Avaya Solution & Interoperability Test Lab

Application Notes for Meru Networks Wireless LAN System with the Avaya IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless voice communication over an Avaya IP Telephony infrastructure using the Meru Networks Wireless LAN System consisting of the Controller 1100 and the Access Point 201 (AP201). The AP201 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 was used to support SpectraLink Voice Priority (SVP) on the Avaya Wireless IP Telephones and the Meru Access Points. An Extreme Networks Alpine 3804 Switch interconnected all the network devices. Emphasis of the testing was placed on verifying quality voice communication for 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 communication over an Avaya IP Telephony infrastructure using the Meru Networks Wireless LAN System consisting of the Controller 1100 and the Access Point 201 (AP201). The AP201 provided network access to the Avaya 3616/3626 Wireless IP Telephones and mobile laptops running Avaya IP Softphone and Avaya Phone Manager Pro. These Avaya wireless IP endpoints registered with either Avaya Communication Manager or Avaya IP Office. The Avaya Voice Priority Processor was used to support SpectraLink Voice Priority (SVP) on the Avaya Wireless IP Telephones and the Meru Access Points. An Extreme Networks Alpine 3804 Switch interconnected all the network devices. Emphasis of the testing was placed on verifying quality voice communication for 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 802.11a/b/g Radio Modes
- Dynamic IP Addressing using DHCP

Figure 1 illustrates the network configuration used to verify the Meru Networks wireless network solution. The Meru Controller and Access Points (APs) are physically connected to standard layer-2 or layer-3 Ethernet Switches, such as the Extreme Networks Alpine 3804 in this configuration. The Meru APs communicate with the Meru Controller, which serves as the central control point for the Meru APs. All of the wireless IP devices depicted in the configuration roamed between the Meru APs for full mobility. Although the Meru APs in VLAN 2 are assigned an IP address via DHCP, 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 ports that connected each network device to the Alpine 3804.

Note: In this configuration, there is an H.323 IP trunk between the Avaya IP Office and the Avaya S8500 Media Server with an Avaya 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 and Avaya IP Office documentation for details.

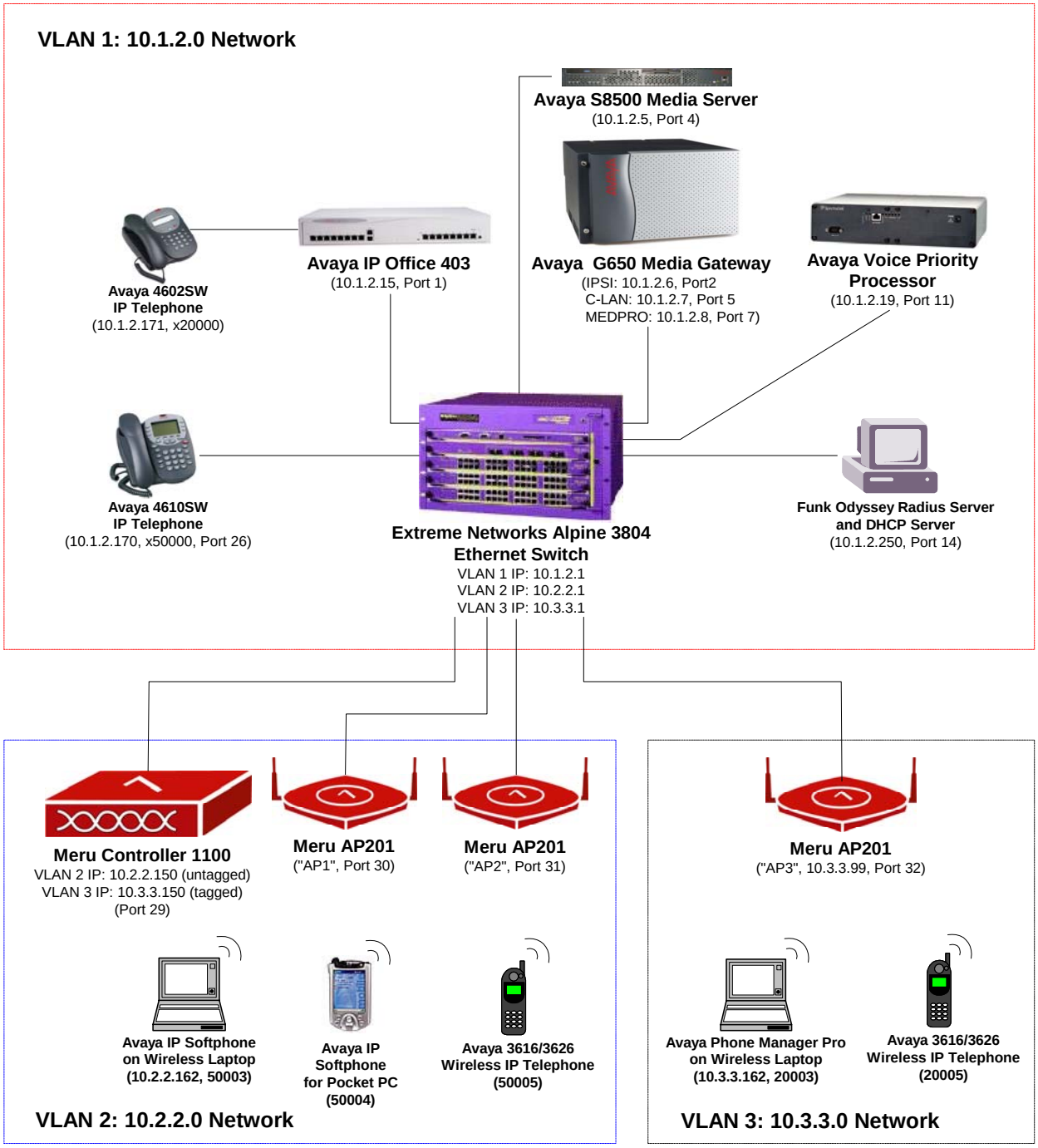

Figure 1: Avaya and Meru Networks Wireless LAN Configuration

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 2.2 (R012x.02.0.111.4)
Avaya IP Office 403	2.1.27
Avaya Voice Priority Processor	33/02
Avaya 4600 Series IP Telephones	2.130 (4610SW), 1.8 (4602SW)
Avaya 3616/3626 IP Wireless Telephones	96.036
Avaya IP Softphone	5.1
Avaya IP Softphone for Pocket PC	2.3
Avaya Phone Manager Pro	2.1.7
Extreme Networks Alpine 3804 Switch	7.2.0 Build 25
Meru Networks Controller 1100	3.0.1.2-1
Meru Networks Access Point 201	3.0.1.2-1
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.

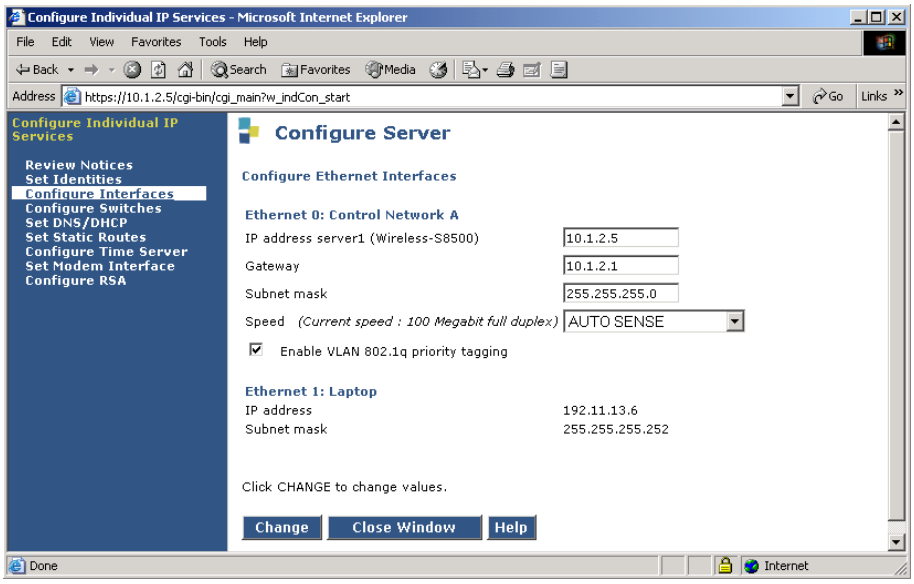

Figure 2: Avaya S8500 Media Server – Configure Server Form

On 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 **Figure 5** and **Figure 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 (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 (10.1.2.1) and it allows VoIP media (RTP) packets to be routed to the IP endpoints in the other VLANs. 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: 4606                         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

 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. The feature license is maintained on a security dongle connected to a USB or parallel port on the PC running **Avaya IP Office Manager**.

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.

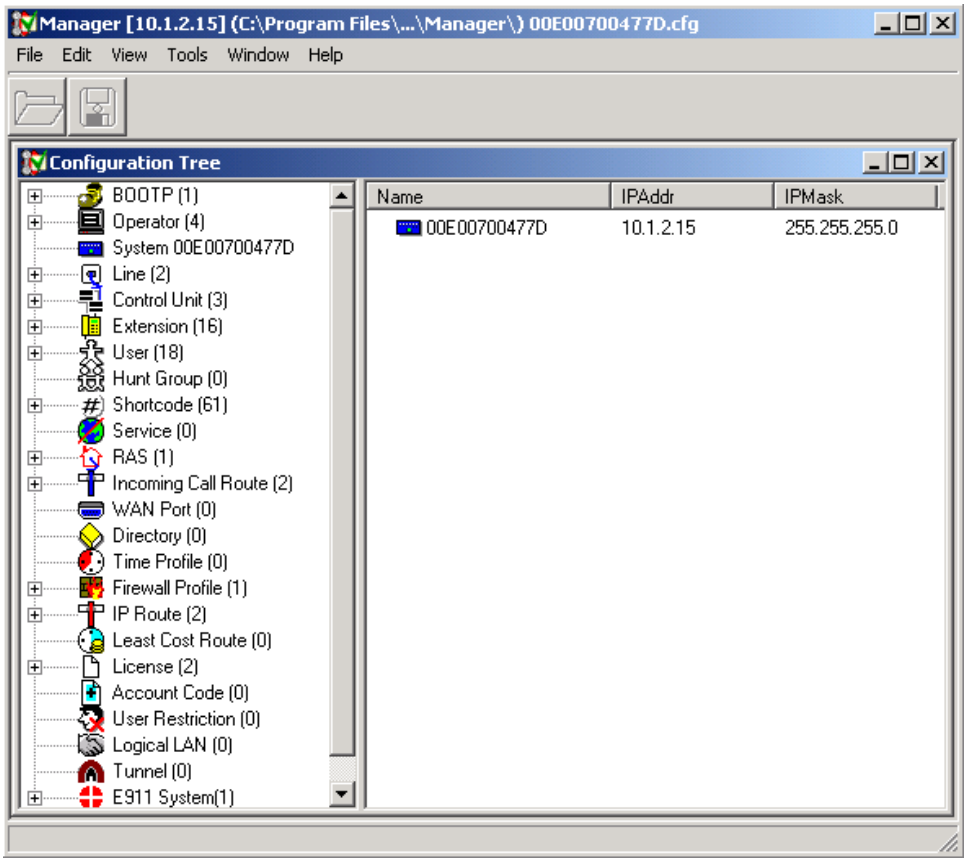

Figure 9: Manager Main Window

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.

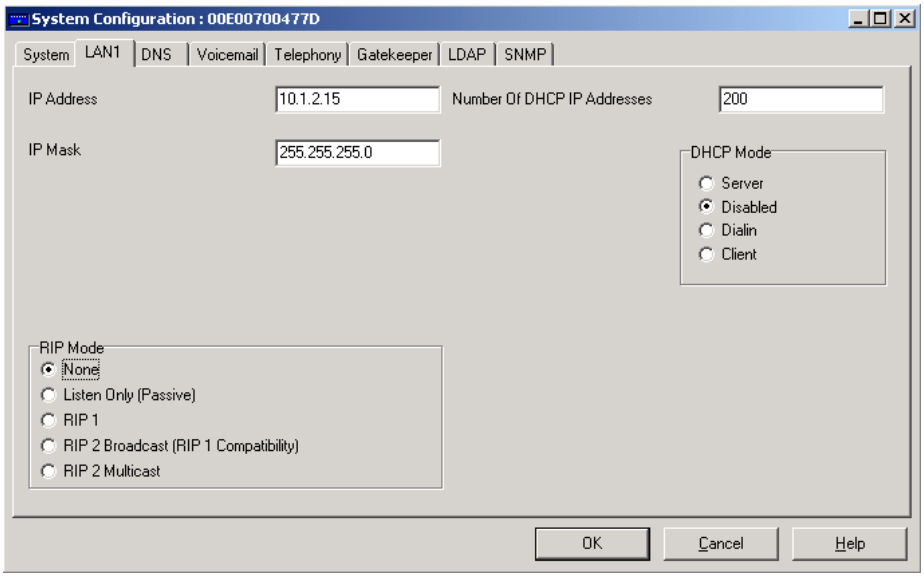

Figure 10: System Configuration – LAN1 Tab

In the **Gatekeeper** tab, select the **Gatekeeper Enable** checkbox to allow H.323 IP endpoints to register with IP Office and adjust the DSCP values according to the QoS settings.

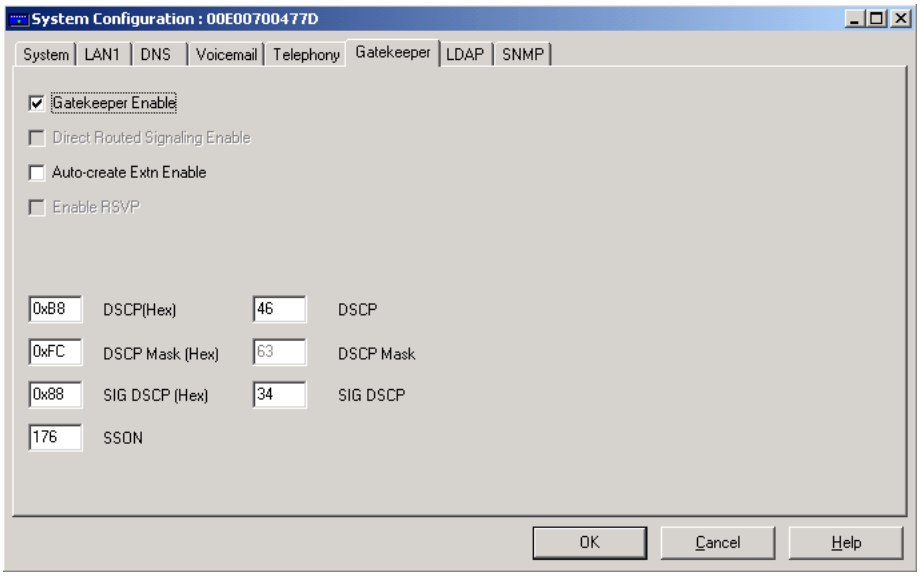

Figure 11: System Configuration - Gatekeeper Tab

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 **Figure 12** and **Figure 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.

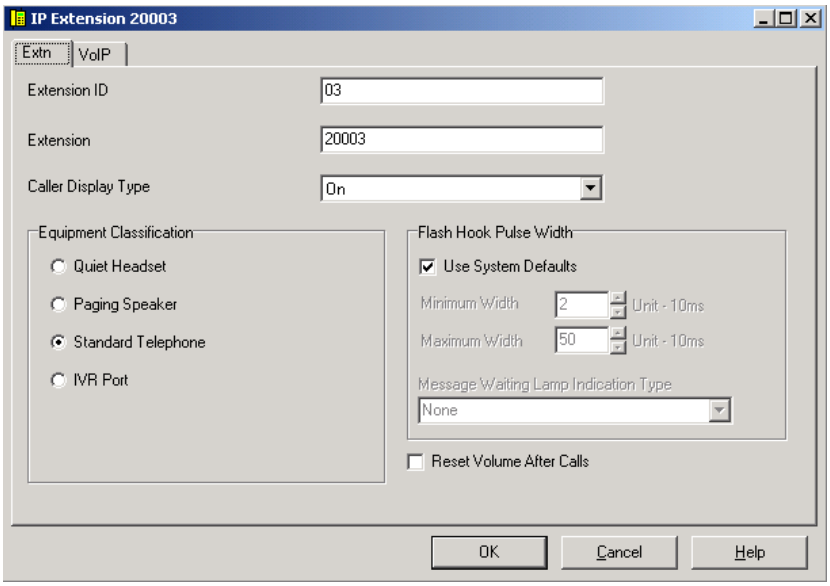

Figure 12: IP Extension – Extn Tab

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

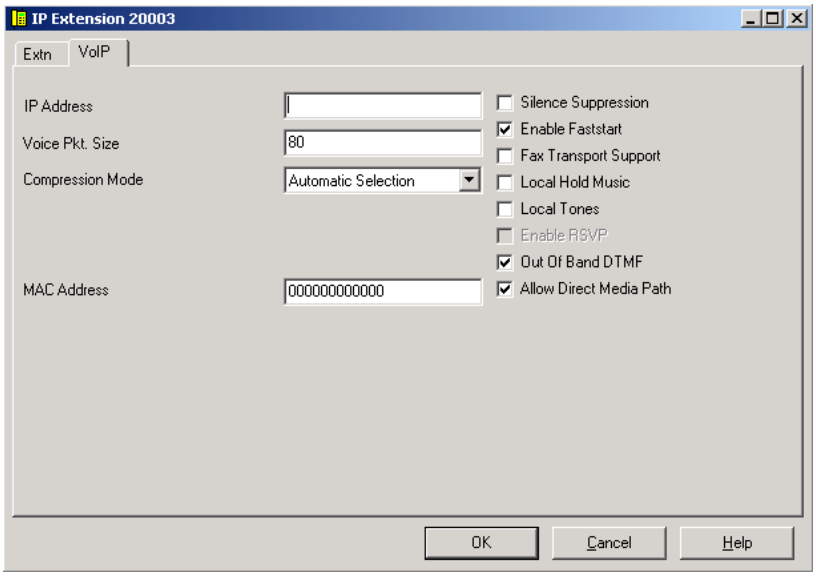

Figure 13: IP Extension – VoIP Tab

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**.

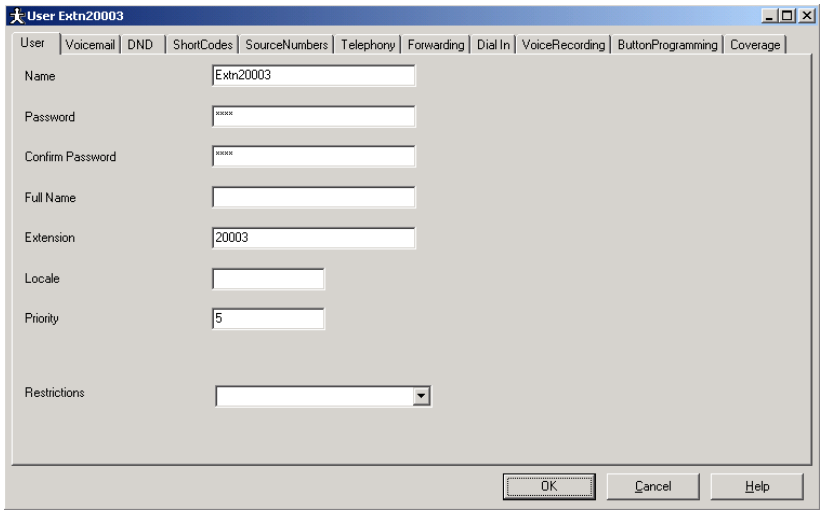

Figure 14: User – User Tab

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

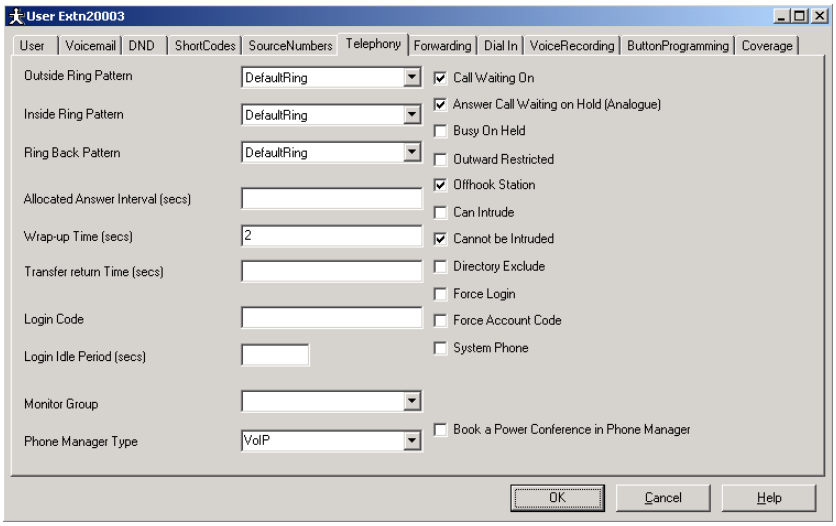

Figure 15: User – Telephony Tab

5. Configure the Avaya Voice Priority Processor

The Avaya Voice Priority Processor 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 201 to enhance voice quality over the wireless network.

The Avaya Voice Priority Processor performs four major functions. First, it is a required component to utilize 11Mbps maximum transmission speed available in the Avaya 3616/3626 Wireless Telephones that support 802.11b. Second, it controls the maximum number of calls supported per access point. Third, SVP allows the Meru AP201 and the Avaya 3616/3626 Wireless IP Telephones to transmit their voice packets immediately, while other wireless 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 Voice Priority Processor is required to serve as a "gateway" between the Avaya Wireless IP Telephones and Avaya Communication Manager and Avaya IP Office. Since the Avaya wireless telephones support SVP, their packets are directed to the Avaya Voice Priority Processor so that the SVP header information can be removed before the packets are forward to the Avaya call server.

To configure the Avaya Voice Priority Processor, connect a PC or laptop to the serial port of the Avaya Voice Priority Processor. 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 Voice Priority Processor login screen is presented. Log in as *admin*. The **Avaya Voice Priority Processor System Menu** is displayed as shown in **Figure 16**. After configuring an IP address for the Avaya Voice Priority Processor, 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: Avaya Voice Priority Processor System Menu

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

```
                          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 Voice Priority Processor 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 Voice Priority Processor was configured to *Automatic*, as shown in **Figure 18**, to allow the wireless telephones to determine the rate (up to 11Mbps), as opposed to the Avaya Voice Priority Processor limiting the transmission rate of the wireless telephones to 1 or 2 Mbps. Since the Meru Access Points were configured in non-virtual AP mode, as opposed to virtual AP mode where all of the Meru APs are viewed by the Avaya Voice Priority Processor as one, the **Phones per Access Point** field specifies the maximum number of calls supported by each Meru AP. 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, if it's 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:       5
     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 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 10.1.2.250`

8.	Save the configuration changes using the following command: `Alpine3804# save configuration`

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 Voice Priority Processor 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 registered 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 H.323 = MCIPADD=10.1.2.7,MCPORT=1719

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 H.323 = MCIPADD=10.1.2.15,MCPORT=1719
```

Note: In the DHCP server, option 151 should be added with a data type of *IP Address* and option 176 should be added with a data type of *String*.

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 non-virtual AP mode. If virtual AP mode were used, the Avaya Voice Priority Processor would recognize all of the Meru Access Points in the wireless network as a single access point. In this case, the total number of calls across all the Meru Access Points would not be able to exceed the value in the **Phones per Access Point** field on the Avaya Voice Priority Processor. The Avaya Voice Priority Processor would also allow each access point to support the configured number of calls, which could result in the access point being oversubscribed. SpectraLink Voice Priority (SVP) support was enabled on each Access Point by default.

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 3 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. Connect to the Controller using the serial port. 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.
	`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`

3.	Configure the three APs in the WLAN configuration depicted in **Figure 1**. By default, since AP 1 and AP 2 are in the same subnet with the Meru Controller, they are

Step	Description

	configured for Layer 2 connectivity, which allows the AP to discover the Controller. No additional configuration beyond the default configuration is required for APs 1 and 2. AP 3 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 3 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**. By default, SpectraLink Voice Priority (SVP) Protocol is enabled on the APs.
	
	`MC1100(config)# ap 3`
	`MC1100(config)# description AP-3`
	`MC1100(config-ap)# connectivity l3-preferred`
	`MC1100(config-ap-connectivity)# controller ip 10.2.2.150`
	`MC1100(config-ap-connectivity)# ip address dhcp`
	`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 enable DHCP pass-through for 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 7.
	`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-passthrough`
	`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 7. Security profile *Funk1x* was configured to support 802.1X authentication with a primary RADIUS server address of 10.1.2.250, 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 10.1.2.250`
	`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.

Step	Description
	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. In this configuration, the following packet types are prioritized: ▪ H.323 Signaling Packets using TCP port 1720 ▪ H.323 RAS Packets using UDP port 1719 ▪ H.323 Audio (RTP) Packets using UDP port numbers configured in the network region form of Avaya Communication Manager ▪ SpectraLink Voice Priority Packets (by default, these packets are prioritized, no additional configuration is required) 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. The drop policy specifies whether to drop the entry at the head or tail of the list. 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**

Step	Description
	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. As mentioned earlier, this SVP QoS rule is configured by default. 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 13400** MC1100(config)# **exit** Prioritize audio (RTP) packets according to the UDP port number. This method was used by the Meru APs to prioritize voice packets from an Avaya IP Softphone and Avaya Phone Manager Pro. These audio packets are not identified by the QoS rules configured above because they do not use the SpectraLink Voice Priority Protocol. The following QoS rules reserve bandwidth for traffic flows that use UDP port 2048 as the 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 Technical Support can provide a utility script that can configure QoS rules for a UDP port range in a single step. The following is an

Step	Description

	example of a QoS rule.
	
	`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`

7.	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 VLAN 3 scope in the DHCP server. By default, ESSID is configured in non-virtual AP mode.
	
	`MC1100(config)# essid meruipo`
	`MC1100(config-essid)# security-profile Funk1x`
	`MC1100(config-essid)# vlan support configured-vlan-only`
	`MC1100(config-essid)# vlan name vlan3`
	`MC1100(config-essid)# no 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*. By default, ESSID is configured in non-virtual AP mode.
	
	`MC1100(config)# essid meruacm`
	`MC1100(config-essid)# security-profile Funk1x`
	`MC1100(config-essid)# no ap-discovery join-virtual-ap`
	`MC1100(config-essid)# exit`

8.	The AP201 contains a single radio that supports 802.11a, 802.11b, 802.11g, and 802.11b/g. To configure the radio mode and the frequency channel, use the following commands:
	
	`MC1100(config)# interface Dot11Radio 1 1`
	`MC1100(config-if-802)# rf-mode 802.11bg`
	`MC1100(config-if-802)# channel 11`
	`MC1100(config-if-802)# exit`
	
	The **show interfaces Dot11Radio 1 1** command may be used to view the wireless interface configuration.

Step	Description
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 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, and Avaya Phone Manager Pro. 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 802.11a/b/g Radio Modes
- 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. The mobile laptops running Avaya IP Softphone and Phone Manager Pro used 802.1X Security and the Avaya 3616/3626 Wireless IP Telephones used 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 802.11a/b/g.

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. Note that the wireless telephones have the same IP address assigned to the Avaya Voice Priority Processor.

```
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   2.130 10.1.2.170      1             10.1.2.7
50001    4606    IP_Phone   1.500 10.1.2.19       1             10.1.2.7
50003    4620    IP_Soft    5.146 10.2.2.162      1             10.1.2.7
50005    4606    IP_Phone   1.500 10.1.2.19       1             10.1.2.7
50006    4606    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 below. This command also indicates whether or not the station is authenticated or using WEP encryption.

```
MC1100# show station

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

00:40:96:a5:af:eb Online        10.2.2.162  Dynamic          AP-3     802.1x   clear
anonymous                0
00:90:7a:01:0f:53 Online        10.2.2.58   DHCP             AP-1     wep      clear
0
00:90:7a:01:2e:bc Online        10.3.3.50   DHCP             AP-3     wep      clear
3
00:90:7a:01:92:ea Online        10.2.2.54   DHCP             AP-1     wep      clear
0
        Station Table(4 entries)
```

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 below.

```
MC1100# show ap
```

```
AP ID  AP Name  Serial Number      Op State  Availibility   Runtime     Connectivity
AP Model AP Type

1      AP-1     00:0c:e6:00:27:0a  Enabled   Online         3.0.1.2-1   L2
AP201    Local
2      AP-2     00:0c:e6:00:1e:6e  Enabled   Online         3.0.1.2-1   L2
AP201    Local
3      AP-3     00:0c:e6:00:1e:2b  Enabled   Online         3.0.1.2-1   L3
AP201    Local
        AP Table(3 entries)
```

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 call. The following example displays an active QoS flow between an Avaya Wireless IP Telephone and the Avaya IP Softphone.

```
MC1100# show qosflows
Qos Flows

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

104   10.1.2.19        0     10.2.2.54        0     119
101   10.1.2.19        10126 10.2.2.162       2048  17
103   10.2.2.54        0     10.1.2.19        0     119
```

11. Support

For technical support on the Meru Networks Wireless LAN System, contact Meru Technical Support via email at support@merunetworks.com or call 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 201 were successfully integrated 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 802.11a/b/g radio modes, 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 9.1, January 2005, Document Number 555-233-504.
[2] *Administrator's Guide for Avaya Communication Manager*, Issue 9, January 2005, Document Number 555-233-506.
[3] *Avaya Voice Priority Processor*, Issue 4, May 2004, Document Number 555-301-102.
[4] *Avaya 3616/3626 Wireless IP Telephone Installation and Configuration Guide*, Issue 3, May 2004, Document Number 555-301-107.
[5] *IP Office 2.1 Manager*, Issue 15c, May 2004.
[6] *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.

[7] *Meru Access Point Installation Guide*, Document Number 880-00011-0010.
[8] *Meru Controller Installation Guide*, Document Number 880-00012-0006.
[9] *Meru Wireless LAN System Getting Started Guide*, Release 3.0.x, Document Number 880-00026-0003.
[10] *Meru Wireless LAN System Configuration Guide*, Release 3.0.x, Document Number 880-00023-0004.
[11] *Meru Wireless LAN System Command Reference*, Release 3.0.x, Document Number 880-00024-0004.

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.