



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Enterasys Wireless Access Point 3000 (RBT3K-AG) to Support Avaya IP Office, Avaya IP Wireless Telephones and Avaya Phone Manager Pro - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Enterasys Wireless Access Point 3000 (RBT3K-AG) to support Avaya IP Office, Avaya IP Wireless Telephones and Avaya Phone Manager Pro.

1. Introduction

These Application Notes describe the steps necessary to configure Enterasys Wireless Access Point 3000 (RBT3K-AG) to support Avaya IP Office, Avaya Wireless Telephones and Avaya Phone Manager Pro. The network infrastructure used for verification is shown in **Figure 1**.

These Application Notes cover the following areas:

- System IP and Wireless 802.11a/b/g radio configurations.
- Wired Equivalent Privacy (WEP) encryption
- 802.1x RADIUS authentication with WPA encryption.

These Application Notes do not cover the configuration for Avaya IP Wireless Telephones, Avaya Phone Manager Pro, Odyssey RADIUS Server and Clients. For detailed configuration on these devices, refer to the Application Notes listed in Section 7.

In the release tested, the Enterasys AP 3000 RBT 3K-AG did not support Spectralink Voice Priority (SVP), which is required for ensuring over the air Quality of Service (QoS).

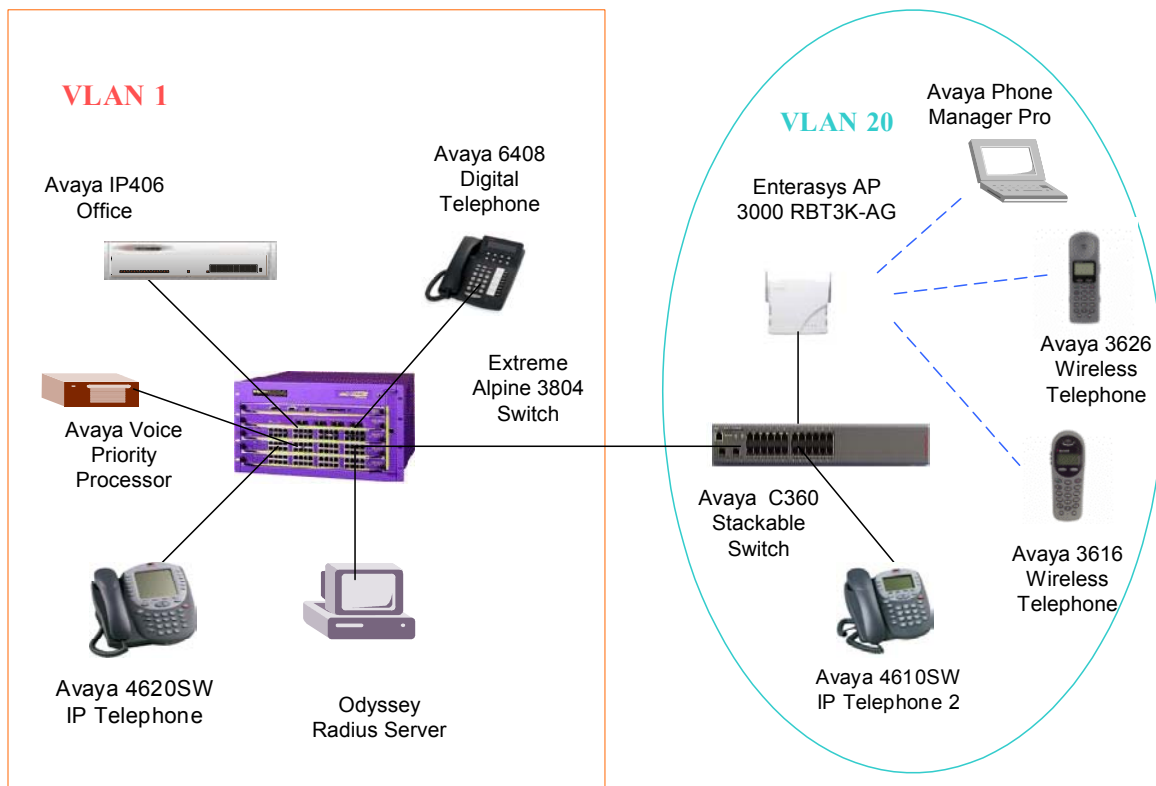


Figure 1: Network Configuration

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

Device	VLAN	IP Address/Mask	Gateway
Avaya IP406 Office	VLAN 1	50.1.1.10 /24	50.1.1.1
Avaya Voice Priority Processor	VLAN 1	50.1.1.9/24	50.1.1.1
Avaya C360 Stackable Switch	VLAN20	20.1.1.2/24	20.1.1.1
Enterasys Wireless Access Point 3000 (RBT3K-AG)	VLAN 20	20.1.1.10/24	20.1.1.1
Extreme Alpine 3804 Switch	VLAN1 VLAN20	50.1.1.1/24 20.1.1.1/24	
Avaya 3626 Wireless Telephone		20.1.1.100	20.1.1.1
Avaya 3616 Wireless Telephone		20.1.1.101	20.1.1.1
Avaya Phone Manager Pro		20.1.1.126	20.1.1.1
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 IP406 Office	IP Office 2.1(29)
Avaya Phone Manager Pro	V2.1.6
Avaya 4620SW/4610SW IP Telephones	R2.01
Avaya 3616/3626 Wireless IP Telephone	96.024
Avaya Voice Priority Processor	R168.112
Avaya C360 Stackable Switch	R4.3.12
Enterasys Wireless Access Point 3000 (RBT3K-AG)	V2.1.2
Extreme Alpine 3804 Switch	V7.2.0b25
Dell Laptop with <ul style="list-style-type: none"> Windows XP 2000 Enterasys RoamAbout 802.11 a/b/g Wireless Card 	5.00.2195 V 3.0.0.111
Odyssey RADIUS Server	V2.01.00.653
Odyssey Client	V3.03.0.1194


Table 2: Equipment and Software Validated

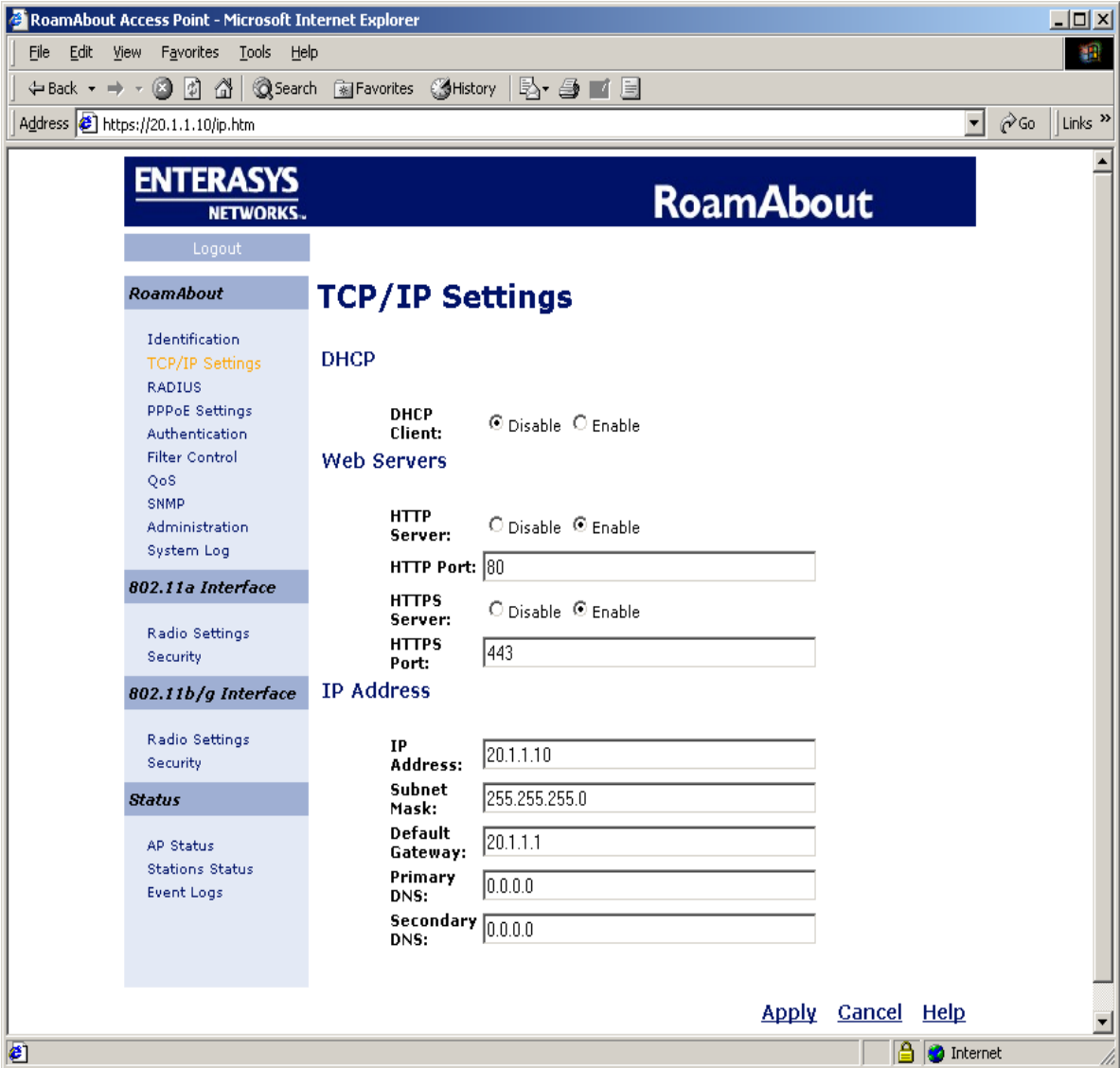
3. Configure Enterasys AP 3000 (RBT3K-AG)

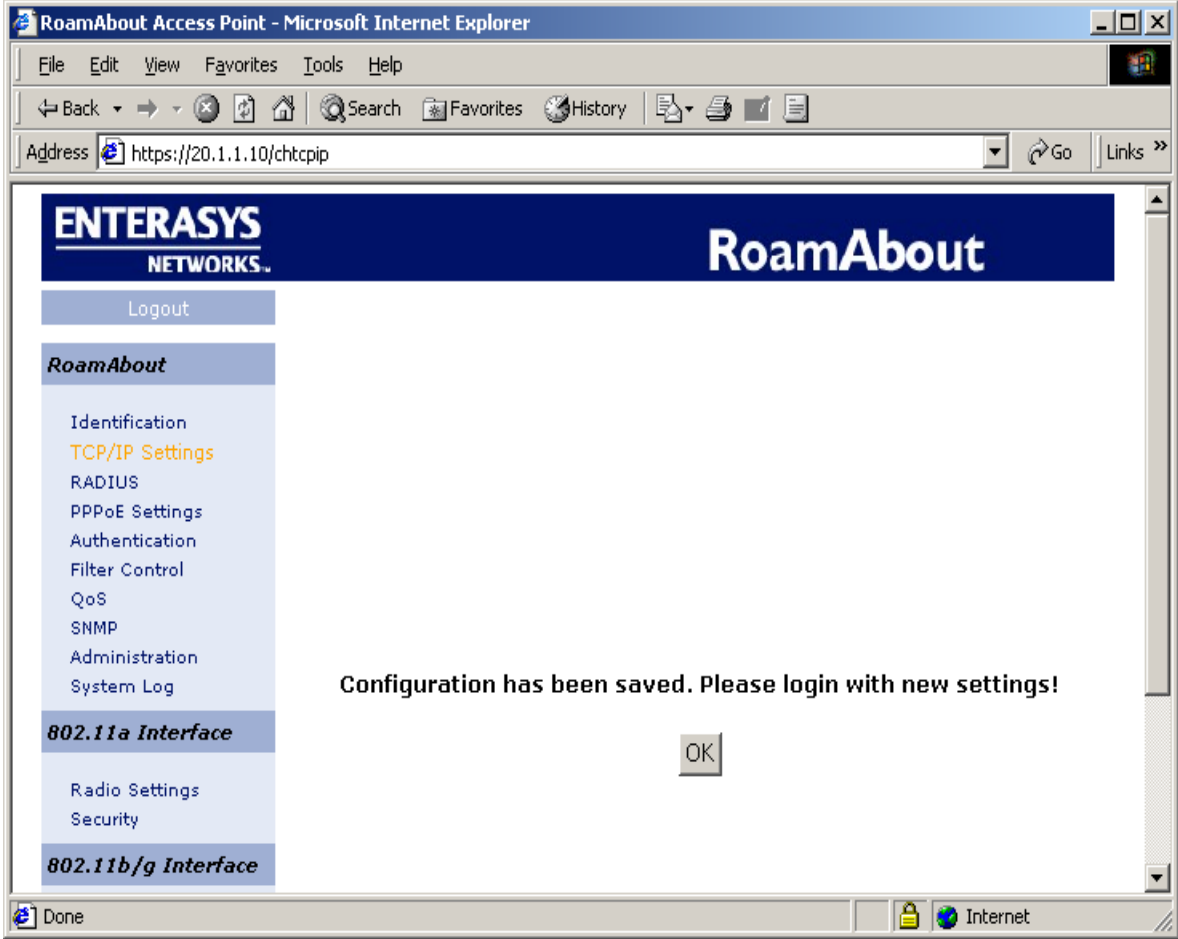
The configuration can be done using a web-based interface. Assume that the IP address 20.1.1.10 has been pre-configured on the Enterasys Wireless Access Point 3000. The following sessions display the related configuration using web-based interface.

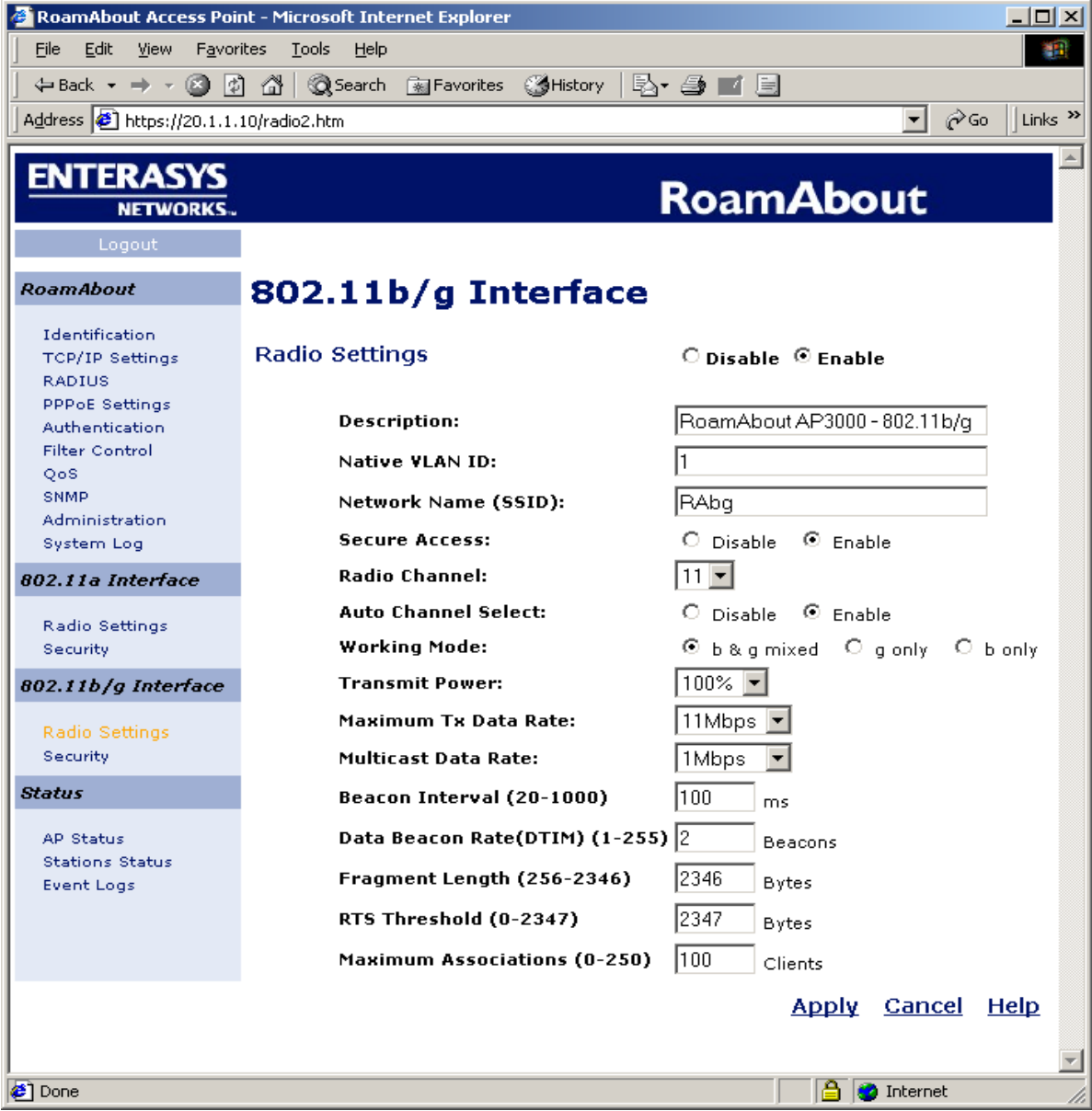
3.1. Basic System and Wired Equivalent Privacy (WEP) Configuration

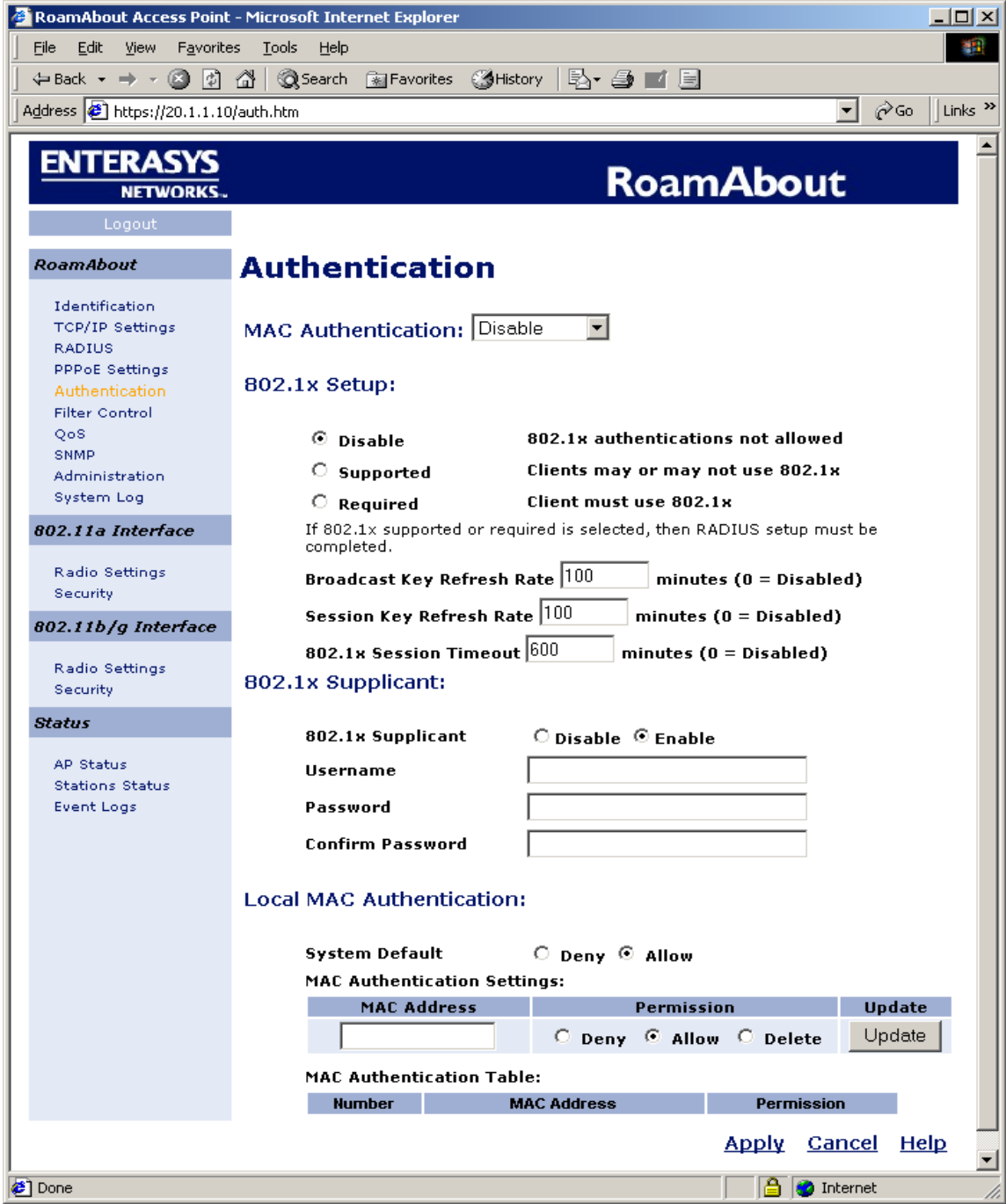
This section presents the steps of basic system wireless and WEP configuration. The Enterasys Wireless Access Point 3000 (RBT3K-AG) has both 802.11a and 802.11g radio interfaces. The 802.11g radio interface supports both 802.11b and 802.11g clients. In these Application Notes, the 802.11g radio is configured to accept both 802.11b and 802.11g clients to support the Avaya IP 3616 and 3626 IP wireless Telephones. Note that the Avaya 3626/3616 series wireless Telephones currently only operate in 802.11b mode. The 802.1x authentication is applied to the Avaya Phone Manager Pro using Odyssey Client.

Step	Description
1.	<ul style="list-style-type: none">Launch a web browser with the URL http://20.1.1.10. Log in the AP with proper user name and password as shown below. 

Step	Description
2.	<ul style="list-style-type: none"> After logging in, click TCP/IP Settings from the left panel. Disable DHCP Client since static IP address is used. Click Enable for HTTP Server and leave HTTP Port 80 as default. (Optional) Click Enable for HTTPS Server and leave port 443 as default. Verify the IP address and Subnet Mask are correct. 

Step	Description
	<ul style="list-style-type: none"> Click OK to login to AP again. 

Step	Description
3.	<p>The following sections display the 802.11b/g interface configuration.</p> <ul style="list-style-type: none"> Click the Radio Settings under 802.11b/g Interface from the left panel. Enter 1 for Native VLAN ID. Enter a unique Network Name (e.g. RAbg) as its SSID. Click Enable for Secure Access. Click Enable for Auto Channel Select. Click b & g mixed for Working Mode to accept both b and g clients. Leave other settings as defaults. Click Apply. 

Step	Description
4.	<p>This section presents the WEP configuration. Because the Avaya 3626 and 3616 wireless Telephones do not support 802.1x, the 802.1x authentication needs to be disabled on AP.</p> <ul style="list-style-type: none"> Click Authentication from left panel and click Disable for 802.1x authentication as shown below. Click Apply when done. 

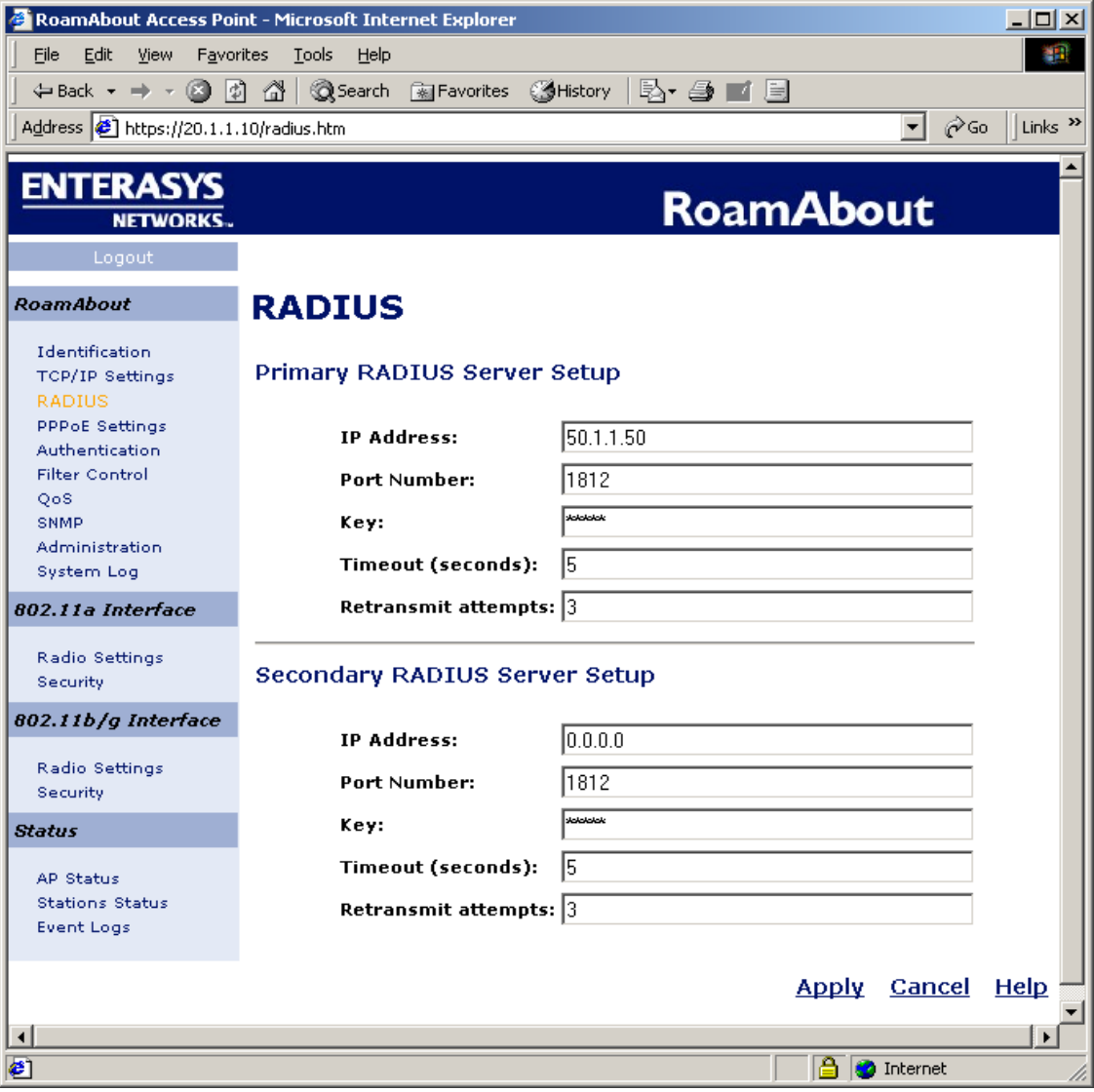
Step	Description
5.	<p>WEP configuration is shown on the next page.</p> <ul style="list-style-type: none"> • Click Security under 802.11b/g Interface from the left panel. • Select Shared Key for Authentication Type Setup. This will only allow users who have the correct key to access AP. • Click Enable for Data Encryption Setup. • Click WEP for Multicast Cipher Mode. • Click 128 Bit for Shared Key Setup (Note that Avaya IP 3626/3616 IP Telephones support both 40 and 128 bit key). • Click Hexadecimal for Key Type. • Enter 26 digits key string in Key1 field. Make sure this key matches the key entered in the IP Wireless Telephone. • Click Apply.

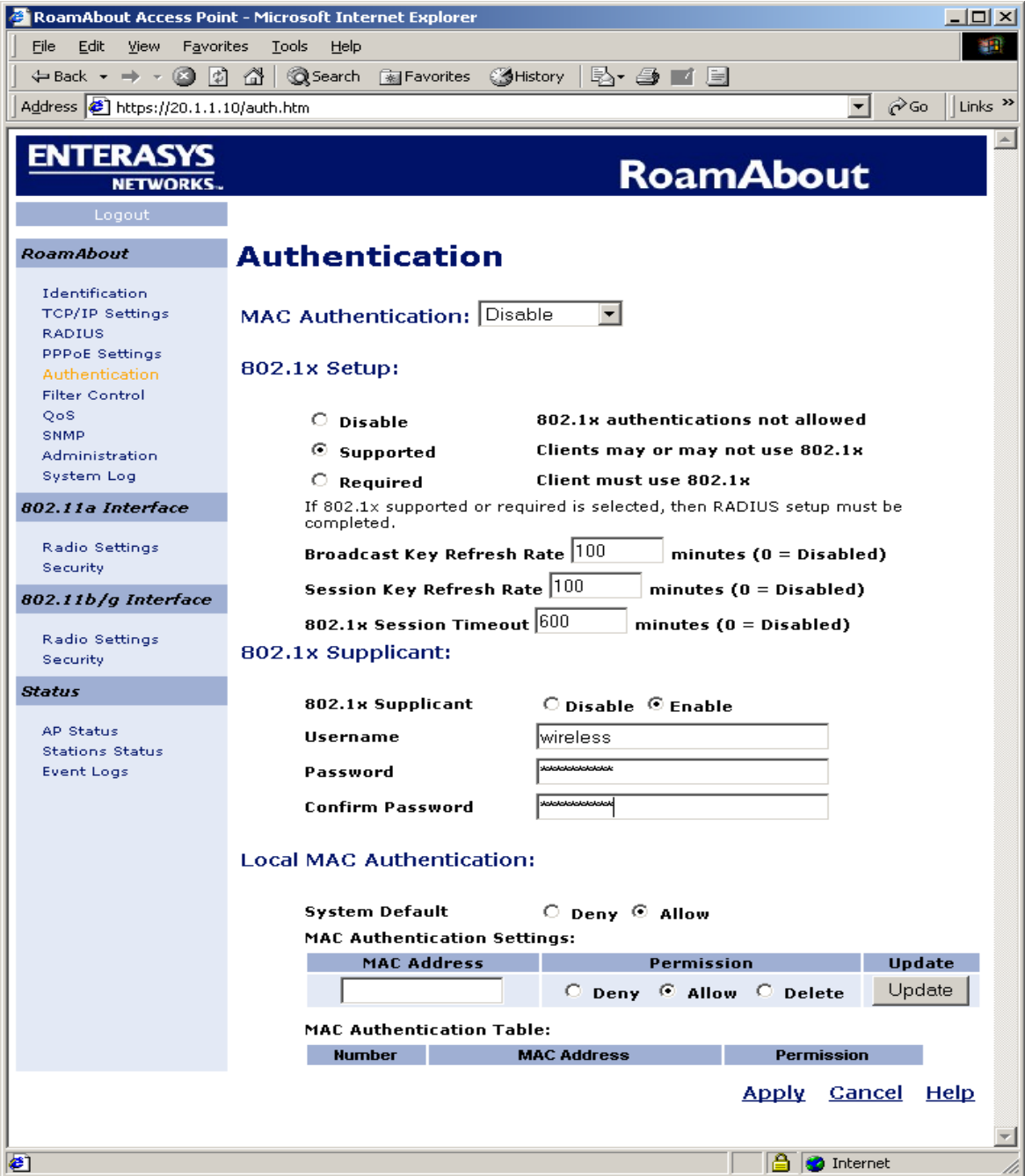
Step	Description															
	<div><div><div><div>RoamAbout Access Point - Microsoft Internet Explorer</div><div>File Edit View Favorites Tools Help</div><div>Back Forward Stop Home Search Favorites History Print</div><div>Address https://20.1.1.10/security2.htm Go Links >></div></div><div><div>RoamAbout</div><div>Identification</div><div>TCP/IP Settings</div><div>RADIUS</div><div>PPPoE Settings</div><div>Authentication</div><div>Filter Control</div><div>QoS</div><div>SNMP</div><div>Administration</div><div>System Log</div><div>802.11a Interface</div><div>Radio Settings</div><div>Security</div><div>802.11b/g Interface</div><div>Radio Settings</div><div>Security</div><div>Status</div><div>AP Status</div><div>Stations Status</div><div>Event Logs</div></div><div><div>802.11b/g Interface</div><div>Security Settings</div><div>Authentication Type Setup</div><div><div><input type="radio"/> Open System</div><div>Allow everyone to access</div></div><div><div><input checked="" type="radio"/> Shared Key</div><div>Allow users with a correct key to access</div></div><div>Data Encryption Setup</div><div><div><input type="radio"/> Disable</div><div><input checked="" type="radio"/> Enable</div></div><div>WPA Clients</div><div><div><input checked="" type="radio"/> Supported</div><div><input type="radio"/> Required</div><div><input type="radio"/> Not Supported</div></div><div>WPA Key Management</div><div><div><input checked="" type="radio"/> WPA authentication over 802.1x</div><div><input type="radio"/> WPA Pre-shared Key</div></div><div>Multicast Cipher Mode</div><div><div><input checked="" type="radio"/> WEP</div><div>Use WEP as WPA Multicast cipher mode</div></div><div><div><input type="radio"/> TKIP</div><div>Use TKIP as WPA Multicast cipher mode</div></div><div><div><input type="radio"/> AES</div><div>Use AES as WPA Multicast cipher mode</div></div><div>WPA Pre-Shared Key Type</div><div><div><input type="radio"/> Hexadecimal</div><div>Enter 64 digits</div></div><div><div><input checked="" type="radio"/> Alphanumeric</div><div>Enter between 8 and 63 characters</div></div><div>WPA Pre-Shared Key</div><div><input type="text"/></div><div>Shared Key Setup</div><div><div><input type="radio"/> 64 Bit</div><div><input checked="" type="radio"/> 128 Bit</div><div><input type="radio"/> 152 Bit</div></div><div>Key Type</div><div><div><div><input checked="" type="radio"/> Hexadecimal</div><div>For 64 Bit enter 10 digits, for 128 Bit enter 26 digits, for 152 Bit enter 32 digits</div></div><div><div><input type="radio"/> Alphanumeric</div><div>For 64 Bit enter 5 characters, for 128 Bit enter 13 characters, for 152 Bit enter 16 characters</div></div></div><div><table><tr><th>Key Number</th><th>Transmit Key Select</th><th>Key</th></tr><tr><td>Key 1</td><td><input checked="" type="radio"/></td><td><input type="text"/></td></tr><tr><td>Key 2</td><td><input type="radio"/></td><td><input type="text"/></td></tr><tr><td>Key 3</td><td><input type="radio"/></td><td><input type="text"/></td></tr><tr><td>Key 4</td><td><input type="radio"/></td><td><input type="text"/></td></tr></table></div><div>Apply Cancel Help</div></div></div></div>	Key Number	Transmit Key Select	Key	Key 1	<input checked="" type="radio"/>	<input type="text"/>	Key 2	<input type="radio"/>	<input type="text"/>	Key 3	<input type="radio"/>	<input type="text"/>	Key 4	<input type="radio"/>	<input type="text"/>
Key Number	Transmit Key Select	Key														
Key 1	<input checked="" type="radio"/>	<input type="text"/>														
Key 2	<input type="radio"/>	<input type="text"/>														
Key 3	<input type="radio"/>	<input type="text"/>														
Key 4	<input type="radio"/>	<input type="text"/>														

3.2. 802.1x Authentication Configuration

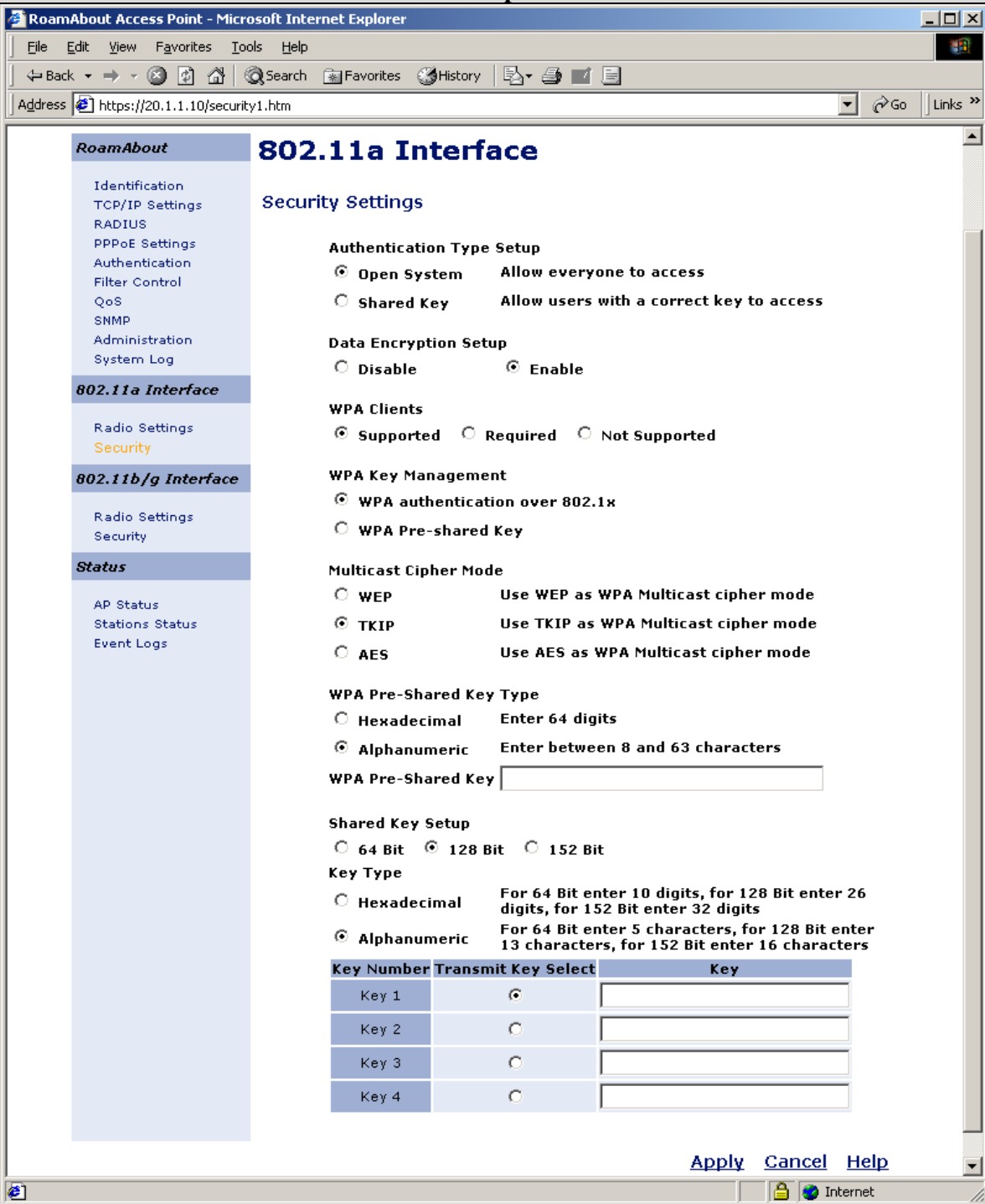
This section presents the 802.1x authentication configuration. This configuration verifies that the Avaya Phone Manager Pro with Odyssey Client can pass 802.1x authentication from the Odyssey RADIUS Server through the AP. Note this configuration does not apply to the Avaya 3626/3616 Wireless Telephones since those telephones do not support 802.1x.

Step	Description
1.	<p>Configure 802.11a Interface.</p> <ul style="list-style-type: none">Click the Radio Settings under 802.11a Interface from the left panel.Enter 1 for Native VLAN ID.Enter a unique Network Name (e.g. RAa) as its SSID.Click Enable for Secure Access.Leave other settings as defaults as shown below.Click Apply.

Step	Description
2.	<p>This section presents the RADIUS Server configuration.</p> <ul style="list-style-type: none"> Click Radius from left panel to enter the radius server information as shown below. Enter IP address 50.1.1.50 for primary RADIUS Server. Leave port number 1812 as default settings. Since only one RADIUS server is used in this configuration, leave IP address 0.0.0.0 in the field for the Secondary RADIUS Server. Enter shared key, 1234567890 is used in this case, in Key field. This Key is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant (Note the Key entered here must match the key entered in the RADIUS Server.). Click Apply. 

Step	Description
3.	<p>This section presents the Authentication configuration.</p> <ul style="list-style-type: none"> Click Authentication from left panel and click Supported under 802.1x Setup. Click Enable for 802.1x Supplicant. Enter wireless as Username and enter password in fields as shown below. Click Apply when done. 

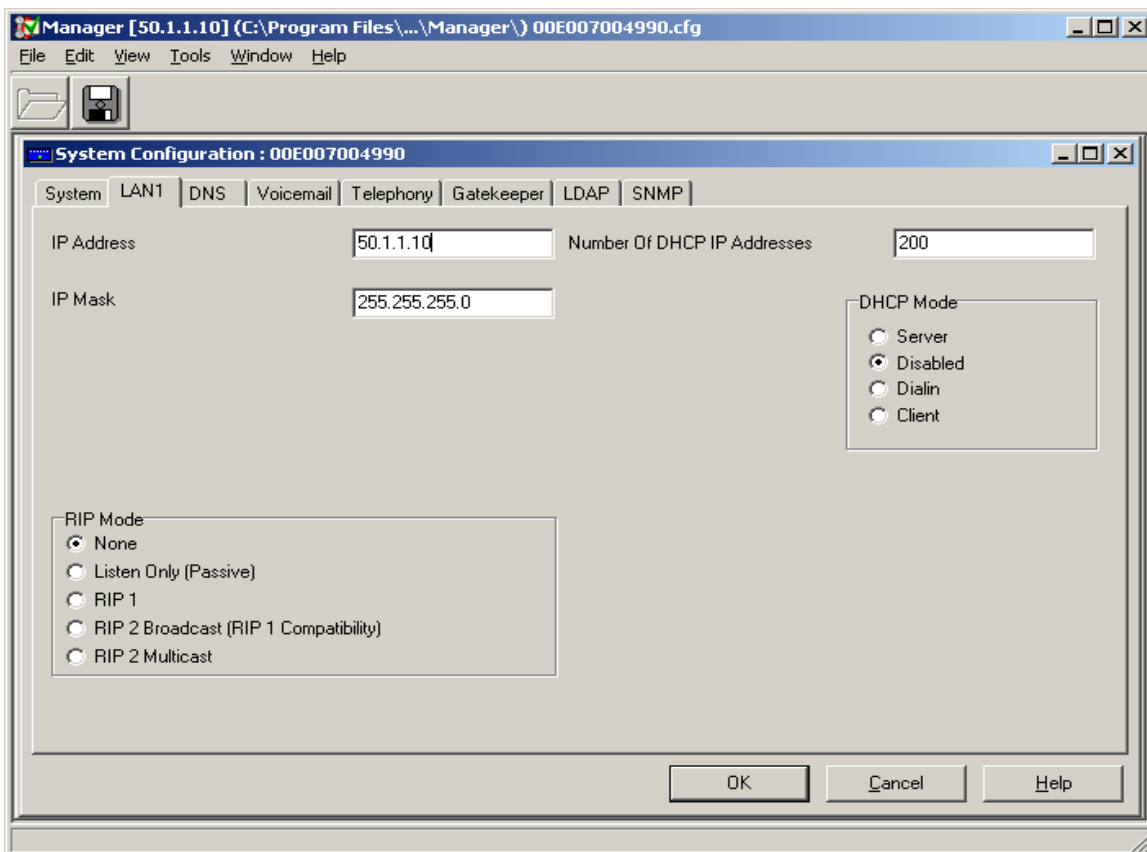
Step	Description
4.	<p>This section presents the WPA (WiFi Protected Access) configuration associated with the 802.1x. WPA includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. The combination of these two mechanisms provides dynamic key encryption and mutual authentication. The configuration screen is shown on the next page.</p> <ul style="list-style-type: none"> • Click Security under 802.11a Interface from left panel. • Click Open System as Authentication Type Setup. • Click Enable for Data Encryption Setup. • Click Supported for WPA Clients. • Click WPA authentication over 802.1x under WPA Key Management. • Click TKIP (Temporal Key Integrity Protocol) under Multicast Cipher Mode for key encryption. (Note: Since the TKIP can provide dynamic key and encryption, the manual key entry is not required for client authentication. Leave both the WPA Pre-Shared Key and Shared Key fields blank.) • Click Apply when done.

Step	Description
	 <p>The screenshot displays the 'RoamAbout Access Point' web interface in a Microsoft Internet Explorer browser window. The address bar shows 'https://20.1.1.10/security1.htm'. The left sidebar contains a navigation menu with the following items: Identification, TCP/IP Settings, RADIUS, PPPoE Settings, Authentication, Filter Control, QoS, SNMP, Administration, and System Log. The main content area is titled '802.11a Interface' and 'Security Settings'. It includes several configuration sections: 'Authentication Type Setup' with radio buttons for 'Open System' (selected) and 'Shared Key'; 'Data Encryption Setup' with radio buttons for 'Disable' and 'Enable' (selected); 'WPA Clients' with radio buttons for 'Supported' (selected), 'Required', and 'Not Supported'; 'WPA Key Management' with radio buttons for 'WPA authentication over 802.1x' (selected) and 'WPA Pre-shared Key'; 'Multicast Cipher Mode' with radio buttons for 'WEP', 'TKIP' (selected), and 'AES'; 'WPA Pre-Shared Key Type' with radio buttons for 'Hexadecimal' and 'Alphanumeric' (selected); 'WPA Pre-Shared Key' with an empty text input field; 'Shared Key Setup' with radio buttons for '64 Bit', '128 Bit' (selected), and '152 Bit'; 'Key Type' with radio buttons for 'Hexadecimal' and 'Alphanumeric' (selected); and a table for 'Key Number' (Key 1 to Key 4) with 'Transmit Key Select' radio buttons (Key 1 is selected) and 'Key' input fields. At the bottom right of the interface are links for 'Apply', 'Cancel', and 'Help'.</p>

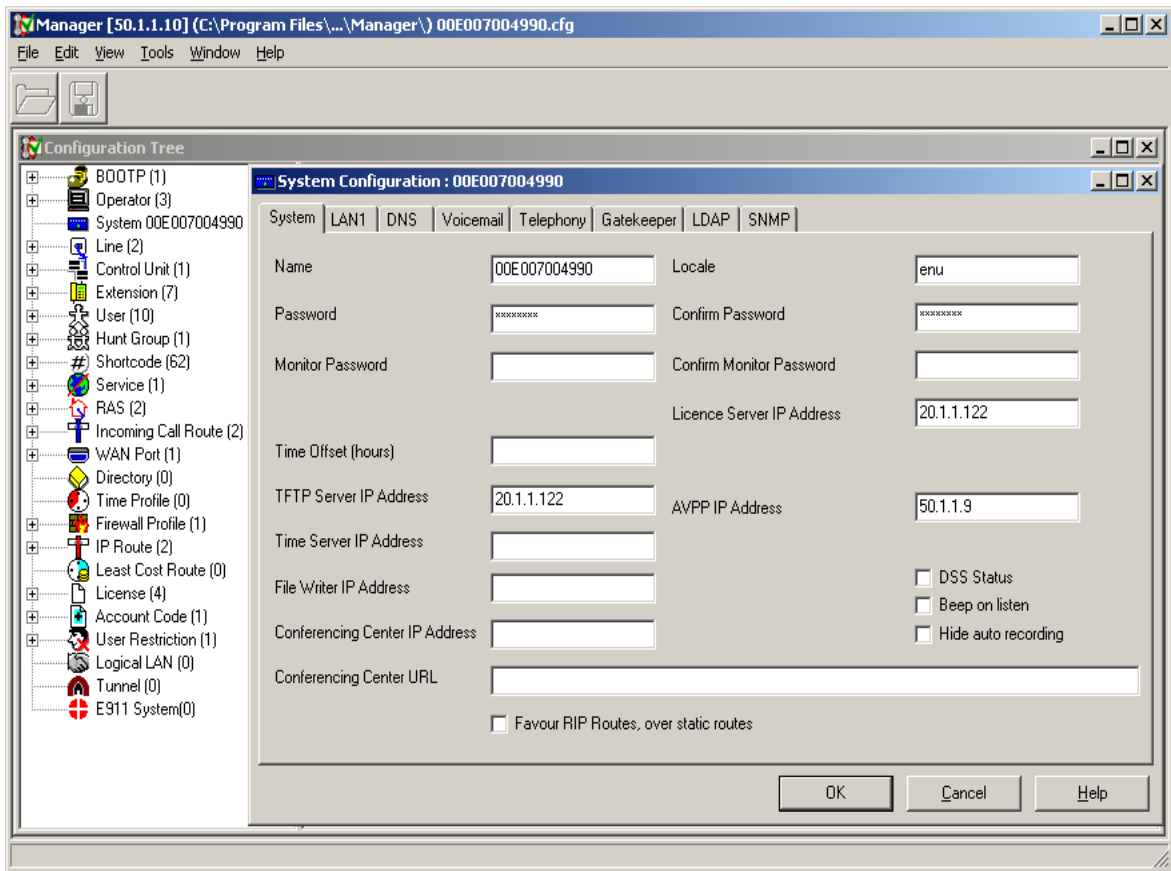
For detailed Avaya Voice Priority Processor, Odyssey Server and Client configuration, refer to the Application Notes listed in Section 7 and other documents from Funk Software web site at <http://www.funk.com>.

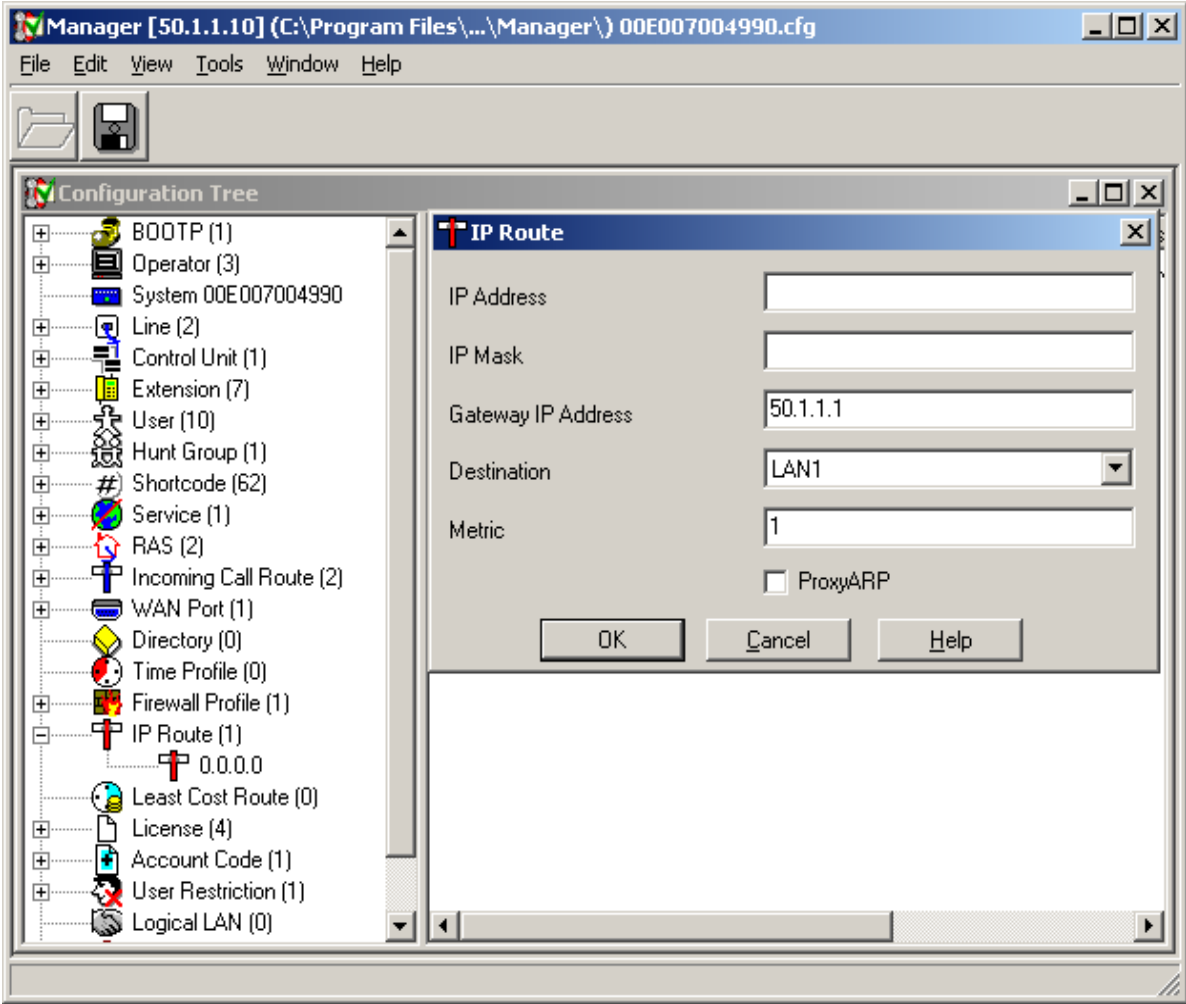
4. Configure Avaya IP406 Office

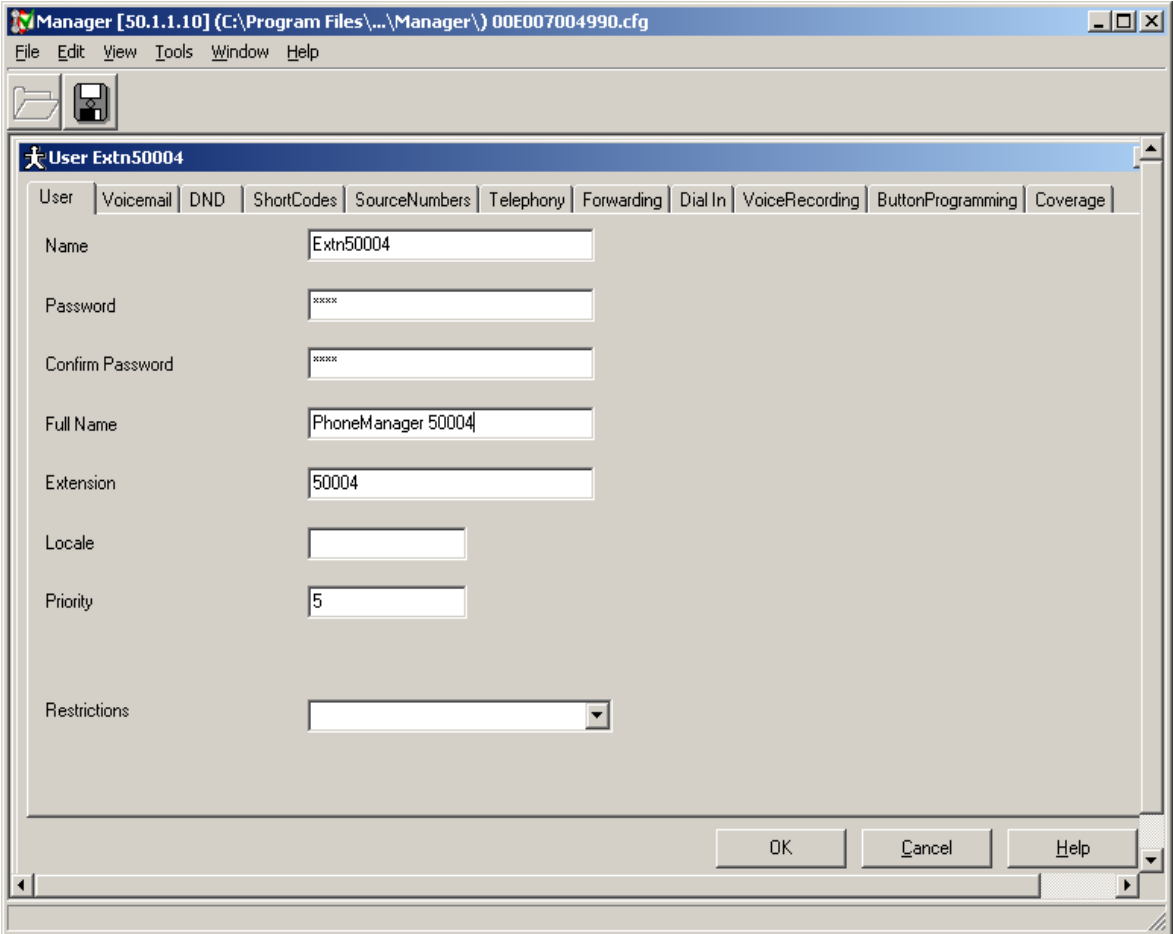
This section describes the steps necessary to configure the Avaya IP406 Office. IP406 Office is configured using the IP Office Manager application. Assume that a proper license has been installed on the Avaya IP406 Office.

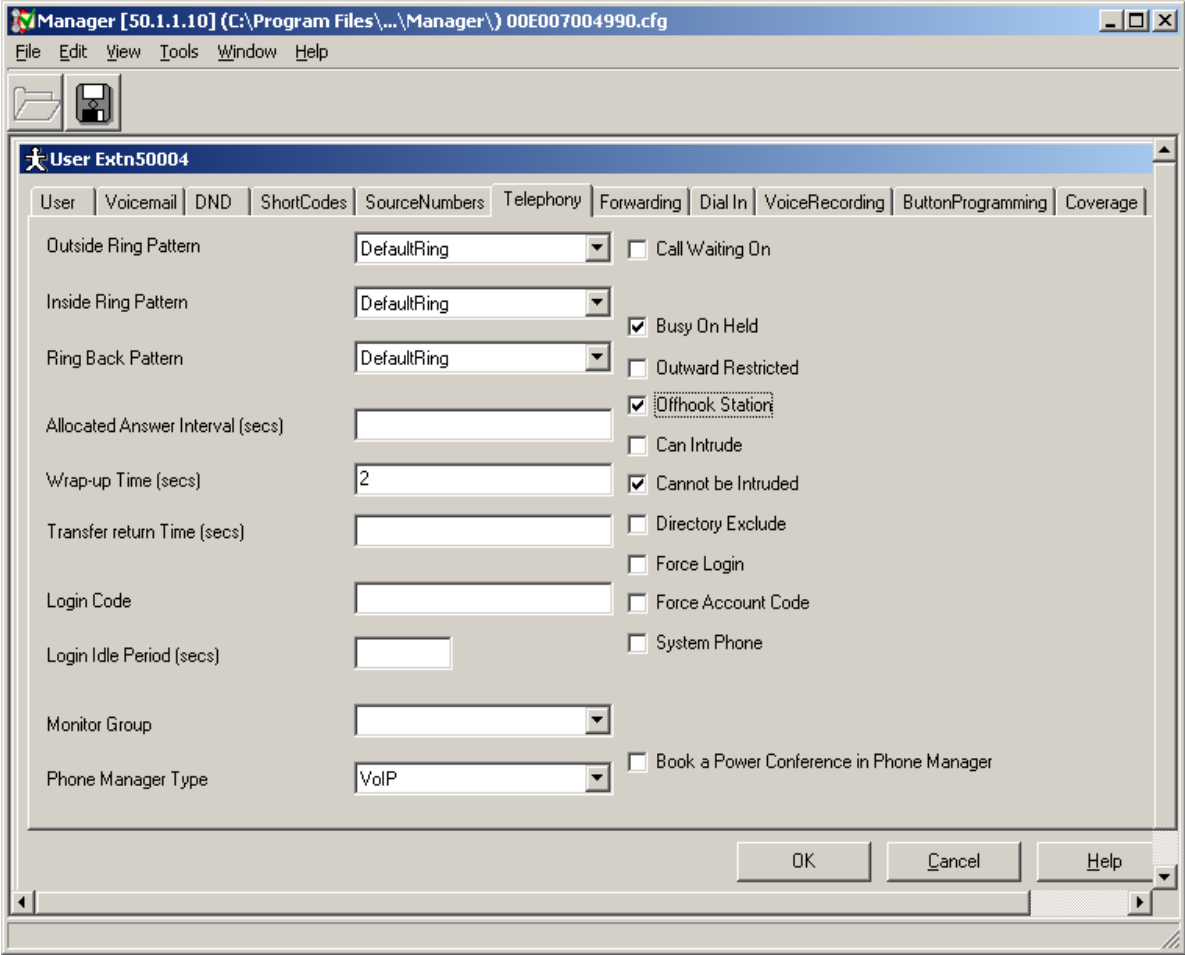
Step	Description
1.	<p><i>Configuring interface LAN1.</i> Using the IP Office Manager, browse the configuration tree and select System Configuration and click on the LAN1 tab.</p> <ul style="list-style-type: none"> Set IP Address to 50.1.1.10 and IP Mask to 255.255.255.0. For the DHCP Mode, select Disabled. Click OK.  <p>The screenshot shows the 'System Configuration : 00E007004990' dialog box with the 'LAN1' tab selected. The 'IP Address' field contains '50.1.1.10' and the 'IP Mask' field contains '255.255.255.0'. The 'Number Of DHCP IP Addresses' is set to '200'. Under 'DHCP Mode', the 'Disabled' radio button is selected. Under 'RIP Mode', the 'None' radio button is selected. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.</p>

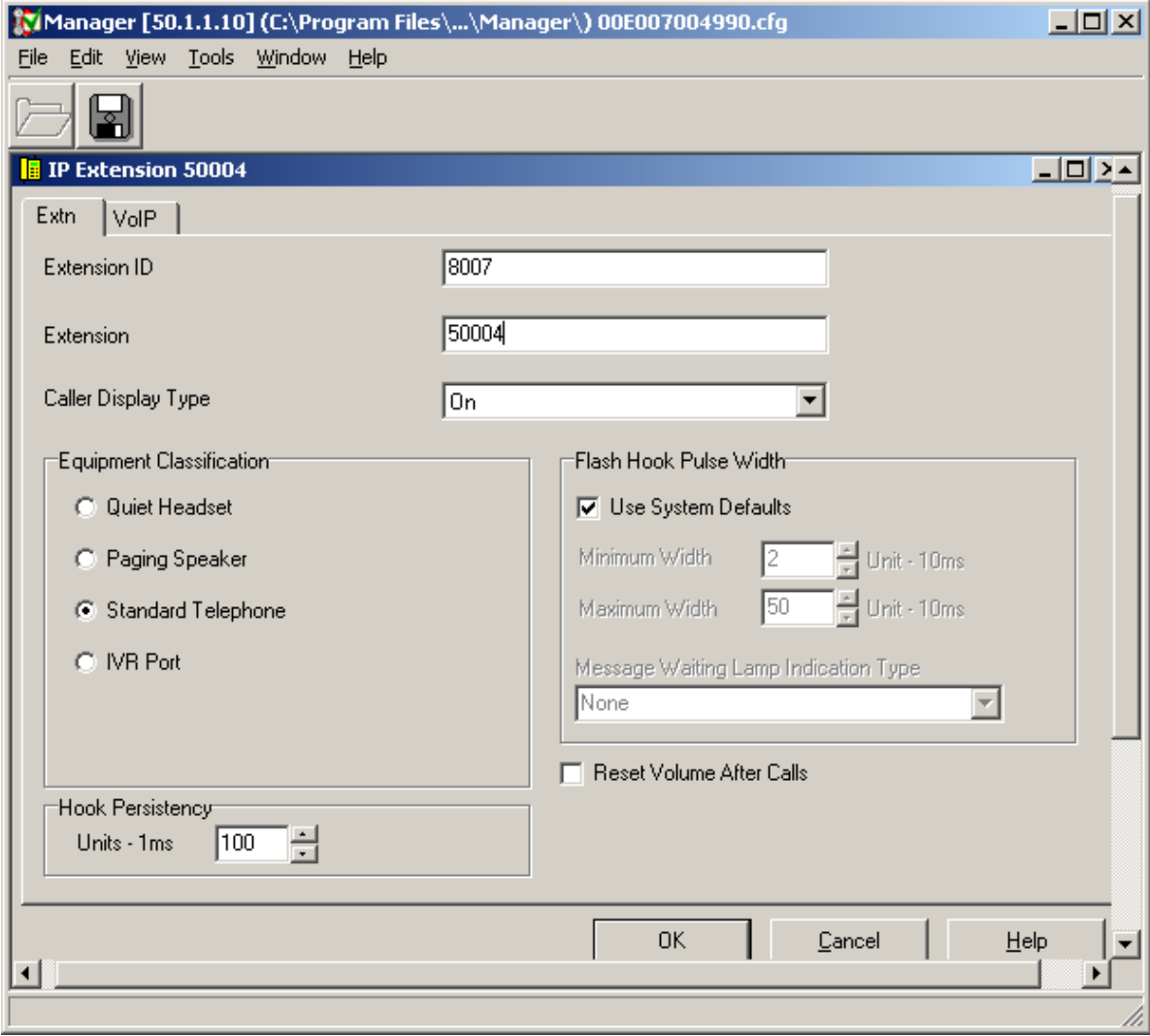
Step	Description
2.	<p><i>Adding Avaya Voice Priority Processor (AVPP) IP Address.</i></p> <p>Using the IP Office Manager, browse the configuration tree and select System Configuration and click on the System tab.</p> <ul style="list-style-type: none"> Enter 50.1.1.9 into AVPP IP Address field. Enter management PC's IP address 20.1.1.122 into TFTP Server and License Server IP Address fields. This is the PC that running IP Office Manager Application. Leave other fields as default. Click OK.

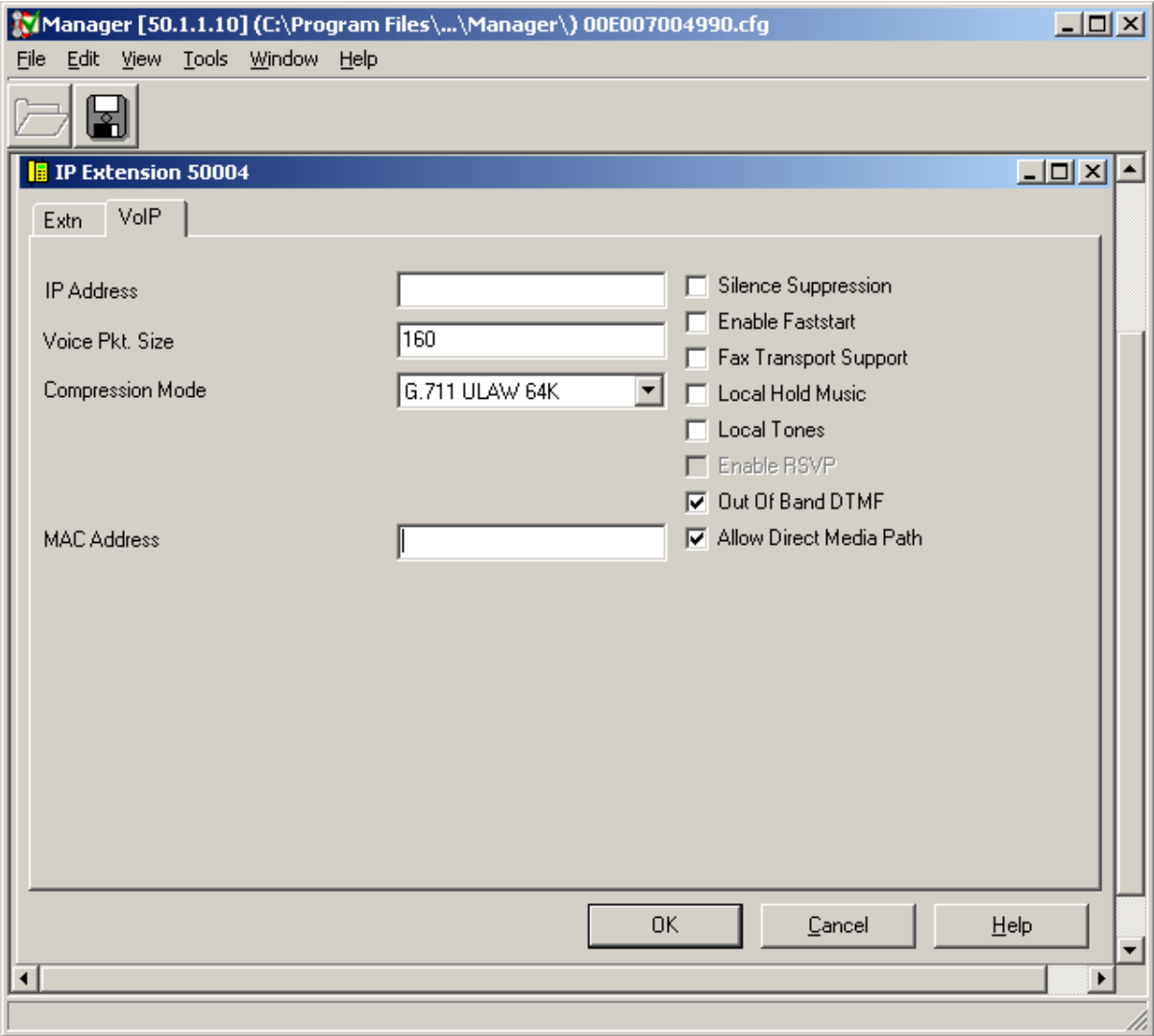


Step	Description
3.	<p data-bbox="267 304 699 340"><i>Configuring the default gateway.</i></p> <p data-bbox="267 378 919 413">Browse the configuration tree and select IP Route.</p> <ul data-bbox="316 420 1377 604" style="list-style-type: none"> • Leave the IP Address and IP Mask fields blank. This sets the default gateway. • Enter 50.1.1.1 as gateway IP address • Select LAN1 as gateway interface. • Enter 1 in Metric field. • Click OK.  <p>The screenshot shows the Manager application window with the title bar 'Manager [50.1.1.10] (C:\Program Files\...\Manager\) 00E007004990.cfg'. The Configuration Tree on the left lists various system components, with 'IP Route (1)' selected. The 'IP Route' dialog box is open, showing fields for 'IP Address', 'IP Mask', 'Gateway IP Address' (set to 50.1.1.1), 'Destination' (set to LAN1), and 'Metric' (set to 1). The 'ProxyARP' checkbox is unchecked. The dialog has 'OK', 'Cancel', and 'Help' buttons.</p>

Step	Description
4.	<p data-bbox="267 268 532 304"><i>Configuring a User.</i></p> <p data-bbox="267 342 1404 415">In the IP Office, every extension created requires a user associated with it. The following example shows how to configure a user for a PhoneManager Pro using extension 50004.</p> <p data-bbox="267 453 1479 527">Using the IP Office Manager, browse the configuration tree and select User. Enter information in the fields as shown below</p> 

Step	Description
	<ul style="list-style-type: none"> • Click the Telephony tab. • Select VoIP in the Phone Manager Type field. • Leave the other parameters as default. • Click OK when done. 

Step	Description
5.	<p data-bbox="269 268 613 304"><i>Configuring an extension.</i></p> <p data-bbox="269 342 1365 378">Using the IP Office Manager Pro, browse the configuration tree and select Extension.</p> <ul data-bbox="318 420 1365 604" style="list-style-type: none"> • Right click Extension and select Add. • Extension ID “8007” is assigned by the Avaya IP Office. Leave it unchanged. • Enter 50004 in the Extension field. • Leave other parameters as default. • Click OK. 

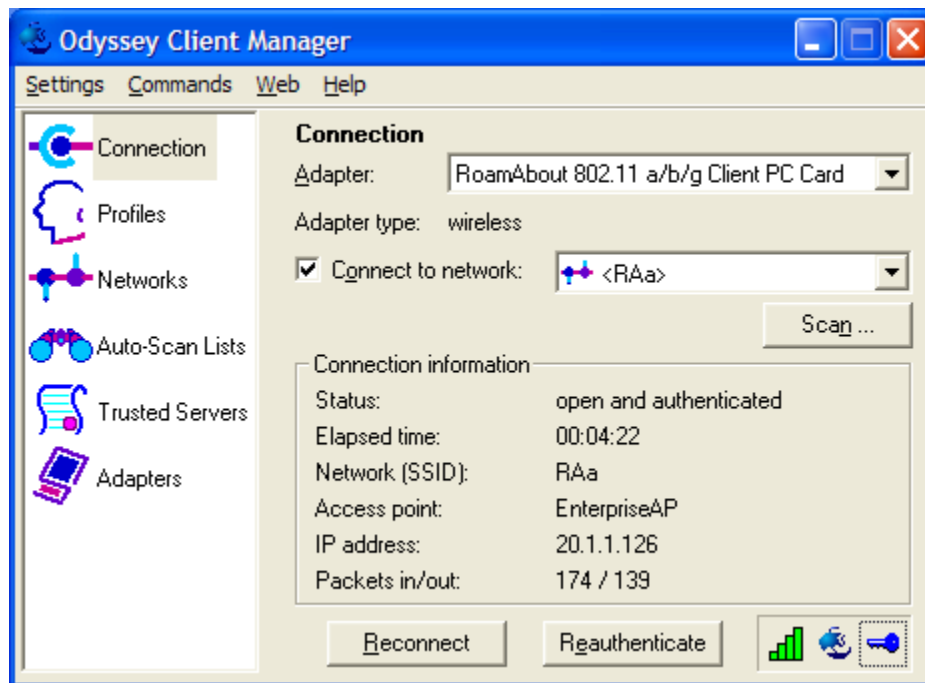
Step	Description
	<ul style="list-style-type: none"> • Select the VoIP tab. • Select G.711 ULAW 64K codec for Compression Mode. • Check Out Of Band DTMF. • Check Allow Direct Media Path. • Click OK when done.  <p>Follow Steps 4 and 5 to create extensions for Avaya 3616 and 3626 wireless IP Telephones.</p>


Step	Description
6.	<p><i>Save changes to the IP Office.</i></p> <ul style="list-style-type: none"> • Under the Manager File Menu item, select Save. At the Sending Config to dialog box, select the option to immediately reboot and press OK. • If the IP Office Server IP address has been changed, update the IP address of the PC running IP Office Manager and edit the IP Office Manager “Preferences” setting under the File menu before reconnecting.

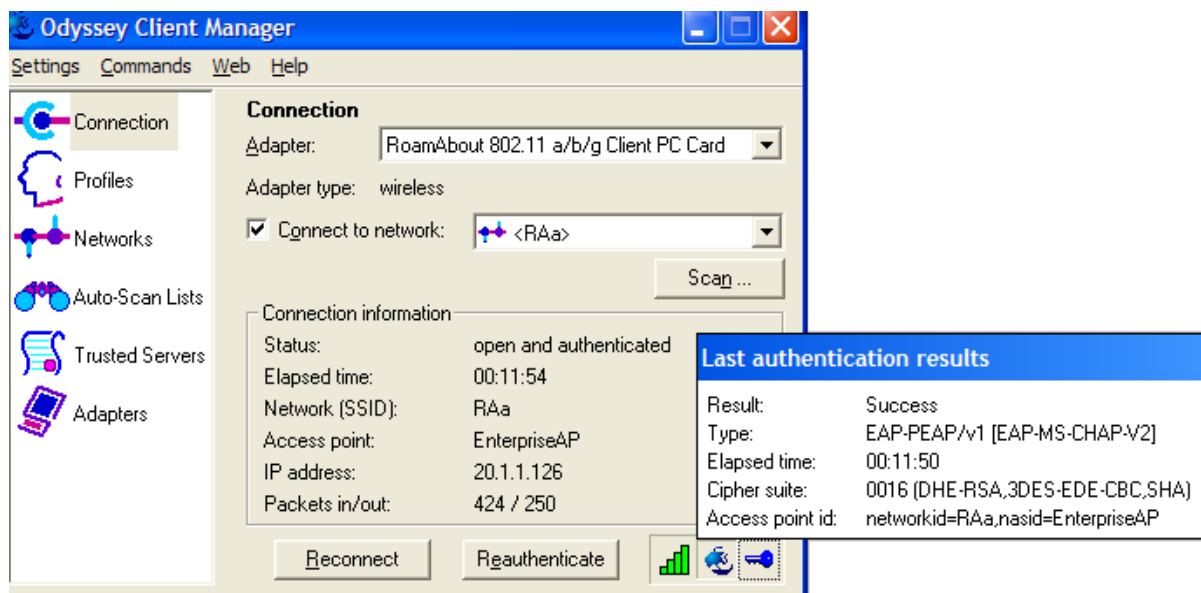
5. Verification Steps

The following verification steps were used in these Application Notes to verify correct system operation:

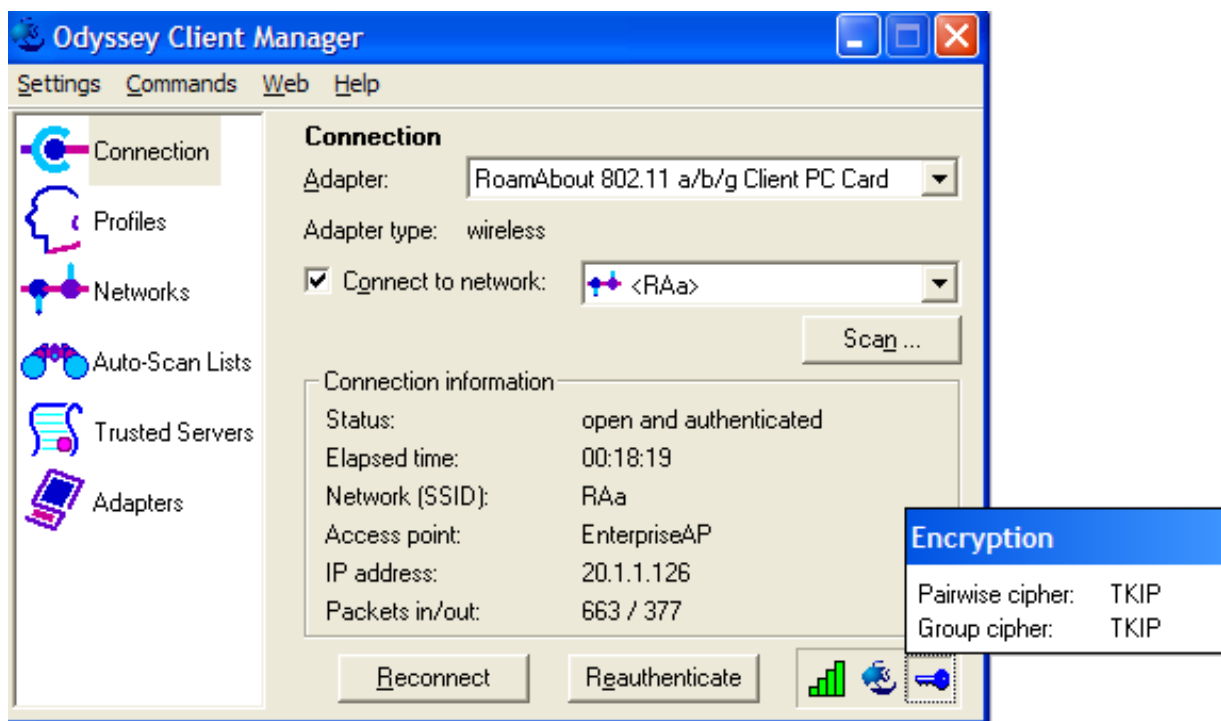
- Verify network connectivity by launching pings between the IP406 Office and the wireless laptop PC. Verify that all pings are successful.
- Enable WEP on both IP Wireless Telephones.
- Power up the Avaya 3616 and 3626 IP Wireless Telephones and verify that they can register with IP406 Office.
- Make a call between these two IP wireless Telephones and verify that the voice quality is good.
- Make a call from the 3626 IP Wireless Telephone to the 4620SW IP Telephone, and verify that the voice quality is good.
- While the call is up, make a conference call to the 4620SW IP Telephone. Verify that all three parties are in conference call and voice quality is good.
- Enable 802.1x on the Odyssey Client and verify that the RADIUS server can authenticate the client. The following screen capture shows the connection status. Note that, under the **Connection information**, the **Status** shows **open and authenticated**. The blue color on **Odyssey** icon shows the client is connected and authenticated. The blue color on the **Key** icon shows that data is encrypted using dynamic keys (TKIP).



- Click icon  to show the last authentication results.



- Click the **Key** icon to show the Key Encryption.



- Launch PhoneManager Pro and verify that the PhoneManager can register with IP406 Office.
- Make a call from the PhoneManager Pro to the 4610SW IP Telephone and verify that voice quality is good.

6. Conclusion

These Application Notes illustrate the procedures necessary for configuring the Enterasys Wireless Access Point 3000 (RBT3K-AG) to support Avaya IP406 Office, Avaya IP Wireless Telephones and Avaya Phone Manager Pro. The Enterasys Wireless Access Point 3000 (RBT3K-AG) is able to support 802.11 a/b/g radio, WPA with 802.1x authentication as well as WEP encryption.

7. References

Use this URL <http://avaya.com/gcm/master-usa/en-us/pillars/iptelephony/index.htm> to access these Application Notes.

- [1] Application Notes for Configuring 3Com Wireless LAN Access Point 8750 to Support Avaya Communication Manager, Avaya IP Wireless Telephone 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
- [4] Implementing Encrypted Conversations between Avaya Softphone Endpoints with Avaya IP Office 403 and Avaya S8300 Media Server – Issue 1.0

Use this URL <http://www.funk.com> to access the configuration documentations for Odyssey products.

©2005 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.