Avaya Solution & Interoperability Test Lab

Configuring Cisco Aironet 1200 Access Point to Support Avaya Communication Manager, Avaya Wireless IP Telephones and Avaya IP Softphone - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Cisco Aironet 1200 Access Point to support Avaya Communication Manager, Avaya Wireless IP Telephones and Avaya IP Softphone.

1. Introduction

These Application Notes describe the steps required to configure Cisco Aironet 1200 Wireless Access Point to support Avaya Communication Manager, Avaya Wireless IP Telephones and Avaya IP Softphone. The network infrastructure used for verification is shown in **Figure 1**. These Application Notes cover the following areas:

- System IP and Wireless 802.11a radio configuration.
- Wireless 802.11g radio configuration.
- Wired Equivalent Privacy (WEP) encryption.
- 802.1x RADIUS authentication with Wi-Fi Protected Access (WPA).
- Quality of Service (QoS) configuration.

These Application Notes do not cover the configuration for Avaya Wireless IP Telephones, Avaya IP Softphone, Odyssey RADIUS Server and Clients. For configuration of these devices, refer to the Application Notes listed in Section 8.

Figure 1 shows the network configuration used for verification.

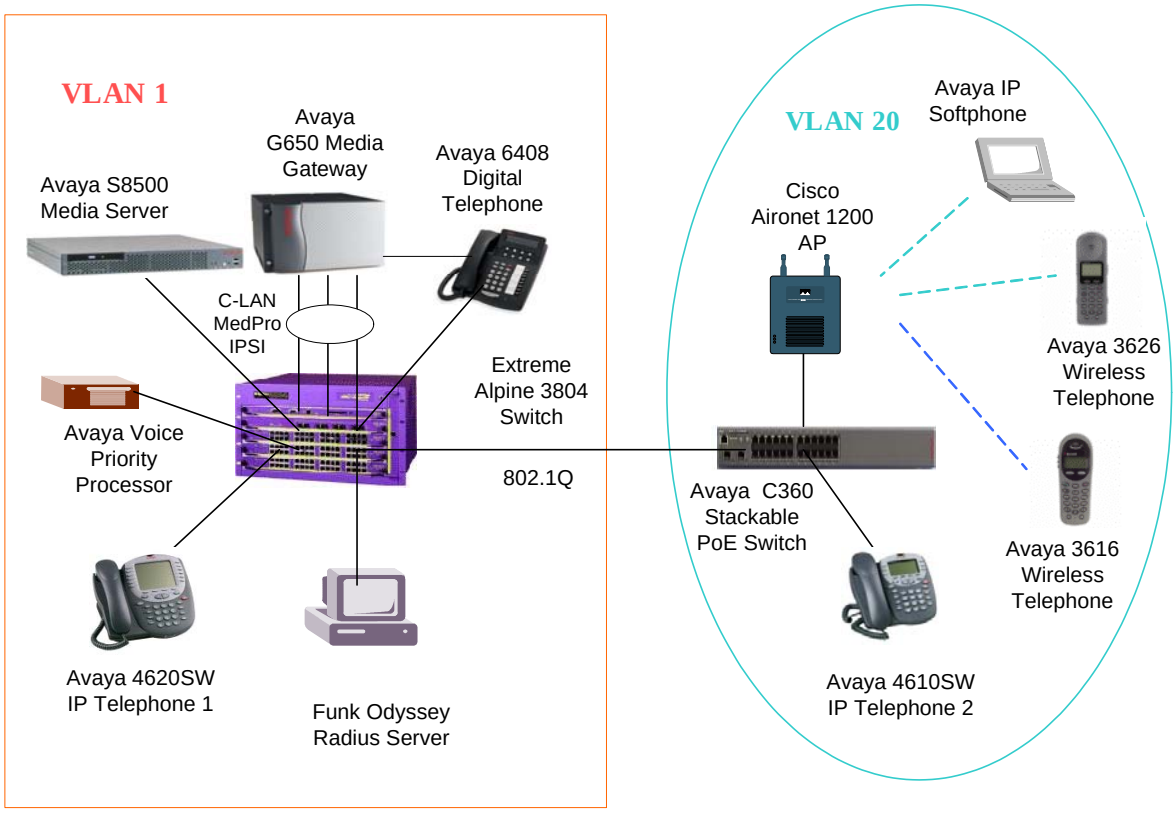


Figure 1: Network Configuration

Table 1 lists the IP addresses and subnet masks for the tested devices.

Device	VLAN	IP Address/Mask	Gateway
Avaya S8500 Media Server	VLAN 1	50.1.1.5 /24	50.1.1.1
Avaya G650 Gateway • IPSI • C-LAN • MEDPRO	VLAN 1	 50.1.1.6/24 50.1.1.7/24 50.1.1.8/24	 50.1.1.1 50.1.1.1 50.1.1.1
Avaya Voice Priority Processor	VLAN 1	50.1.1.9/24	50.1.1.1
Avaya 3626 Wireless Telephone Avaya 3616 Wireless Telephone	VLAN20 VLAN20	20.1.1.120 20.1.1.121	20.1.1.1 20.1.1.1
Avaya C360 PWR Switch	VLAN20	20.1.1.2/24	20.1.1.1
Avaya IP Softphone	VLAN20	20.1.1.126	20.1.1.1
Cisco Aironet 1200 Wireless Access Point	VLAN 20	20.1.1.14/24	20.1.1.1
Extreme Alpine 3804 Switch	VLAN1 VLAN20	50.1.1.1/24 20.1.1.1/24	N/A N/A
Funk Odyssey RADIUS Server	VLAN 1	50.1.1.50/24	50.1.1.1

Table 1: Devices IP Address and Gateway

2. Equipment and Software Validated

Table 2 lists the equipment and software version used for the configuration.

Equipment	Software
Avaya S8500 Media Server/G650 Media Gateway	Communication Manager 2.2 (R012x.02.0.111.4)
Avaya IP Softphone	V5.0.1.2
Avaya 4620SW/4610SW IP Telephones	R2.01
Avaya 3616/3626 Wireless IP Telephones	96.036
Avaya Voice Priority Processor	R168.112
Avaya C360 Stackable Switch	R4.3.12
Cisco Aironet 1200 Wireless Access Point	12.2(15) XR2
Extreme Alpine 3804 Switch	V7.2.0b25
Dell Laptop with ▪ Windows XP ▪ Cisco Wireless a/b/g card	 XP with Service Pack 1 V 3.0.0.111
Funk Odyssey RADIUS Server	V2.01.00.653
Funk Odyssey Client	V3.03.0.1194

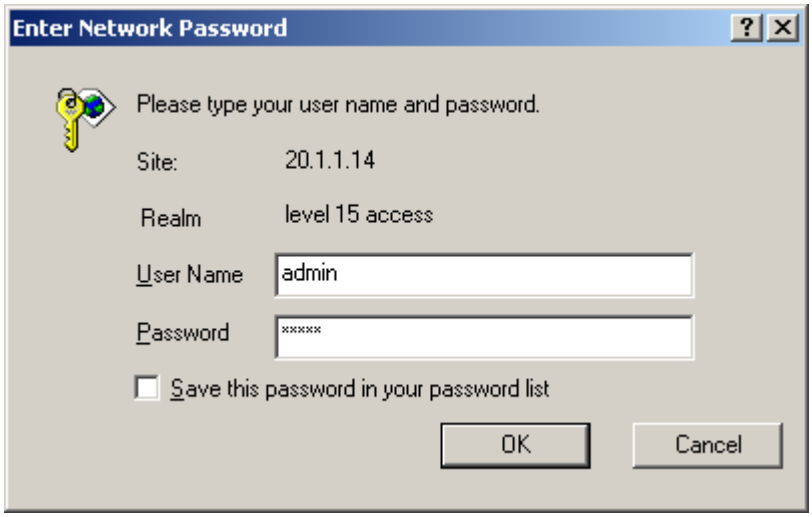
Table 2: Equipment and Software Validated

3. Configure the Cisco Aironet 1200 Access Point

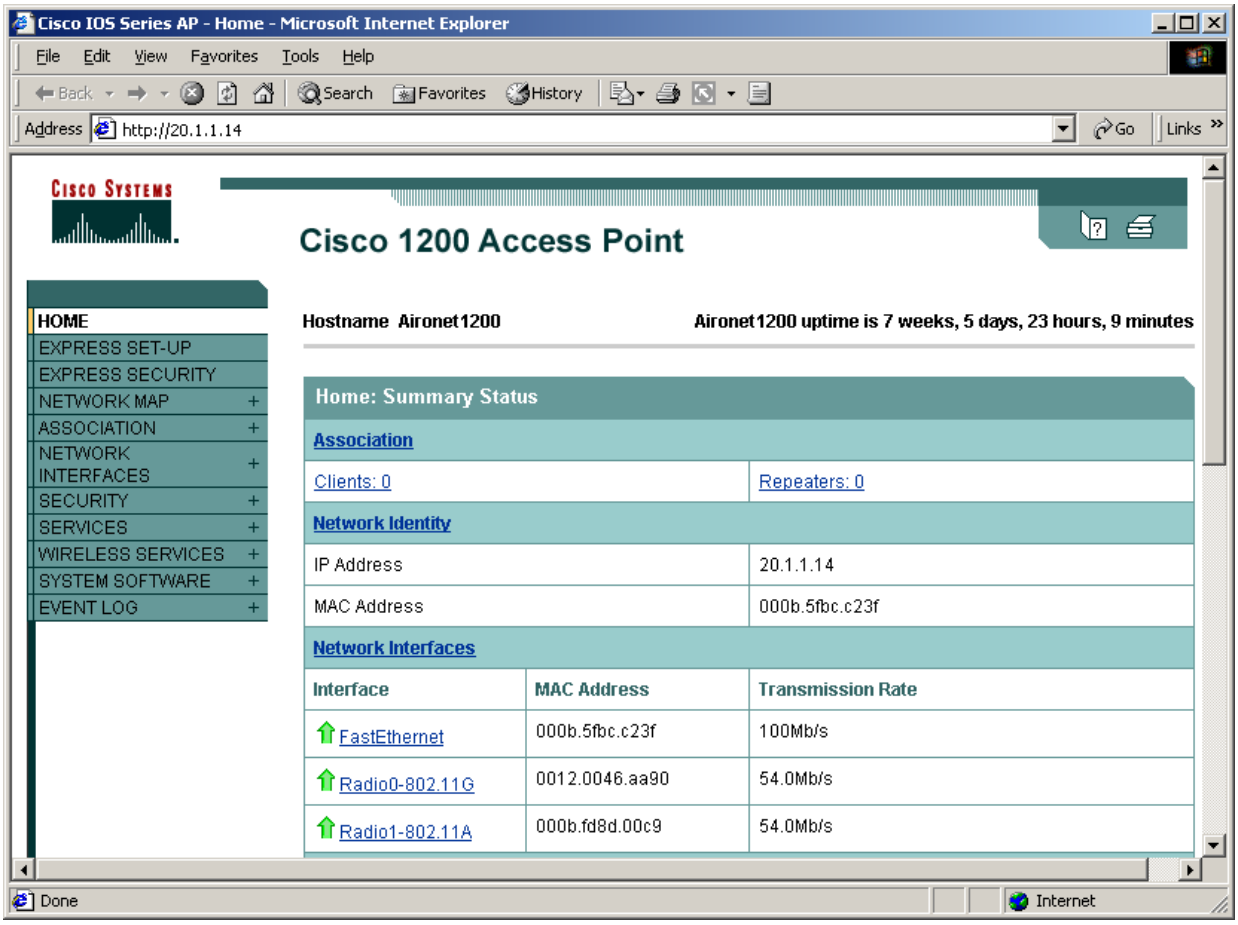
Assume that an IP address 20.1.1.14 has been pre-configured on the Access Point. For assigning an IP address to the Access Point via a console connection, refer to the Cisco Aironet 1200 configuration documentation at http://www.cisco.com/. The following sessions display the related configuration using a web-based interface.

3.1. Basic System and Wired Equivalent Privacy (WEP) Configuration

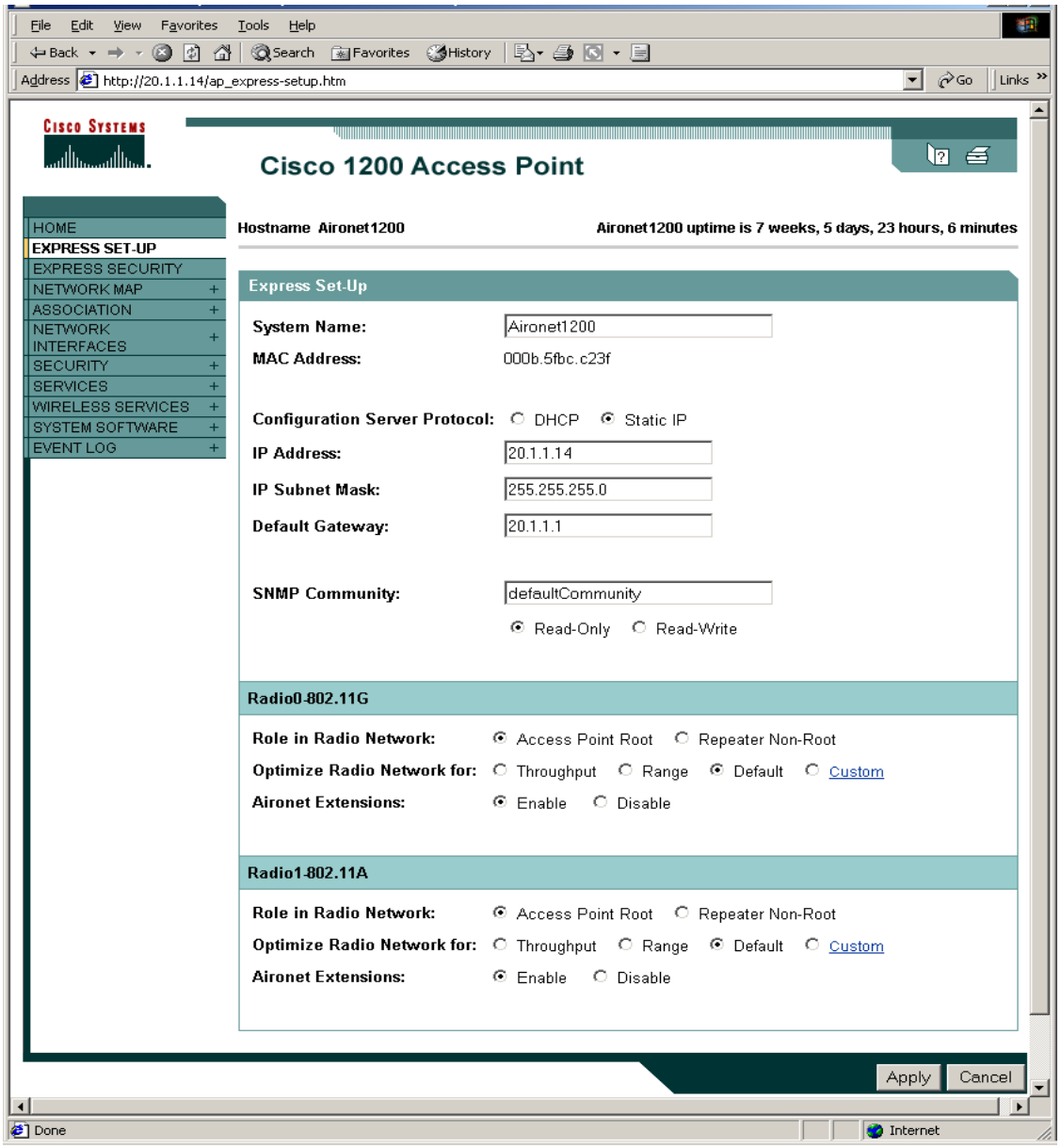
This section presents the steps for basic system IP and WEP configuration for the 802.11g radio interface. The Cisco Aironet 1200 Access Point used in these Application Notes has two radio interfaces (802.11a and 802.11g). The 802.11g radio interface is configured to also accept 802.11b clients to support Avaya 3616 and 3626 Wireless IP Telephones. The Avaya 3626 and Avaya 3616 IP Wireless Telephones operate at 802.11b mode and support WEP encryption.

Step	Description
1.	• Launch a web browser with the URL **http://20.1.1.14**. Log into the AP. • **Click** OK**.** 

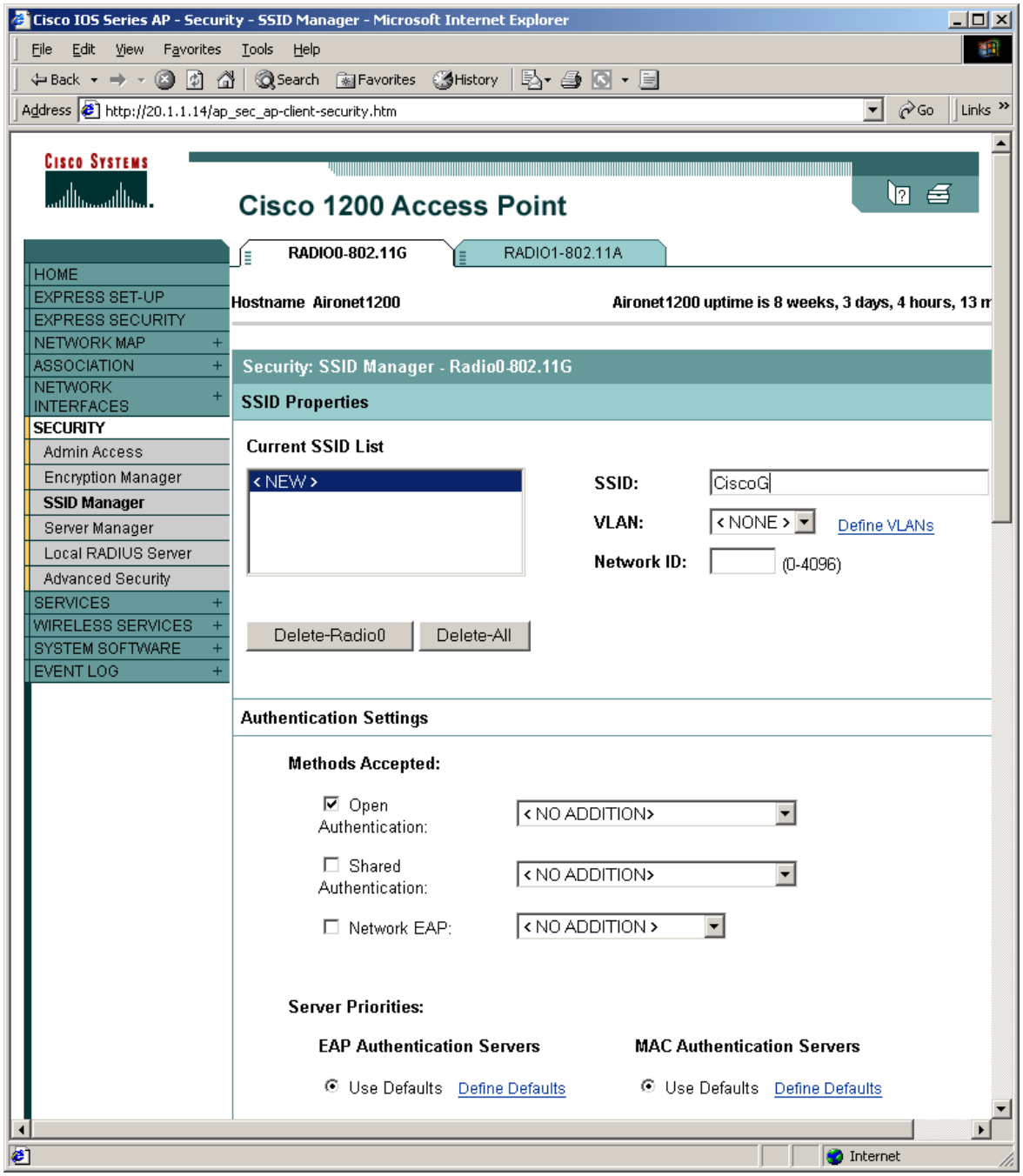
Step	Description
2.	The main configuration menu is shown below. All configurations are performed by choosing from the left panel.
3.	• Click **EXPRESS SET-UP** from the left panel and enter the information as shown below. • Verify that the **IP address**, **Subnet Mask** and **Default Gateway** are correctly configured.

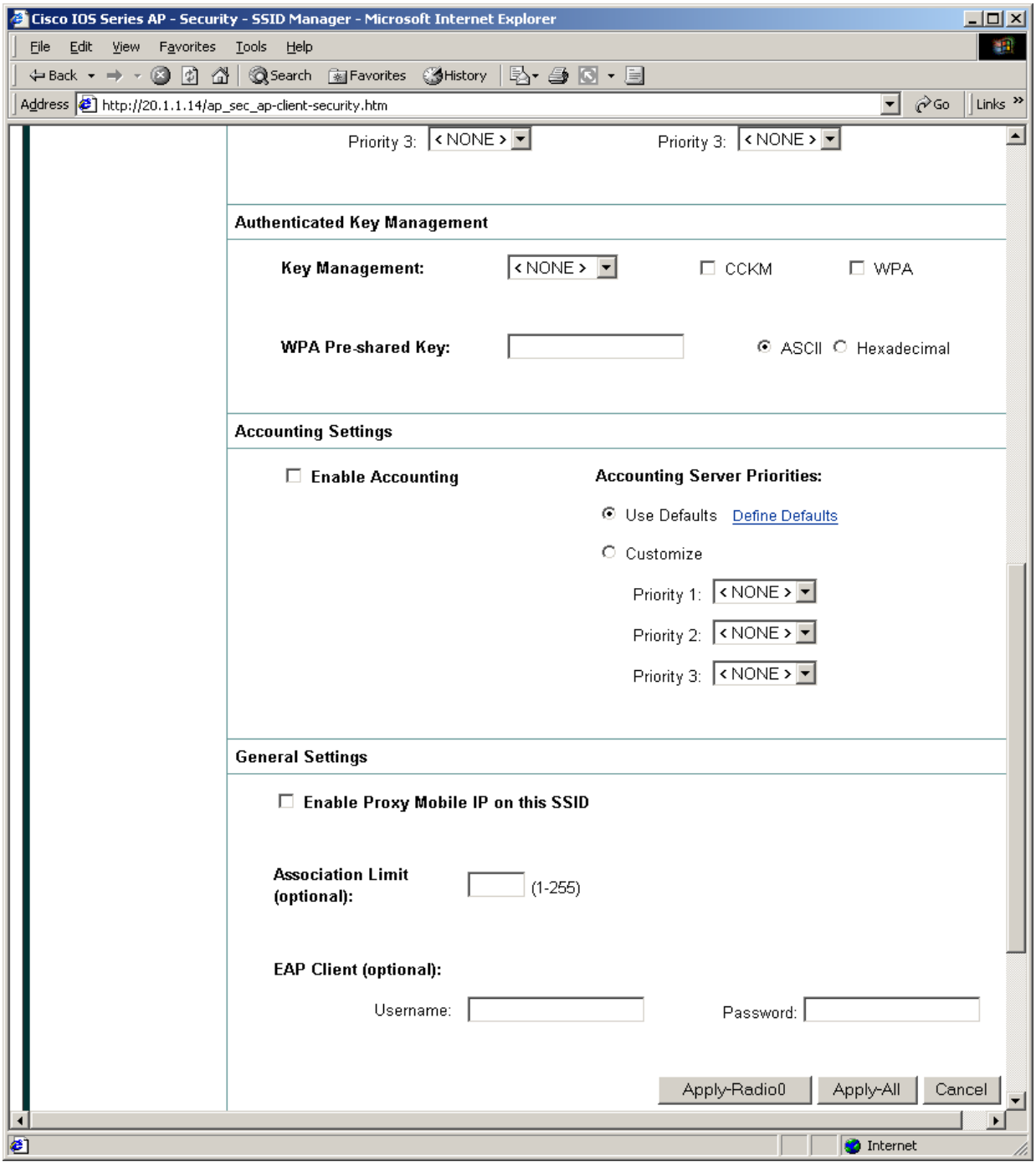


Step	Description
	• Leave **SNMP Community** as **defaultCommunity** and click **Read-Only**. • Click **Access Point Root** for **Role in Radio Network** for both interfaces. Note that the access point is configured as a root device when it is connected to the wired LAN. If the AP is not connected with a wired LAN, it should be configured as a repeater (non-root) device. • Leave the default settings as shown below. • Click **Apply**.

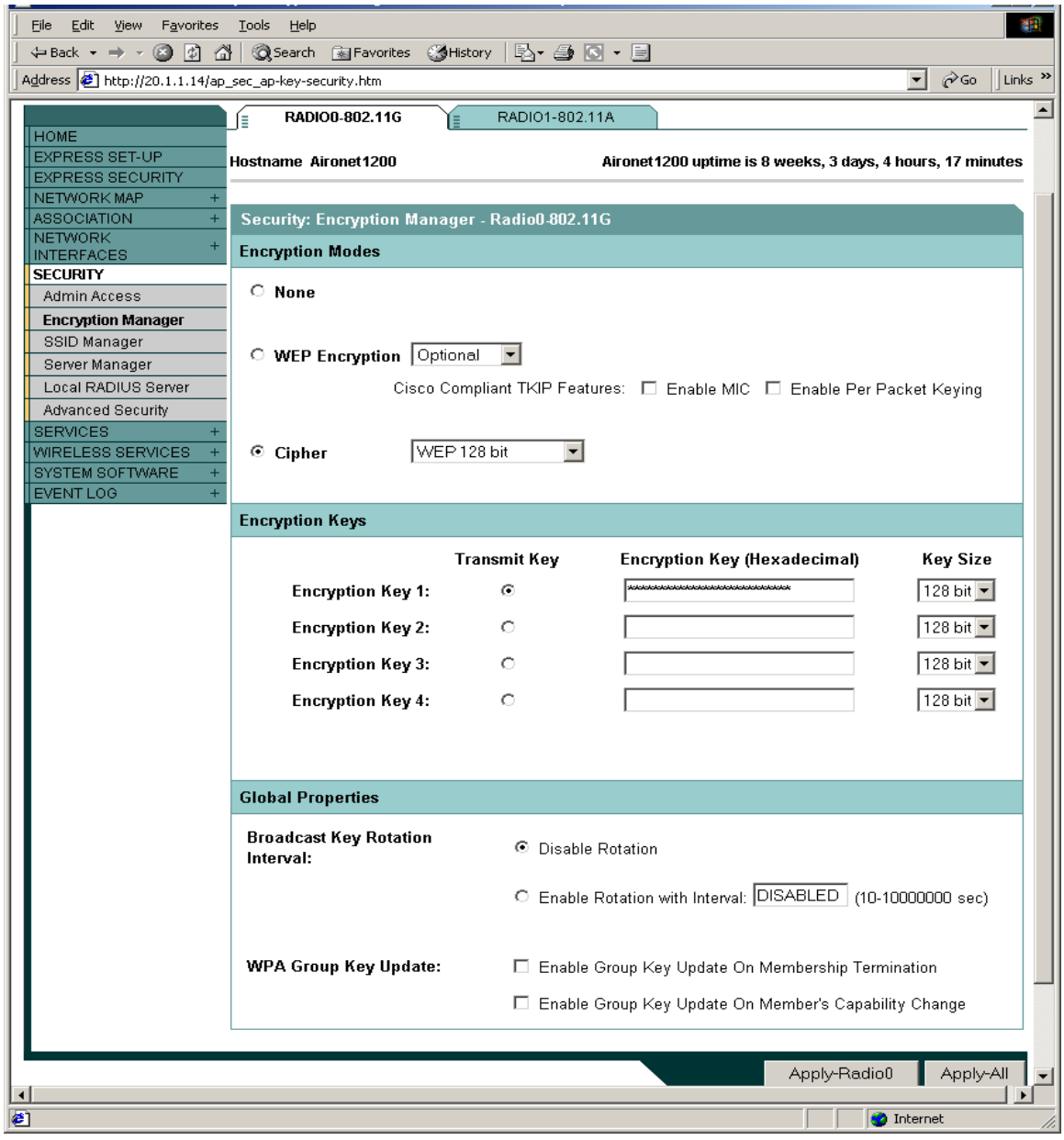


Step	Description
4.	The following screen displays the SSID and authentication settings for the 802.11g radio interface. • Click **SECURITY → SSID Manager** from left panel. • Enter a unique **SSID** (e.g., **CiscoG**) in the **SSID** field for the 802.11g radio interface. • Click **Open Authentication** for the **Authentication Settings**.



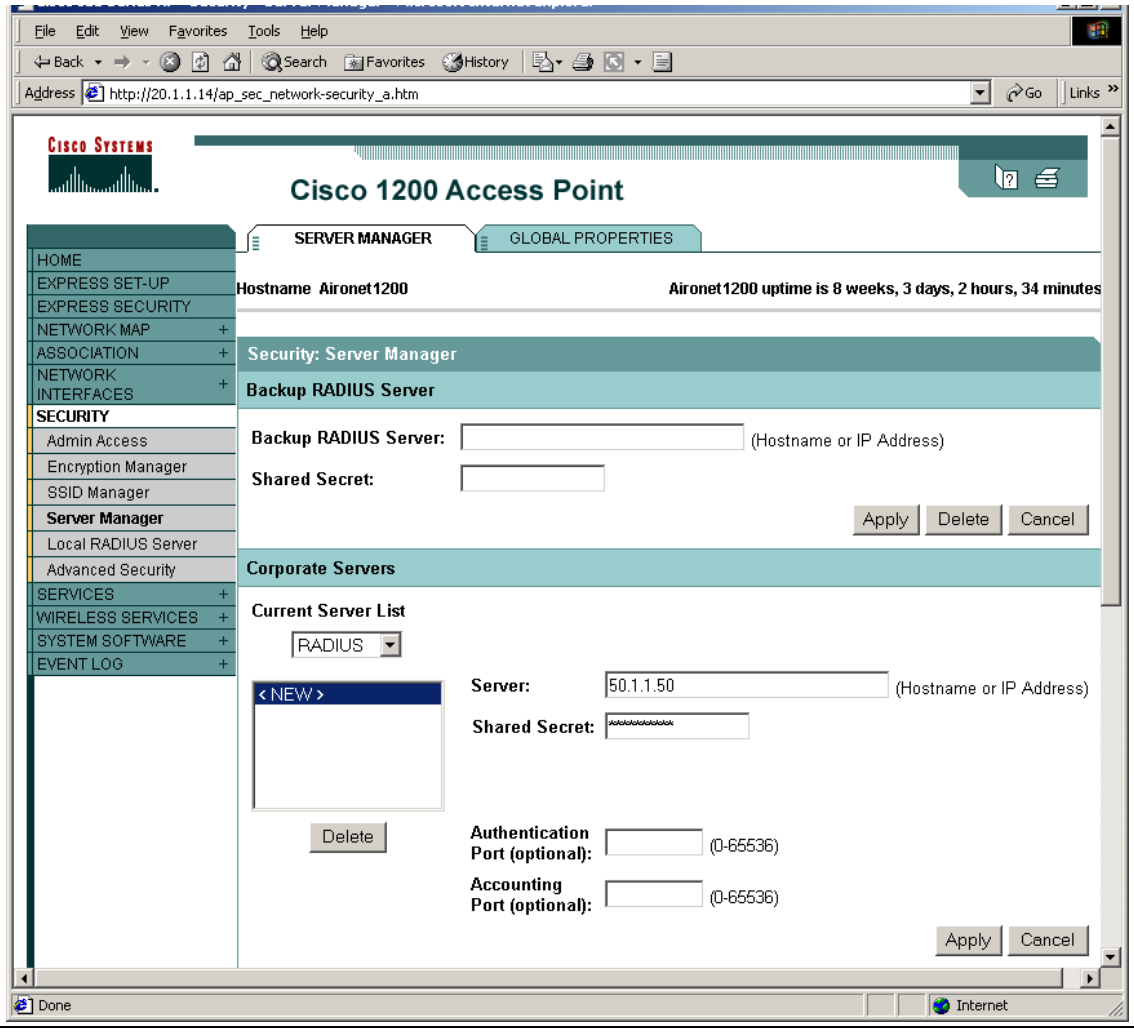
Step	Description
5.	• Leave default settings. • Click **Apply-Radio0.** (Note: Radio0 is the 802.11g radio interface) 

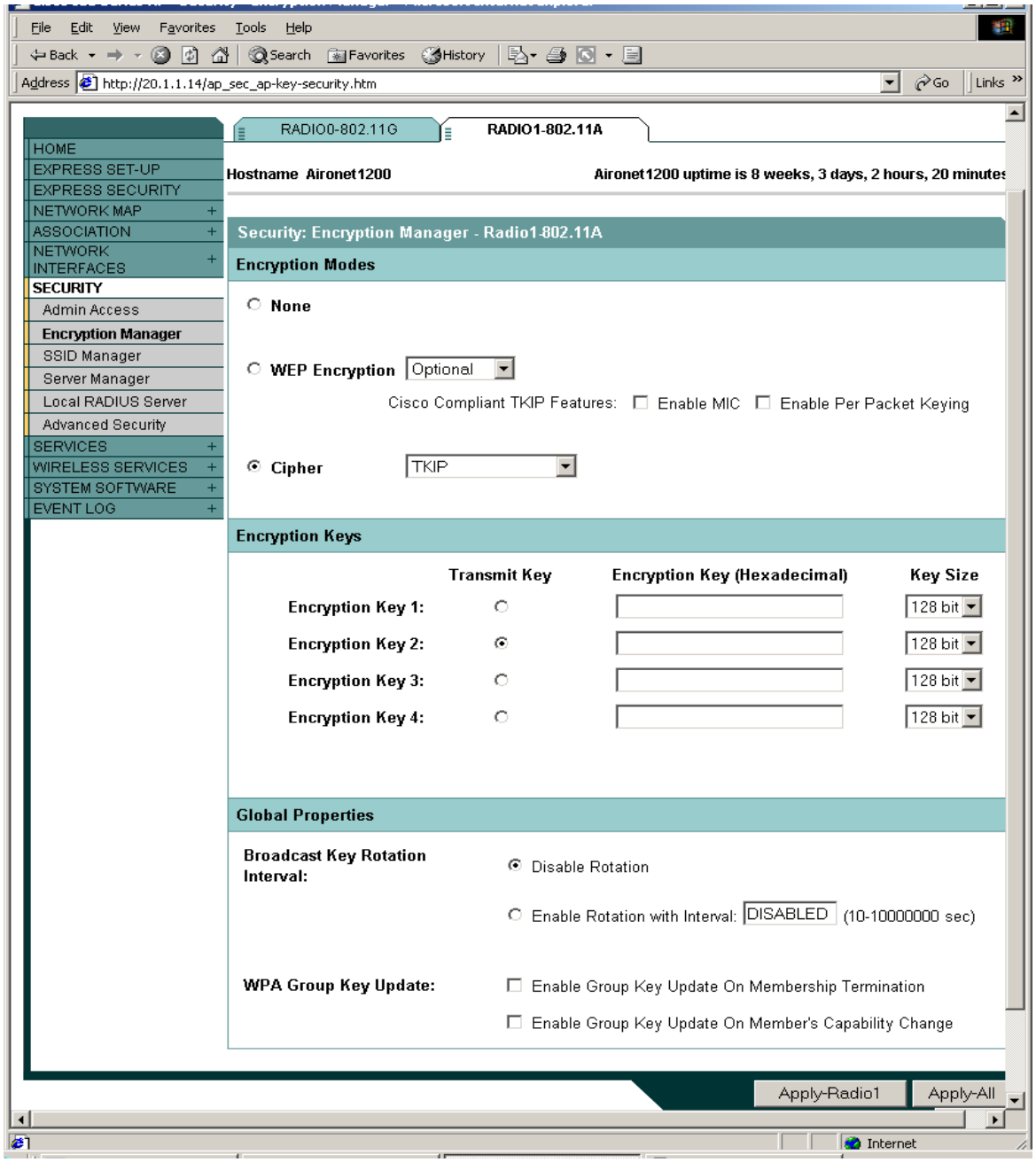
Step	Description
6.	The following screen displays the encryption settings for the 802.11g radio interface. • Click **SECURITY → Encryption Manager** from the left panel. • Click **Cipher** and select **WEP 128 bit** for encryption. • Click **Encryption Key 1** and enter 26 digits for **Encryption Key**. Note this key must match the key entered in the Wireless IP Telephones. • Click **Apply-Radio0**.



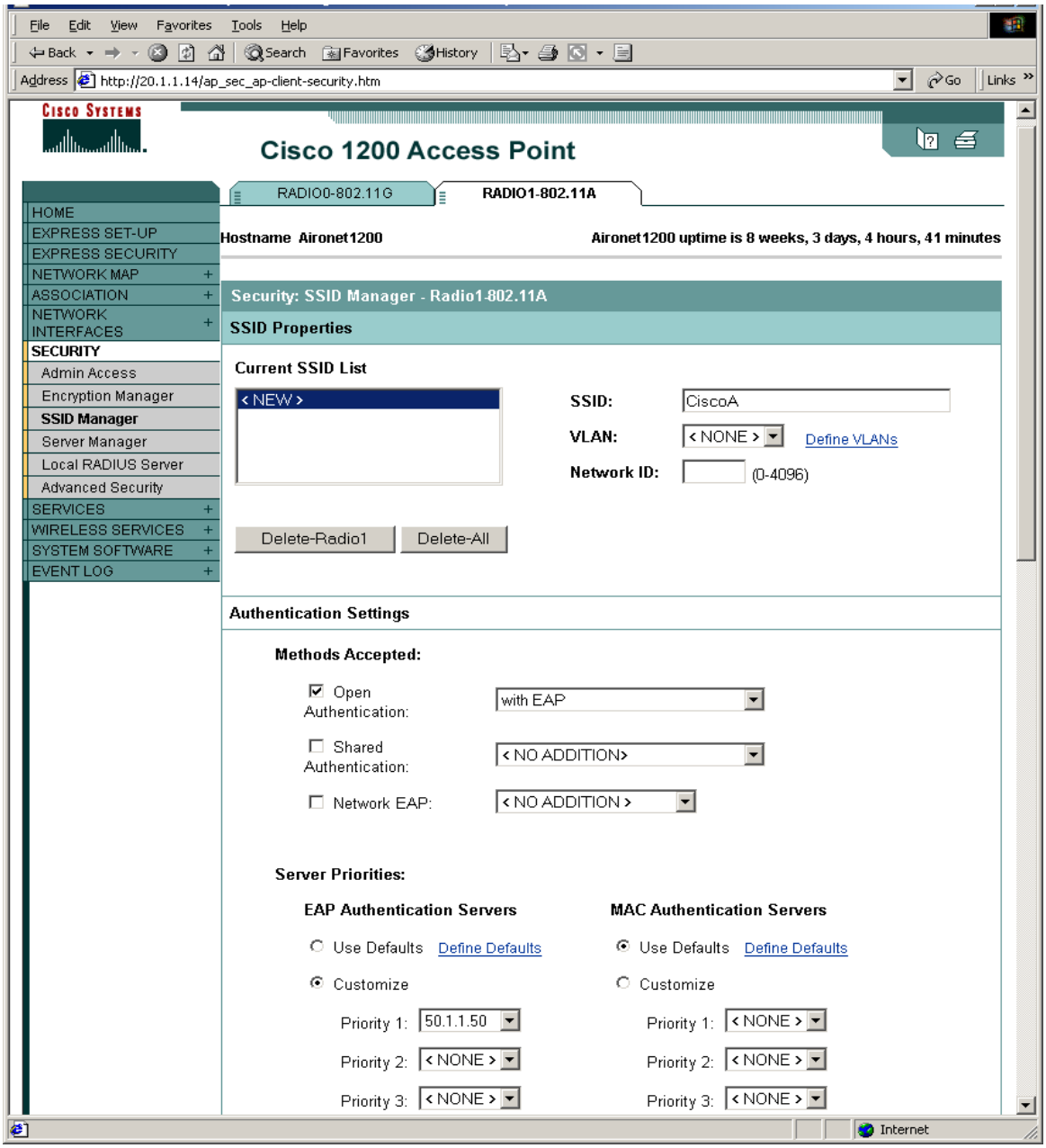
3.2. 802.1x Authentication Configuration for 802.11a Radio Interface

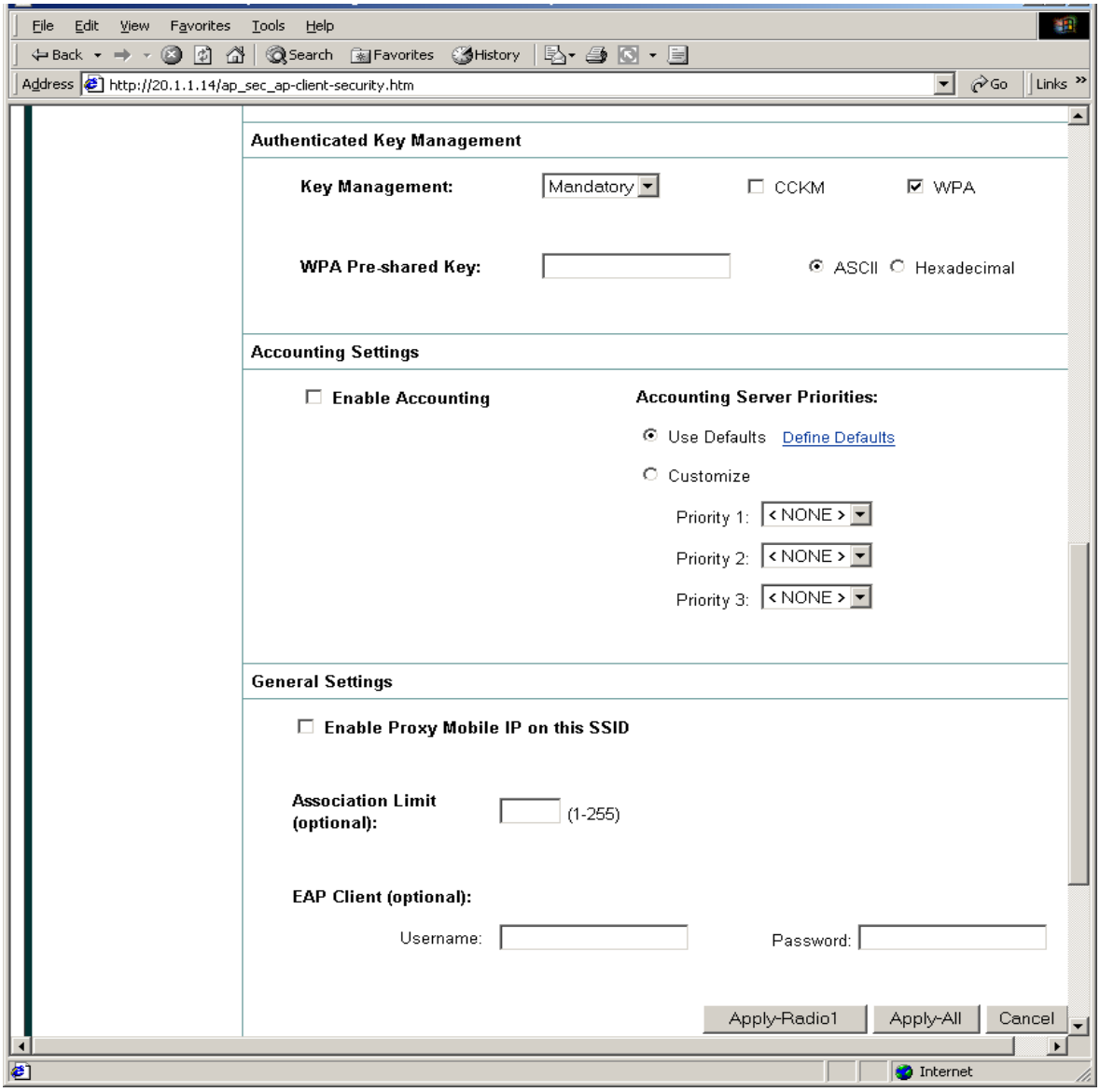
The 802.11a radio interface is configured to work with the Odyssey RADIUS Server and Client providing 802.1x authentication for the computer running Avaya IP Softphone. This section presents the RADIUS Server and the 802.1x authentication configuration for 802.11a radio interface. This configuration verifies that the computer running Avaya IP Softphone with Odyssey Client can pass 802.1x authentication from the Odyssey RADIUS Server through the Aironet 1200 Access Point.

Step	Description
1.	The following screen displays the Access Point's configuration related to the RADIUS Server. • Click **SECURITY → Server Manager** from left panel as shown below. • Select **RADIUS** under **Current Server List**. • Enter the RADIUS Server's IP address **50.1.1.50** into the **Server** field and **password** into **Shared Secret** field. Note the shared secret entered here must match the one entered in the RADIUS Server. • Click **Apply**. 

Step	Description
2.	The following screen displays the encryption settings for the 802.11a radio interface. • Click **SECURITY → Encryption Manager** from the left panel as shown below. • Click **Cipher** for the **Encryption Modes** and select **TKIP** (Temporal Key Integrity Protocol). • Leave other default settings. • Click **Apply-Radio1**. 

Step	Description
3.	The following screen displays the SSID and authentication settings for the 802.11a radio interface. • Click **SECURITY → SSID Manager** from the left panel as shown below. • Enter a unique **SSID** (e.g. CiscoA) in the **SSID** field for the 802.11a radio interface. • Check **Open Authentication** and select **with EAP** for **Authentication Settings**. • Click **Customize** and select **50.1.1.50** in the **Priority 1** field under **EAP Authentication Servers**.



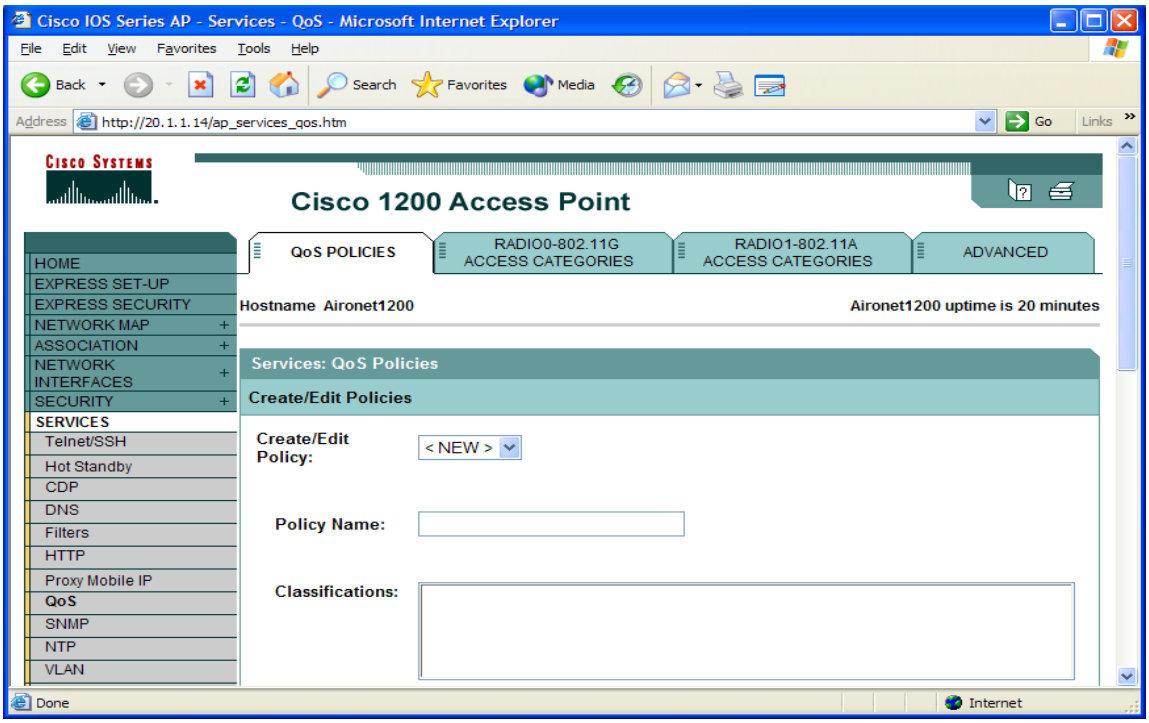
Step	Description
4.	• Select **Mandatory** and **WPA** under **Authenticated Key Management**. • Leave other as default settings. • Click **Apply-Radio1**. 

For detailed Funk Odyssey RADIUS Server and Client configuration, refer to the Application Notes [3] listed in the Reference section and documents from Funk Software web site at http://www.funk.com/.

3.3. Configure Quality of Service (QoS)

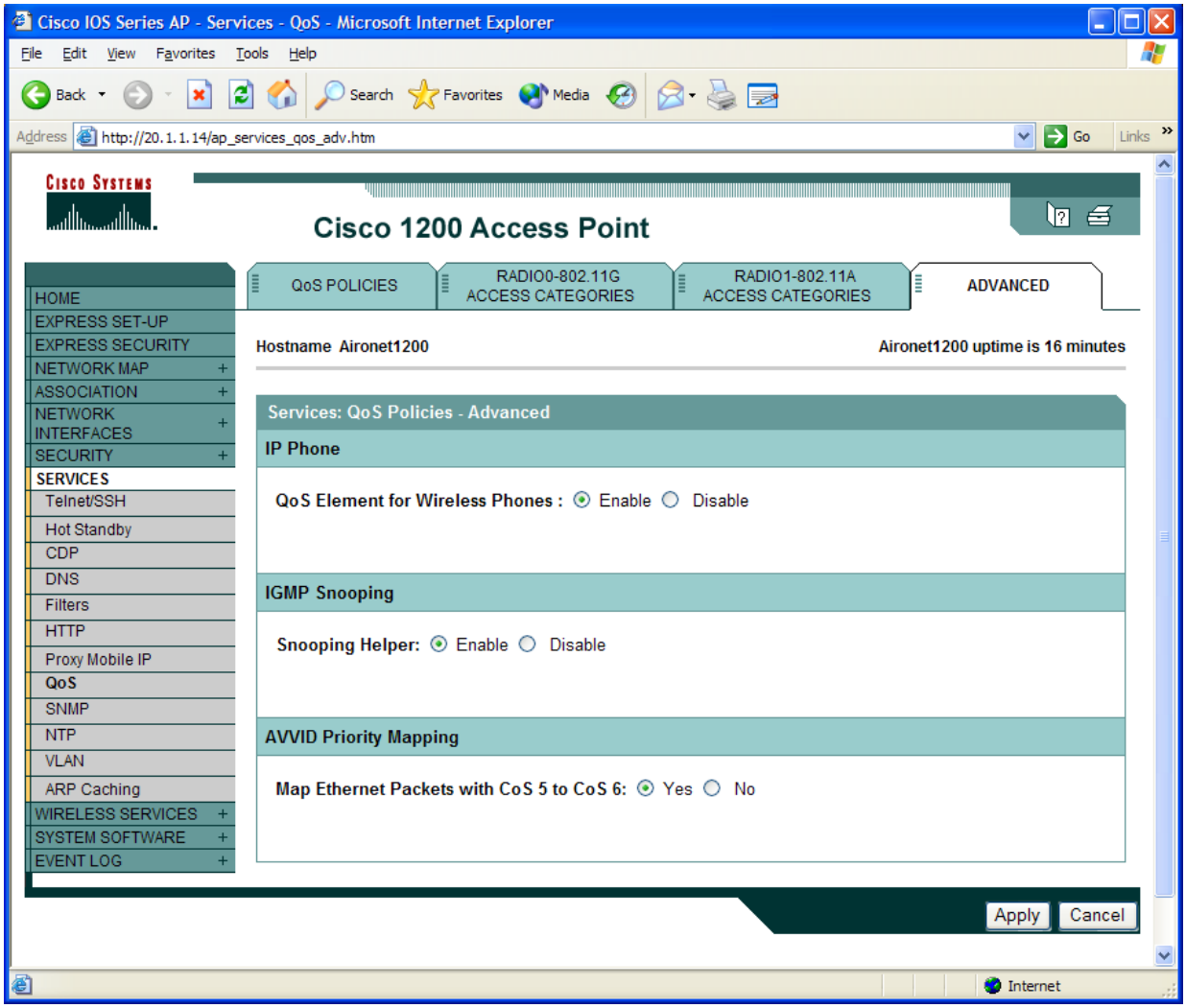
This section presents the QoS configuration for Cisco Aironet 1200 AP. The QoS implementation for wireless LANs differs from QoS implementations on other Cisco devices. For detailed QoS implementation for Aironet 1200 Access Point, refer to "Cisco Aironet 1200 Series Access Point Installation and Configuration Guide" at http://cisco.com.

Cisco Aironet 1200 Access Point can be configured to give priority for all voice traffic via a global QoS configuration. It can also be configured to prioritize voice traffic using individual policies based on either CoS or DSCP value, or protocol type. By default, once the QoS is globally enabled, the Aironet 1200 Access Point will give voice traffic priority based on DSCP values 34 (af41) for signaling and 46 (ef) for audio, or protocol type 119 (SpectraLink protocol). A global QoS configuration is used in these Application Notes. The QoS configuration generated by the Access Point is applied to both 802.11g and 802.11a radio interfaces.

Step	Description
1.	**Enable QoS for all Voice Traffic** Avaya 3626 and 3616 series Wireless IP Telephones use protocol 119 (SpectraLink protocol) for communication. The command "change IP-network-region" in the Communication Manager SAT screens will be used to configure the DSCP value for Avaya IP Softphone. Refer to Application Notes [4] for detailed configuration. Follow the steps below to enable QoS on the Cisco Aironet Access Point 1200. • Click **SERVICES** from the left side panel. When the list of services expands, click **QoS**. The **QoS POLICIES** page appears as shown below. 

2.

- Click the **ADVANCED** tab.
- Click **Enable** for **QoS Element for Wireless Phones**.
- Leave the default setting **Enable** for **Snooping Helper**.
- Leave default setting **Yes** for **Map Ethernet Packets with CoS 5 to CoS 6**.
- Click **Apply**.



Once the QoS is enabled from the web interface, the Aironet 1200 Access Point automatically adds the following to the configuration file. Below is the display of the results of QoS configuration generated from the Aironet 1200 Access Point command line interface.

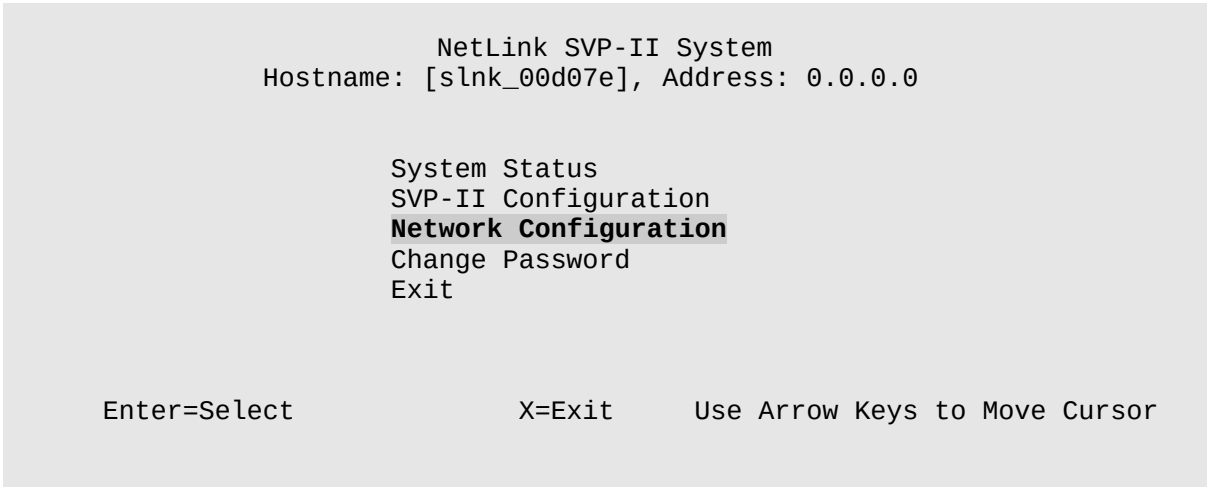
```
class-map match-all _class_VoIP2
    match ip dscp af41
  class-map match-all _class_VoIP0
    match ip protocol 119
  class-map match-all _class_VoIP1
     match ip dscp ef
 !
  policy-map VoIP
   class _class_VoIP0
    set cos 6
   class _class_VoIP1
   set cos 6
  class _class_VoIP2
   set cos 6

 interface Dot11Radio0
  no ip address
  service-policy input VoIP
  service-policy output VoIP
  no ip route-cache
!
 interface Dot11Radio1
  no ip address
  service-policy input VoIP
  service-policy output VoIP
  no ip route-cache

!
 interface FastEthernet0
  no ip address
  service-policy input VoIP
  service-policy output VoIP
  no ip route-cache
```

4. Configure the Avaya Voice Priority Processor

The Avaya Voice Priority Processor functions as a Wireless VoIP gateway and provides voice priority service for Avaya Wireless IP Telephones. The following steps describe the configuration.

Step	Description
1.	Using a console cable, connect the Avaya Voice Priority Processor to a PC's serial port.
2.	Start a HyperTerminal session to the Avaya Voice Priority Processor. • Bits per second **9600** • Data bits **8** • Parity **None** • Stop bits **1** • Flow control **None**
3.	Provide the **User Name** and **Password** to access the Avaya Voice Priority Processor. • The following **NetLink SVP-II System** window is displaced. • Select **Network Configuration** • Press **Enter**  NetLink SVP-II System Hostname: [slnk_00d07e], Address: 0.0.0.0 System Status SVP-II Configuration **Network Configuration** Change Password Exit Enter=Select X=Exit Use Arrow Keys to Move Cursor

Step	Description
4.	The **Network Configuration** window will be displayed. • Provide the following information: o **IP Address** = 50.1.1.9 o **Subnet Mask** = 255.255.255.0 o **Default Gateway** = 50.1.1.1 o Press **Enter**

```
                          Network Configuration
                Hostname: [slnk_00d07e], Address: 0.0.0.0

     Ethernet Address (fixed):      00:90:7A:00:D0:7E
     IP Address:                    50.1.1.9
     Hostname:                      slnk_00d07e
     Subnet Mask:                   255.255.255.0
     Default Gateway:               50.1.1.1
     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
```

Step	Description
5.	On the **NetLink SVP-II System** window: • Select **SVP-II Configuration**, • Press **Enter**. NetLink SVP-II System Hostname: [slnk_00d07e], Address: 50.1.1.9 System Status **SVP-II Configuration** Network Configuration Change Password Exit Enter=Select X=Exit Use Arrow Keys to Move Cursor
6.	On the **SVP-II Configuration** window: • Select **Reset System**, • Press **Enter**. This will reconfigure the Avaya Voice Priority Processor with current settings. SVP-II Configuration Hostname: [slnk_00d07e], Address: 50.1.1.9 Phones per Access Point: 5 SVP-II Mode: Netlink IP System Locked: N Maintenance Lock: N Reset System Enter=Change Esc=Exit Use Arrow Keys to Move Cursor

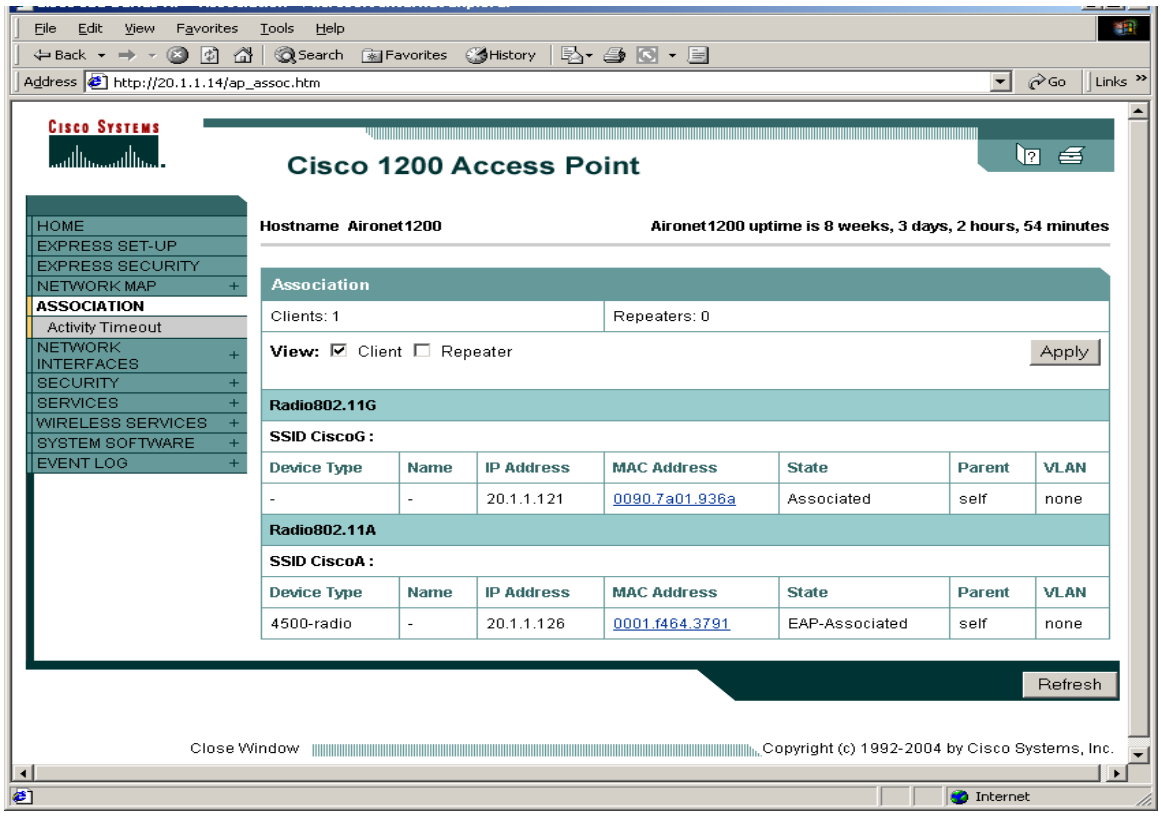
5. Configure the Avaya S8500 Media Server with the Avaya G650 Media Gateway

Refer to Application Note [1] for Avaya S8500 Media Server and Avaya G650 Media Gateway configuration.

6. Verification Steps

The following verification steps were used to verify correct system operation:

- Verify network connectivity by launching pings between the S8500 Media Server and Wireless laptop PC. Verify that all pings are successful.
- Power up the Avaya 3616 and 3626 IP Wireless Telephones. Enable WEP on both IP Wireless Telephones and verify that they can register with the S8500 Media Server.
- Make a phone call between the two Wireless IP Telephones and verify that the voice quality is good.
- Make a call from the 3626 Wireless IP Telephone to the 4620SW IP Telephone, and verify that the voice quality is good.
- Then create a conference call to the 4610SW IP Telephone. Verify that all three parties are in the conference call and voice quality is good.
- Enable 802.1x on the Odyssey Client and verify that the Odyssey RADIUS server can authenticate the Client.
- Launch the Avaya IP Softphone and verify that the Avaya IP Softphone can register with the S8500 Media Server.
- Make a call from the Avaya IP Softphone to the Avaya 4610SW IP Telephone and verify that voice quality is good.
- Select **ASSOCIATION** from Aironet 1200Access Point menu to display the clients' status as shown below.



7. Conclusion

These Application Notes illustrate the procedures necessary to configure the Cisco Aironet 1200 Wireless Access Point to support Avaya Communication Manager, Avaya IP Wireless Telephones and Avaya IP Softphone. The Cisco Aironet 1200 Access Point support 802.11 a, 802.11b and 802.11g radios.

8. References

Use this URL http://www.avaya.com/ to access these Application Notes.

[1] Application Notes for Configuring 3Com Wireless LAN Access Point 8750 to Support Avaya Communication Manager, Avaya IP Wireless Telephones and Avaya IP Softphone - Issue 1.0

[2] Configuring the Avaya 3606 Wireless Telephone with Compatible 802.11b Access Points from Avaya and Other Vendors - Issue 1.0

[3] Configuring the Funk Odyssey Software, Avaya Access Point 3 and Avaya 802.11a/b Wireless Client for User Authentication (802.1x) and Data Encryption - Issue 1.0

Use the following URL http://www.funk.com to access configuration documentation for Funk Odyssey products.

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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com