



**3Com® AirConnect®
9550 11n 2.4+5GHz PoE
Access Point**

**3Com® AirConnect®
9150 11n 2.4GHz PoE
Access Point
User Guide**

www.3com.com

Part number: 10016853 USER
GUIDE, AIRCONNECT 9550/9150
11N 2.4/5GHZ AP
M/N: WL-605 / WL-604
Published June 2008



3Com Corporation 350 Campus Drive Marlborough, MA 01752-3064

Copyright © 2008, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense.

Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Microsoft, Windows, Windows 2000, Windows XP and Windows Vista are registered trademarks of Microsoft Corporation.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labeled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

INTRODUCTION

Key Product Features	7
Security	7
Performance and Reliability	8
Manageability	8
Wireless Network Standards	9
802.11a	9
802.11b/g	10
IEEE 802.3af	11
Installing Your 3com Wireless Access Point.....	12

CONFIGURING THE WIRELESS ACCESS POINT

Networks with a DHCP Server.....	13
Networks without a DHCP Server	14
Launch the 3Com Wireless Infrastructure Device Manager (Widman) utility	15
Launching the 3Com Wireless Infrastructure Device Manager First Time Only	19
System Status	19
System Summary	19
Wireless Station List	21

Event Log List.....	22
System Configuration	23
Setup Wizard	23
System Properties.....	26
Access Point mode	27
Wireless Bridge Mode.....	27
IP Settings.....	28
Wireless Network	29
Wireless Mode	30
Standard Channel	30
Current Profiles	30
SSID	32
BSSID	32
Suppressed SSID	32
VLAN ID	32
Station Separation.....	32
Security	33
WEP	33
WPA Only.....	34
WPA2-Only	35
WPA2-Mixed	36

Profile (SSID) Isolation	36
WDS Link Settings	36
WDS Security Settings.....	38
Wireless Advanced Settings	39
Transmit Power	39
Beacon Interval	40
Data Beacon Rate	40
Association Timeout.....	40
Fragment Length	40
RTS/CTS Threshold	40
802.11d support.....	41
Distance.....	41
Antenna Type.....	41
Aggregation Support	41
QoS	42
Service.....	43
Management VLAN	43
IAPP.....	44
802.11F (IAPP) Support	44
Ack-Policy	46
SNTP.....	48

Syslog Function.....	50
System Log	50
Syslog Server.....	51
Syslog Port.....	51
Syslog Level.....	51
Management.....	52
Administration	52
SNMP	53
MAC Filtering.....	54
Rogue AP Detection	55
Backup/ Restore Settings.....	56
Firmware Auto Upgrade.....	57
Firmware Manual Upgrade.....	58
Rebooting	60
Connecting Through the Com Port	61
Restoring Factory Settings.....	62

TROUBLESHOOTING

Diagnosing Problems	63
---------------------------	----

OBTAINING SUPPORT FOR YOUR 3COM PRODUCT

Telephone Technical Support and Repair	68
--	----

END-USER LICENSE AGREEMENT

APPENDIX

Antennas Used per Mode	72
Console Cable Pin-out	74

INDEX

1

INTRODUCTION

The 3Com AirConnect 9550 11n 2.4+5GHz PoE Access Point and the 3Com AirConnect 9150 11n 2.4GHz PoE Access Point are high performance access points that allow you to join isolated wired Ethernet networks into a unified wireless local area network (WLAN). The Access Point (AP) supports Wi-Fi Protected Access security standards to provide a higher level of security for network data and communications. The AP is also fully compatible with IEEE 802.11a (the 9550 AP only), 802.11b, 802.11g, and 802.11n.

Key Product Features

The product operates using 11a (9550 AP only), 11b, 11g, or 11n modes. This AP creates an enterprise-class wireless LAN, supporting up to 64 simultaneous users.

Security

3Com offers one of the most robust suites of standards-based security on the market today. To protect sensitive data broadcast over the wireless LAN, 3Com supports Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA and WPA2).

3Com strengthens this basic security mechanism with additional security features, including MAC address access control lists, IEEE 802.1x per-port user authentication with RADIUS server authentication support, Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), Wireless Protected Access (WPA), and Extensible Authentication Protocol (EAP) support: EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP.

Performance and Reliability

3Com wireless access point performance features ensure reliable and seamless connections for users wherever they roam. Automatic channel selection automatically finds the least loaded channel for interference-free communication. Auto network connect and dynamic rate shifting keep users connected through a wide variety of conditions by changing to the optimum connection speed as they move through the network.

Manageability

3Com offers a wide range of standards-based management support, from SNMP to 3Com Network Supervisor and HP OpenView for seamless integration with your wired network. Wireless Infrastructure Device Manager and Wireless LAN Device Discovery tools let you configure parameters, run diagnostics, backup and restore configurations, and monitor performance from anywhere on the network using an embedded web server browser.

With Power over Ethernet (PoE) support, the same Category 5 cable that connects your access point to the data network also provides its power. A single cable installation dramatically improves your choice of mounting configurations because you no longer need to consider AC power outlet locations. PoE support makes it easier than ever to overcome installation problems with difficult-to-wire or hard-to-reach locations.

Wireless Network Standards

Understanding the characteristics of the 802.11a and 802.11g standards can help you make the best choice for your wireless implementation plans.

802.11a

Ratified in 2002, 802.11a operates at the 5GHz band and supports data rates up to 54Mbps. Because there are fewer devices in the 5GHz band, there's less potential for RF interference. However, because it is at an entirely different radio spectrum, it is not compatible with 802.11b and 802.11g.

The higher spectrum provides about 50m (164ft) of coverage. Consider 802.11a when you need high throughput in a confined space and you are:

- Running high-bandwidth applications like voice, video, or multimedia over a wireless network that can benefit from a five-fold increase in data throughput.

- Transferring large files like computer-aided design files, preprint publishing documents or graphics files, such as MRI scans for medical applications that demand additional bandwidth.
- Supporting a dense user base confined to a small coverage area. Because 802.11a has a greater number of non-overlapping channels, you can pack more wireless devices in a tighter space.

802.11b/g

802.11b, 802.11g and 802.11n all operate in the 2.4GHz band. 802.11b can support data rate up to 11Mbps. 802.11g can support data rate up to 54Mbps. 802.11n can support data rate up to 300Mbps. They all support the widest coverage – up to 100m (328ft). It is however, subject to a greater risk of radio interference because it operates in the more popular 2.4GHz band.

Consider 802.11n when you need wider coverage and vendor compatibility and you are:

- Maintaining support for existing 802.11b and 802.11g users and the existing wireless investment while providing for expansion into 802.11n.
- Implementing a complete wireless LAN solution, including Ethernet Adapters, gateways, access points and clients; Wi-Fi certification guarantees compatibility among vendors.

- Providing access to hot spots in public spaces such as coffee shops or university cafeterias.

IEEE 802.3af

The IEEE 802.3af-2003 Power over Ethernet (PoE) standard defines terminology to describe a port that acts as a power source (PSE) to a powered device (PD). The IEEE 802.3af standard states that power may be delivered by an end-point PSE, using either the active data wires of an Ethernet port or the spare wires, to a powered device. An end-point PSE, such as a Power over Ethernet capable Ethernet switch, may implement either scheme. If a mid-span PSE is used, then the mid-span PSE can only implement power delivery over the spare pairs of the copper cabling and cannot be used to deliver PoE over 1000BASE-T connections. It should be noted that even if a device supports both methods of providing power, only one mechanism may be used to deliver power to a powered device.

The first mechanism is to use the data pairs (pins 1, 2 & 3, 6) to transmit power, which is sometimes referred to as "phantom" power. The second power delivery mechanism is to use the unused, from a 10/100BASE-T perspective, pairs (pins 4, 5 & 7, 8) to deliver power that is supported within mid-span power delivery.

Installing Your 3com Wireless Access Point

To set up and install your 3Com Wireless Access Point, please refer to the 3Com® AirConnect® 9550 11n 2.4+5GHz PoE Access Point 3CRWE955075 / WL-605 3Com® AirConnect® 9150 11n 2.4GHz PoE Access Point 3CRWE915075 / WL-604 Quick Start Guide (Part Number 10016854).

2

CONFIGURING THE WIRELESS ACCESS POINT

If the default AP configuration does not meet your network requirements, or if you want to customize the settings for your own network, you can use these tools to change the configuration:

- Launch the 3Com Wireless Infrastructure Device Manager (Widman) utility
- Directly connect to the device through its Ethernet port or console port

Networks with a DHCP Server

If your network has a DHCP server, an IP address is automatically assigned to the AP. It takes between one and two minutes for the Access Point to determine if there is a DHCP server on the network. Use the 3Com Wireless Infrastructure Device Manager (Widman) included on the 3Com Installation CD to locate the Access Point on the network and view its IP address.

After you determine the AP's IP address, you can enter that IP address into a web browser on a computer on the same subnet to view the Access Point's system status or change its configuration.

Networks without a DHCP Server

If your network does not have a DHCP server, the Access Point uses a factory assigned IP address (169.254.2.111). You can use that IP address to configure the Access Point, or you can assign a new IP address to the Access Point.

To verify that the Access Point is using the default IP address assigned at the factory:

- 1 Connect a computer directly to the Access Point using the supplied standard Category 5 UTP Ethernet cable.
- 2 Enter the Access Point's default IP address (169.254.2.111) into the computer's web browser. If the Configuration Management System starts, the Access Point is using the factory assigned IP address. You can configure the Access Point with the following login information:
 - Login name: **admin**
 - Password: **password**

If the Configuration Management System does not start, the Access Point is on a different subnet than the computer. Install and start the 3Com Wireless Infrastructure Device Manager to discover the Access Point's IP address.

Launch the 3Com Wireless Infrastructure Device Manager (Widman) utility

- 1 Turn on the computer.
- 2 Insert the 3Com Installation CD into the CD-ROM drive.
The CD will Autorun. If it does not Autorun, you can start the setup menu from the Windows Start menu. For example: **Start > Run > d:\setup.exe**.
- 3 In the menu click **Tools and Utilities**.
- 4 In the next screen, click the software you want to install.
- 5 Follow the on screen instructions to complete the installation.
Reboot the computer if prompted to do so.

Launching the 3Com Wireless Infrastructure Device Manager

To be able to configure the Access Point you need to run the Wireless Infrastructure Device Manager. Go to **Start > Programs > 3Com Wireless > Wireless Infrastructure Device Manager**

If the device is working correctly the following screen should be seen.

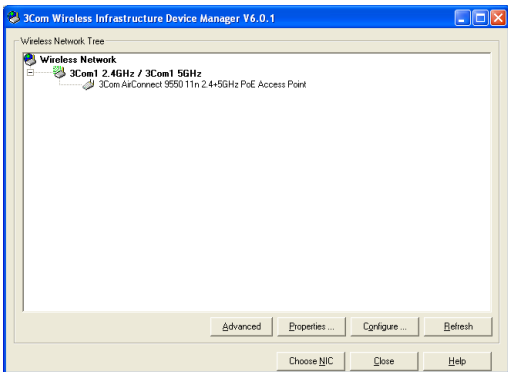


Figure 1 3Com Wireless Infrastructure Device Manager

Directly connect to the device through its Ethernet port or console port.

Follow the instructions below to log into the AP Configuration screen:

- 1 Load a web browser and enter **http://169.254.2.111**
- 2 The Log On screen appears



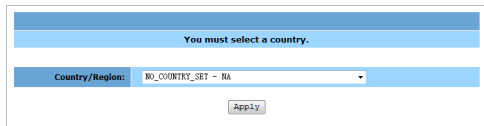
Figure 3 Logon Screen

To log on to the Web interface:

- 1 Username, type **admin** (case sensitive)
- 2 Password, type **password**
- 3 Click **Log On**.

First Time Only

After you have logged on for the first time you will be asked to select your country from the drop down menu.



The screenshot shows a web interface with a blue header bar containing the text "You must select a country." Below this is a form field labeled "Country/Region:" with a dropdown menu currently displaying "NO_COUNTRY_SET - NA". Below the dropdown is an "Apply" button.

Figure 4 Country Selection

System Status

The Web interface has been designed to enable you to easily perform advanced configuration tasks and view information about the AP.

System Summary

After you click Log On from the Log On Screen, you'll see the system status page on the screen. The System summary page is the default page that will pop up once you successfully log on.

The system summary page shows all the configuration information about your AP, as shown in Figure 5.

The screenshot shows the 'System Summary' page for a 3COM AirConnect 9550 11n 2.4+5GHz PoE Access Point. The page is divided into a left-hand navigation menu and a main content area.

Navigation Menu (Left):

- System Status
 - System Summary
 - Wireless Status List
 - Event Log List
- System Configuration
 - Setup Wizard
 - System Properties
 - IP Settings
- 2.4G Radio Configuration
 - Wireless Network
 - WiFi Link Settings
 - WiFi Security Settings
 - Wireless Advanced Settings
 - WiFi
- 5G Radio Configuration
 - Wireless Network
 - WiFi Link Settings
 - WiFi Security Settings
 - Wireless Advanced Settings
 - WiFi
- Services
 - Management VLAN
 - ARP
 - SNTP
 - Trunking
- Management
 - Administration
 - SNMP
 - MAC Filtering
 - Region AP Function
 - Backup/Restore Settings
 - Firmware Auto Upgrade
 - Firmware Upgrade
 - Reboot

Main Content Area (Right):

System Information

System Name	3COM AirConnect 9550 11n 2.4+5GHz PoE Access Point
Operation Mode	Access Point
Ethernet MAC Address	00:18:0E:11:35:01
2.4G Wireless MAC Address	00:18:0E:11:35:01
5G Wireless MAC Address	00:18:0E:11:35:02
Country	UNITED STATES
Firmware Version	AP Software 1.4.10 built on Jun 19, 2009

Current IP Settings

IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.97
SNTP Client	Enabled

2.4G Radio

Wireless Mode	2.4GHz 802.11b/g/n
Radio Band	Standard 20MHz Channel
Channel / Frequency	Channel 11 / 2462MHz
Primary Profile (SSID)	3COM 2.4GHz
Primary Profile (Security)	Open System
WDS	Disabled

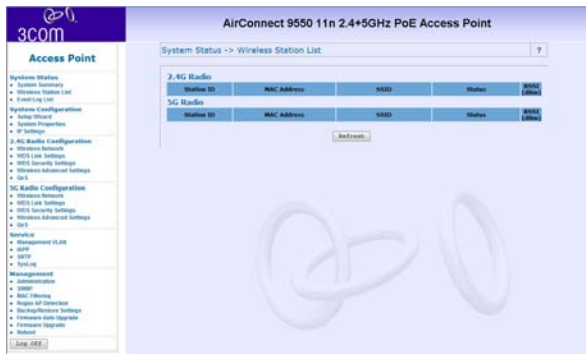
5G Radio

Wireless Mode	5GHz 802.11a/n
Radio Band	Standard 20MHz Channel
Channel / Frequency	Channel 44 / 5200MHz
Primary Profile (SSID)	3COM 5.5GHz
Primary Profile (Security)	Open System
WDS	Enabled

Figure 5 System Summary

Wireless Station List

Through the Wireless Station List page, you can easily identify the adjacent wireless stations. It will automatically observe the adjacent wireless station's ID (if specified), MAC address, SSID, and current status.



The screenshot displays the configuration interface for an AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar contains a navigation menu with categories like System Status, System Configuration, 2.4G Radio Configuration, 5G Radio Configuration, Network, and Management. The main content area is titled "System Status -> Wireless Station List" and features two tables for monitoring wireless stations.

2.4G Radio

Station ID	MAC Address	SSID	Status	SSID (Blue)
------------	-------------	------	--------	-------------

5G Radio

Station ID	MAC Address	SSID	Status	SSID (Blue)
------------	-------------	------	--------	-------------

Buttons for "Refresh" and "Log Off" are visible at the bottom of the main content area.

Figure 6 Wireless Station List

Event Log List

The event log list stores a record of all the events within this designated WLAN.

The screenshot displays the web management interface for a 3COM AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar contains a navigation menu with categories like System Status, System Configuration, 2.4GHz Radio Configuration, 5GHz Radio Configuration, and Management. The main content area is titled "System Status -> Event Log List" and features a table with the following data:

Msg.	Time	Message Level	Event
1	2008 Jun 01 00:00:00	Notice	Login successful.
2	2008 Jun 01 00:00:01	Warning	Login failed from IP 192.168.0.110
3	2008 Jun 01 00:00:00	Notice	Logout from Web UI.

Below the table are buttons for "Clear" and "Refresh".

Figure 7 Event Log List

System Configuration

In this section, you will learn how to configure the basic functions of your AP.

Setup Wizard

The Setup Wizard will walk you through setting up the AP. To start the Setup Wizard, click Setup Wizard.

- 1 Figure 8** allows you to set up the following information:
 - **SSID** (Service Set Identifier) – This is the name of wireless network. Input 1-32 characters
 - **Wireless Mode** – Choose the required network mode from the drop down menu.
 - **Standard Channel** – Choose a channel from the drop down menu or select SmartSelect (recommended) to let the device select a channel.

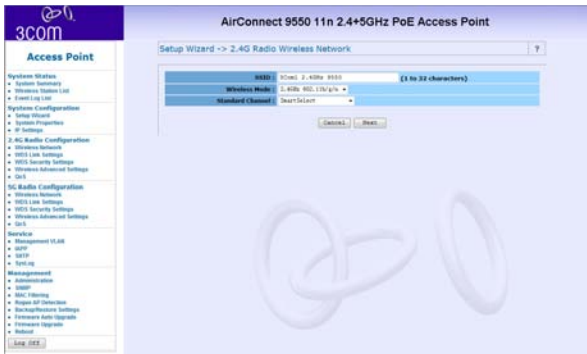


Figure 8 2.4G Radio Wireless Network

- 2 Click **Next** to continue the configuration or click **Cancel** to start again.
- 3 **Figure 9** allows you to set up the following information:
 - **IP Network Setting** – Check to either obtain an IP address via DHCP or specify an IP Address manually.
 - **IP Address** – Enter the IP address that you want to assign.
 - **IP Subnet Mask** – Enter your networks subnet address.
 - **Default Gateway** – If used, enter the gateway address that the device should go through.

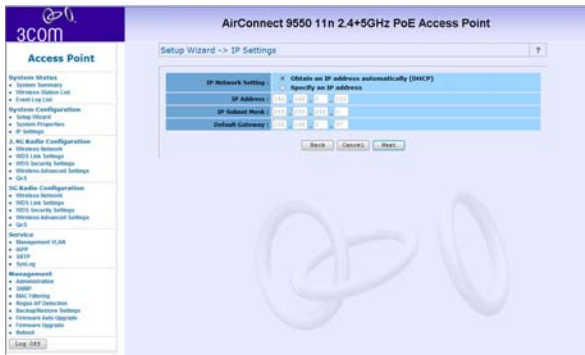


Figure 9 IP Settings

- 4 **Figure 10** allows you choose the security settings. Choose from the following settings in the drop down menu:
- No security
 - WEP
 - WPA - Only
 - WPA2 - Only
 - WPA2 - Mixed

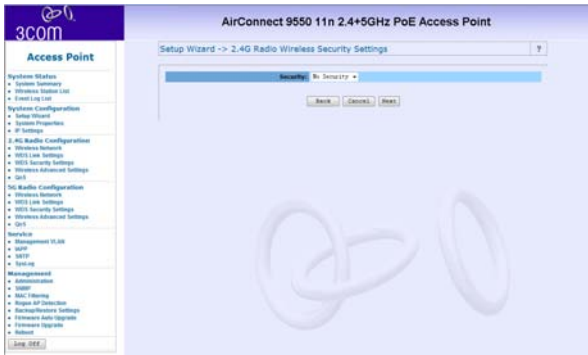


Figure 10 2.4G Wireless Security Settings

- 5 Click **Cancel** to close without saving, click **Finish** to save the settings, or click **Back** to return to Figure 9.

System Properties

The System properties page allows you to define Device name, location, operation modes and Load Type.

There are two operation modes to choose from:

Access Point mode

A Wireless LAN data transceiver that uses radio waves to connect a wired network with wireless station.

Wireless Bridge Mode

A wireless bridge connects two separate networks operating on the 802.11 standard.

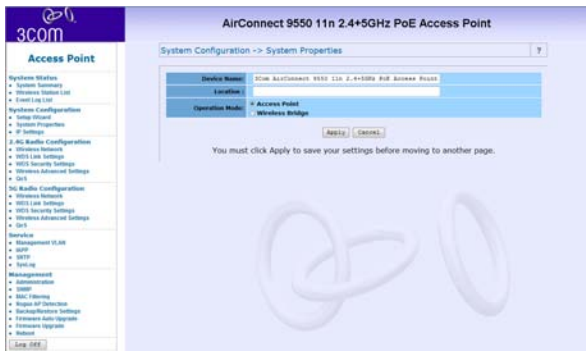


Figure 11 System Properties

IP Settings

This setting must match the network's method of IP address assignment. Choose Dynamic Host Configuration Protocol (DHCP) or Static IP. With DHCP, IP addresses are assigned for predetermined periods of time. Choose Static IP if your network does not have an automatic system for IP address assignment.

The screenshot displays the configuration interface for an AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar shows a navigation menu with categories like System Status, System Configuration, 2.4G Radio Configuration, 5G Radio Configuration, Service, and Management. The main content area is titled "System Configuration -> IP Settings" and contains the following settings:

IP Network Settings	
<input checked="" type="radio"/> Obtain an IP address automatically (DHCP)	
<input type="radio"/> Specify an IP address	
IP Address	192.168.1.100
IP Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

Web-GUI Protocol	
<input checked="" type="radio"/> HTTP	HTTP Port: 80
<input type="radio"/> HTTPS	HTTPS Port: 443

Buttons:

Message: You must click Apply to save your settings before moving to another page.

Figure 12 IP Settings

Wireless Network

The Wireless Access Point supports Multiple SSIDs which allows it to act as multiple APs appearing in a Wireless LAN network. You can configure up to 4 SSIDs on the device.

The screenshot shows the configuration interface for the 3COM AirConnect 9550 11n 2.4+5GHz PoE Access Point. The page is titled "5G Radio Configuration -> Wireless Network:" and features a left-hand navigation menu and a main configuration area.

Access Point Navigation Menu:

- Systems Status
 - System Overview
 - System Status List
 - Event Log List
- System Configuration
 - Setup Wizard
 - System Properties
 - IP Settings
 - 2.4G Radio Configuration
 - Wireless Network
 - WDS Link Settings
 - WDS Security Settings
 - Wireless Advanced Settings
 - SSID
 - 5G Radio Configuration
 - Wireless Network
 - WDS Link Settings
 - WDS Security Settings
 - Wireless Advanced Settings
 - SSID
- Service
 - Management VLAN
 - SNMP
 - SSH
 - SNMPv3
- Management
 - SNMP
 - SNMPv3
 - Reset AP Function
 - Reconfiguration Settings
 - Factory Data Upgrade
 - Firmware Upgrade
 - Reboot

Wireless Network Configuration:

Wireless Mode: 802.11n/a
 Radio Band: Standard 2.4GHz Channel
 Standard Channel: SmartSelect
 Extension Channel: [None]

Current Profiles:

Primary	SSID	Security	WDS	Enable	Edit
1	3Com2 5GHz	Open System	1	<input type="checkbox"/>	Edit
2	3Com2 5GHz	Open System	2	<input type="checkbox"/>	Edit
3	3Com2 5GHz	Open System	3	<input type="checkbox"/>	Edit
4	3Com2 5GHz	Open System	4	<input type="checkbox"/>	Edit

Profile 1 (SSID: [blank]):

- No Exclusion
- Exclude All Profiles (SSIDs) from each other
- Use VLAN (802.1Q) standard

Buttons: [Apply] [Cancel]

Message: You must click Apply to save your settings before moving to another page.

Figure 13 Wireless Network

Wireless Mode

You can select your desired wireless operating mode from the drop-down box.

Standard Channel

Select the channel for your wireless LAN in Standard Channel block. The default setting is SmartSelect. It selects the channel which provides the best transmission quality. The available frequencies vary depending on which wireless mode you select.

Current Profiles

A maximum of four profiles can be configured. Check the **Enable** button to activate a profile. Click the **Edit** button to change its configuration.



Figure 14 SSID Profile Settings

SSID

Service Set Identifier. This is the assigned name for a wireless Wi-Fi network. Stations must use this unique identifier to communicate with an Access Point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

BSSID

Basic Service Set Identifier. This is the assigned MAC address of the station in the access point. This unique identifier is in Hex format.

Suppressed SSID

If you want to disable the broadcast of your SSID, you should check the **Suppressed SSID** box. It is also known as SSID Broadcast disable or Hide SSID.

VLAN ID

If your network uses VLANs, you can assign an SSID to a VLAN. Client devices using the SSID are grouped in that VLAN.

Station Separation

Enable Station Separation if you want to prevent stations connected to this profile from accessing each other.

Security

There are four levels of security available and all have differing properties:

WEP

Wired Equivalent Privacy data encryption provides data security. WEP Share Key authentication and WEP data encryption will block all but the most determined hacker.

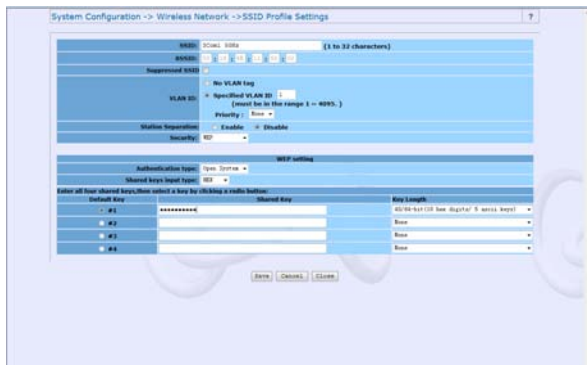


Figure 15 SSID Profile Settings

- 1 To add WEP, from the drop down list choose **open-system** or **shared key** authentication.
- 2 Select the desired input method (HEX or ASCII)
- 3 From the drop down list choose from 40/64, 104/128, 128/152 key lengths.

WPA Only

Wi-Fi Protected Access was constructed to provide improved data encryption, (which was weak in WEP), and to provide user authentication.

The screenshot shows the 'System Configuration -> Wireless Network -> SSID Profile Settings' window. The configuration is as follows:

- SSID:** 2008-3008 (1 to 32 characters)
- BSSID:** 00 00 00 00 00 00
- Suppressed SSID:**
- VLAN ID:** No VLAN tag; Specified VLAN ID: 1 (must be in the range 1 - 4095.)
- Priority:** Best
- Station Separation:** Enable; Disable
- Security:** WPA2-PSK
- Cipher Type:** TKIP
- Group Key Update Interval:** 1800 (30-3600) seconds (0: Disabled)
- Authentication Mode:** PSK - 802.1X
- PassPhrase:** (8-63 ASCII characters or 64 hexadecimal digits)
- RADIUS Server:** 192.168.1.1
- RADIUS Port:** 1812
- RADIUS Secret:** (empty)

Buttons at the bottom: Save, Cancel, Close.

Figure 16 SSID Profile Settings

Only allows WPA clients to connect to the VAP.

You can choose TKIP or AES as the encryption method

The Group key update interval is configurable; the default value is 1800 seconds

You can choose personal mode (PSK) or enterprise mode (802.1X) authentication The default is PSK.

If you choose PSK, you will need to enter a pass phrase of 8-63 ASCII characters or 64 hexadecimal digits.

If you choose 802.1X, you will need access to a RADIUS server, port and secret.

WPA2-Only

Only allows WPA 2 clients to connect to the VAP.

You can choose TKIP or AES for the encryption method

The Group key update interval is configurable, with a default value of 1800 seconds

You can choose personal mode (PSK) or enterprise mode (802.1X) authentication. The default is PSK.

If you choose PSK, you will need to enter a pass phrase of 8-63 ASCII characters or 64 hexadecimal digits.

If you choose 802.1X, you will need access to a RADIUS server, port and secret.

WPA2-Mixed

Only allows WPA and WPA2 clients to connect to the VAP.

You can choose TKIP or AES as the encryption method.

The Group key update interval is configurable, with a default value of 1800 seconds.

You can choose personal mode (PSK) or enterprise mode (802.1X) authentication. The default setting is PSK.

If you choose PSK, you will need to enter a pass phrase of 8-63 ASCII characters or 64 hexadecimal digits.

If you choose 802.1X, you will need access to a RADIUS server, port and secret.

Profile (SSID) Isolation

Stations connected to different profiles cannot access each other.

Choose from **No Isolation** (Full access), or to Isolate all Profiles (SSIDs) from each other, check **use VLAN (802.1Q) standard**.

WDS Link Settings

Wireless Distribution System (WDS) allows access points to communicate with one another wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required.

The screenshot shows the configuration interface for an AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar contains a navigation menu with categories like System Status, System Configuration, J-Flux Radio Configuration, 5G Radio Configuration, Service, and Management. The main content area is titled '2.4G Radio Configuration -> WDS Link Settings' and features a section to 'Enable WDS'. Below this is a table with columns for ID, MAC Address, and Radio. The table lists several APs with their MAC addresses and radio status (Enable/Disable). At the bottom of the table are 'Apply' and 'Cancel' buttons, and a note stating 'You must click Apply to save your settings before moving to another page.'

ID	MAC Address	Radio
1	08 00 27 00 00 00	Enable +
2	08 00 27 00 00 00	Disable +
3	08 00 27 00 00 00	Disable +
4	08 00 27 00 00 00	Disable +
5	08 00 27 00 00 00	Disable +
6	08 00 27 00 00 00	Disable +
7	08 00 27 00 00 00	Disable +
8	08 00 27 00 00 00	Disable +

Figure 17 WDS Link Settings

Supports up to 8 point to multipoint WDS links. Check **Enable WDS** and then **Enable** on the MAC addresses want to link to. Enter the MAC addresses of any other APs you want to link to.

Example of a WDS topology:

AP1 <- WDS -> Master AP (our AP) <- WDS -> AP3 <- WDS -> AP4

WDS Security Settings

The screenshot shows the configuration interface for an AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar contains a navigation menu with categories like System Status, System Configuration, 2.4G Radio Configuration, 5G Radio Configuration, Service, and Management. The main content area is titled '5G Radio Configuration -> WDS Security Settings'. It features a 'Security' dropdown menu currently set to 'None'. Below it, there is a 'WEP Key' field with a 'Show/Hide WEP Key' toggle and a 'Passphrase' field containing the text '8-43 ABC12'. A red note states: 'Note: When using WPA-PSK, the WDS setting among WDS peers should be identical.' At the bottom of the form are 'Apply' and 'Cancel' buttons. A message at the bottom of the page reads: 'You must click Apply to save your settings before moving to another page.'

Figure 18 WDS Security Settings

Choose the required security level from:

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)

If using **WEP** security, enter the WEP key. If using **WPA**, enter the passphrase.

Wireless Advanced Settings

To configure advanced wireless settings, click **Wireless Advanced Settings**. The toolbar and Wireless Advanced Settings menu appears.

The screenshot displays the configuration interface for an AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar shows a navigation menu with categories like System Status, System Configuration, and SG Radio Configuration. The main content area is titled "SG Radio Configuration -> Wireless Advanced Settings" and contains several configuration fields:

- Transmit Power: Full
- Beacon Interval: 100 (20-1000) ms
- Data Reserve Rate (DTRM): 5 (1-35)
- Association Timeout: 5 (3-60) min
- Fragment Length: 2344 (236-2344) Bytes
- RTS/CTS Threshold: 2347 (236-2347) Bytes
- 802.11E Support: Shutable Enable
- Distance: 3 (1-30) km
- Antenna Type: Internal Antenna External Antenna
- Aggregation Support: A-MPSU A-MGSM

Buttons for "Apply" and "Cancel" are located at the bottom of the configuration area. A note below the buttons states: "You must click Apply to save your settings before moving to another page."

Figure 19 Wireless Advanced Settings

Transmit Power

Choose one of the following power levels: Full, Half (-3dB), Quarter (-6dB), Eighth (-9dB) or Minimum. The default is Full.

Beacon Interval

Choose an interval time between 25ms and 1000ms for each beacon transmission. The default is 100ms.

Data Beacon Rate

The Delivery Traffic Indication Message (DTIM). Specify the data beacon rate between 1 and 255. The default is 1.

Association Timeout

Set the value for the maximum time allowed for a wireless association to be established. When this time is exceeded, the connection is lost. The default value is 5 mins.

Fragment Length

Specify maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.

RTS/CTS Threshold

Request To Send threshold. Specify the packet size used to determine if it should use the CSMA/CA mechanism or the CSMA/CD mechanism.

802.11d support

802.11d allows the device to communicate in areas where the 802.11 standard is not allowed. It adds features and restrictions to ensure compliance.

Distance

The maximum distance between client or AP and device. The default value is 1km.

Antenna Type

If you would like to use external antennas (to replace the original internal antennas), check **External Antenna**. Then specify one of the antenna types from the drop down menu, where the options are:

- 3CWE591 3com 6/8dBi Dual-Band Omni Antenna
- 3CWE596 3com 18/20dBi Dual-Band Panel Antenna
- 3CWE598 3com 8/10dBi Dual-Band Panel Antenna

Aggregation Support

Sets the aggregation type:

- A-MPDU : Aggregate MAC protocol data unit.
- A-MSDU : Aggregate MAC service data unit.

The default value is A-MPDU.

QoS

This section provides the administrator with the Quality of Service (QoS) data.

The QoS setting is only available in AP Mode.

The QoS Setting should be modified with caution because radio behavior is affected. These parameters can be modified when QoS service is Enabled.

Service

Management VLAN

If you reconfigure the Management VLAN, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

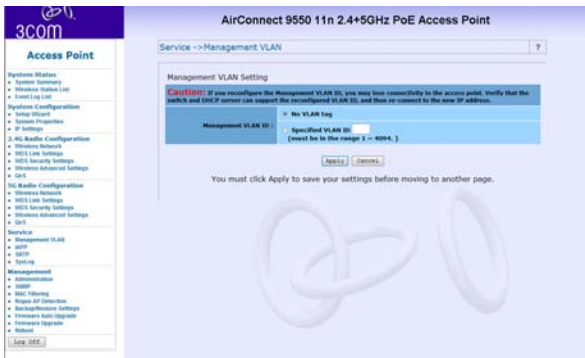


Figure 20 Management VLAN

IAPP

Inter-Access Point Protocol (IAPP)

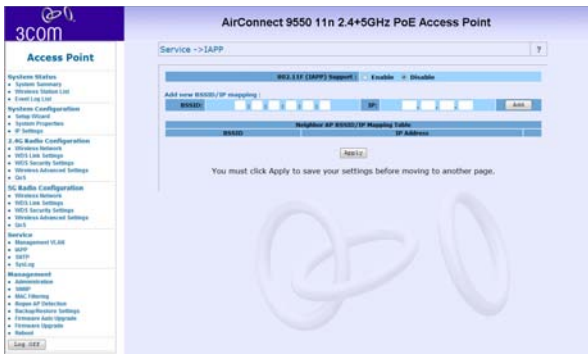


Figure 21 IAPP

802.11F (IAPP) Support

Choose either Enable or Disable

IAPP allows multiple access points to communicate and pass location information about their associated stations. If you enable 802.11F support you should manually add BSSID/IP mapping:

- 1 Enter the BSSID and IP addresses of the AP.



2 Click **Add**

Only stations roaming from one of the listed APs to this AP are allowed to re-associate with this AP. Others will be requested to go through the full association process.

3COM
Access Point

System Status

- System Summary
- System Status List
- Event Log List

System Configurations

- Setup Wizard
- System Properties
- IP Settings

3. Air Radio Configuration

- Wireless Network
- WDS Link Settings
- WDS Security Settings
- Wireless Advanced Settings
- QoS

5G Radio Configuration

- Wireless Network
- WDS Link Settings
- WDS Security Settings
- Wireless Advanced Settings
- QoS

Management

- Administration
- SNMP
- RAC Filtering
- Router AP Function
- Backup/Restore Settings
- Firmware Auto Upgrade
- Firmware Upgrade
- Reboot

Log Out

AirConnect 9550 11n 2.4+5GHz PoE Access Point

5G Radio Configuration -> WME Parameters of Access Point

WME (QoS) Enable Disable
 Adm Policy

AC Type	Min Connection Interval (L2/L3, x.com.be:0-10)	Max Connection Interval (L2/L3, x.com.be:0-10)	Hand Off Time (0-15)	Forward Capacity (0-55535 p/s)	Admission Control
AC_W1	0	10	0	0	<input checked="" type="checkbox"/>
AC_W2	0	0	0	0	<input checked="" type="checkbox"/>
AC_W3	0	0	0	55535	<input checked="" type="checkbox"/>
AC_W4	0	0	0	1500	<input checked="" type="checkbox"/>

Apply Cancel

You must click Apply to save your settings before moving to another page.

Figure 22 VME Parameters of Access Point

Ack-Policy

When the Ack-Policy is checked. The device will not send ACK frames. The default value is disabled.

Setting	Description
Min Contention Window	For each access category, enter the minimum contention window value. Channel access is prioritized by assigning smaller contention window values to a higher priority traffic class. If a channel is busy or a transmission collides, a node chooses a random number between 0 and the current contention window minimum.
Max Contention Window	For each access category, enter the maximum contention window value. The minimum contention window value is doubled each time a collision occurs until the maximum is reached. A small contention window value decreases the access delay but increases the probability of a collision.
Fixed Slot Time	For each access category, enter the fixed slot time. Channel access can be strictly prioritized by assigning smaller contention window values to a higher priority traffic class. Traffic in the access category must wait for this fixed number of slots after each packet is received before resuming its random back-off.
Transmit Opportunity Limit	Enter the number of microseconds that qualified transmitters can transmit through the normal back-off procedure with a set of pending packets. Larger values allow a client to control the channel for longer periods of time, allowing it to achieve higher throughput in this access category at the expense of longer access times for all access categories.

Setting	Description
Admission Control	Note: In this release, clients are blocked from using an access category when they select Enable for Admission Control. The Admission Control check box controls client use of the access categories. When you enable admission control for an access category, clients associated to the access point must complete the WMM admission control procedure before they can use that access category. However, access points do not support the admission control procedure in this release, so clients cannot use the access category when you enable Admission Control. default : disable

The default value table:

AC TYPE	Min Contention Window (2x-1; x can be 0-10)	Max Contention Window (2x-1; x can be 0-10)	Fixed Slot Time (0-15)	Transmit Opportunity (0-65535 μ S)
AC_BK	4	10	7	0
AC_BE	4	6	3	0
AC_VI	3	4	1	3008 (6016 when 11b)
AC_VO (3)	2	3	1	1554 (3264 when 11b)

SNTTP

Simple Network Time Protocol (SNTTP) allows the administrator to configure the network time settings.

The screenshot shows the configuration interface for an AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar contains a navigation menu with categories like 'Systems Status', 'Systems Configuration', '2.4G Radio Configuration', '5G Radio Configuration', 'Services', and 'Management'. The main content area is titled 'Service -> SNTTP' and contains the following settings:

- SNTTP Status:** Enable Disable
- Net Time:** Year: 2011, Month: 1, Day: 1, Hour: 0, Min: 0
- Time Zone:** GMT Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
- Daylight Saving:** Enable Not start/end dates
- From:** [] To: []
- Primary Server:** [] [] [] []
- Primary Port:** 37
- Secondary Server:** [] [] [] []
- Secondary Port:** 37

Buttons for 'Apply' and 'Cancel' are located below the settings. A message at the bottom states: 'You must click Apply to save your settings before moving to another page.'

Figure 23 SNTTP

The following settings can be configured.

SNTP client enable/disable	Click enable or disable. If it is disabled, the user has to input time manually. If it is enabled, the device will try to fetch time from configured SNTP servers.
Set Time	Specify Year, Month, Day, Hour, and Minute. These fields are grayed out and un-configurable if SNTP is enabled.
Timezone selection	This selection adjusts the time obtained from the SNTP server. Note: This selection does not affect manual time input as they are considered to be input at the same time.
Daylight Saving	The start/end date of daylight saving changes automatically based on the time zone selection. Note: Start and End dates can be input manually, to avoid any regional policy changes.
Primary and Secondary SNTP server/port setting	If SNTP is enabled, this device will try to fetch time from the Primary server first. The timeout for Primary NTP server is 5 seconds. If the Primary NTP server fails after 5 seconds the Secondary NTP server will be tried for 5 seconds. In the event that the Secondary server fails, the device will wait for 60 seconds before trying the Primary server again. This continues until a time is available.

To avoid using an invalid NTP server address, this device stores the fetched/configured time. After it boots up, it uses the stored time first and adjusts time if time is fetched.

Syslog Function

In the event of an error the device can send a message to a specified server.

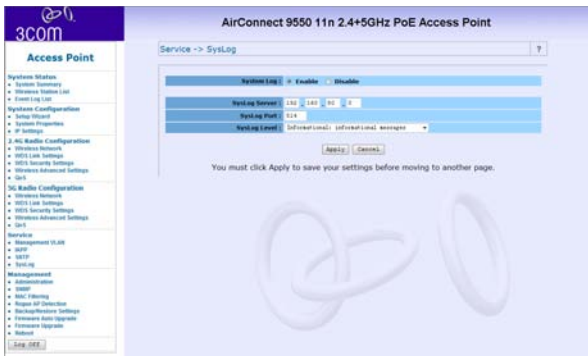


Figure 24 SysLog

System Log

Click either Enable or Disable to activate or deactivate the system log function.

Syslog Server

Enter the IP address of the server that receives the error information. The default IP address is 0.0.0.0

Syslog Port

Enter the port number that your server can be accessed by. The default port number is 514.

Syslog Level

Choose from the following levels, listed in order of severity of the detail to be recorded. The default setting is Error.

- Emergency - System is unusable
- Alert - Action must be taken immediately
- Critical - Critical condition
- Error - Error condition
- Warning - Warning condition
- Notice - Normal, but significant condition
- Informational - Informational messages

Management

This section describes how to use the management and information features of your Wireless Access Point.

Administration

In this section, you can change the user administrator name and password. The default Administrator name is **admin** (case sensitive), and password is **password**. Click Apply to save changes.

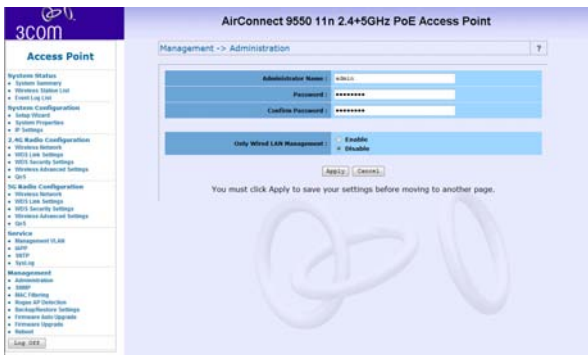


Figure 25 Administration

SNMP



Figure 26 SNMP

The Simple Network Management Protocol (SNMP) administrative functions are changed through this screen. The following functions can be changed:

- Enable/Disable SNMP
- Contact info
- Community names for read-only and read/write
- Trap destination IP address
- Community name

MAC Filtering

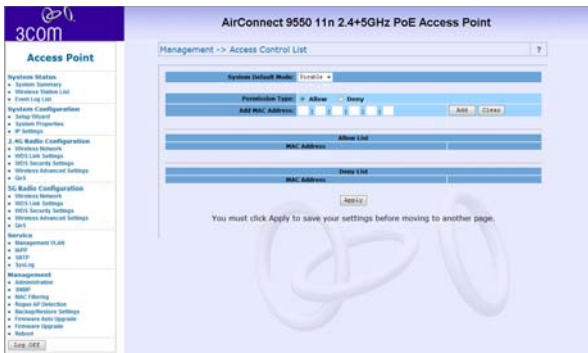


Figure 27 Access Control List

MAC filtering allows the administrator to filter MAC addresses of network cards that can access the access point. On this screen you can:

- Enable/Disable filter
- Change filter rule to allow or deny
- Add/delete MAC addresses in the filter table

This function is only available in AP mode.



Rogue AP Detection

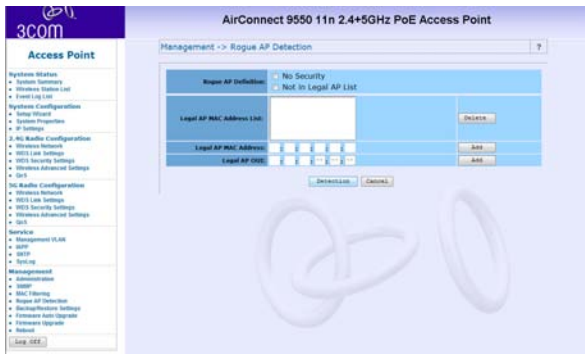


Figure 28 Rogue AP Detection

Unspecified Access Points may try to access the network through this device. Rogue AP detection can prevent this.

- Change Rogue AP definition.
- Legal AP list - The list of allowed access points.
- Detect rogue AP – All channels are scanned and Access Points without security, or not in legal AP, are considered rogue.



This function is only available in AP mode.

Backup/ Restore Settings

This screen allows the user to backup the Access Point's current settings and restore back to the factory default. Once you have the Access Point working properly you should backup the information to have it available if something goes wrong.

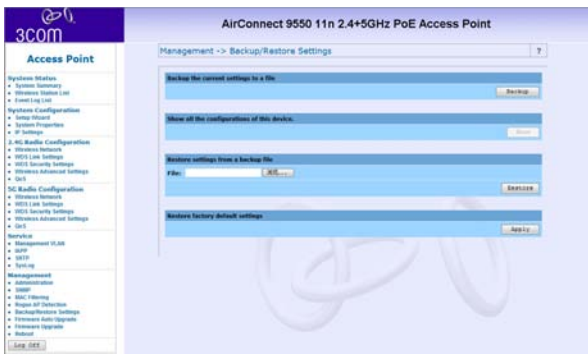


Figure 29 Backup/Restore Settings

Firmware Auto Upgrade

The Wireless Access Point can auto upgrade the firmware if there is a newer version available. If you enable the Auto Upgrade function, the Wireless Access Point will automatically check for an updated version of firmware in the assigned FTP server for each time interval assigned. Remember to insert the correct FTP server IP address, username, password, and path to the FTP server.

The screenshot displays the management interface for an AirConnect 9550 11n 2.4+5GHz PoE Access Point. The left sidebar shows a navigation menu with categories like System Status, System Configuration, 2.4 GHz Radio Configuration, 5G Radio Configuration, Services, and Management. The main content area is titled "Management -> Firmware Auto Upgrade" and contains the following settings:

- Auto Upgrade:** A dropdown menu set to "Enable".
- Refresh:** Radio buttons for "Yes" and "No".
- Time Interval:** A dropdown menu set to "Days".
- Last Firmware Run:** A red "NOTICE" box states: "The length of the filename (including extension) should be no more than 30 characters, or the file will be invalid!" Below this, it indicates "Different version found" and "Later version found".
- FTP Server IP Address:** A text input field.
- FTP Login Name:** A text input field.
- FTP Password:** A text input field.
- Firmware Path:** A text input field.

At the bottom of the settings area are "Apply" and "Cancel" buttons. Below the buttons, a message reads: "You must click Apply to save your settings before moving to another page."

Figure 30 Firmware Auto Upgrade

Firmware Manual Upgrade

On this screen, you can see the current firmware version of your AP. You can also manually upgrade your firmware by entering the path to your new firmware file.



Figure 31 Firmware Upgrade

Once you have chosen the upgrade file click **Upgrade**.

The screenshot displays the management interface for a 3Com AirConnect 9550 11n 2.4+5GHz PoE Access Point. The interface is divided into a left-hand navigation menu and a main content area.

Navigation Menu (Left):

- Access Point**
- System Status
 - System Summary
 - Wireless Status List
 - Event Log List
- System Configuration
 - Setup Wizard
 - System Properties
 - IP Settings
- 2.4G Radio Configuration
 - Wireless Network
 - WDS Link Settings
 - WDS Security Settings
 - Wireless Advanced Settings
 - QoS
- 5G Radio Configuration
 - Wireless Network
 - WDS Link Settings
 - WDS Security Settings
 - Wireless Advanced Settings
 - QoS
- Services
 - Management VLAN
 - SNMP
 - SNMP
 - SNMP
 - Event Log
- Management
 - Administration
 - SNMP
 - SNMP
 - SNMP
 - Wagner AP Detection
 - Hardware/Software Settings
 - Firmware Auto Upgrade
 - Firmware Upgrade
 - Reboot

Main Content Area:

Management -> Firmware Update -> Result

Firmware Updated Successfully

Received: 576/454 Bytes

Reminder: Go to the [Reboot Page](#) for changes to take effect

The background of the main content area features a faint, stylized graphic of two interlocking rings.

Figure 32 Result

Rebooting

You can reboot the Wireless access point from the browser interface.

After you click reboot, the following window displays.

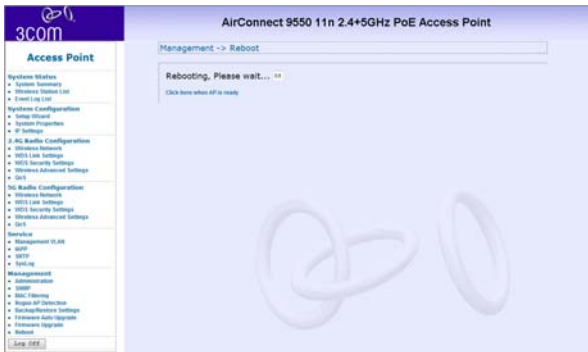


Figure 33 Reboot

After rebooting, the login page automatically displays.

Connecting Through the Com Port

Instead of using an IP address to configure the Access Point a Null modem cable, connected to the RJ-45 Console Port, can be used.

In your terminal settings ensure that the following configuration is met:

- Bits per Second – 15200
- Data Bits – 8
- Parity – None
- Stop bits – 1
- Flow Control - none

Once connected enter the user name and password. The default values are as follows:

- Username: **admin**
- Password: **password**

Once logged in, type “?” for a list of commands.

Restoring Factory Settings

The Access Point can be reset to the default factory settings either through the web browser (see “Backup/ Restore Settings” on page 56) or manually.

To restore the settings manually, insert a pointed object (such as the end of a straightened paper clip) into the reset hole on the side of the Access Point, and hold for five seconds.

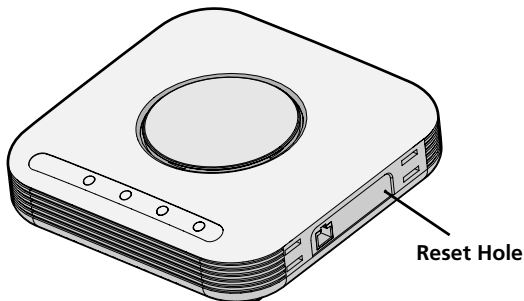


Figure 34 Reset Hole Location

A TROUBLESHOOTING

Diagnosing Problems

If you have difficulty with the Access point, try the following solutions.

Symptom

After you change the IP address, restore a backup configuration, or reset the Access Point to factory defaults, the Configuration Management System stops responding and you cannot continue configuring the Access point. If you change the IP address and click Apply, you cannot continue to configure the device using the old IP address. Similarly, after you restore a backup configuration or reset the Access Point to factory defaults, the IP address setting may be changed.

Solution

To recover from this situation and continue configuring the Access Point:

- 1 Close your browser.

- 2 Return to the 3Com Wireless Infrastructure Device Manager and click Refresh.
- 3 Select the device and click Configure to start a new configuration session and set its IP address.

Symptom

The Wireless Network Tree does not appear in the 3Com Wireless Infrastructure Device Manager window.

Solution

Verify that you are using the correct network adapter. In the device manager window, click Choose NIC. Select the network adapter for the network you want to scan, and click OK.

Symptom

The Access point has a yellow exclamation point (!) next to it in the Wireless Infrastructure Device Manager.

Solution

The Access Point is on a different subnet than the computer attempting to configure it. To recover from this situation and continue configuring the Access point:

- 1 Close your browser.
- 2 Return to the 3Com Wireless Infrastructure Device Manager and click Refresh.
- 3 Select the device and click Configure to start a new configuration session.

- 4 Make sure the subnet address matches that of the computer.

Symptom

Two Access Points cannot communicate in ad-hoc mode.

Solution

Adjust the positions of the Access Points to improve reception.

To ensure correct operation in ad-hoc mode, the settings on the two Access Points must match exactly.

Launch the Access Point Configuration Management System and make sure that the Wireless LAN Service Area, channel selections, Data Preamble setting, and security setting are the same on both Access points.

Symptom

You are running Windows NT. After you connect the Access Point, your computer cannot obtain a valid IP address.

Solution (s)

The Access Point configuration settings may not be compatible with the network. If they are not, and your Windows NT computer is set up to obtain its IP address from a DHCP server, the Access Point is unable to associate with the network to obtain the IP address.

To work around this, set a static IP address on your computer. Then set the Access Point configuration to match the network. When the Access Point is able to associate, reset your computer to obtain its IP address from the DHCP server. If the Access Point

should also obtain its IP settings from the DHCP server, make sure this is configured properly on the IP Network page and applied just before ending the session.

Symptom

Disconnecting the Access Point

Solution

To disconnect the Access Point:

CAUTION: Disconnecting the Access Point ends the network association. To avoid possible data loss, exit all networking applications on connected devices before you disconnect the Access Point.

- 1 Unplug the Access point Ethernet cable from the hub or other device.
- 2 Unplug the Access point power cord.

Symptom

Uninstalling Software and Documentation

Solution

If you want to uninstall the 3Com 11a/b/g/n Wireless Workgroup Access point software and documentation, you can either use the standard operating system procedure for removing programs or use the following shortcut:

From the Windows Start menu, select Start > Programs > 3Com Wireless > Uninstall 3Com Wireless Infrastructure Device Manager.

When prompted to confirm, click OK.

Symptom

Upgrading Access Point Firmware.

Solution

Firmware is the software that is installed on the Access Point at the factory. Some problems can be solved by installing a new version of the firmware.

For details on how to download a firmware update from the 3Com customer support Web site and install it on your Access Point, see “Firmware Auto Upgrade” on page 57 or “Firmware Manual Upgrade” on page 58.

B OBTAINING SUPPORT FOR YOUR 3COM PRODUCT

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

<http://eSupport.3Com.com/>

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender's expense. If your product is registered

and under warranty, you can obtain an RMA number online at **<http://eSupport.3Com.com/>**. First-time users must apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:

<http://csoweb4.3Com.com/contactus/>

C

END-USER LICENSE AGREEMENT

Customer shall take all steps necessary to protect Wind River's and its licensors' proprietary rights in the Run-Time Module and to ensure that each Run-Time Module distributed by Customer will be accompanied by a localized copy of an End-User License Agreement.

Such End-User License Agreement shall prohibit the End User from: (i) copying the Run-Time Module, except for archive purposes consistent with the End User's archive procedures; (ii) transferring the Run-Time Module to a third party apart from the Target Application; (iii) modifying, decompiling, disassembling, reverse engineering or otherwise attempting to derive the Source Code of the Run-Time Module; (iv) exporting the Run-Time Module or underlying technology in contravention of applicable U.S. and foreign export laws and regulations; and (v) using the Run-Time Module other than in connection with operation of the Target Application.

In addition, the End-User License Agreement shall: (i) state that the Run-Time Module is licensed, not sold and that Customer and its licensors retain ownership of all copies of the Run-Time Module; (ii) expressly disclaim all implied warranties, including

without limitation the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement; (iii) exclude liability for any special, indirect, punitive, incidental and consequential damages; and (iv) require that any further distribution of the Run-Time Module be subject to the same restrictions set forth herein.

The End-User License Agreement shall also state that, with respect to the Run-Time Module, Wind River and its licensors are third party beneficiaries of the End-User License Agreement and that the provisions related to the Run-Time Module are made expressly for the benefit of, and are enforceable by, Wind River and its licensors.

D APPENDIX

Antennas Used per Mode

The AP has three external antenna connectors, labelled A, B and C, as shown below.

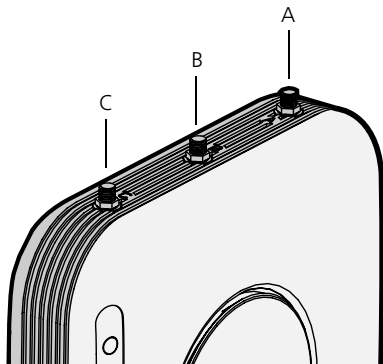


Figure 35 External Antenna Connectors

In some modes, not all of the connectors are in use.

The following table defines which external antenna connectors are used in which mode:

Mode	Antennas Used
2x3	A,B,C
2x2	A,C
1x1	A

Note: When using 1x1 mode, either in WDS mode or in AP mode using the 3CWE591 Omni antenna, only connector A is active. This is the connector on the far right, looking at the AP with the 3Com logo facing you. No other connectors are active in this mode.

When in WDS mode:

- select 1X1 mode when peers are omni-directional, distributed around the central node in a point-multipoint link.
- select 2X2 mode for a point-to-point link, using either the 3CWE596 or 3CW598 panel antenna. The antennas must both point in the same direction, with one antenna rotated 90 degrees, in order for MIMO to function correctly.

Note: In 2x2 mode, the two outer connectors (A and C) are active. The connector in the middle (B) is not active and should not be used.

Console Cable Pin-out

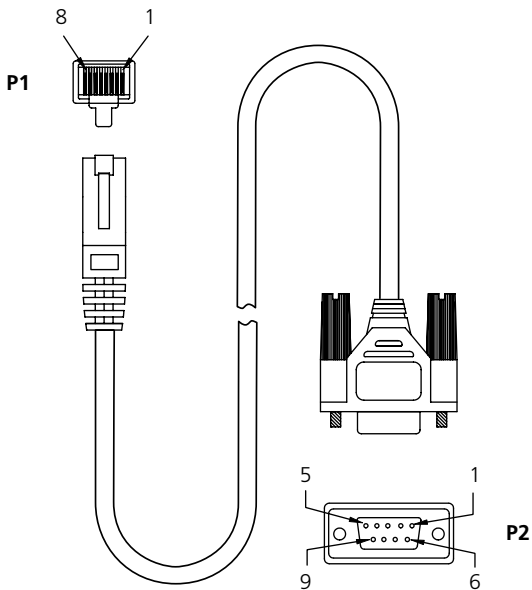


Figure 36 RJ45 to D-SUB 9 pin cable

P1	WIRE COLOR	P2
Pin no.		Pin no.
8	YELLOW	1
6	BROWN	2
2	GRAY	3
1	GREEN	4
5	RED	5
3	BLUE	6
4	BLACK	7
7	WHITE	8

For part numbers and purchasing information, visit the 3COM Web site (<http://www.3com.com>).

INDEX

Numerics

802.11a	9
802.11b/g	10
802.11d	41

A

Access Point mode	27
Administration	52
Advanced Settings	39
Antennas Used per Mode	72

B

Backup	56
Beacon Interval	40
BSSID	32

C

Com Port	61
Configuring	13
Console Cable	74
Contention	46

D

Data Beacon Rate	40
default IP address	14, 51
Delivery Traffic Indication Message (DTIM)	40
Device Manager ...	8, 13, 15, 67
DHCP Server	13

F

factory settings	62
Firmware	67
Auto Upgrade	57
Manual Upgrade	58
Fixed Slot Time	46
Fragment Length	40

I

IAPP	44
IEEE 802.3af	11
Inter-Access Point Protocol	44
IP Settings	28

L		
login	14, 18	
M		
MAC Filtering	54	
Management VLAN	43	
P		
Password	14, 18, 52, 61	
Power over Ethernet (PoE)	9	
Q		
Quality of Service (QoS)	42	
R		
Rebooting	60	
Restore	56	
Rogue AP Detection	55	
RTS Threshold	40	
S		
Security	7	
Setting Up	23	
Simple Network Management Pro-		
ocol (SNMP)	53	
Simple Network Time Protocol		
(SNTP)	48	
SSID	23, 32	
Suppressed SSID	32	
System Properties	26	
System Summary	19	
T		
terminal settings	61	
Transmit Power	39	
U		
Username	61	
V		
VLAN ID	32	
W		
WDS	36	
Security Settings	38	
Wi-Fi Protected Access	34	
Wired Equivalent Privacy (WEP)	33	
Wireless Distribution System ...	36	

Wireless Network Standards	9
WPA	34
WPA2	35, 36

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC / IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance **20cm** between the radiator & your body.

Canada C Request

"Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device."

"To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication"

"This device has been designed to operate with an antenna having a maximum gain of **20** dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms."

"To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication."

The County Code Selection feature is disabled for products marketed in the US/Canada

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

FCC NOTICE: To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

Only the antennas listed below are allowed to be used with the radio.

Ant.	Antenna Type	Model Name	Product description	2.4/5 GHz Gain (dBi)	Tx/Rx mode
1	Omni Ant	3CWE591	3Com® 6/8dBi Dual-Band Omni Antenna	6/8	1T1R
2	Omni Ant	S24513BPX	CUSHCRAFT 2.4~2.5& 4.9~5.9 GHz DUAL BAND OMNI ANTENNA	6/6.5	1T1R
3	Omni Ant	SS-200-AT-AN-30	Airtight 2.4~2.5& 4.9~5.9 GHz Dual-band Omnidirectional Indoor/outdoor antenna	6/6.5	1T1R
4	Omni Ant	TGX-102XNXXX	Joymax Base Station Antenna	6/6	1T1R
5	Panel Ant	3CWE596	3Com® 18/20dBi Dual-Band Panel Antenna	18/20	2T2R
6	Panel Ant	3CWE598	3Com® 8/10dBi Dual-Band Panel Antenna	8/10	2T2R
7	Panel Ant	SL24513P12SMF	CUSHCRAFT Tri-mode, dual band 802.11b/a/g ceiling mounted Omnidirectional panel antenna	3/3	2T2R
8	Panel Ant	SS-200-AT-AN-10	Airtight dual band 802.11b/a/g Omnidirectional Indoor panel antenna	3/3	2T2R
9	Monopole Ant	3CWE590	3Com 2dBi Dual-Band Omni Antenna Kit	2/2	2T3R
10	PCB Antenna	TFF-A015MPAX-361	Integrated PCB Antenna	3/3	2T3R