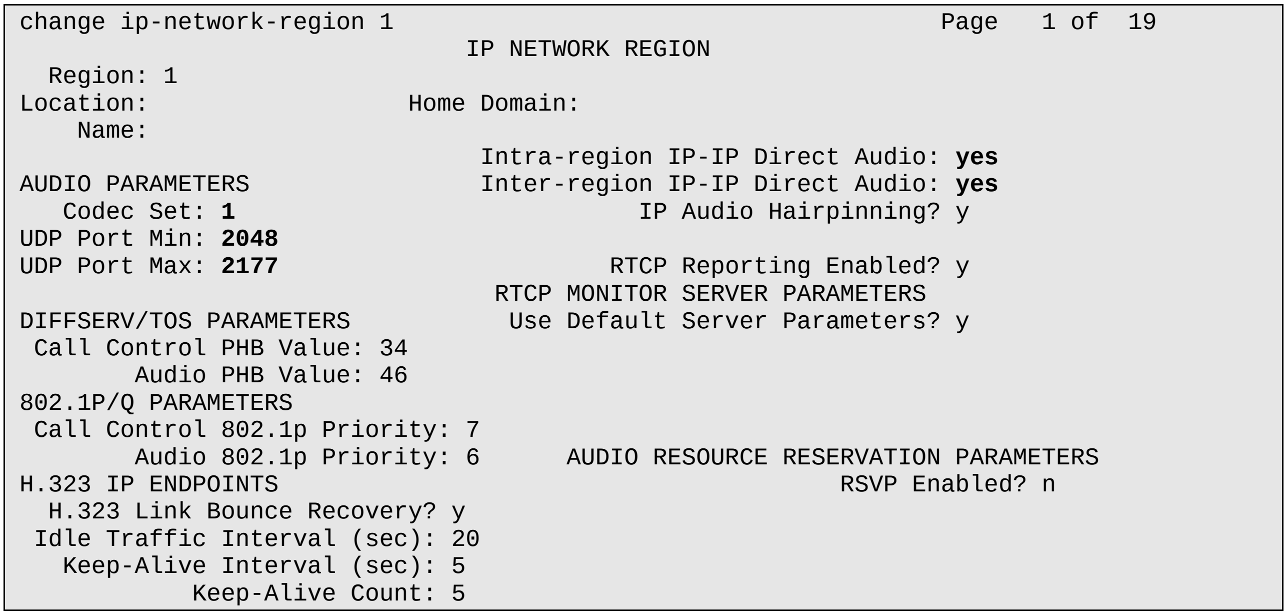
IP address: 192.11.13.6

Subnet mask: 255.255.255.252

Click CHANGE to change values.

Figure 2: Avaya S8500 Media Server – Configure Server Form

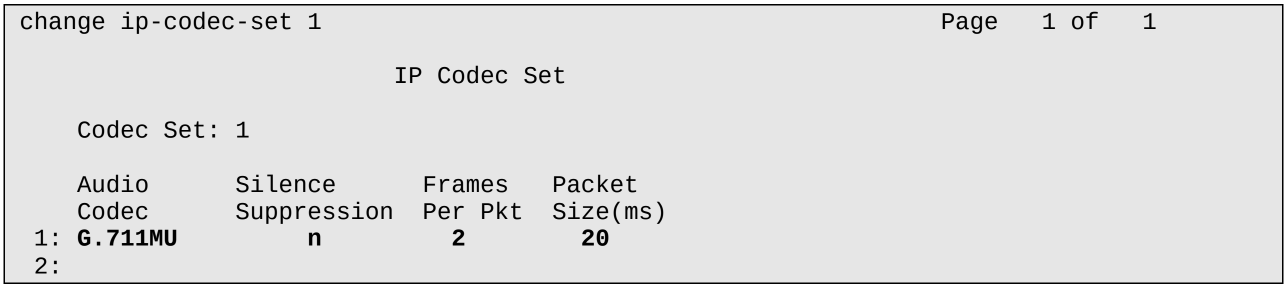
From the System Access Terminal (SAT), enter the **change ip-network-region 1** command to configure the network region that will be assigned to the C-LAN and IP Media Processor (MEDPRO) boards in the G650 Media Gateway and to the wireless IP endpoints. IP Network Region '1' specifies the codec set that 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 the 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: 2177                       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

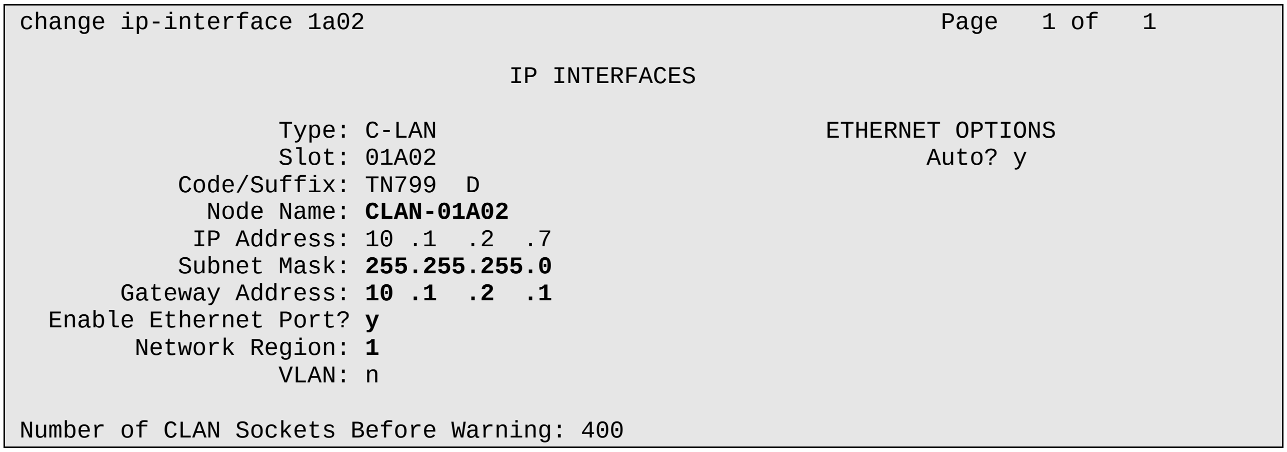
On the **ip-codec-set** form, select the audio codec type to be used by the IP Media Processor and the IP endpoints in network region 1. Note that IP codec set '1' was specified in IP Network Region '1' in **Figure 3**. The form is accessed via the **change ip-codec-set 1** command. The default settings 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

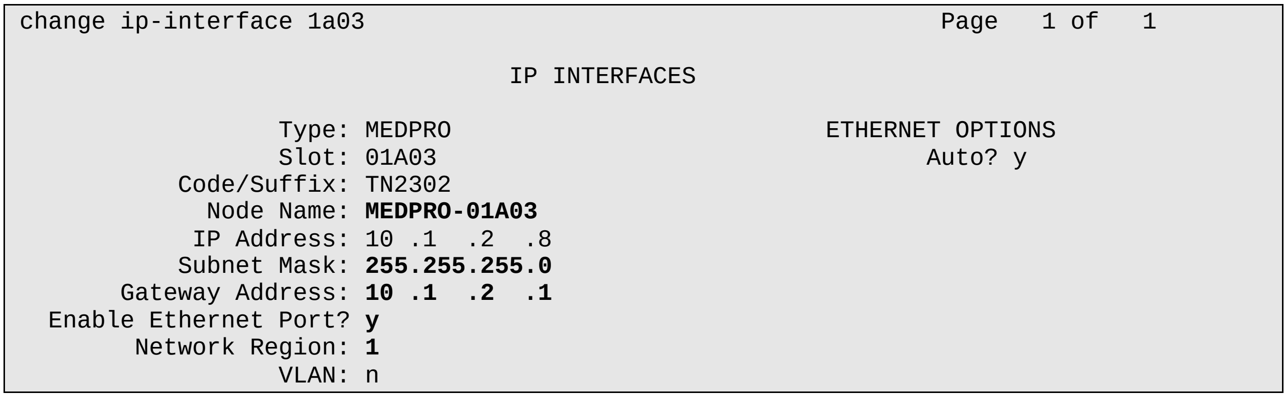
Assign a default gateway and network region to the C-LAN board in location 1a02 via the **change ip-interface 1a02** form. The **Node Name** was mapped to the **IP Address** in the **Node-Names IP** form (not shown here). The default gateway is the Alpine 3804 Ethernet switch (10.1.2.1). The default 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

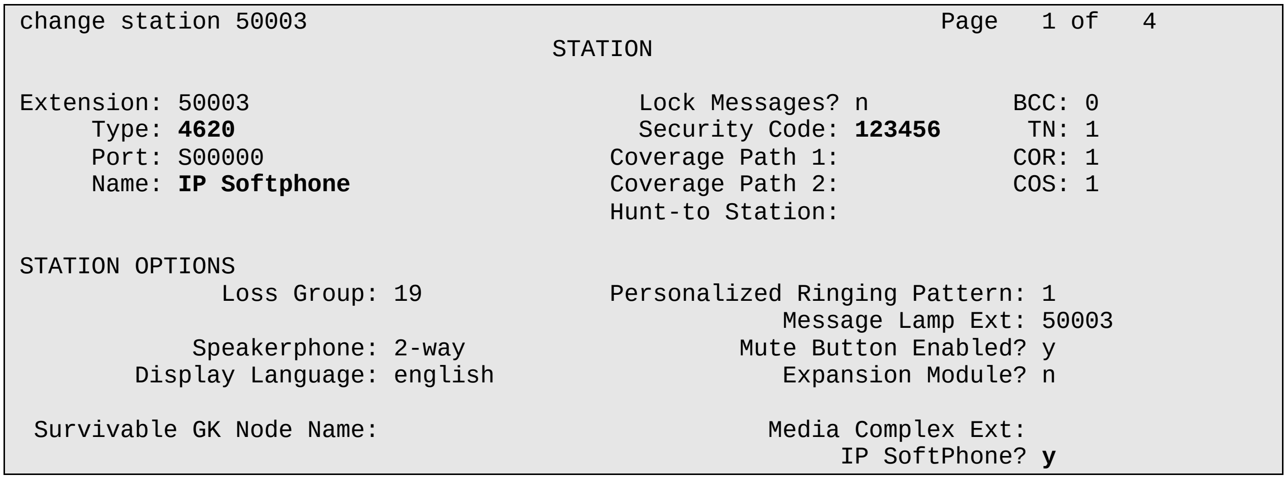
Assign a default gateway and IP network region to the IP Media Processor in location 1a03 via the **change ip-interface 1a03** form. The **Node Name** was mapped to the **IP Address** in the **Node-Names IP** form (not shown here). The default gateway is the Alpine 3804 Ethernet switch (10.1.2.1) and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

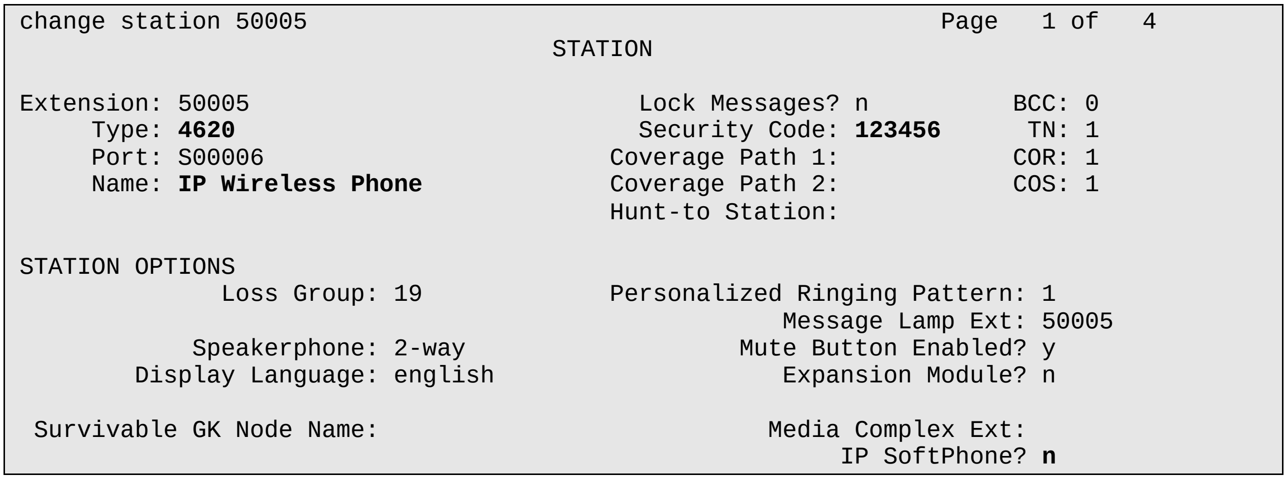
Lastly, configure the stations that correspond to each of the wireless IP endpoints, including the Avaya IP Softphones and the Avaya 3616/3626 Wireless IP Telephones. The station configuration for the IP Softphone is shown in **Figure 7**. Set the **Type** field to *4620*, set the **IP Softphone** field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

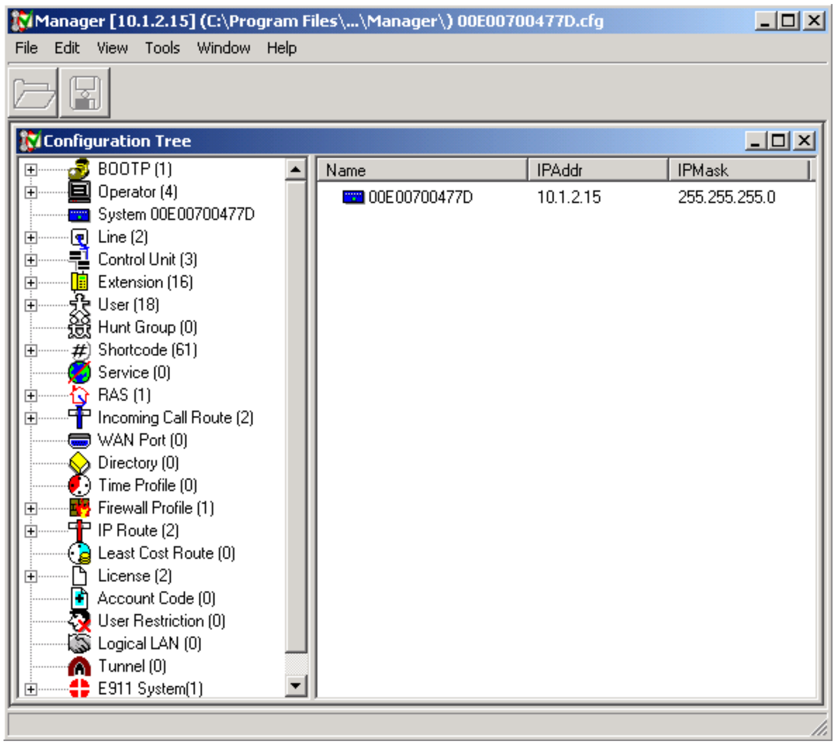
Figure 8: Station Form for the Avaya 3616/3626 Wireless IP Telephones

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 further 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. A feature license that includes *IP-Endpoints* and *Phone Manager Pro* is required in order to use the Avaya Phone Manager Pro application.

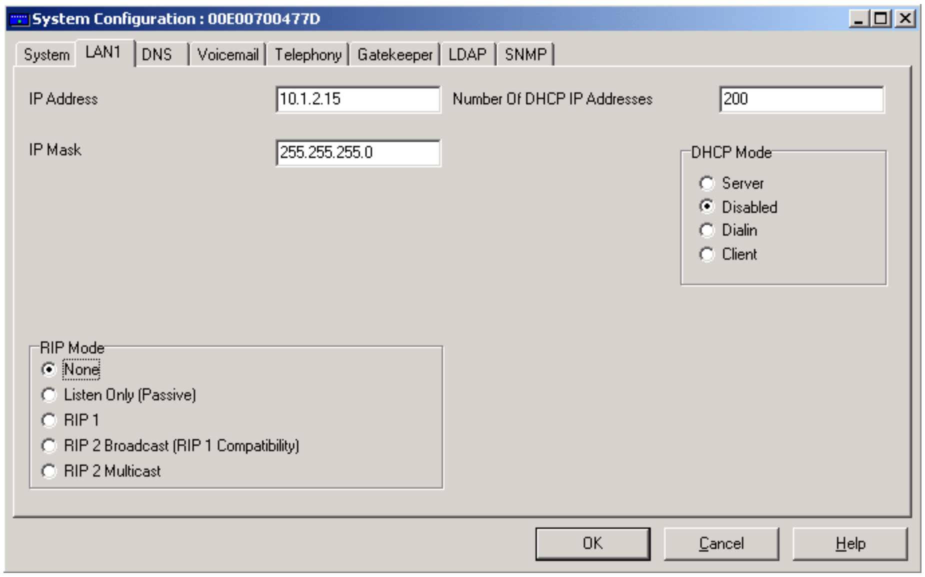
Avaya IP Office was configured using the **Avaya IP Office Manager** application. To configure the Avaya IP Office, open the **Manager** application from a PC with IP connectivity to the IP Office. Initially, the IP Office is assigned IP address 192.168.42.1 with a subnet mask of 255.255.255.0. The **Manager** 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 an 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.



System Configuration : 00E00700477D

IP Address: 10.1.2.15

Number Of DHCP IP Addresses: 200

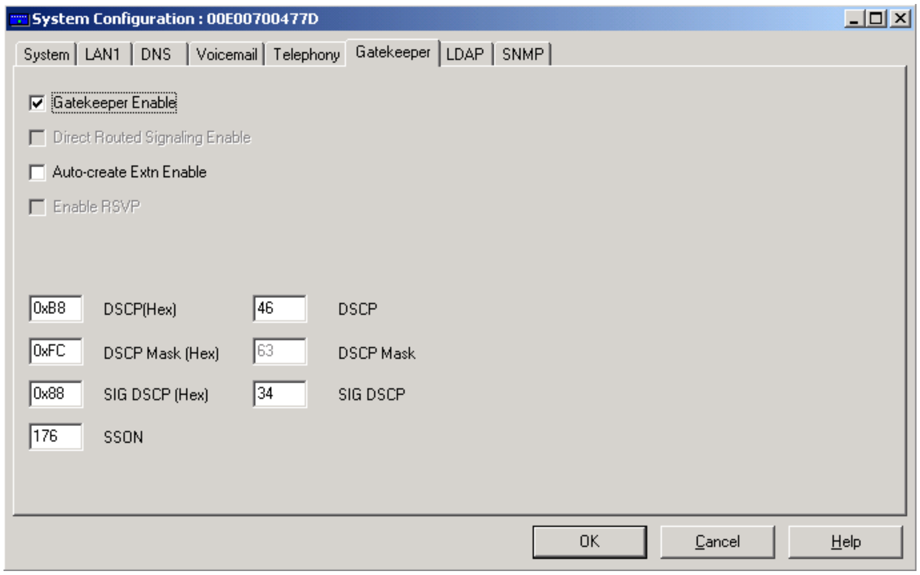
IP Mask: 255.255.255.0

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.



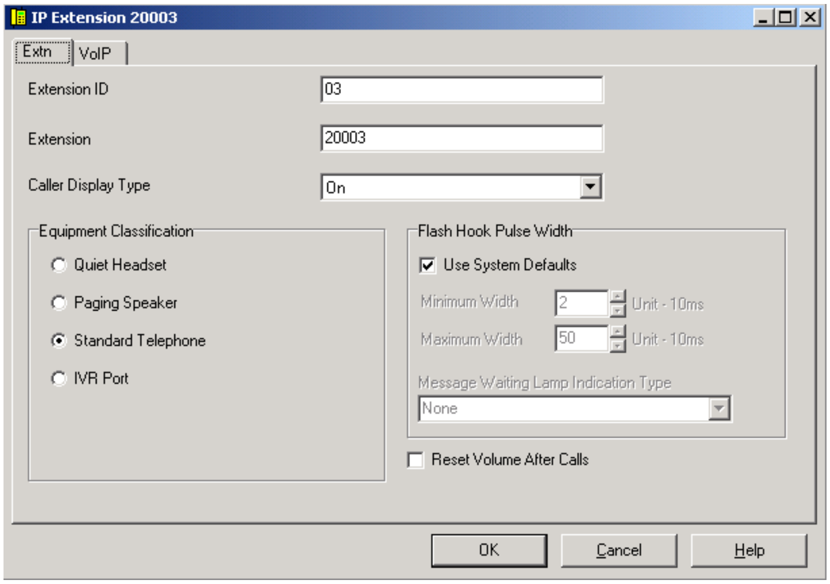
System Configuration : 00E00700477D

- ☑ 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 the 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.



Extension ID: 03

Extension: 20003

Caller Display Type: On

Equipment Classification

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

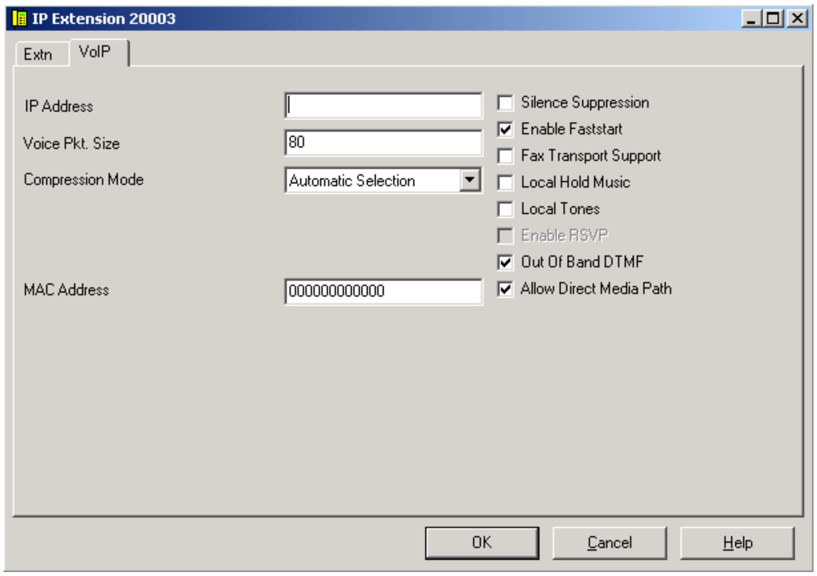
Flash Hook Pulse Width

- ☑ 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

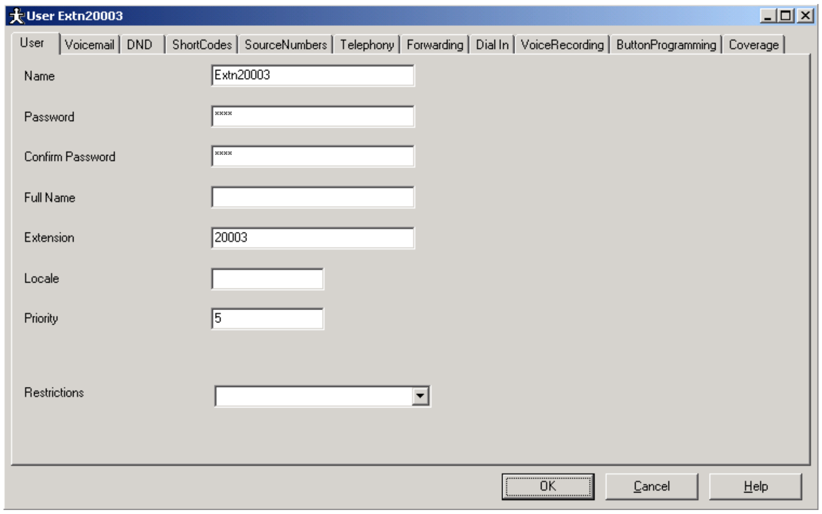
Compression Mode: Automatic Selection

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

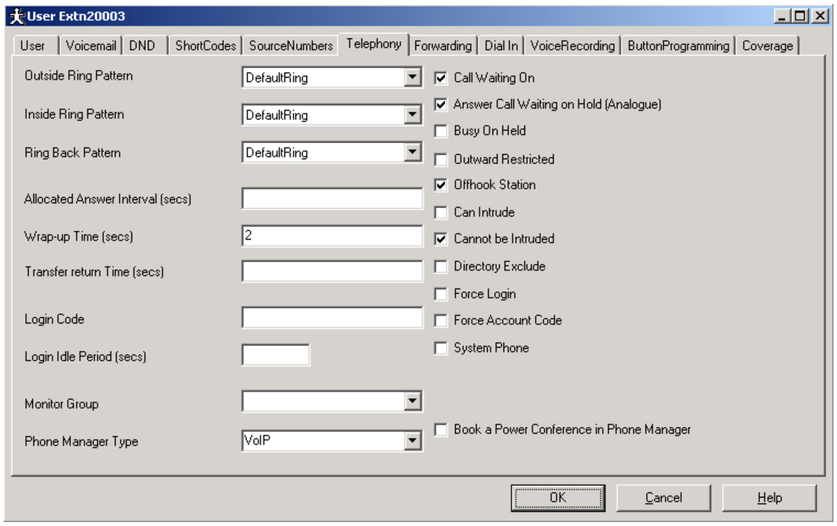
Next, select **User** from the **Manager** main window. On the right pane, use the right-mouse click and select **New** from the pop-up menu to display the **User** window displayed in **Figure 14**. In the **User** tab, specify the endpoint's **Name**, **Password**, and **Extension** as shown in **Figure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

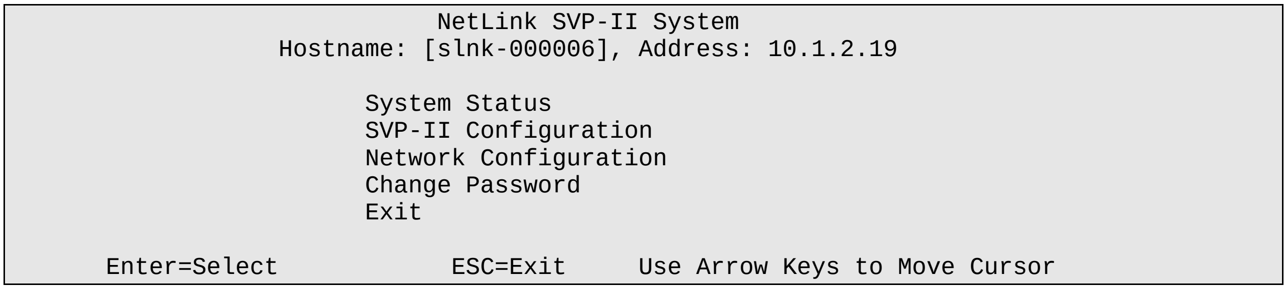
The Avaya Voice Priority Processor (VPP) utilizes SpectraLink Voice Priority (SVP) as the Quality of Service (QoS) mechanism supported by the Avaya 3616/3626 Wireless IP Telephones and the Meru Access Point 100 to reduce jitter and delay for voice traffic over the wireless network.

The Avaya VPP performs three 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. Secondly, SVP allows the Meru Access Points 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 delay for the voice packets. Lastly, 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

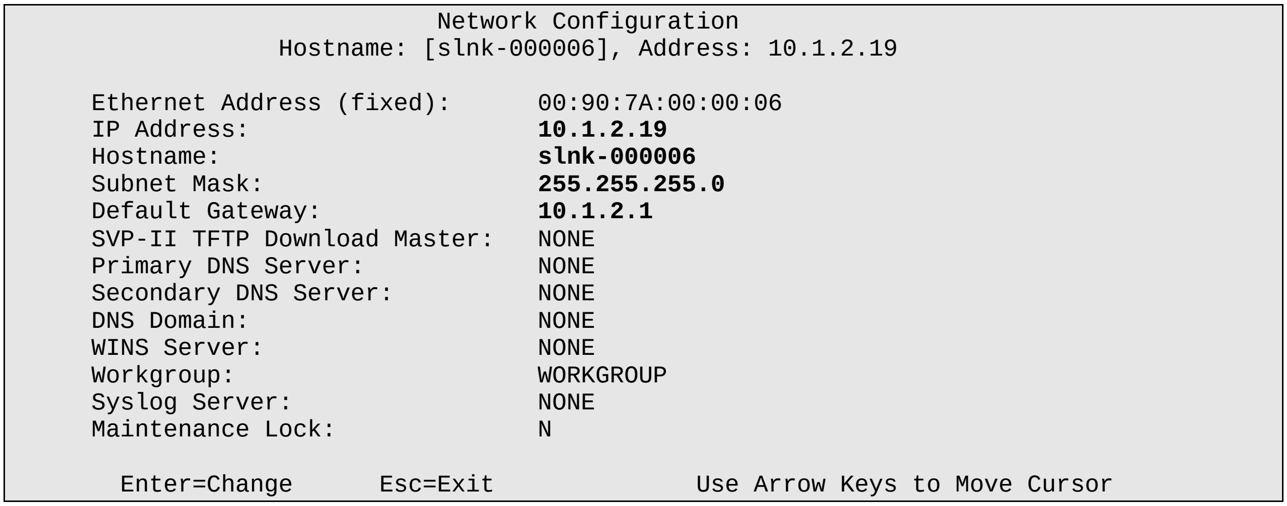
Once connected, the Avaya VPP login screen is presented. Log in as *admin*. The **Avaya VPP System Menu** is displayed as shown in **Figure 16**. After configuring an IP address for the Avaya VPP, a Telnet session may be used to modify the Avaya VPP configuration.



```
                              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: Avaya VPP System Menu

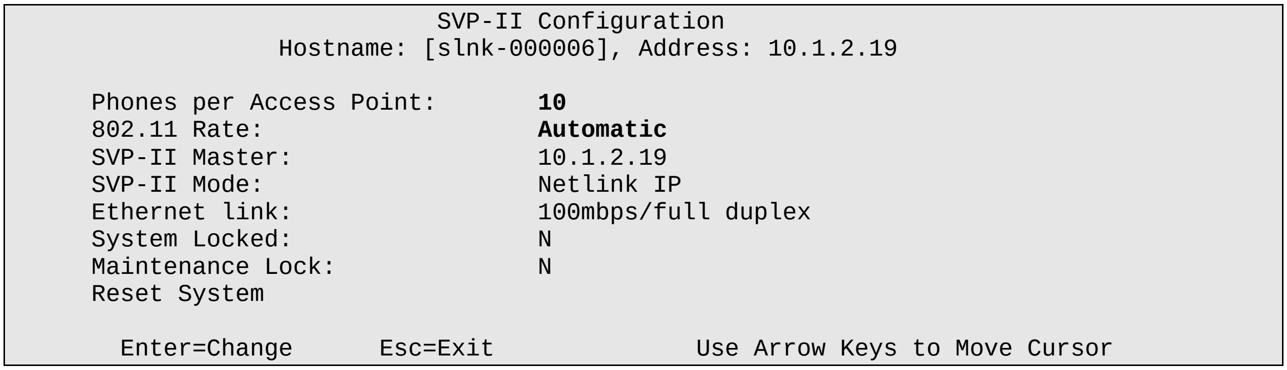
From the **AVPP System Menu**, select **Network Configuration** to configure the IP address, subnet mask, and default gateway of the AVPP.



```
                              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 **Avaya VPP 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** of the Avaya VPP was configured to *Automatic*, as shown **Figure 18**, to allow the wireless telephones to determine the rate (up to 11Mbps), as opposed to the Avaya VPP limiting the transmission rate of the wireless telephones to 1/2 Mbps. As mentioned in Section 8, the Meru Access Points are configured in Virtual AP mode which means that the Avaya VPP views all of the access points as one. Therefore, the **Phones per Access Point** field should specify the maximum number of calls supported by the entire system of Access Points.



```
                              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 Meru Networks Controller and Access Points. Specifically, the configuration related to VLANs 2 and 3, and the Ethernet ports used by the Meru Controller and Access Points 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.	Associate Ethernet ports with VLANs 2 and 3. VLAN 3 was assigned to port 29 as tagged to enable 802.1Q trunking to the Meru Controller.
	`Alpine3804# configure vlan vlan2 add port 1:29-1:31 untagged`
	`Alpine3804# configure vlan vlan3 add port 1:29 tagged`
	`Alpine3804# configure vlan vlan3 add port 1:32 untagged`

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

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

7. Configure the DHCP Server

The Avaya Wireless IP Telephones, the laptops running IP Softphone and Phone Manager Pro, and the Meru Access Points obtained their IP configuration, Avaya VPP IP address (Option 151), and Option 176 settings from a DHCP server. The DHCP server was configured with two scopes that served wireless IP endpoints that register with either Avaya Communication Manager or Avaya IP Office. IP endpoints registered with IP Office were in ESSID *meruipo*, VLAN 3, and they received their IP configuration from the Avaya IP Office scope. 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 Meru Controller and Access Points

This section covers the configuration of the Meru Controller and Access Points. Configuration was performed on the Controller, which serves as the central control point for the Access Points. The Meru Access Points communicate with the Meru Controller through tunneled communications and download their configuration from the Controller during startup. In this configuration, the Meru Access Points were configured in Virtual AP mode with all of the Access Points using the same channel. These are default settings. This allows the system to perform seamless client handoffs between Access Points without the client devices needing to perform an 802.11 or 802.1X re-association procedure to the new Access Point. When utilizing Virtual Mode, the AVPP will recognize all of the Access Points as one. SpectraLink Voice Priority (SVP) was enabled on each Access Point.

Note: Initially, the Meru APs are configured while they are in the same Ethernet segment (i.e., subnet/VLAN) as the Meru Controller. This applies only to the configuration performed in Step 3. After the APs are configured, they can be moved to a different subnet/VLAN. This was the case for AP 12 in the configuration.

Step	Description
1.	To perform the initial configuration of the Meru Controller, set up a serial connection from a PC or laptop. On the PC or laptop, set up a terminal session as follows: ▪ 115200 baud ▪ 8 bits ▪ no parity ▪ 1 stop bit Log in as *admin* to access the Meru command-line interface (CLI). The CLI prompt displayed depends on the hostname of the Controller. At the CLI prompt, type **configure terminal** to enter configuration mode. After assigning an IP address to the Controller in the step below, a telnet session may be used to access the CLI of the Controller.

2.	Assign a host name, IP address, and default gateway to the Controller. The default gateway is the Alpine 3804 Ethernet switch. In addition, specify the IP address of the DHCP server. This enables DHCP relay on the Controller to allow dynamic IP addressing for the wireless IP endpoints. The Controller does not get its IP address from the DHCP server.
	`MC1100# configure terminal`
	`MC1100(config)# hostname MC1100`
	`MC1100(config)# ip address 10.2.2.150 255.255.255.0`
	`MC1100(config)# ip default-gateway 10.2.2.1`
	`MC1100(config)# ip dhcp-server 10.1.2.80`

3.	Configure the three APs in the WLAN configuration depicted in **Figure 1**. Since AP 10 and AP 11 are in the same subnet with the Meru Controller, they are configured for

Layer 2 connectivity, which allows the AP to discover the Controller. AP 10 and AP 11 communicate with the Controller using MAC addresses only. AP 12 is in a different subnet than the Meru Controller so it is configured for Layer 3 connectivity, which requires the Controller IP address to be specified. AP 12 was configured while it was on the same subnet/VLAN as the Meru Controller and then moved to VLAN 3 as shown in **Figure 1**. Dynamic IP addressing is enabled on AP 10 and 11. SpectraLink Voice Priority (SVP) Protocol is enabled on each AP.

```
MC1100(config)# ap 10
MC1100(config)# description AP-10
MC1100(config-ap)# boot-script svp.scr
MC1100(config-ap)# connectivity l2-preferred
MC1100(config-ap-connectivity)# ip address dhcp
MC1100(config-ap-connectivity)# end

MC1100(config)# ap 11
MC1100(config)# description AP-11
MC1100(config-ap)# boot-script svp.scr
MC1100(config-ap)# connectivity l2-preferred
MC1100(config-ap-connectivity)# ip address dhcp
MC1100(config-ap-connectivity)# end

MC1100(config)# ap 12
MC1100(config)# description AP-12
MC1100(config-ap)# boot-script svp.scr
MC1100(config-ap)# connectivity l3-preferred
MC1100(config-ap-connectivity)# ip address 10.3.3.99 255.255.255.0
MC1100(config-ap-connectivity)# ip default-gateway 10.3.3.1
MC1100(config-ap-connectivity)# controller ip 10.2.2.150
MC1100(config-ap-connectivity)# end
```

4. The wireless IP endpoints that register with Avaya IP Office are assigned to VLAN 3. Create a VLAN named *vlan3* with a tag of ‘3’. Assign an IP address, default gateway, and DHCP server to the VLAN interface. VLANs, when used in conjunction with multiple ESSIDs, allow multiple wireless networks to be supported on a single access point. This enables 802.1Q trunking on the Meru Controller for VLAN 3 only. In this configuration, VLAN 3 was mapped to ESSID *meruipo*, configured in Step 8.

```
MC1100(config)# vlan vlan3 tag 3
MC1100(config-vlan)# ip address 10.3.3.150 255.255.255.0
MC1100(config-vlan)# ip default-gateway 10.3.3.1
MC1100(config-vlan)# ip dhcp-server 10.1.2.80
MC1100(config-vlan)# exit
```

5. To require the wireless IP endpoints to use either 802.1X security or WEP encryption, create a security profile that will be assigned to the ESSIDs in Step 8. Security profile *Funk1x* was configured to support 802.1X authentication with a primary RADIUS server address of 10.1.2.80, primary RADIUS port of 1812, and a primary RADIUS secret of *secure-secret*. 802.1X authentication was enabled on the wireless laptops running Avaya IP Softphone and Avaya Phone Manager Pro.

```
MC1100(config)# security-profile Funk1x
MC1100(config-security)# allowed-l2-modes 802.1x
MC1100(config-security)# radius-server primary ip-address 10.1.2.80
MC1100(config-security)# radius-server primary key <secure-secret>
MC1100(config-security)# radius-server primary port 1812
MC1100(config-security)# radius-server primary enable
```

Furthermore, this security profile was also configured to support WEP encryption with a static 64-bit WEP key defined as *wep-key*. It allowed an 802.1X rekey period of 600 seconds. WEP encryption was enabled on the Avaya 3616/3626 IP Wireless Telephones.

```
MC1100(config-security)# allowed-l2-modes wep
MC1100(config-security)# encryption-modes wep64
MC1100(config-security)# static-wep key <wep-key>
MC1100(config-security)# static-wep privacy auto
MC1100(config-security)# rekey period 600
MC1100(config-security)# exit
```

Note: Configuration of the Funk Odyssey RADIUS server and client are beyond the scope of these Application Notes. Refer to the RADIUS server documentation for details.

6. Configure QoS rules to allow the Meru APs to prioritize VoIP signaling and media packets. QoS rules can be configured to provide priority-based or reserved QoS. QoS is applied with reserved traffic being allocated the first portion of the total bandwidth, followed by each priority level, and finally by the best-effort (default) traffic class. For priority-based QoS, one of eight levels of priority may be specified in the rule using the **priority** command. For reserved QoS, the average packet rate and the token bucket rate parameters may be specified. For G.711mu-law with a packet rate of 20ms, the average packet rate is set to 50 and the token bucket rate is set to 10000 kbps.

Prioritize H.323 call control signaling packets, which use TCP port 1720, and assign them to the highest priority of 8. In the examples below, the TCP protocol is denoted by ‘6’. The following QoS rules will prioritize TCP packets with a source or destination port of 1720.

```
MC1100(config)# qosrule 1 netprotocol 6 qosprotocol none
MC1100(config-qosrule)# dstport 1720
MC1100(config-qosrule)# srcport 0
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# priority 8
MC1100(config)# exit

MC1100(config)# qosrule 2 netprotocol 6 qosprotocol none
MC1100(config-qosrule)# dstport 0
MC1100(config-qosrule)# srcport 1720
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# priority 8
```

```
MC1100(config)# exit
```

Prioritize H.323 RAS packets, which use UDP port 1719, and assign them to the highest priority of 8. In the examples below, the UDP protocol is denoted by ‘17’. The following QoS rules will prioritize UDP packets with a source or destination port of 1719.

```
MC1100(config)# qosrule 3 netprotocol 17 qosprotocol none
MC1100(config-qosrule)# dstport 1719
MC1100(config-qosrule)# srcport 0
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# priority 8
MC1100(config)# exit
```

```
MC1100(config)# qosrule 4 netprotocol 17 qosprotocol none
MC1100(config-qosrule)# dstport 0
MC1100(config-qosrule)# srcport 1719
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# priority 8
MC1100(config)# exit
```

Prioritize audio packets sent or received by the Avaya Wireless IP Telephones. These audio packets are identified by the SVP protocol, which is denoted by ‘119’ below. Use reserved QoS and configure the **avgpacketrate** and **tokenbucketrate** as shown below. The following QoS rules will reserve bandwidth for each G.711 traffic flow that is carrying voice traffic within an SVP packet.

```
MC1100(config)# qosrule 5 netprotocol 119 qosprotocol none
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy head
MC1100(config-qosrule)# avgpacketrate 50
MC1100(config-qosrule)# tokenbucketrate 10000
MC1100(config)# exit
```

Prioritize audio (RTP) packets carried in a UDP packet. This can be done in a couple of ways. The Meru APs can prioritize UDP packets with port numbers within a specific range or prioritize UDP packets sent or received by a device with a specific IP address. Both methods, illustrated below, were used by the Meru APs to prioritize voice packets from an Avaya IP Softphone or an Avaya Phone Manager Pro. These audio packets are not identified by the QoS rules configured above.

The following QoS rules reserve bandwidth for traffic flows that use UDP port 2048 as the source or destination port. Note that the UDP port range can be configured in the IP network region form of Avaya Communication Manager or in the **Advanced** tab of the **Login Settings** of Avaya IP Softphone. Each UDP port needs to be configured separately on the Meru Controller or Meru Networks can provide a utility script that will configure QoS rules for a UDP port range in a single step.

```
MC1100(config)# qosrule 6 netprotocol 17 qosprotocol none
MC1100(config-qosrule)# dstport 2048
MC1100(config-qosrule)# srcport 0
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# avgpacketrate 50
MC1100(config-qosrule)# tokenbucketrate 10000
MC1100(config-qosrule)# exit

MC1100(config)# qosrule 7 netprotocol 17 qosprotocol none
MC1100(config-qosrule)# dstport 0
MC1100(config-qosrule)# srcport 2048
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# avgpacketrate 50
MC1100(config-qosrule)# tokenbucketrate 10000
MC1100(config-qosrule)# exit
```

The following QoS rules reserve bandwidth for traffic flows whose source or destination IP address matches the configured IP address in the QoS rule.

```
MC1100(config)# qosrule 8 netprotocol 17 qosprotocol none
MC1100(config-qosrule)# dstip 10.3.3.162
MC1100(config-qosrule)# dstmask 255.255.255.0
MC1100(config-qosrule)# srcip 0.0.0.0
MC1100(config-qosrule)# srcmask 0.0.0.0
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# avgpacketrate 50
MC1100(config-qosrule)# tokenbucketrate 10000
MC1100(config-qosrule)# exit

MC1100(config)# qosrule 9 netprotocol 17 qosprotocol none
MC1100(config-qosrule)# dstip 0.0.0.0
MC1100(config-qosrule)# dstmask 0.0.0.0
MC1100(config-qosrule)# srcip 10.3.3.162
MC1100(config-qosrule)# srcmask 255.255.255.0
MC1100(config-qosrule)# action forward
MC1100(config-qosrule)# droppolicy tail
MC1100(config-qosrule)# avgpacketrate 50
MC1100(config-qosrule)# tokenbucketrate 10000
MC1100(config-qosrule)# exit
```

7. MAC filtering is a method of controlling WLAN access by denying access based on specific MAC addresses. In the following example, the MAC address corresponds to a wireless telephone. To add a MAC address to the deny access control list, type the following:

```
MC1100(config)# access-list deny 00:90:7a:01:0f:53
```

Next, enable the state of MAC filtering so that the deny list is enabled. The deny list is enabled as follows:

```
MC1100(config)# access-list deny on
```

8. Wireless IP endpoints that register with the S8500 Media Server and the IP Office were assigned to ESSIDs *meruacm* and *meruipo*, respectively. By default, all of the discovered access points are associated with each ESSID. The **ess-ap** <*ap-id*> commands can be used to manually associate an AP with an ESSID.

Create ESSID *meruipo* and assign security profile *Funk1x* and VLAN 3 to this ESSID. By assigning VLAN 3 to this ESSID, wireless IP endpoints in ESSID *meruipo* will obtain their IP configuration from a specific scope in the DHCP server.

```
MC1100(config)# essid meruipo
MC1100(config-essid)# security-profile Funk1x
MC1100(config-essid)# vlan vlan3
MC1100(config-essid)# ap-discovery join-virtual-ap
MC1100(config-essid)# exit
```

Create ESSID *meruacm* and assign security profile *Funk1x* to this ESSID. Wireless IP endpoints that register with the S8500 Media Server will be assigned to ESSID *meruacm*.

```
MC1100(config)# essid meruacm
MC1100(config-essid)# security-profile Funk1x
MC1100(config-essid)# ap-discovery join-virtual-ap
MC1100(config-essid)# exit
```

9. After making the configuration changes, save the changes using the following command:

```
MC1100# copy running-config startup-config
```

10. Some configuration commands require a Controller reboot for the changes to take effect. To manually reboot the Controller and its associated Access Points, use the following command:

```
MC1100# reload all
```

9. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and performance testing. Feature functionality testing verified the ability of the Meru Networks Wireless LAN System to provide network access to the Avaya 3616/3626 Wireless IP Telephones, Avaya IP Softphone, Avaya Phone Manager Pro, and other wireless clients. 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:

- Layer-2 and Layer-3 Connectivity
- 802.1X Security and WEP Encryption
- Quality of Service (QoS) based on Priority Queuing and Reserved Bandwidth
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Seamless Roaming
- SpectraLink Voice Priority (SVP)
- IEEE 802.11b
- Dynamic IP Addressing using DHCP

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, serviceability, and performance test cases passed. The Meru Controller and APs provide 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 Meru Networks QoS implementation. The Meru APs communicated with the wireless devices using 802.11b.

10. Verification Steps

This section provides the 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 on wireless calls.

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 its association with a Meru AP. At the Controller CLI, type the **show station** command to see the stations associated with each Meru AP as shown in the figure below. This command also indicates whether or not the station is authenticated or using WEP encryption.

```
MC1100# show station
Station Table

MAC Address        Availability  Client IP   Address Type  AP Name  L2 Mode  L3 Mode
Authenticated User Name

00:20:a6:4f:08:72  Online        10.2.2.162  Dynamic       AP-10    802.1x   Idle
anonymous
00:90:7a:01:0f:53  Online        10.3.3.50   Dynamic       AP-10    wep      Idle
00:90:7a:01:91:c8  Online        10.2.2.52   Dynamic       AP-10    wep      Idle
```

3. Verify that the Meru APs are recognized by the Meru Controller by typing the **show ap** command in the Controller CLI. This command displays high-level information about all APs currently in the system as shown in the figure below.

```
MC1100# show ap
AP Table

AP ID AP Name     Serial Number      Op State  Avail    Runtime   Connectivity Layer

10    AP-10       00:0c:e6:00:06:61  Enabled   Online   2.0.2-31  L2
11    AP-11       00:0c:e6:00:06:9b  Enabled   Online   2.0.2-31  L2
12    AP-12       00:0c:e6:00:05:df  Enabled   Online   2.0.2-31  L3
```

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

5. While there is an active wireless call, enter the **show qosflows** command in the Controller CLI to display all active QoS flows as shown in the screen below. If no entries are displayed, this indicates that QoS is not being applied to any active calls. The following example displays an active QoS flow between an Avaya Wireless IP Telephone and the Avaya VPP.

```
MC1100# show qosflows
Qos Flows

ID    Source IP    Source   Destination IP  Dest  Prot  Token Average Status
                   Port                     Port        BRate BRate

100   10.2.2.52    0       10.1.2.19        0     udp   10000 50      Active
101   10.1.2.19    0       10.2.2.52        0     udp   10000 50      Active
100   10.2.2.52    0       10.1.2.19        0     119
101   10.1.2.19    0       10.2.2.52        0     119
```

11. Support

For technical support on the Meru Networks Wireless LAN System, contact Meru Technical Assistance Center at support@merunetworks.com or at 888-MERU-WLAN.

12. Conclusion

These Application Notes describe the configuration steps required for integrating the Meru Networks Wireless LAN System with an Avaya IP Telephony infrastructure. The Meru Controller 1100 and Access Point 100 interoperated successfully with Avaya Communication Manager, Avaya IP Office, Avaya Voice Priority Processor, Avaya Wireless IP Telephones, and Avaya IP Softphone/Phone Manager Pro. The Meru Controller and APs supported 802.11b Radio Mode, VLAN Tagging, QoS, and 802.1X Security as well as WEP Encryption. Seamless roaming at Layer-2 and Layer-3 was also verified. The Meru solution yielded good voice quality on the wireless IP endpoints.

13. References

This section references the Avaya and Meru 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 Meru Networks product documentation is provided by Meru Networks. For additional product and company information, visit http://www.merunetworks.com.

[6] *Meru Access Point 100 Installation Guide*, Release 2.0.x, Document Number 880-00011-0003.

[7] *Meru Controller 1100 Installation Guide*, Release 2.0.x, Document Number 880-00012-0003.

[8] *Meru Wireless LAN System Configuration Guide*, Release 2.0.x, Document Number 880-00013-0004.

[9] *Meru Wireless LAN System Command Reference*, Release 2.0.x, Document Number 880-00014-0004.

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.