Avaya Solution & Interoperability Test Lab

Application Notes for the Colubris Networks CN320 Access Point 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 Colubris Networks CN320 Access Point. The CN320 provided network access to the Avaya Wireless IP Telephones, IP Softphone, and Phone Manager Pro, which registered with either Avaya Communication Manager or Avaya IP Office. The Avaya Voice Priority Processor (VPP) was used to support SpectraLink Voice Priority (SVP) on the Avaya Wireless IP Telephones and the CN320 Access Points. An Extreme Networks Alpine 3804 Ethernet Switch interconnected all the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with Avaya wireless IP devices. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using the Colubris Networks CN320 Access Point. The CN320 connected Avaya 3616/3626 Wireless IP Telephones and wireless laptops running Avaya IP Softphone or Phone Manager Pro to the wired network and allowed them to register with either Avaya Communication Manager or Avaya IP Office. The Avaya Voice Priority Processor (VPP) was used to support the SpectraLink Voice Priority (SVP) Protocol on the Avaya Wireless IP Telephones and the CN320 Access Points. An Extreme Networks Alpine 3804 Ethernet Switch was used to interconnect all the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with Avaya wireless IP devices.

The following features supported by the Colubris Networks CN320 Access Point were verified during the compliance testing:

- Quality of Service (QoS) based on Differentiated Services (DiffServ)
- 802.1X Security and WEP Encryption
- VLANs and 802.1Q Trunking
- Layer-2 Roaming
- SpectraLink Voice Priority (SVP)
- 802.11a/b/g Radio Modes

Figure 1 illustrates the network configuration used to verify the Colubris Networks solution. All the wireless IP devices depicted in the configuration roamed between the CN320 Access Points at layer-2 for full mobility. There were three VLANs configured in the network. VLAN 2 was assigned to wireless devices that register with Avaya Communication Manager, VLAN 3 was assigned to wireless devices that register with Avaya IP Office, and VLAN 4 was assigned to the CN320 management LAN network. VLANs 2 and 3 were assigned different SSIDs.

Note: In this configuration, there is an H.323 IP trunk between the Avaya IP Office and the Avaya S8500 Media Server with a G650 Media Gateway. However, the trunk group, signaling group, and call routing administration are not described in these Application Notes. Refer to Avaya Communication Manager and Avaya IP Office documentation for details.

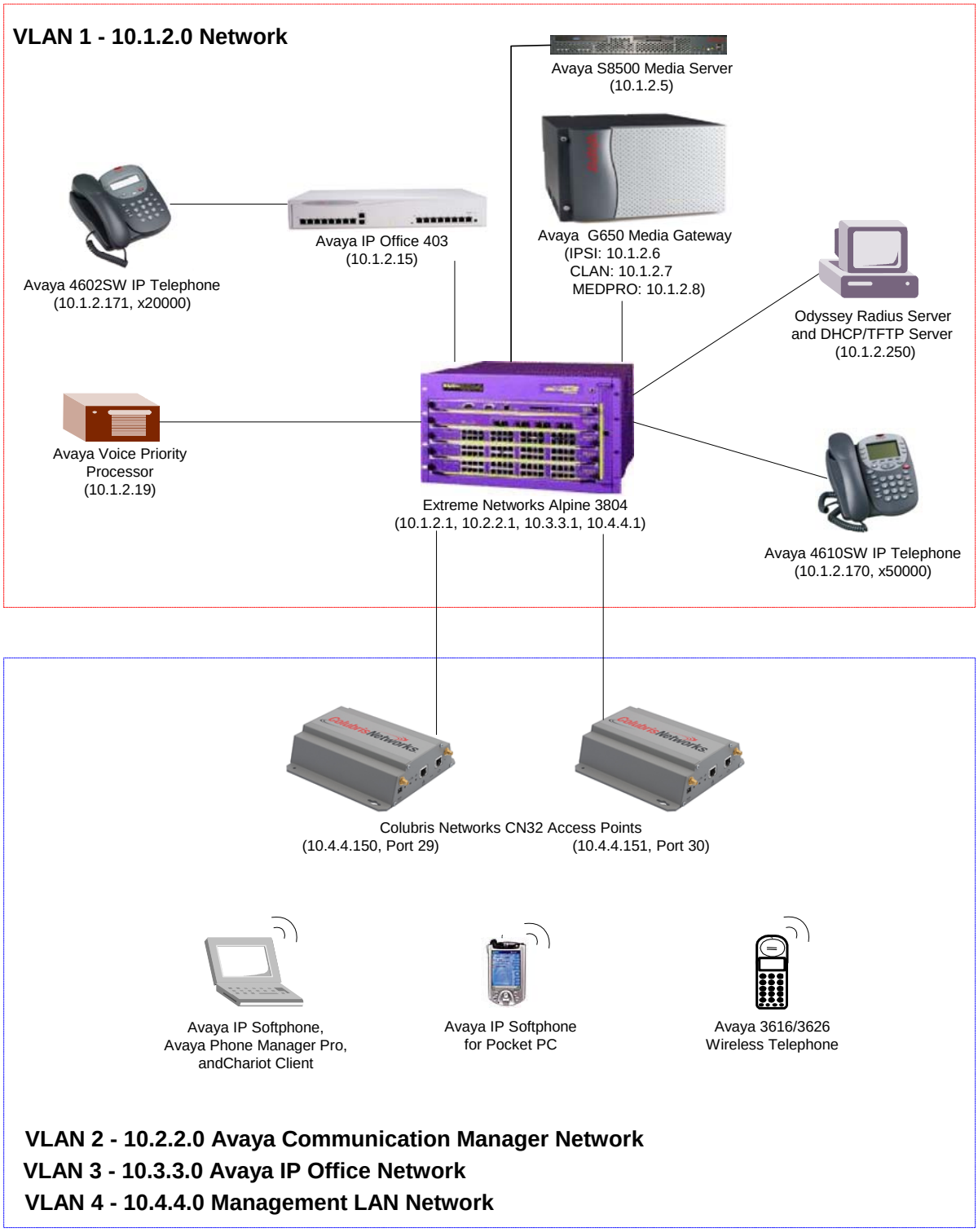


Figure 1: Avaya and Colubris Networks Wireless LAN Configuration

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	1.8
Avaya 4610SW 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
Colubris Networks CN320 Access Point	2.3.1
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.

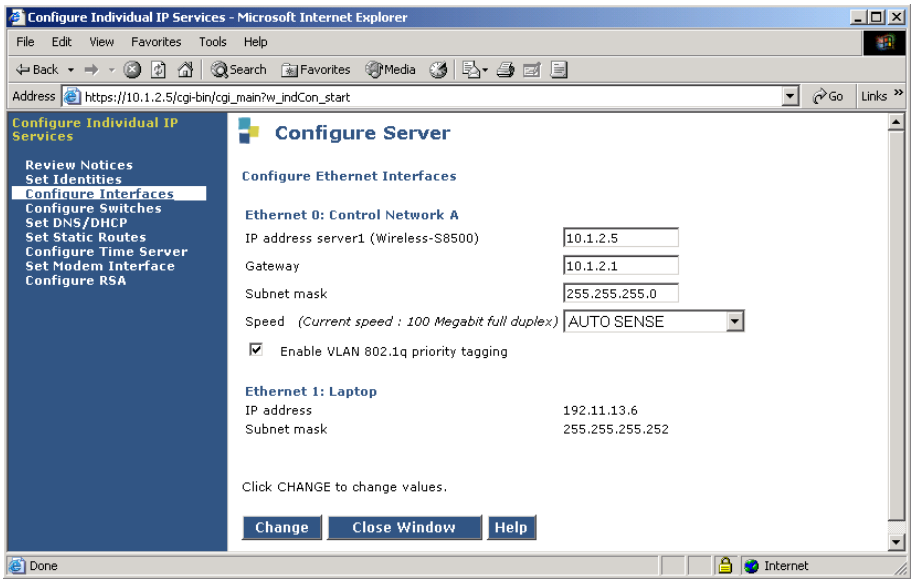


Figure 2: Avaya S8500 Media Server – Configure Server Form

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

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:                  Home Domain:
    Name:
                                Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS                Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                           IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 65535                     RTCP Reporting Enabled? y
                               RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS         Use Default Server Parameters? y
 Call Control PHB Value: 48
        Audio PHB Value: 48
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 3: IP Network Region Form

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

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

                          IP Codec Set

    Codec Set: 1

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

Figure 4: IP Codec Set Form

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

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

                                 IP INTERFACES

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

Number of CLAN Sockets Before Warning: 400
```

Figure 5: IP Interface Form for C-LAN

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

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

                                 IP INTERFACES

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

Figure 6: IP Interface Form for IP Media Processor

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

```
change station 50003                                        Page   1 of   4
                                  STATION

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

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

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

Figure 7: Station Form for IP Softphone

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

```
change station 50005                                        Page   1 of   4
                                  STATION

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

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

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

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

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

4. Configure the Avaya IP Office 403

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

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

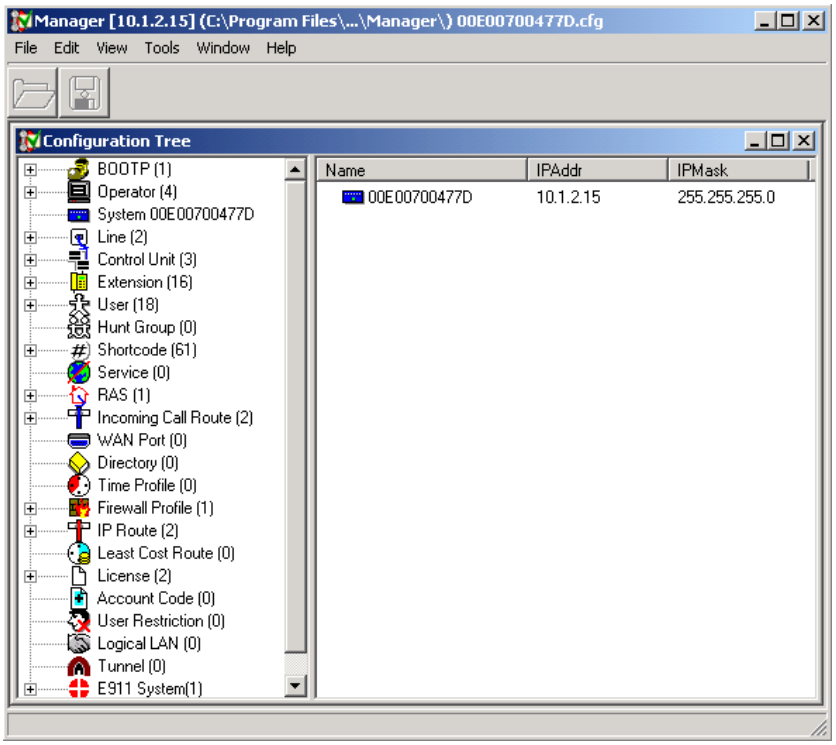


Figure 9: Manager Main Window

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

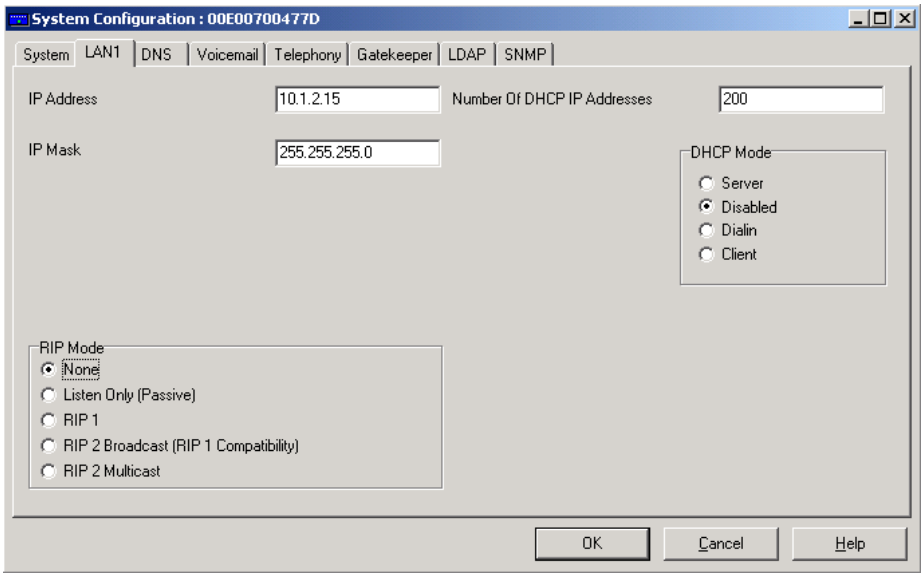


Figure 10: System Configuration – LAN1 Tab

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

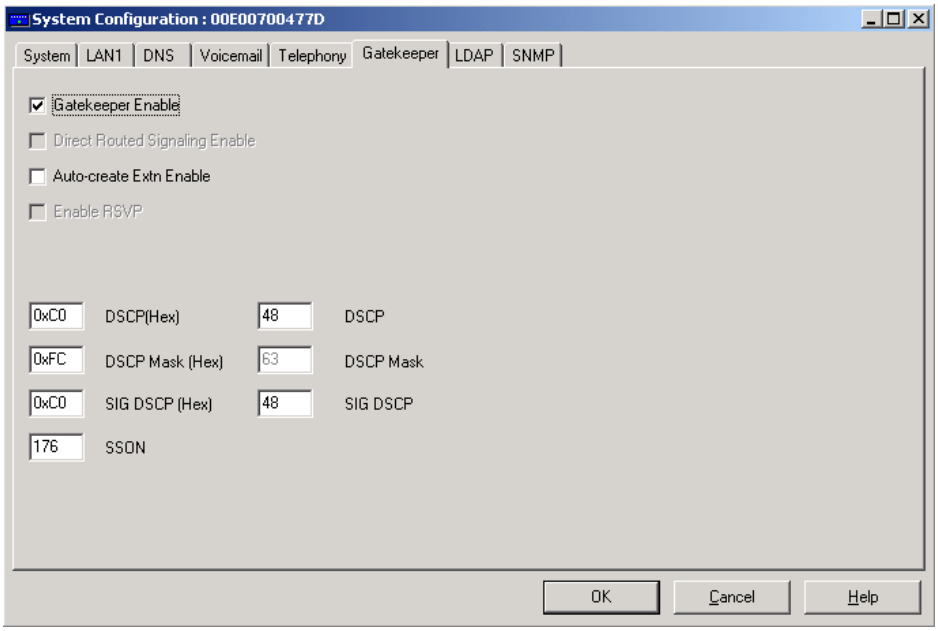


Figure 11: System Configuration - Gatekeeper Tab

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

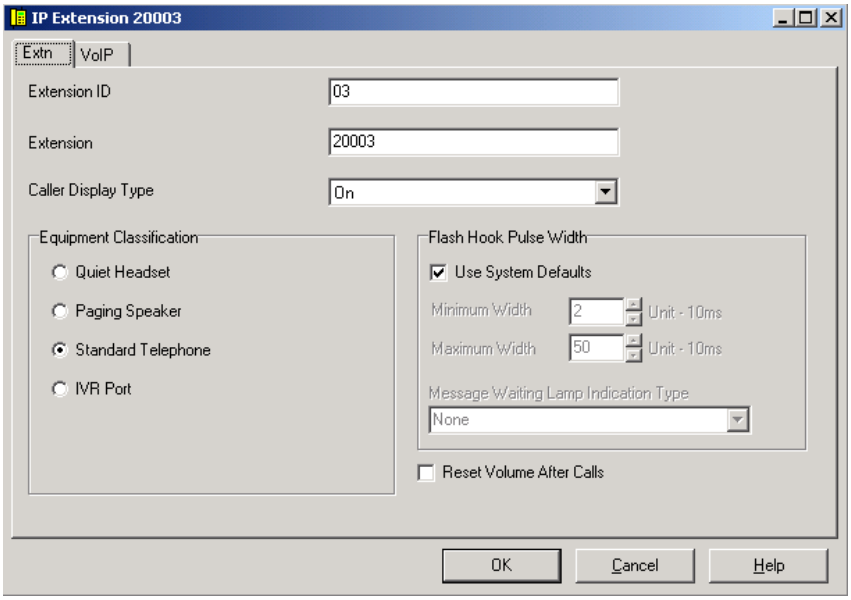


Figure 12: IP Extension – Extn Tab

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

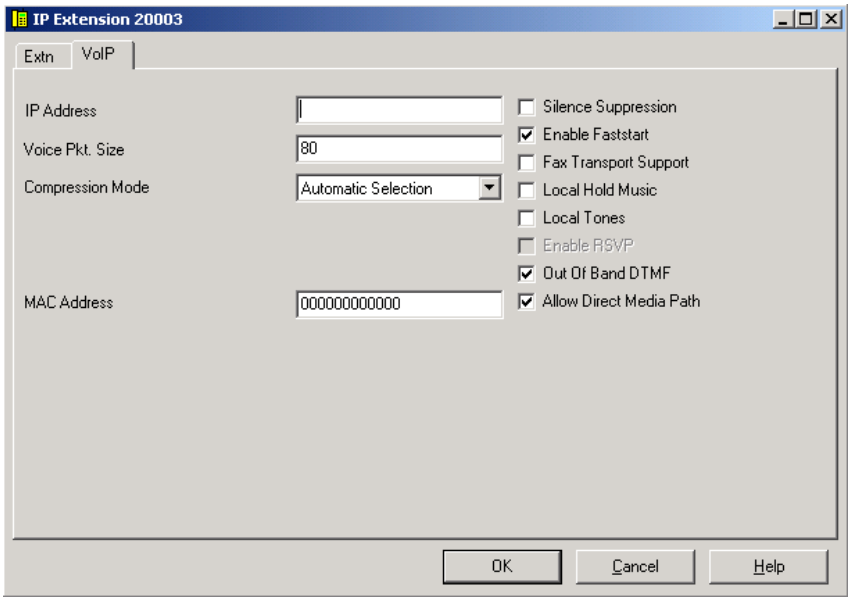


Figure 13: IP Extension – VoIP Tab

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 shown in **Figure 14**. In the **User** tab, specify the endpoint's **Name**, **Password**, and **Extension** as shown in **Figure 14**.

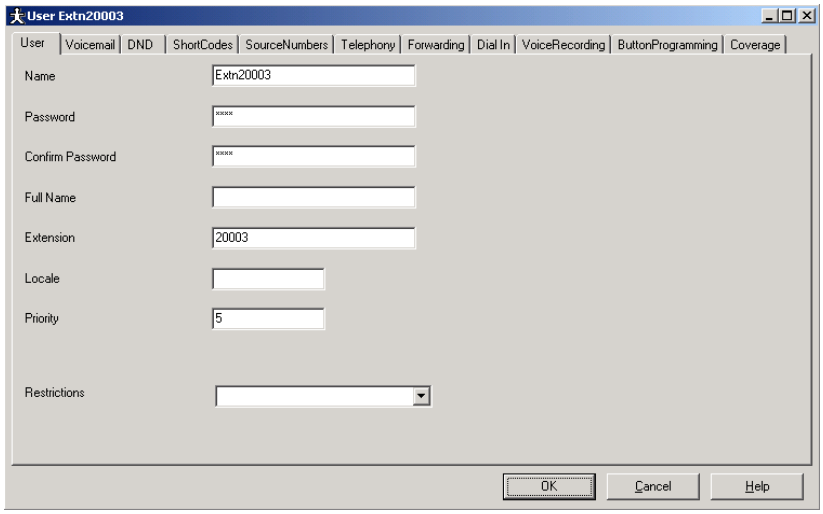


Figure 14: User – User Tab

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

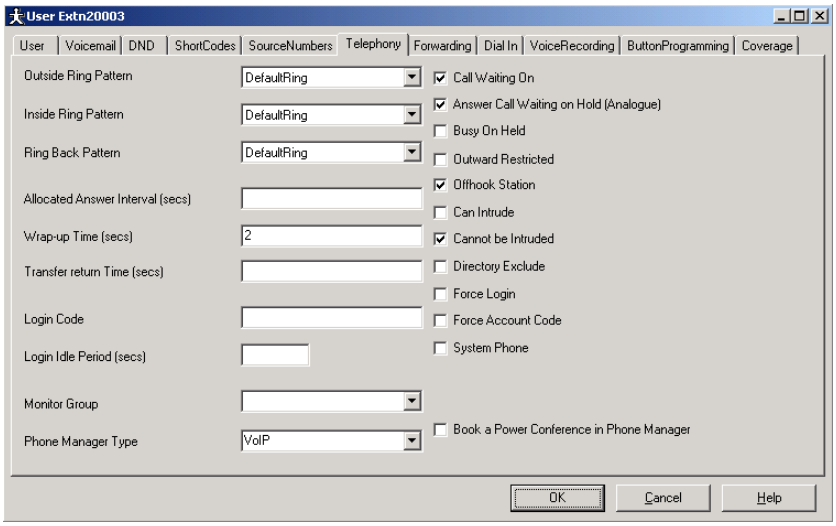


Figure 15: User – Telephony Tab

5. Configure the Avaya Voice Priority Processor

The Avaya Voice Priority Processor (VPP) utilizes SpectraLink Voice Priority (SVP) as the Quality of Service (QoS) mechanism supported by the Avaya 3616/3626 Wireless IP Telephones and the Colubris Networks CN 320 Access Point to enhance voice quality over the wireless network.

The Avaya VPP performs four major functions. First, it is a required component to utilize the 11Mbps maximum transmission speed available in the Avaya Wireless Telephones that support 802.11b. Second, it controls the maximum number of calls supported per access point. Third, SVP allows the CN320 and the Avaya Wireless IP Telephones to transmit their voice packets immediately, while other devices must wait a random backoff period as required by the 802.11 standard. This reduces jitter and delay for the voice packets. Finally, the Avaya VPP is required to serve as a "gateway" between the Avaya Wireless IP Telephones and the Avaya IP Telephony infrastructure. Since the Avaya wireless telephones support SVP, their packets are directed to the Avaya VPP so that the SVP header information can be removed before the packets are forwarded to Avaya Communication Manager.

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

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

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

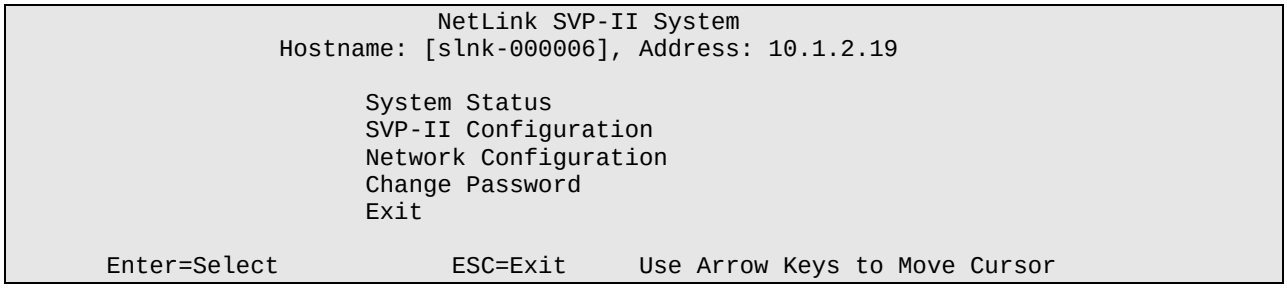


Figure 16: System Menu

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

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

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

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

Figure 17: Network Configuration

From the **System Menu**, select **SVP-II Configuration** to configure the **Phones per Access Point** and the **802.11 Rate** fields. In this configuration, the **802.11 Rate** was configured to *Automatic*, as shown in **Figure 18**, to allow the wireless telephone to determine the rate (up to 11Mbps), as opposed to the Avaya VPP limiting the transmission rate of the wireless telephone to 1/2 Mbps. The **Phones per Access Point** field should specify the maximum number of calls supported by each CN320. 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 CN320 within range, or will be denied with a "Net Busy" error message.

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

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

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

Figure 18: SVP-II Configuration

6. Configure the Extreme Networks Alpine 3804

This section covers the configuration of the Extreme Networks Alpine 3804 Ethernet switch that is relevant to the Colubris Networks CN320. Specifically, the configuration related to the VLANs 2, 3 and 4 and the Ethernet ports used by the CN320 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, 3 and 4 on the Alpine 3804. Wireless endpoints that registered with Avaya Communication Manager were assigned to VLAN 2 and wireless endpoints that registered with Avaya IP Office were assigned to VLAN 3. VLAN 4 was used for the CN320 management network.
	Note: The configuration of VLAN 1 is not shown in these Application Notes.
	`Alpine3804# create vlan vlan2`
	`Alpine3804# create vlan vlan3`
	`Alpine3804# create vlan vlan4`

3.	Assign a tag to VLANs 2, 3 and 4.
	`Alpine3804# configure vlan vlan2 tag 2`
	`Alpine3804# configure vlan vlan3 tag 3`
	`Alpine3804# configure vlan vlan4 tag 4`

4.	Enable IP Forwarding on the VLAN interfaces to allow the Alpine 3804 to route between VLANs 2, 3 and 4.
	`Alpine3804# enable ipforwarding vlan vlan2`
	`Alpine3804# enable ipforwarding vlan vlan3`
	`Alpine3804# enable ipforwarding vlan vlan4`

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`
	`Alpine3804# configure vlan vlan4 ipaddress 10.4.4.1 255.255.255.0`

6.	Assign VLANs 2, 3 and 4 to Ethernet ports 1:29 and 1:30. VLANs 2, 3 and 4 were assigned to ports 1:29 and 1:30 as tagged to enable 802.1Q trunking to the CN320 Access Points.
	`Alpine3804# configure vlan vlan2 add port 1:29-1:30 tagged`
	`Alpine3804# configure vlan vlan3 add port 1:29-1:30 tagged`
	`Alpine3804# configure vlan vlan4 add port 1:29-1:30 tagged`

Step	Description

7.	Enable DHCP Relay and specify the IP address of the DHCP server. The Avaya wireless IP endpoints 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# **copy running-config startup-config**`

7. Configure the DHCP Server

The Avaya Wireless IP Telephones and the laptops running IP Softphone and Phone Manager Pro obtained their IP configuration, Avaya VPP IP address (Option 151), and Option 176 settings from a DHCP server. The DHCP server was configured with two scopes that served wireless IP endpoints that register with either Avaya Communication Manager or Avaya IP Office. The following scopes were defined on the DHCP server:

```
Scope [10.2.2.0] Avaya Communication Manager
Address Pool
  Start IP Address = 10.2.2.50
  End IP Address = 10.2.2.70
Option 003 Router = 10.2.2.1
Option 151 AVPP = 10.1.2.19
Option 176 IP Telephone =
  MCIPADD=10.1.2.7,MCPORT=1719,TFTPSRVR=10.1.2.250

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=10.1.2.250
```

8. Configure the Colubris Networks CN320 Access Points

This section covers the configuration of the CN320 Access Points using the **CN320 Management Tool**, a Web-based configuration tool. The following configuration is illustrated for the CN320 with IP address 10.4.4.150, but it also applies to the other CN320 in the configuration. The configuration for the two CN320 Access Points is the same, except for the IP address. It is assumed that the CN320 Access Points have already been configured with an IP address.

Note: When configuring DiffServ-based QoS on the CN320, refer to [6] to determine how the different DSCP values are prioritized. The CN320 supports four priority hardware queues. In this configuration, DSCP value 48 was used which is mapped to the highest priority queue by the CN320.

1. Start a Web browser and specify **https://<CN320 IP Address>** in the URL. After accepting the Colubris Networks security certificate, the management tool **Login** page opens as shown in **Figure 19**. Log in as *admin* with the appropriate password.

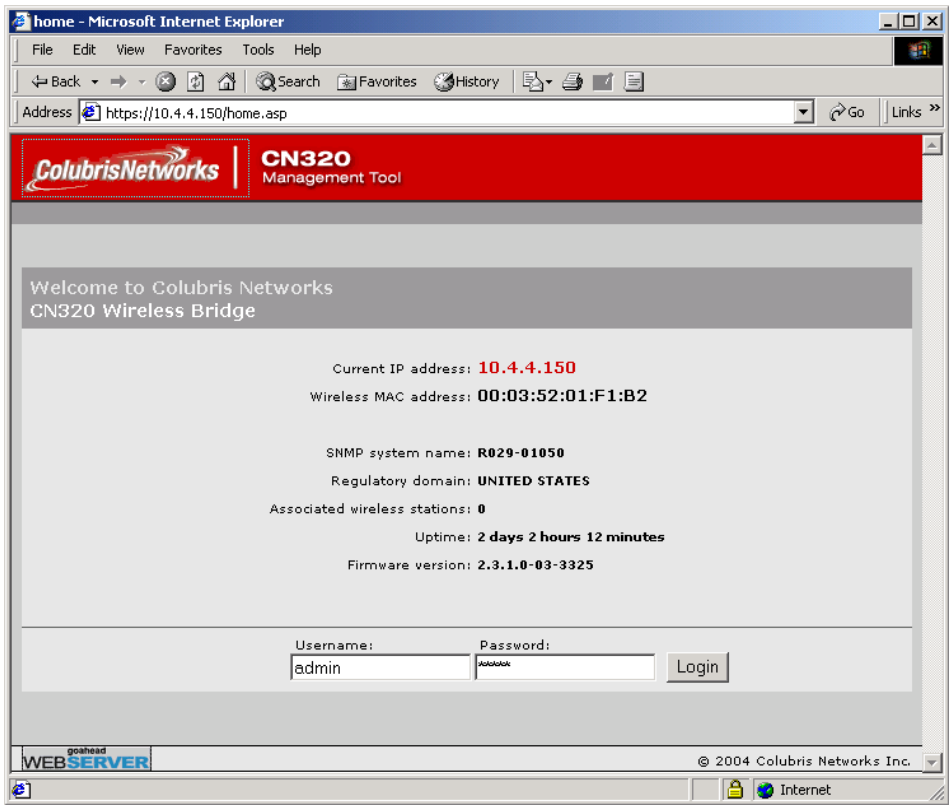


Figure 19: Login Page

2. After logging in successfully, the CN320 Management Tool **Main** page is displayed as shown in **Figure 20**.

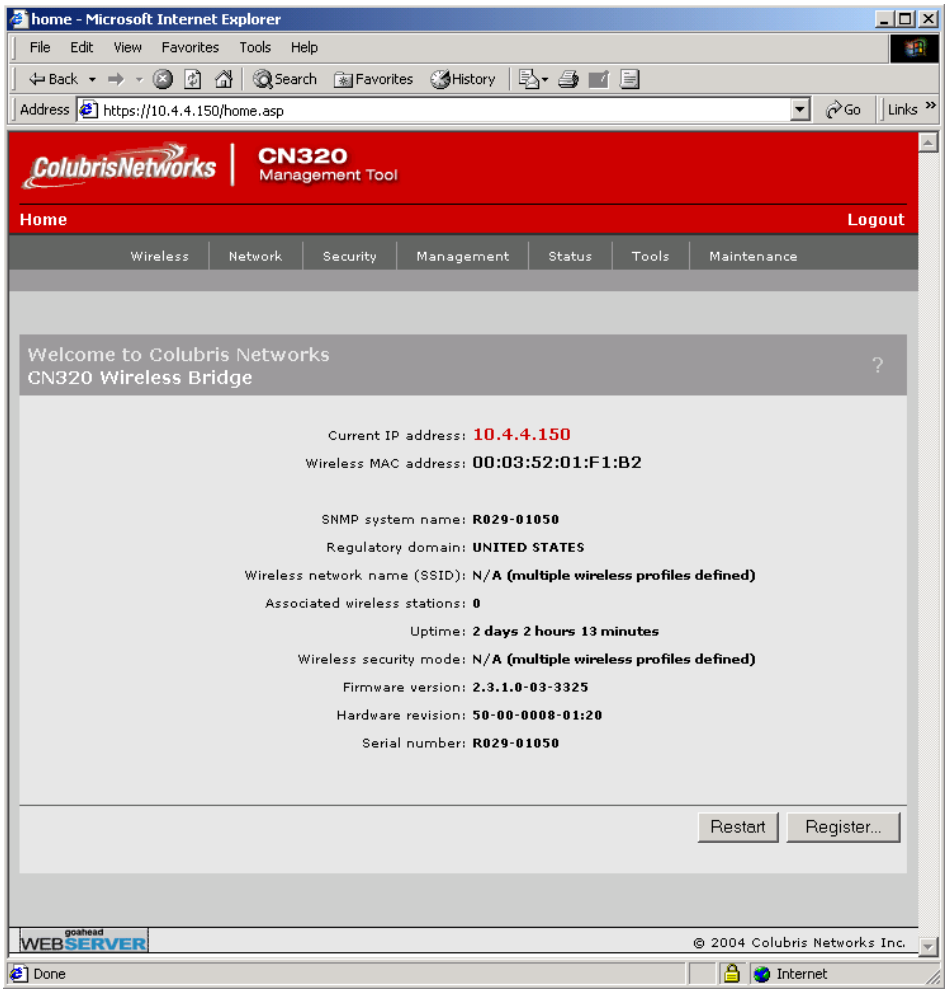


Figure 20: Main Page

3. To modify the IP configuration of the management LAN interface, click on the **Network** tab and then select the **Ports** sub-tab. The management interface on the CN320 is configured with a static IP address and assigned to VLAN 4. After specifying the network configuration, click on the **Save** button.

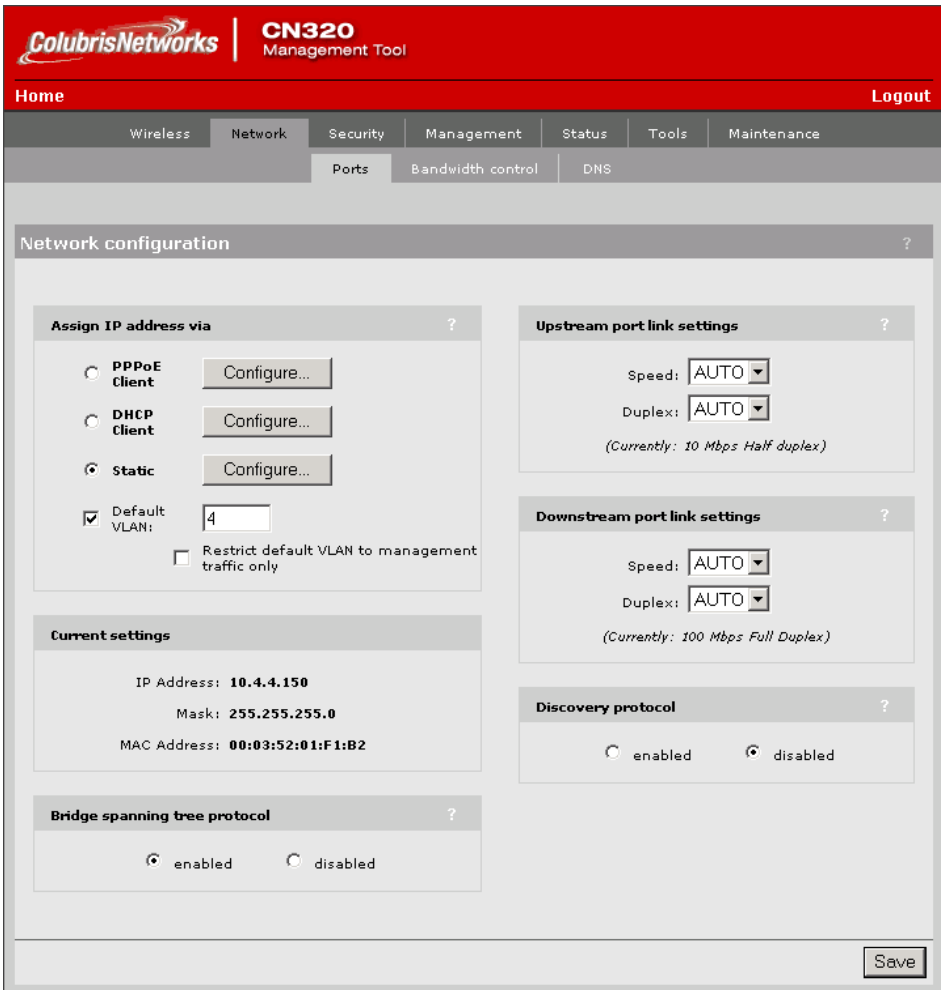


Figure 21: Network Configuration

4. From the **Network Configuration** screen shown in **Figure 21**, click on the **Configure** button by the **Static** radio button to specify the IP configuration of the CN320. The **Static IP Address Configuration** page is displayed as seen in **Figure 22**. Specify the IP **Settings** and then click on the **Save** button.

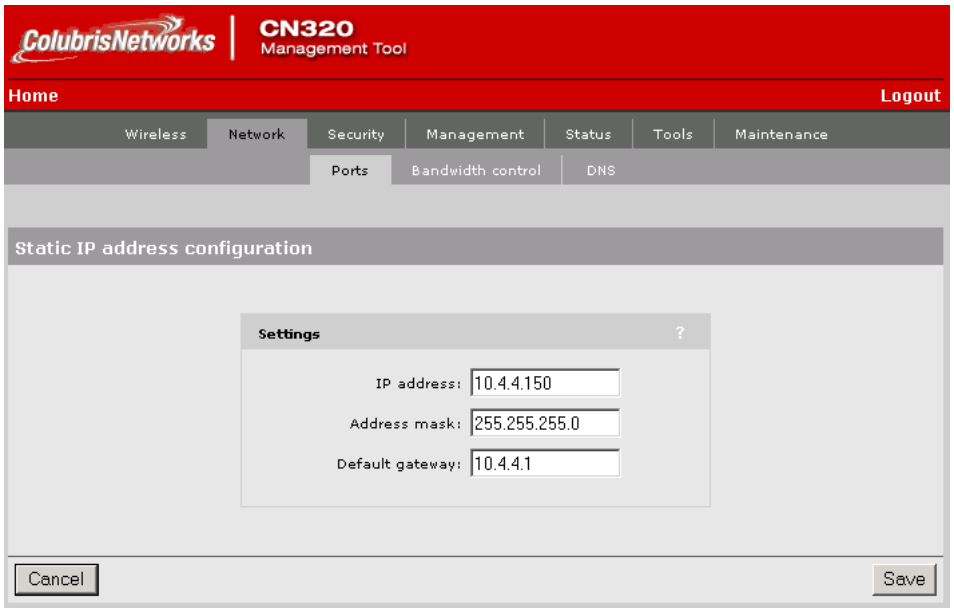


Figure 22: Static IP Address Configuration

5. To configure a RADIUS profile to be used later in a WLAN profile, select the **Security** tab and then click on the **RADIUS** sub-tab. The **RADIUS Profiles** page is displayed as shown in **Figure 23**. To add a new RADIUS profile, click on the **Add New Profile** button.

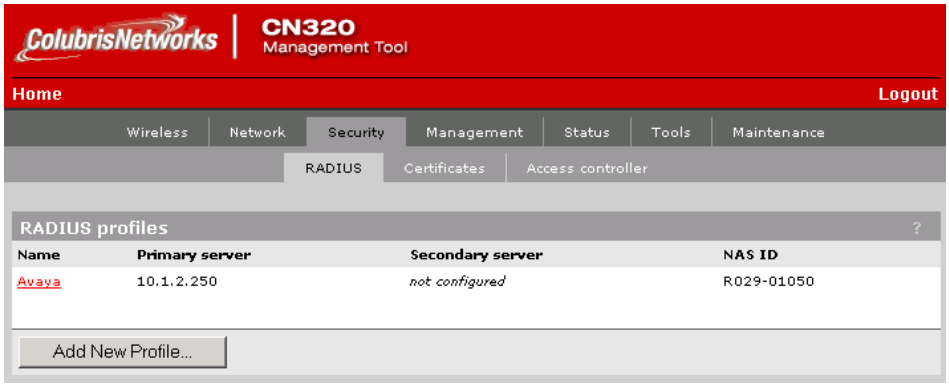


Figure 23: RADIUS Profiles List

6. Configure the RADIUS profile as shown in **Figure 24**. This RADIUS profile will be assigned to WLAN profiles that require 802.1X security using EAP-TTLS authentication. In the profile, specify a profile name, the IP address of the RADIUS server, the shared secret, and the authentication port. When the configuration is completed, click on the **Save** button.

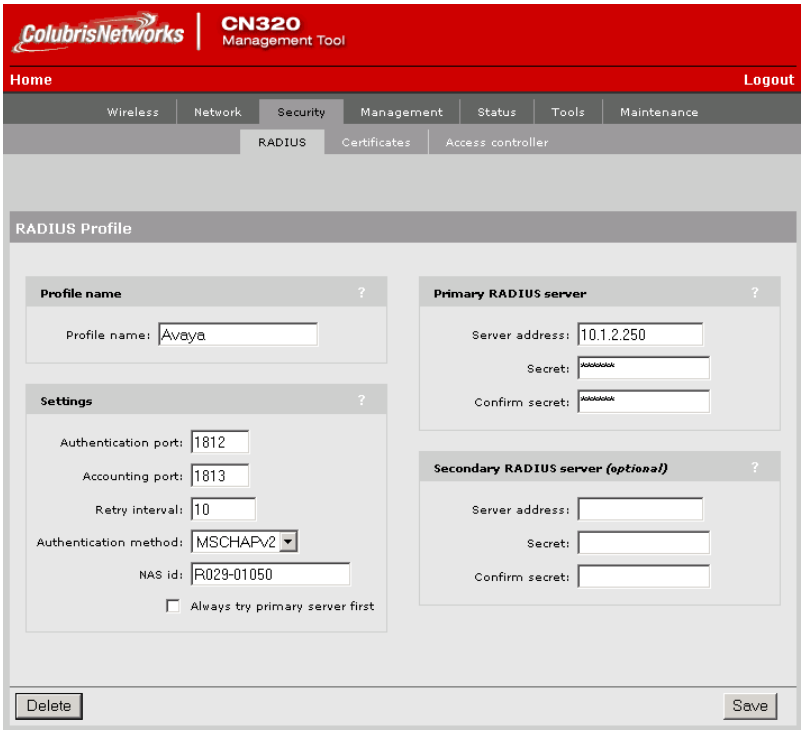


Figure 24: RADIUS Profile

7. To configure the **WLAN Profiles**, click on the **Wireless** tab and then select the **WLAN Profiles** sub-tab. The **WLAN Profiles** page in **Figure 25** is displayed. For the compliance testing, the **WLAN Profiles** listed in **Figure 25** were used.

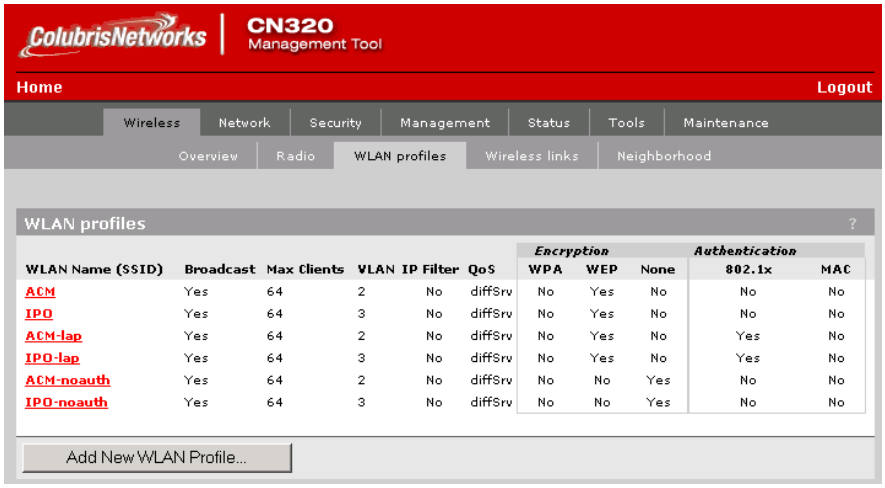


Figure 25: WLAN Profiles

8. To add a new WLAN profile, click on the **Add New WLAN Profile** button in **Figure 25**. Set the **WLAN name (SSID)**, the **QoS Priority Mechanism**, and the **Wireless Protection**. The following WLAN profile was used for the Avaya 3616/3626 Wireless Telephones that register with Avaya Communication Manager. It supported DiffServ-based QoS and WEP Encryption with a static key. By default, all profiles have SVP enabled, except when *Disabled* is selected in the **QoS Priority Mechanism** field. Note that the **Key Format** is set to *HEX*. In addition, the WLAN profile is configured to serve VLAN 2. Finally, enable **Permit traffic exchange between wireless client stations** to allow direct communication (shuffling) between wireless devices on the same CN320. Configure the other WLAN profile parameters as shown in **Figure 26**. When done with the configuration on this page, click on the **Save** button. See [6] for more information on implementing QoS on the CN320.

   Note: The first WLAN Profile allows up to four WEP keys to be specified. Subsequent WLAN profiles only allow a single WEP key to be specified.

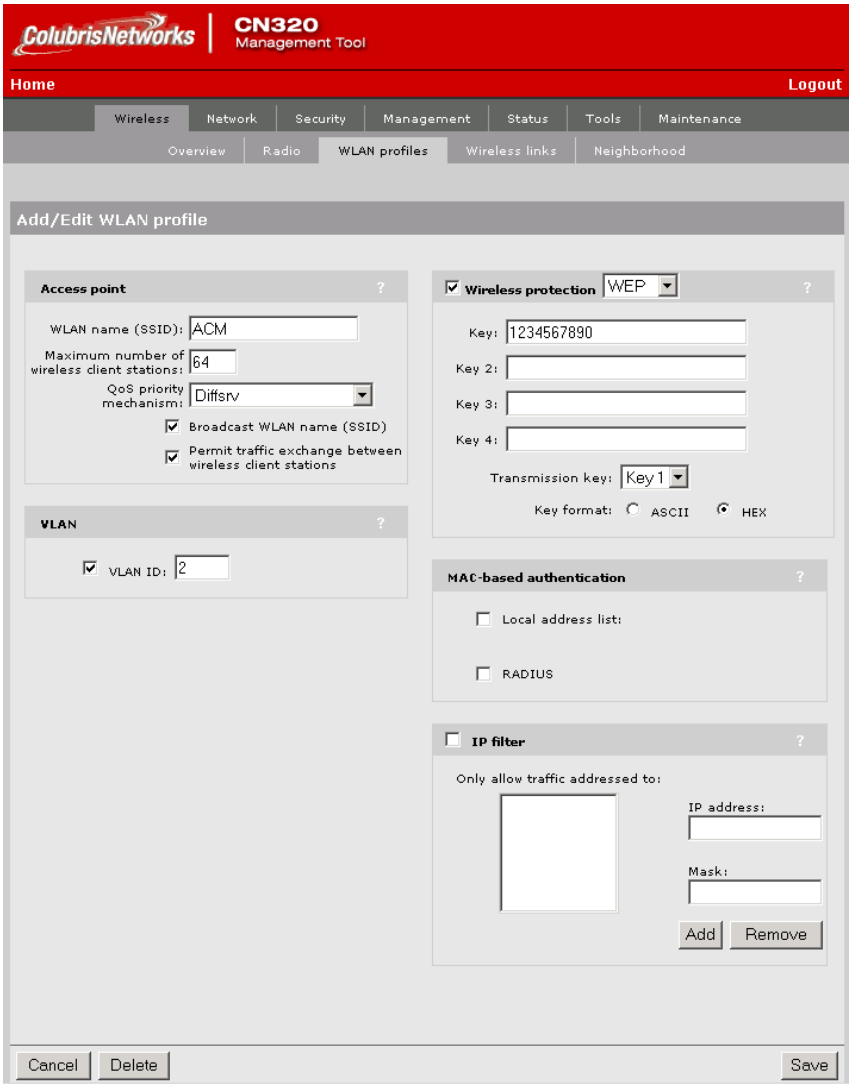


Figure 26: Add/Edit WLAN Profile

9. **Figure 27** shows a WLAN profile with 802.1X Security and WEP Encryption enabled. To disable wireless protection, deselect the **Wireless Protection** and **WEP Encryption** checkboxes. In this example, MAC-based authentication was used to block access to the wireless device with the specified MAC address. When done with the configuration on this page, click on the **Save** button.

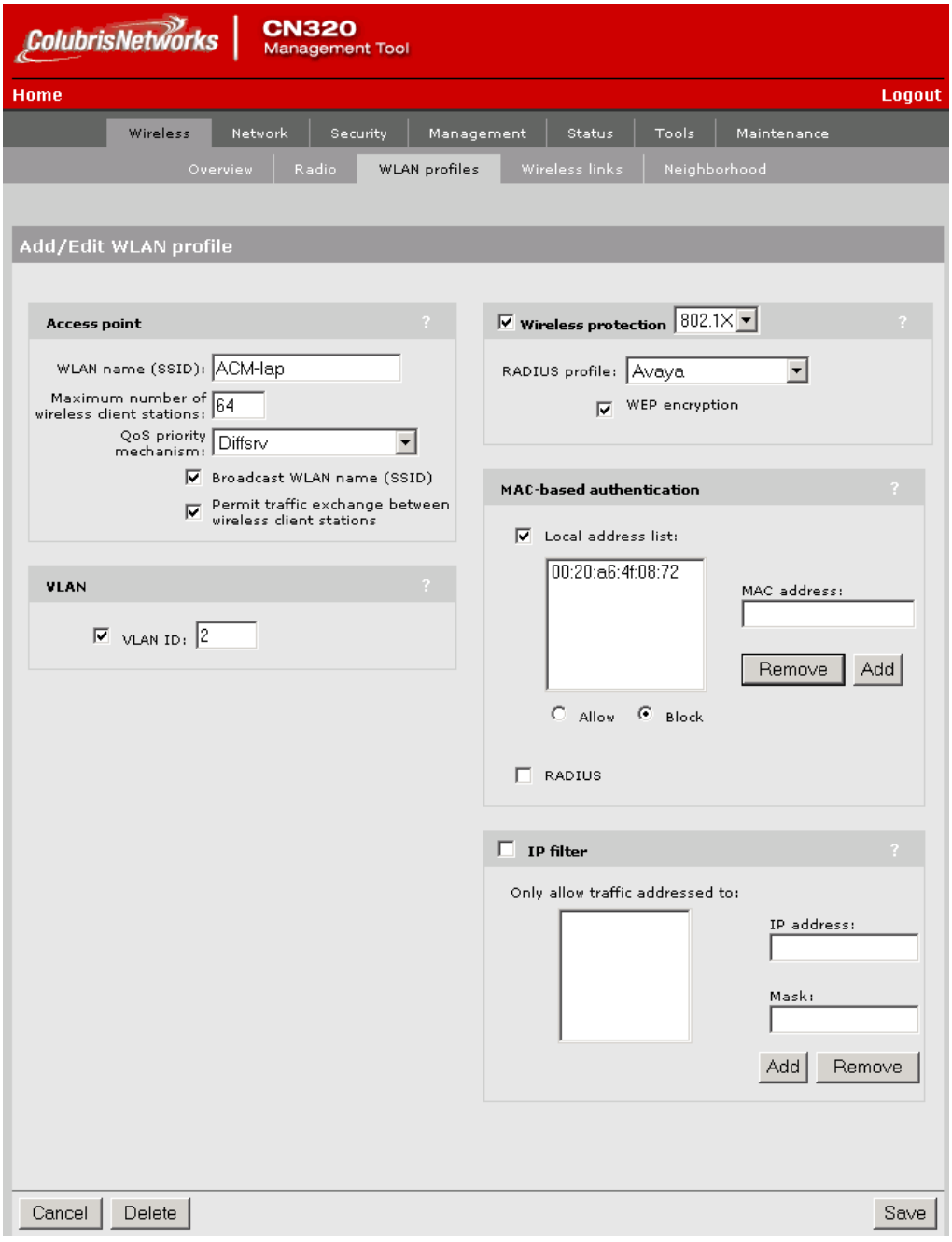


Figure 27: WLAN Profile with 802.1X and WEP Encryption

10. Finally, configure the radio in the CN320 Access Point. The CN320 supports 802.11a/b/g with the radio mode being software selectable. The Avaya 3616/3626 Wireless Telephones support 802.11b and the mobile laptops support 802.11a/b/g. In the **Wireless Configuration** page shown in **Figure 28**, the **Wireless Mode** was set to *802.11b*. The **Wireless Mode** field may be set to *802.11a*, *802.11b + 802.11g*, or *802.11g*. On this page, the **Operating Frequency** is also set and the CN320 Access Point is enabled. When done with the configuration, click on the **Save** button.

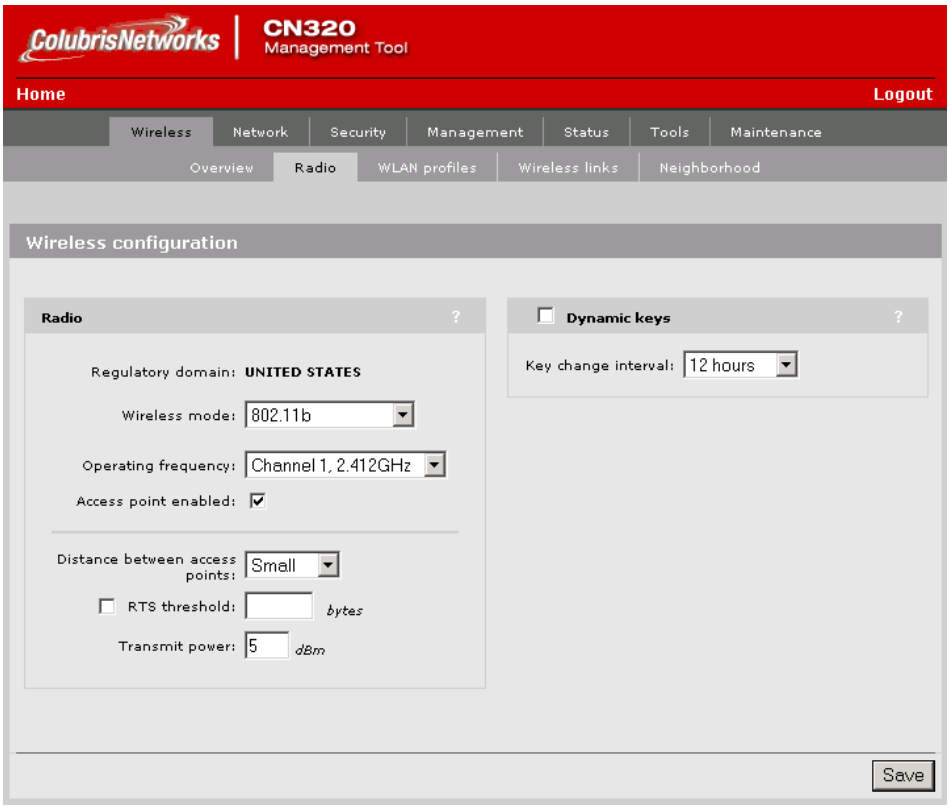


Figure 28: Wireless Configuration

9. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality and performance testing. Feature functionality testing verified the ability of the Colubris Networks CN320 Access Point 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 CN320 QoS implementation in order to achieve good voice quality, Radius authentication, WEP encryption, and layer-2 roaming.

9.1. General Test Approach

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

- Quality of Service (QoS) based on DiffServ
- 802.1X Security and WEP Encryption
- VLANs and 802.1Q Trunking
- Layer-2 Roaming
- SpectraLink Voice Protocol (SVP)
- 802.11a/b/g

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

9.2. Test Results

All feature functionality and performance test cases passed. The Colubris Networks CN320 Access Point provided network access to the Avaya wireless IP endpoints using 802.1X Security and WEP Encryption. Good voice quality was achieved on wireless voice calls through the use of the Colubris Networks QoS implementation and the Avaya VPP. The CN320 communicated with the wireless devices using 802.11a/b/g.

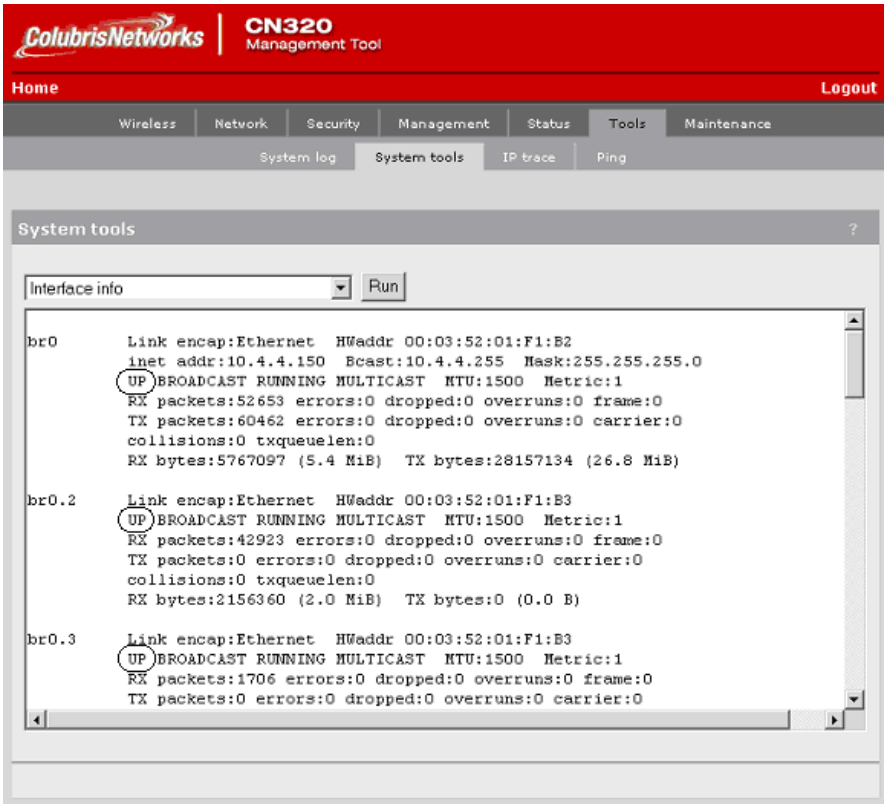
10. Verification Steps

This section provides verification steps that may be performed in the field to verify that the wireless IP endpoints have connectivity to the network and that good voice quality is being provided for wireless calls. The following commands are entered on the CN320 unless otherwise specified.

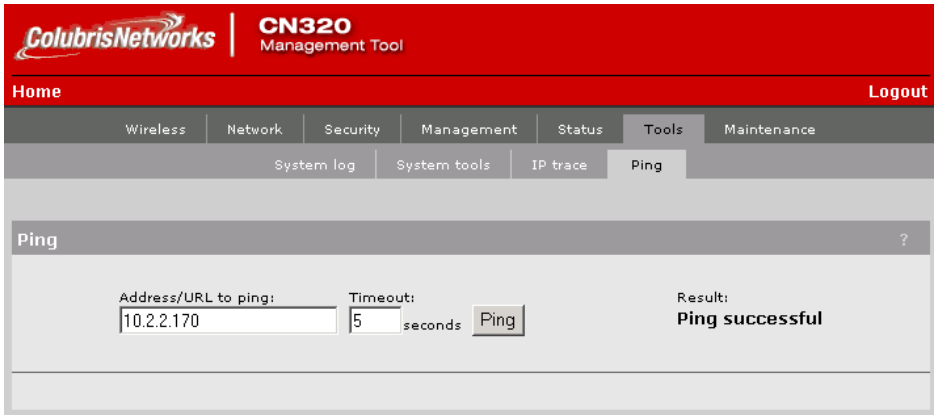
1. Check that the Avaya wireless IP endpoints have successfully registered with Avaya Communication Manager by typing the **list registered-ip-stations** command on the SAT. A sample output of the command is shown below.

```
list registered-ip-stations

                          REGISTERED IP STATIONS

Station  Set      Product    Prod  Station         Net Orig      Gatekeeper
Ext      Type     ID         Rel   IP Address      Rgn Port      IP Address
50000    4610     IP_Phone   2.100 10.1.2.170      1             10.1.2.7
50003    4620     IP_Soft    5.146 10.2.2.170      1             10.1.2.7
50005    4620     IP_Phone   1.500 10.1.2.19       1             10.1.2.7
50006    4620     IP_Phone   1.500 10.1.2.19       1             10.1.2.7
```

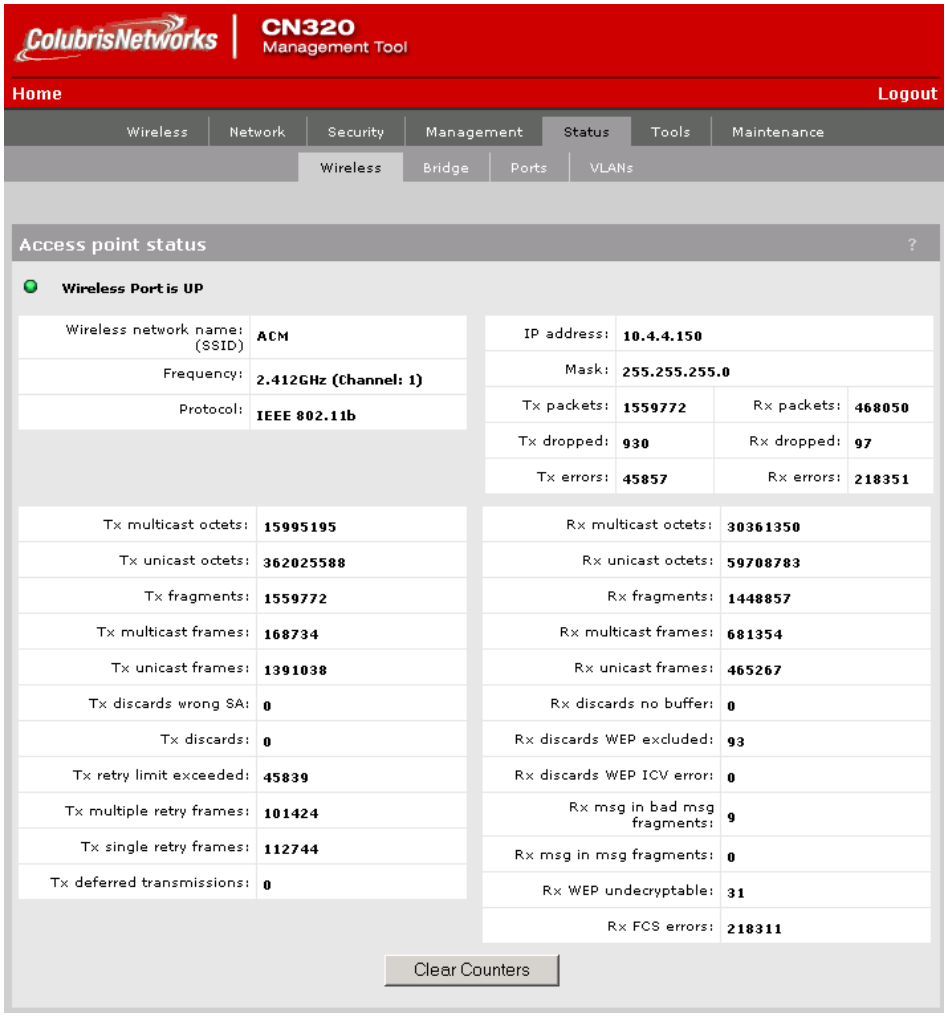
2. Verify that the network interfaces on the CN320 Access Point are in-service. From the **Tools** tab, select **System Tools** and then set the drop-down textbox to **Interface Info**. A sample partial output is provided below.



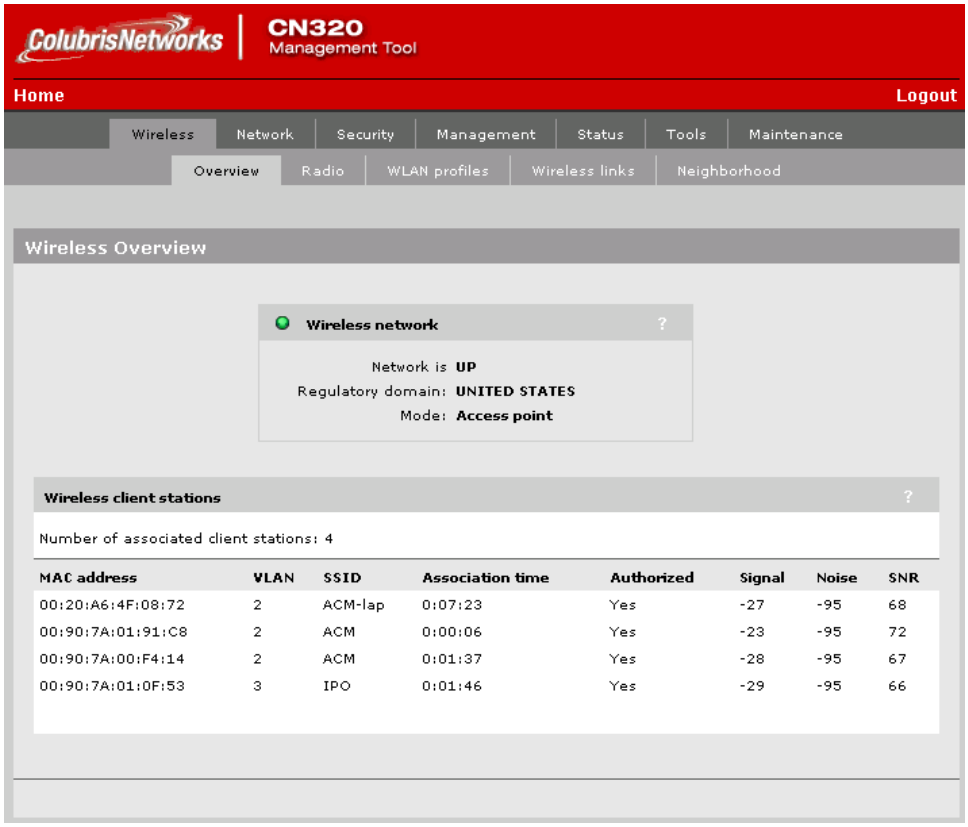
3. From the CN320 Access Point, verify IP communication with the other devices in the network. To ping from the CN320, select **Ping** from the **Tools** tab and enter the IP address to ping.



4. Check the access point status by selecting the **Wireless** option from the Status tab.



5. To check the wireless devices that are associated with the CN320, select **Overview** from the **Wireless** tab. The wireless client stations on the CN320 are displayed.



6. Place a call between two wireless IP devices and verify that good voice quality is obtained.

11. Support

For technical support on the Colubris Networks CN320 Access Point, call Colubris Networks Customer Support at (866) 241-8324 or send email to support@colubris.com.

12. Conclusion

These Application Notes describe the configuration steps required for integrating the Colubris Networks CN320 Access Point with an Avaya IP Telephony infrastructure. The CN320 was successfully integrated into an enterprise network consisting of Avaya Communication Manager, Avaya IP Office, Avaya Voice Priority Processor, Avaya Wireless IP Telephones, Avaya IP Softphone, and Avaya Phone Manager Pro. The CN320 supported 802.11a/b/g radio modes, VLAN tagging, DiffServ-based QoS, SpectraLink Voice Priority, 802.1X security, and WEP encryption. Seamless layer-2 roaming was also verified. The Colubris Networks solution yielded good voice quality on the wireless IP telephony devices.

13. References

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

[6] *Colubris Networks CN320 Administrator's Guide*, Fourth Edition V2.2 (August 2004), 43-10-0320-05.

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.