

airClient™ Nexus PRO TOTAL sB3412



User Guide

Version 1.0

TABLE OF CONTENTS

About This Document	4
Technical Support Center	5
1. Introduction	6
SYSTEM REQUIREMENTS.....	6
1.1.....	6
1.2. CHECKLISTS	7
2. aCNPT Configuration	11
USER LOGIN AND LICENSE AGREEMENT	11
2.1.....	11
2.2. WEB GUI ADMINISTRATOR PASSWORD CHANGE.....	13
2.3. USING THE CONFIGURATION PAGES	14
2.4. DEVICE MODE CONFIGURATION.....	18
2.5. ACNPT ROUTER/NAT TO ACNPT BRIDGE.....	19
2.6. ACNPT BRIDGE TO ACNPT ROUTER/NAT.....	20
2.7. ACNPT BRIDGE CONFIGURATION	21
2.7.1. Ethernet Configuration	21
2.7.2. Wireless Configuration	22
2.7.3. Bridge Configuration.....	24
2.7.4. Configuring Spanning Tree Protocol (STP).....	24
2.7.5. STP Settings Configuration	25
2.8. ACNPT ROUTER/NAT CONFIGURATION.....	28
2.8.1. Ethernet Configuration	28
2.8.2. Wireless Configuration	29
2.8.3. DHCP Configurations	31
2.8.4. DHCP Relay Configurations.....	33
2.8.5. Routing Table	34
2.8.6. Wireless Settings Management.....	35
2.8.7. Wireless Settings.....	36
2.8.8. Security	37
3. Performance Parameters and Bandwidth Controller.....	42
3.1. LINK PERFORMANCE PARAMETERS AND FEATURES.....	42
3.2. BANDWIDTH CONTROLLER.....	44
4. Quality of Service (QoS)	46
5. Site Survey Tool.....	54
6. Antenna Alignment.....	55
7. Traffic Statistics.....	57
8. Tools	60
8.1 SYSTEM CONFIGURATION.....	60
8.1.1 SNMP Security	62
8.1.2 Reset Options.....	63

8.1.3	NTP Time Server Setup	64
8.2	PROFILE MANAGER	64
8.2.1	Save Profile	66
8.2.2	Load Operating Profile	66
8.2.3	Profile Calendar	66
8.3	LINK TEST	67
8.4	LINK BUDGET PLANNING	69
9.	Firmware Upgrade	72
	Appendix A – SNMP Trap	74
	Appendix B – Useful terms and definitions	75
	Appendix C – License	78

About This Document

This User Guide is for the networking professional who configures and manages the smartBridges' Intelligent Nexus Platform of wireless client device, the airClient™ Nexus PRO TOTAL (sB3412).

It provides detailed information on using the web-based configuration GUI to configure the airClient Nexus PRO TOTAL unit, hereafter shortened to aCNPT. This manual will help you gain a better understanding of how the various components work.

To configure smartBridges' products, you need to have fundamental understanding of the concepts and technology of Local Area Networks (LAN) and wireless networking. The system installer will require expertise in the following areas:

- Outdoor radio equipment installation
- Network configuration
- Use of web browser for system configuration, monitoring and fault finding

In this chapter, you will find an overview of the User Guide and where to obtain additional information regarding installation and set-up.

Overview of User Guide

The checklists for pre-and post- installation are provided in Chapter 1. Chapter 2 shows the three modes that the airClient Nexus PRO TOTAL can work in: Bridge, Router and NAT and the procedures for configuring the various parameters in each mode.

Chapter 3 gives instructions for editing the wireless radio protocol parameters to optimize radio performance and changing the Bandwidth Controller. The Quality of Service (QoS) features are explained in Chapter 4.

Accessing the Site Survey page is shown in Chapter 5 and the antenna alignment process is outlined in Chapter 6. Wireless and Ethernet Traffic Statistics and the explanations is given in Chapter 7. Finally, the firmware upgrade process for aCNPT Nexus is explained in Chapter 9.

Related Publications

These documents provide complete information about the Nexus series of radio units: airHaul™, airPoint™ and airClient™.

- Quick Install Guide (QIG)
- Release Notes
- Technical Specification

For the latest information on smartBridges products, please visit our website at <http://www.smartbridges.com/>

Technical Support Center

Comprehensive technical support by dedicated smartBridges engineers is available to all customers through the smartBridges support center website. The website provides updated tools and documents to help troubleshoot and resolve technical issues related to smartBridges products and technologies. To access the technical support resources, please visit the support center website at <http://www.smartbridges.com/support/>

You will need to register for certain services and downloads on the smartBridges support center website.



1. Introduction

This User Guide provides information on how to set-up and deploy the airClient Nexus PRO TOTAL unit. A web-based management tool is provided to assist the user to configure the aCNPT.

The aCNPT web-based management tool provides the user with the following features:

1. System configuration
2. Device operational mode configuration
3. Ethernet and wireless IP configurations
4. Radio (SSID, domain, channel, etc) parameter configuration
5. Network bridge (STP, etc) parameter configuration
6. Bandwidth management
7. Security
8. QoS
9. Antenna alignment
10. Traffic Statistics
11. Site Survey
12. Profile management
13. User management
14. Link Test
15. Link Budget Planning Calculator
16. Firmware Upgrade

1.1. System Requirements

The following are the minimum system requirements for the aCNPT web-based configuration management tool:

1. Operating System: either Windows 98/2000/XP/NT or Linux
2. Connection to the internet for downloading the latest firmware and Sun JRE
3. Web browser: either Internet Explorer 5.0 and higher, Netscape 7.2 and higher, Mozilla 1.7 and higher or Mozilla Firefox 0.8 and higher
4. SUN JRE: v1.5 and above. You may download it from <http://java.sun.com/j2se/1.5.0/download.jsp>

1.2. Checklists

Pre-Installation Checklist for airClient Nexus PRO TOTAL

Organization Name/Site Name	
Address	
City	
State	
Zip Code	
Telephone Number	

Site Survey and Link Planning				
No	Parameters	Units	Site A	Site B
1	Regulatory Standard to be followed	For example, FCC, ETSI, etc		
2	Frequency Band	2.4GHz 5.25-5.35 5.47-5.725 5.725-5.805		
3	Maximum Output Power as per the Regulatory Authority	100mW/1W/4W		
4	Latitude	Deg Min Sec		
5	Longitude	Deg Min Sec		
6	UPS Installed	Yes/No		
7	UPS specification if any	KVA		
8	Line Voltage	90V-264V AC,50-60 Hz		
9	Near Line of site between sites	Yes/No		
10	Height of tower	Feet/Meters		
11	Repeater required to achieve a link	Yes/No		
12	If Repeater required, then reason why	For example, to achieve long distance/LOS etc		
13	No. of repeaters required	No		
14	Required Throughput	Mbps		
15	Gain of antenna	dBi (Internal antenna dBi is 15 for 802.11b/g and 17 for 802.11a)		
16	Antenna Polarization	Horizontal/Vertical		
17	Distance between sites	Miles/km		
18	Antenna Type (if using external antenna)	Parabolic/sector		
19	Antenna Mfg. (if using external antenna)	smartBridges/Name of other manufacturer		
20	Beam width of antenna (if using external antenna)	Horizontal – deg		
		Vertical – deg		

No	Parameters	Units	Site A	Site B
21	Type of external cable type	LMR 400/LMR600/		
22	Length of external cable connecting a Radio and antenna	Feet/meters		
23	Fade Margin taken into account for a link budgeting	Ideally between 10 to 20 dBm		
24	Model of smartBridges aCNPT equipment selected for a link. Please refer to note below for selecting the right equipment	sB3412		
25	Grounding- Earth to Neutral Voltage	Ideally less than 2 Volts		
26	Length of the Ethernet cable required for powering a unit	Feet/meters		
27	Choose a best channel which can be used on the basis of site survey with a help of scanning tools like Netstumbler	Specify channel number		

Pre Installation Lab Testing of Equipment				
No	Parameters	Units	Site A	Site B
1	Network diagram along with IP address of all the interfaces for link to be setup in place	Yes/No		
2	Availability of Quick Installation Guide	Yes/No		
3	Availability of User Guide and CD	Yes/No		
4	Ensure that all items listed in the "Package Contents" of Quick Installation Guide are included in the shipment	Yes/No		
5	Availability of Installation Kit	Yes/No		
6	Radio MAC address of Access Point	Yes/No		
7	Configured for pre installation testing	Yes/No		
8	Ping response	Ms		
9	Ping Success Rate	Percentage %		
10	Throughput test (Upload/Download)	Varies depending on the Bandwidth Control, signal strength, link quality and distance		

Signature of Engineer:	
Name:	
Email:	
Date:	

Post-Installation Checklist for aCNPT

Organization Name/Site Name	
Address	
City	
State	
Zip Code	
Telephone Number	

General Configuration Information				
No	Parameters	Units	Site A	Site B
1	Radio operations Mode	Bridge/Router/NAT		
2	SSID of a Radio	Up to 32 characters		
3	IP address of Ethernet Port	32-bit numeric address		
4	IP address of Wireless Port	32-bit numeric address		
5	Noise Floor	dBm		
6	RSSI	dBm		
7	Channel selected for Link			
8	Radio TX Output Power	(-5 to +23 dBm)		
9	Model of smartBridges aCNPT equipment selected for a link.	SB3412		
10	Antenna Gain	dBi (Internal antenna dBi is 15 for 802.11b/g and 17 for 802.11a)		
11	Antenna Polarization	Horizontal/Vertical		
12	Antenna Type (if using external antenna)	Parabolic/sector		
13	Antenna Mfg. (if using external antenna)	smartBridges/Name of other manufacturer		
14	Beam width of antenna (if using external antenna)	Horizontal – deg		
		Vertical – deg		

Checklist				
No	Parameters	Units	Site A	Site B
1	Check the crimping of the Ethernet cable at both the ends	Yes/No		
2	Check the proper grounding of the equipment	Yes/No		
3	Ensure that there are no extreme bends or kink's in the cable	Yes/No		
4	Ensure that the Ethernet cable is not running near a sharp edge	Yes/No		
5	Ensure that the aCNPT along with antenna is fixed properly on a tower with the help of nuts and bolt supplied in packaging	Yes/No		
6	Ensure that the device/ external antenna is pointed to get the best RSSI and link quality	Yes/No		
7	Ping response	Ms		
8	Ping success rate	Percentage		
9	Throughput test (Upload/Download)	Mbps		
10	Link stability based on observation for 1 Hr	Yes/No		

Signature of Engineer:	
Name:	
Email:	
Installation Date:	
Commissioned Date:	

For the latest information on smartBridges products, please visit our website at: <http://www.smartbridges.com/>

2. aCNPT Configuration

The airClient Nexus PRO TOTAL can work in one of three modes: Bridge, Router and NAT. The procedures for configuring the various parameters in each mode are outlined in this chapter.

2.1. User Login and License Agreement

The aCNPT unit comes with a pre-configured default Ethernet (wired-side) IP address: **192.168.0.210** and subnet mask: **255.255.255.0**. This default device IP address should be used when accessing the device configuration management interface for the first time using a web-browser (Enter **http://192.168.0.210** for the URL address). In addition, the Sun Java Plug-in should be installed. The PC must be on the same subnet as the aCNPT.

Follow the steps below to login as an Administrator to the web-based configuration management interface system:

1. Connect the aCNPT using the Power over Ethernet (PoE) to a PC or network via the ETH A or ETH B port. (Please refer to the Quick Install Guide for more information on connections).
2. Open a web browser on the PC and enter the device IP address 192.168.0.210 in the web browser address field and press the Enter key.
3. A user login box will appear. Enter the 'User name' and 'Password' and check the 'Remember my password' checkbox if you want the system to remember the password. The default user name is **Administrator** and the password is **smartBridges** (case sensitive).



Figure 2-1 Administrator Login

4. Click the 'OK' button. A license agreement page will appear as shown in Fig 2-2 below.
5. Click 'Accept'. The aCNPT 'Nexus Summary Information' page (Fig 2-3) will appear.

Terms of use :

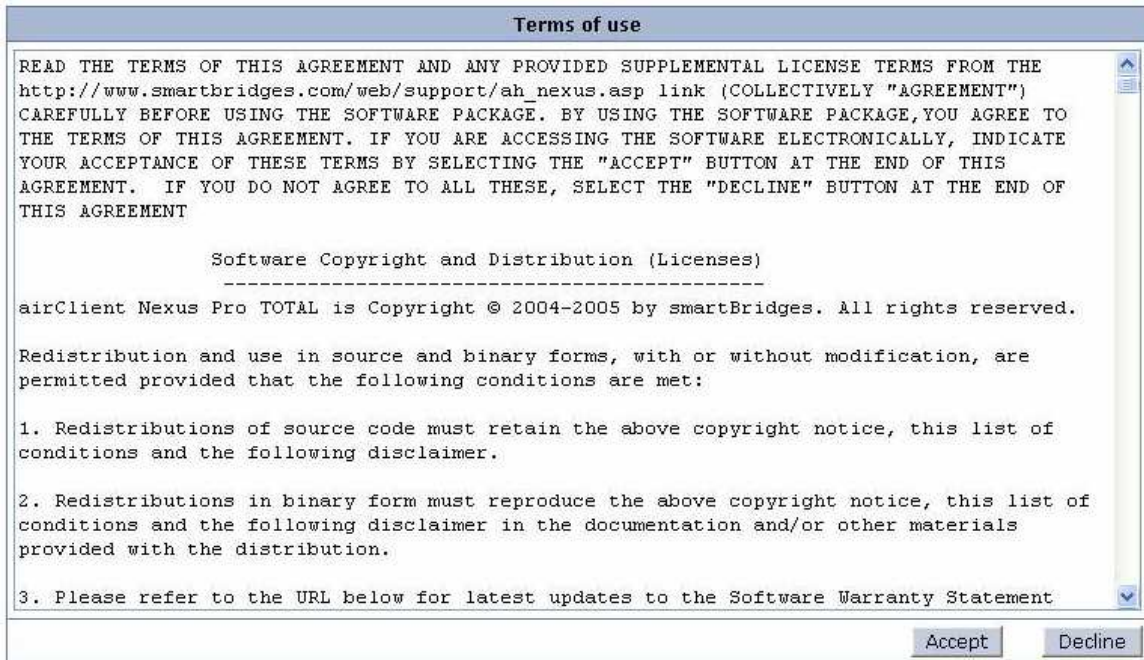


Figure 2-2 License Agreement Page

Summary Information :

airClient TOTAL (sB3412) - [NAT mode](#)

Wireless Configuration	
IP Address	192.168.1.210
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled
SSID	airPointSB3210
Channel	0 - (2407 MHz)
Association Status	Not Associated
RSSI	-

Ethernet Configuration	
IP Address	192.168.0.210
IP Mask	255.255.255.0

Port Information	
ETH A MAC Address	00:30:1A:1C:3D:B7
ETH B MAC Address	00:30:1A:1C:3D:B8
Radio MAC Address	00:30:1A:1F:48:19

Figure 2-3 aCNPT Summary Information Page

The page information descriptions are provided in the table below:

Table 2-1 Description of Parameters

Page Item	Descriptions	
Ethernet Configuration	IP Address	Editable Ethernet IP Address.
	IP Mask	Editable Ethernet IP subnet Mask
	Gateway	Editable Gateway IP address.
	DHCP	Editable DHCP status Disabled / Enabled User can enable DHCP by ticking the check box to obtain an IP address from the network DHCP server
Wireless Configuration	SSID	Device SSID.
	Channel	Device operation channel.
	RSSI	RSSI value when associated
	Maximum Wireless Throughput	Maximum Wireless Throughput in kbps
Port Information	ETH A MAC Address	Ethernet A (wired side) MAC address. Display only
	ETH B MAC Address	Ethernet B (wired side) MAC address. Display only
	Radio MAC Address	Radio MAC address. Display only
Operational Mode	Device operational mode	Current device operational mode, either as Bridge, Router, NAT

2.2. Web GUI Administrator Password Change

By default the administrator password is **smartBridges** (case sensitive).

Follow the steps below to change the Administrator password:

1. Click on the **Tools | User Manager** drop down menu in the navigation menu bar. An **Administrator Password Change** GUI will appear.
2. Enter the fields for **Old Password**, new **Authentication Password** and **Confirm new Authentication Password**.
3. Click on the **Apply Changes** button to change the password.

Tools : User Manager airClient TOTAL (sB3412) - [Bridge mode](#)

Administrator Password Change

Enter Old Password :

Enter new Authentication Password :

Confirm new Authentication Password :

Figure 2-4 Administrator Password Change

2.3. Using the Configuration Pages

The aCNPT Nexus configuration system comprises several pages for configuring each parameter. A common navigation menu bar is provided at the top of each page for easy navigation as shown in the figure below.

Home	Networking	Radio	Tools	Help	Logout
Summary Information :			airClient TOTAL (sB3412) - NAT mode		
Wireless Configuration			Ethernet Configuration		
IP Address	192.168.1.210	IP Address	192.168.0.210		
IP Mask	255.255.255.0	IP Mask	255.255.255.0		
Gateway	0.0.0.0				
DHCP	Disabled				
SSID	airPointSB3210				
Channel	0 - (2407 MHz)				
Association Status	Not Associated				
RSSI	-				
			Port Information		
			ETH A MAC Address	00:30:1A:1C:3D:B7	
			ETH B MAC Address	00:30:1A:1C:3D:B8	
			Radio MAC Address	00:30:1A:1F:48:19	

Figure 2-5 Navigation Menu Bar showing editable boxes for parameters

System configuration information is displayed as read-only in each page. As shown in the 'Summary Information' page in the above figure, 'Ethernet Configuration', 'Wireless Configuration' and 'Port Information' parameters are displayed as read only.

Clicking on the **UNDERLINED** parameter heading allows you to edit the configuration parameters. To change the 'Ethernet Configuration' parameters, click on the 'Ethernet Configuration' link. Similarly, clicking on the 'Wireless Configuration' link, the 'Radio Configuration page' will be displayed to edit any wireless settings. The figure below shows the 'Ethernet Configuration' parameters in editable boxes.

To save the changes to the system, click on the 'Apply Changes' button.

Note: Clicking the web browser's Back button returns to the previous screen *without* saving any changes. Changes are saved only when the user clicks the '**Apply Changes**' button

The Navigation menu bar contains menu items that allow user to go to different configuration pages. The following table summarizes functionalities available for the menu item links.

Table 2-2 Description of Menus

Menu Item	Menu Sub-items	Description
Home	Summary Information	Displays summary page with information such as Ethernet and Wireless IP settings. Allows user to set the IP settings for Ethernet (wired side) and Wireless interfaces depending on the device operational mode.

Menu Item	Menu Sub-items	Description
Networking	Bridge Configuration	Displays the bridge address, generic bridge port table, spanning tree port table for ports ETH A, ETH B, Radio A., etc Bridge configuration option is available when aCNPT is configured in aCNPT Bridge mode.
	DHCP	Configure DHCP server or Relay This option is available only if aCNPT is configured in aCNPT Router/NAT mode.
	Traffic Statistics	Displays the Ethernet and Wireless Traffic Statistics
	Bandwidth Controller	Allows bi-directional bandwidth management of the wireless link.
	Routing Table	Allows user to view, add and delete static routes. Routing table is only available for aCNPT Router mode.
	QoS	The primary goal of QoS is to provide priority such as dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.
Radio	Main	<p>Wireless Settings: Allows user to set SSID, Channel, ACL Controls and Country, as well as Dial-a-Power. Provides a link to view association Link Status.</p> <p>Performance: Allows user to set Fragment Length, RTS/CTS Length, RSSI Threshold and Throughput Optimizer. Radio Operation mode is set to mixed 802.11a/b/g by default.</p> <p>Wireless Traffic Statistics: Displays the Wireless Traffic Statistics.</p>

	Security	<p>Security: Allows user to set the WEP Keys and to choose between Open/Shared System modes of authentication.</p> <p>WPA-PSK: Where encryption keys are automatically changed (called rekeying) and authenticated between devices after a specified period of time, or after a specified number of packets has been transmitted.</p> <p>WPA-RADIUS: Provides encryption via the Temporary Key Integrity Protocol (TKIP) using the RC4 algorithm. It is based on the 802.1x protocol and addresses the weaknesses of WEP.</p> <p>WPA2-PSK: Based on the 802.11i standard, WPA2 was released in 2004 and uses a stronger method of encryption</p> <p>WPA2-RADIUS: The enterprise version of WPA2 is WPA2-RADIUS which uses an external RADIUS server for authentication which uses EAP (Extended Authentication Protocol).</p> <p>Note: The Default Security is None</p>
		<p>Reset to Defaults: Resets the device to factory default values.</p> <p>Ethernet MTU Size: Allows user to set the Ethernet MTU size for different applications.</p> <p>Syslog server IP Address: Allows user to set the Syslog server IP and log level.</p> <p>SNMP Trap server IP Address: Allows user to set the SNMP Trap server IP for SNMP trap forwarding.</p> <p>LED Control: Allows user to turn on/off LED .</p>

		<p>Operational mode: Allows the User to set the Radio Operational mode.</p>
	Profile Manager	<p>Save Profile: Allows user to define and save up to three device operating profiles for easy device management. One installation profile is always available.</p> <p>Operating Profile: Allows user to load the profile from saved profiles and shows last loaded profile</p> <p>Profile Calendar: Allows user to plan and manage the use of different profiles at different times efficiently.</p>
	Link Test	Allows user to do a throughput test and ping test. These tools could be very helpful during the installation phase.
	Link Budget Planning Calculator	Allows user to calculate the Link Budget.
	Antenna alignment	Shows the link status, link quality, RSSI.
	Site Survey	Shows all the wireless devices operating in the area.
	User Manager	Allows the administrator to change the Administrator password.
	Firmware Upgrade	Allows user to update to new firmware versions.
Help	Technical Support	Information on Technical Support
	User Guide – Online	Links to online User Guide
	Product Registration and Feedback	Allows user to register product and provide feedback or suggestions.
	Check for Updates	Links to smartBridges website for any software updates.
	About aCNPT	General system description, software version information and warranty information.

2.4. Device Mode Configuration

The device operational mode is displayed at the top right hand corner of each page. The Device Mode Configuration allows the user to configure the aCNPT in Bridge, Router and NAT.

NAT: This is the default operating mode. This mode allows a Local Area Network (LAN) to use one set of IP addresses for internal traffic and a single wireless IP for external traffic. It provides a type of firewall by hiding internal IP addresses and allows sharing by many computers behind the aCNPT. Since these are done in the LAN there is no possibility of conflict with IP addresses in the public or wireless network. This is in the Client Infrastructure mode.

Router: A normal routing functionality is provided in this mode. This is in Client Infrastructure mode.

Bridge: A transparent bridging functionality is provided in this mode which uses WDS implementation.

Home	Networking	Radio	Tools	Help	Logout
------	------------	-------	-------	------	--------

System Configuration : airClient TOTAL (sB3412) - [NAT mode](#)

System Configuration	
System Name	Nexus
System Description	Nexus
SNMP Security	SNMP Security
Reset	Reset
Delayed Reset	Delayed Reset
NTP Server	NTP Server Settings Time Server Not available
Firmware Version	v0.00.04 Release Notes
Radio Firmware Version	1.1.2.16
Edit Configuration	IP Configuration Radio : Performance
Reset To Factory Defaults	Reset To Defaults
Ethernet MTU Size	1512 bytes
Syslog server IP Address	0.0.0.0 Log level : -
SNMP Trap server IP Address	0.0.0.0
Watch Guard	Enabled Suspend
LED Control	On

Current Operational Mode
<input type="radio"/> Bridge <input type="radio"/> Router <input checked="" type="radio"/> NAT

Figure 2-6 Device mode settings (similar for Router/NAT/Bridge)

2.5. aCNPT Router/NAT to aCNPT Bridge

Follow the steps below to change aCNPT Router/NAT mode to aCNPT Bridge Mode

1. Go to 'Tools | System Configuration' drop down menu. The 'System Configuration' will be displayed.
2. Click on the 'Current Operational Mode' link to go to the 'System Configuration' page. Choose 'Bridge' under the 'Remote Device' option.
3. Click on 'Apply Changes'. A confirmation pop-up window will be displayed.
4. Enter the fields for 'IP Address', 'IP Mask' and Gateway for 'Ethernet Configuration'.
5. Enter the MAC address and the SSID of the remote radio.
6. Enter the Channel and Domain.
7. Click on the 'Apply Changes' button to change the settings.
8. The device will be rebooted and set to the chosen operational mode.

Confirm Configuration :	
Wireless Configuration	
SSID	NEXUS_MASTER
MAC Address	00:30:1A:1F:4A:30
Domain	FCC
Channel	1 - (2412 MHz)
Ethernet Configuration	
IP Address	192 . 168 . 0 . 7
IP Mask	255 . 255 . 255 . 0
Gateway	0 . 0 . 0 . 0
DHCP	<input type="checkbox"/>
Apply Changes	

Figure 2-7 Changing aCNPT Router/NAT to aCNPT Bridge

2.6. aCNPT Bridge to aCNPT Router/NAT

Follow the steps below to change aCNPT Bridge mode to aCNPT Router/NAT mode

1. Go to 'Tools | System Configuration' drop down menu. The 'System Configuration' will be displayed.
2. Click on the 'Current Operational Mode' link to go to the 'System Configuration' page. Choose 'Router' (or NAT) under the 'Remote Device' option.
3. Click on 'Apply Changes'. A confirmation pop-up window will be displayed.
4. Enter the fields for 'IP Address', 'IP Mask' and 'Gateway' for 'Ethernet Configuration' and 'Wireless Configuration'.
5. Enter the SSID and the Domain of a remote radio.
6. Click on 'Apply Changes' button to change the settings. The device will be rebooted and set to the chosen operational mode.

Confirm Ethernet and Wireless Configuration :

Ethernet Configuration	
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="7"/>
IP Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Wireless Configuration	
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="2"/> . <input type="text" value="207"/>
IP Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Gateway	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
DHCP	<input type="checkbox"/>
SSID	<input type="text" value="NEXUS_MASTER"/>
Domain	<input type="text" value="FCC"/> ▼

Figure 2-8 Changing aCNPT Bridge to aCNPT Router/NAT

2.7. aCNPT Bridge Configuration

The aCNPT in Bridge mode can associate only with a smartBridges airPoint access point in bridge mode (SB3210) as they both use WDS link implementation. It can associate with any third party bridge but the link is more effective with a smartBridges airPoint.

The following sections outline the procedures for changing the settings for bridge mode.

2.7.1. Ethernet Configuration

The Ethernet IP is configured when the operational mode was changed to the bridge mode.

Follow these steps below if you need to re-configure the aCNPT Bridge Ethernet parameters:

1. From the 'Summary Information' page, click on the 'Ethernet Configuration' link.
2. Select DHCP enable/disable radio button. Enter the 'IP address', 'IP mask', 'Gateway' for non DHCP. Assign the unit a unique IP Address in the designated IP subnet.
3. Click on the 'Apply Changes' button to effect the changes.

Summary Information :

Wireless Configuration	
IP Address	192.168.1.210
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled
SSID	airPointSB3210
Channel	0 - (2407 MHz)
Association Status	Not Associated
RSSI	-

airClient TOTAL (sB3412) - NAT mode

Ethernet Configuration	
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="210"/>
IP Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Port Information	
ETH A MAC Address	00:30:1A:1C:3D:B7
ETH B MAC Address	00:30:1A:1C:3D:B8
Radio MAC Address	00:30:1A:1F:48:19

Figure 2-9 aCNPT Bridge Ethernet Configuration

2.7.2. Wireless Configuration

The wireless parameters need to be configured to allow the aCNPT in Bridge mode to associate with an airPoint™ (sB3210) in Bridge mode.

Follow the steps below to configure the aCNPT Bridge Mode wireless association parameters:

1. Select 'Main – aCNPT Bridge Mode' from the 'Radio' drop-down menu on the menu bar.
2. Enter the SSID and access point's radio MAC address.
3. Choose a radio regulatory domain and channel from the drop down lists.
4. Select the transmit power of the radio from the Dial-a-Power drop down menu and select the appropriate gain of the antenna.
5. Enter the RF cable loss based on the cable specifications.
6. Click 'Apply Changes'. The units will attempt to associate.
7. Click on the 'View Association Table' to check for the associated clients.

Radio Configuration : airClient Bridge - Main **airClient TOTAL (sB3412) - [Bridge mode](#)**

Wireless Settings	
SSID	<input type="text" value="NEXUS_MASTER"/>
MAC Address	<input type="text" value="00:30:1A:1F:4E:75"/>
Domain	FCC <input type="button" value="v"/>
Radio Operating Mode	Mixed (802.11 a/b/g) <input type="button" value="v"/>
Antenna Selection	Internal <input type="button" value="v"/>
Channel	11 - (2462 MHz) <input type="button" value="v"/>
Rates	<input type="radio"/> 1 Mbps <input type="radio"/> 2 Mbps <input type="radio"/> 5.5 Mbps <input type="radio"/> 11 Mbps <input type="radio"/> 6 Mbps <input type="radio"/> 9 Mbps <input type="radio"/> 12 Mbps <input type="radio"/> 18 Mbps <input type="radio"/> 24 Mbps <input type="radio"/> 36 Mbps <input type="radio"/> 48 Mbps <input checked="" type="radio"/> 54 Mbps
Auto rate Fallback	<input checked="" type="checkbox"/>
Dial a Power	18 dBm <input type="button" value="v"/> Antenna Gain (dBm): 23 <input type="button" value="v"/> RF Cable Loss(dBm) : <input type="text" value="3"/>
Status	<input type="button" value="Apply Changes"/>

Figure 2-10 aCNPT Bridge Wireless Settings

Radio Configuration : airClient Bridge - Main

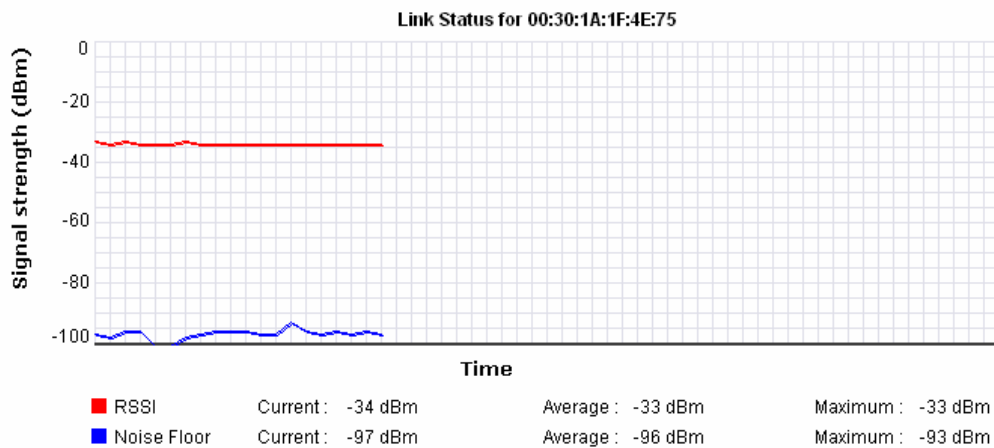
airClient TOTAL (sB3412) - [Bridge mode](#)

Wireless Settings			
SSID	NEXUS_MASTER Associated		
MAC Address	00:30:1A:1F:4E:75		
Domain	FCC		
Radio Operating Mode	Mixed (802.11 a/b/g)		
Antenna Selection	Internal		
Channel	11 - (2462 MHz)		
Rates	1 Mbps 6 Mbps 24 Mbps	2 Mbps 9 Mbps 36 Mbps	5.5 Mbps 12 Mbps 48 Mbps 11 Mbps 18 Mbps 54 Mbps
Auto rate Fallback	Enabled		
Dial a Power	18 dBm	Antenna Gain (dBm):23	RF Cable Loss(dBm) :3
Status			

Figure 2-11 Radio Main (Wireless Settings Page) - Associated

Click on 'Status' to view the association link-status graph.

Radio Configuration - Bridge : Status	
State	Associated MAC : 00:30:1A:1F:4E:75
Current Channel	11 - (2462 MHz) Associated
Antenna Alignment Tone	<input type="radio"/> On <input checked="" type="radio"/> Off



If you are not able to see the graph, please download the Sun JRE, available at URL <http://java.sun.com/j2se/1.5.0/download.jsp>

Figure 2-12 Link Status

Noise Floor is the measure of the signal created from the sum of all the noise sources and unwanted signals within a measurement system.

Note: If the association status window does not appear, click on the Java link to download the JRE.

2.7.3. Bridge Configuration

In Bridge mode the aCNPT unit acts as a transparent bridge between the Radio and the Ethernet interfaces. The figure below shows the bridge configuration and the table of bridge forwarding information. The STP (Spanning Tree Protocol) is disabled by default.

Networking : Bridge Configuration

airClient TOTAL (sB3412) - [Bridge mode](#)

Bridge Configuration			
Bridge Address	00:30:1A:1C:3D:B7	Number of Ports	3
Type of Bridging	Transparent	Spanning Tree Protocol	Disabled

[Transparent Aging Time](#) : 300 (seconds)

Forwarding Table for Transparent Bridge			
Sr.no	MAC Address	Port Number	Local?
1	00:30:1A:01:97:42	2	no
2	00:30:1A:16:24:13	4	no
3	00:30:1A:1C:3D:B7	1	yes
4	00:30:1A:1C:3D:B8	2	yes
5	00:30:1A:1F:48:19	3	yes

[Refresh](#)

Figure 2-13 Bridge Configuration Information

2.7.4. Configuring Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two redundant links.

To create a fault-tolerant network, there needs to be a loop-free path between all nodes in the network. The Spanning Tree Algorithm calculates the best loop-free path throughout a Layer 2 network. Infrastructure devices such as wireless bridges and switches send and receive spanning tree frames, called Bridge Protocol Data Units (BPDUs), at regular intervals. The devices do not forward these frames but use them to construct the loop-free path.

Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Infrastructure devices might also learn end-station MAC addresses on multiple Layer 2 interfaces. Such conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all infrastructure devices in the Layer 2 network.

STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the Spanning Tree Algorithm recalculates the spanning tree topology and activates the standby path.

When two interfaces on a device are part of a loop, the spanning tree port priority and path cost settings determine which interface is put in the forwarding state and which is put in the blocking state. The port priority value represents the location of an interface in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

2.7.5. STP Settings Configuration

STP is disabled by default. The table below lists the default STP settings when the STP is enabled.

Table 2-3 Default STP Values

Setting	Default Value	Range	Purpose
Bridge priority	32768	0-65535	A parameter used to identify the root bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root.
Bridge max age	20	6-40	The interval a bridge will wait for a hello packet from the root bridge before initiating a topology change.
Bridge hello time	2	1-10	The interval of time between each configuration BPDU sent by the root bridge.
Bridge forward delay	15	4-30	The period of time a bridge will wait (the listen and learn period) before beginning to forward data packets.
Ethernet port (ETH A) path cost	100	0-65535	The cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.
Ethernet port (ETH A) priority	128	0-255	The preference that STP gives to this port relative to the other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority; thus, the highest priority is 8.
Ethernet port (ETH B) path cost	100	0-65535	The cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.

Ethernet port (ETH B) priority	128	0-255	The preference that STP gives to this port relative to the other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority; thus, the highest priority is 8.
Radio port (Radio A) path cost	100	0-65535	The cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.
Radio port (Radio A) priority	128	0-255	The preference that STP gives to this port relative to the other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority; thus, the highest priority is 8.

The Radio and Ethernet interfaces are assigned to bridge group by default. When the user enables STP and assigns a priority on bridge, STP is enabled on the radio and Ethernet interfaces. The interfaces adopt the priority assigned to bridge.

The user can edit STP Priority, Bridge Max age, Bridge hello time, Forward Delay, STP Port priority and STP Port Path cost.

The **Transparent Aging Time** determines the time to refresh entries in the Forwarding Table. The Transparent Aging Time default value is 300 seconds.

Follow the steps below to configure the bridge STP for device in aCNPT Bridge:

1. Click on 'Networking | Bridge Configuration' to access the Bridge Configuration page.
2. Choose 'Enable' from the Spanning Tree Protocol pull down list.
3. Click on the 'Generic Port Table' link to change the Generic Parameters.
4. Enter a value for the 'STP Priority'.
5. Enter a value for the 'Bridge Max Age'.
6. Enter a value for the 'Bridge Hello Time'.
7. Enter a value for the 'Bridge Forward Delay'.
8. Click on 'Transparent Aging Time' link to change the 'Transparent Aging Time'.
9. Click on the 'Spanning Tree Port Table' link to change the 'STP Ethernet Port' parameters.

10. Enter the values of Ethernet Port Priority and/or Port Path Cost for ETHA.
11. Enter the values of Ethernet Port Priority and/or Port Path Cost for ETHB.
12. Enter the values of Ethernet Port Priority and/or Port Path Cost for Radio A
13. Click on 'Apply Changes' Button to save to the current configuration file.

Networking : Bridge Configuration

airClient TOTAL (sB3412) - [Bridge mode](#)

Bridge Configuration

Bridge Address	00:30:1A:1C:3D:B7	Number of Ports	3
Type of Bridging	Transparent	Spanning Tree Protocol	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> Disable ▼ </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px; width: fit-content;"> Enable Disable </div>

[Transparent Aging Time](#) : **300** (seconds)

Forwarding Table for Transparent Bridge			
Sr.no	MAC Address	Port Number	Local?
1	00:30:1A:01:97:42	2	no
2	00:30:1A:16:24:13	4	no
3	00:30:1A:1C:3D:B7	1	yes
4	00:30:1A:1C:3D:B8	2	yes
5	00:30:1A:1F:48:19	3	yes

Figure 2-14 Bridge Configuration

2.8. aCNPT Router/NAT Configuration

The aCNPT unit can also be configured in Router or NAT mode which behaves like Infrastructure mode. The procedures for configuring the parameters in Router/NAT mode are given below. In this mode, the units will associate with any access point.

Note: The configuration procedure of parameters in NAT mode is the same as for Router mode.

2.8.1. Ethernet Configuration

The Ethernet IP is configured during the operational mode change to aCNPT Router mode.

Follow these steps below if you need to re-configure the aCNPT Router Ethernet parameters:

1. From the 'Summary Information' page, click on the 'Ethernet Configuration' link to change Ethernet parameters.
2. Enter the 'IP address' and 'IP mask'.
3. Click on 'Apply Changes' to effect the changes.

Summary Information :

Wireless Configuration	
IP Address	192.168.1.210
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled
SSID	CH157
Channel	0 - (2407 MHz)
Association Status	Not Associated
RSSI	-

airClient TOTAL (sB3412) - Router mode

Ethernet Configuration	
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="210"/>
IP Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Port Information	
ETH A MAC Address	00:30:1A:1C:3D:B7
ETH B MAC Address	00:30:1A:1C:3D:B8
Radio MAC Address	00:30:1A:1F:48:19

Figure 2-15 aCNPT Router Ethernet Configuration

2.8.2. Wireless Configuration

The wireless parameters need to be configured to allow the aCNPT Router/NAT unit to associate with an airPoint or any third party access point.

Follow these steps below to configure the aCNPT Router/NAT Mode Wireless IP Settings parameters:

1. Click on the 'Wireless Configuration' link from the 'Summary Information' page.
2. Enter the wireless 'IP address', 'IP Mask', 'Gateway IP' address for the aCNPT unit.
3. Check the 'Enable DHCP' checkbox if the IP address can be obtained automatically from the wireless link.
4. Click on the 'Apply Changes' to change the settings.

Summary Information :

Wireless Configuration	
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="210"/>
IP Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Gateway	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
DHCP	<input type="checkbox"/>
SSID	CH157
Channel	0 - (2407 MHz)
Association Status	Not Associated
RSSI	-

airClient TOTAL (sB3412) - Router mode

Ethernet Configuration	
IP Address	192.168.0.210
IP Mask	255.255.255.0

Port Information	
ETH A MAC Address	00:30:1A:1C:3D:B7
ETH B MAC Address	00:30:1A:1C:3D:B8
Radio MAC Address	00:30:1A:1F:48:19

Apply Changes

Figure 2-16 aCNPT Router Wireless IP Configuration

In order for the aCNPT Router/NAT device to associate with the access point, the user needs to configure the access point's SSID and any security option if enabled, for example WEP.

Follow these steps below to configure the aCNPT Router/NAT Mode wireless association parameters:

1. Click on 'Main aCNPT Router Mode' from the 'Radio' drop-down menu.
2. Enter the SSID and domain.
3. Select the Transmit power of the radio from Dial in Power drop down menu.
4. Select the gain of the antenna from the drop down menu as per the gain of the antenna being used with the equipment.
5. Enter the RF cable loss based on the cable specifications.
6. Click 'Apply Changes'. The units will attempt to associate.

Note: Clicking on 'Status' will display further details on the association.

Radio Configuration : airClient Router - Main

airClient TOTAL (sB3412) - [Router mode](#)

Wireless Settings	
SSID	airPointSB3210 Not Associated
Domain	FCC
Dial a Power	18 dBm Antenna Gain(dBm) : 23 RF Cable Loss(dBm): 3
Antenna Selection	Internal
Radio Operating Mode	Mixed (802.11 a/b/g)
Channel	0 - (2407 MHz)
Rates	<input type="radio"/> 1 Mbps <input type="radio"/> 2 Mbps <input type="radio"/> 5.5 Mbps <input type="radio"/> 11 Mbps <input type="radio"/> 6 Mbps <input type="radio"/> 9 Mbps <input type="radio"/> 12 Mbps <input type="radio"/> 18 Mbps <input type="radio"/> 24 Mbps <input type="radio"/> 36 Mbps <input type="radio"/> 48 Mbps <input checked="" type="radio"/> 54 Mbps
Auto rate Fallback	<input checked="" type="checkbox"/>
Status	<input type="button" value="Apply Changes"/>

Figure 2-17 aCNPT Router Wireless Association Settings

Click on 'Status' to view the association link-status graph.

After getting the associated the page looks as follows

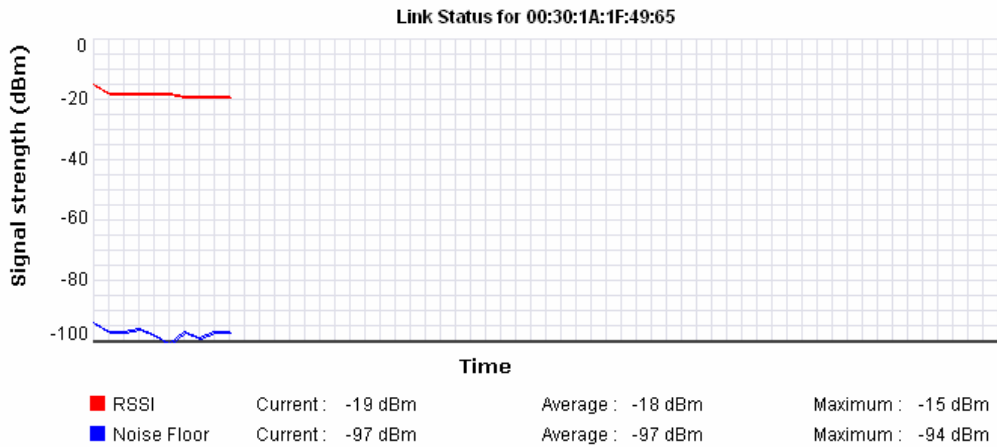
Radio Configuration : airClient Router - Main

airClient TOTAL (sB3412) - [Router mode](#)

Wireless Settings	
SSID	airPointSB3210 Associated
Domain	FCC
Dial a Power	18 dBm Antenna Gain(dBm) : 23 RF Cable Loss(dBm): 3
Antenna Selection	Internal
Radio Operating Mode	Mixed (802.11 a/b/g)
Channel	11 - (2462 MHz)
Rates	1 Mbps 2 Mbps 5.5 Mbps 11 Mbps 6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps
Auto rate Fallback	Enabled
Status	

Figure 2-18 Wireless Settings Page (Associated)

Radio Configuration - Router : Status		
State	Associated MAC : 00:30:1A:1F:49:65	
Current Channel	11 - (2462 MHz)	Associated
Antenna Alignment Tone	<input type="radio"/> On <input checked="" type="radio"/> Off	



If you are not able to see the graph, please download the Sun JRE, available at URL <http://java.sun.com/j2se/1.5.0/download.jsp>

Figure 2-19 Link status Page

Noise Floor is the measure of the signal created from the sum of all the noise sources and unwanted signals within a measurement system.

Note: If the association status window does not appear, click on the Java link to download the JRE.

2.8.3. DHCP Configurations

The aCNPT Router/NAT unit can be used as a DHCP server or DHCP relay agent. DHCP (Dynamic Host Configuration Protocol) allows a host to be automatically assigned a new IP address out of a pool of IP addresses for his network.

A DHCP server/relay can only be configured when the device is in the aCNPT Router/NAT Mode.

Follow the steps below to configure the aCNPT Router unit as a DHCP server:

1. Click on 'Networking' | 'DHCP Server' from the menu bar to access the DHCP configuration page.
2. Click on 'Enable DHCP' to start the DHCP server configuration.
3. Enter the starting IP address for the IP pool range that can be assigned to a DHCP client.
4. Enter the Max number of users for the maximum number of clients which can be assigned an IP address at a time by the DHCP server.
5. Enter Max Lease Time in Days, Hours and Minutes for all the clients.

6. Enter DNS Server IP address(es).
7. Click on the 'Apply Changes' to change the settings.

Note: The system will validate the input parameters and notify users of invalid entries. The Starting IP address will be in the same network segment as the device wired-side Ethernet IP address. IP address 0.0.0.0 for the DNS Server IP indicates no DNS Server is being used. The DHCP Server is only available to hosts connected to the same LAN segment as the device wired-side Ethernet port.

Networking : DHCP Server Configuration

airClient TOTAL (sB3412) - [Router mode](#)

DHCP Server Configuration	
DHCP	<input checked="" type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay <input type="radio"/> Disable DHCP and DHCP Relay
Starting IP Address	192.168.0. <input type="text" value="206"/>
Max number of users	<input type="text" value="49"/>
Max Lease Time	Days <input type="text" value="0"/> Hours <input type="text" value="02"/> Minutes <input type="text" value="00"/> : : :
DNS Server IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Secondary DNS Server IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

[Apply Changes](#)

Figure 2-20 DHCP Server Configurations

Follow the steps below to disable the aCNPT Router/NAT DHCP server:

1. Click on 'Networking' | 'DHCP Server' from the menu bar to access the DHCP configuration page.
2. Click on 'Disable DHCP and DHCP Relay' to disable the DHCP server configuration.
3. Click on the 'Apply Changes' to change the settings.

Networking : DHCP Server Configuration

airClient TOTAL (sB3412) - [Router mode](#)

DHCP Server Configuration	
DHCP	<input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay <input checked="" type="radio"/> Disable DHCP and DHCP Relay

[Apply Changes](#)

Figure 2-21 Disable DHCP and DHCP Relay

2.8.4. DHCP Relay Configurations

If the user has a DHCP Server, the aCNPT Router can be configured as a DHCP Relay agent of the DHCP Server for IP address assignment.

Follow the steps below to configure the aCNPT Router unit as a DHCP Relay Agent:

1. Click on 'Networking' | 'DHCP Server' from the drop down menu to access the DHCP Configuration page.
2. Click on 'Enable DHCP Relay' to choose DHCP Relay mode.
3. Enter a valid DHCP Server IP.
4. Click on the 'Apply Changes' to start the DHCP relay agent.

Note: The system will validate the input parameters and notify users of invalid entries. The DHCP Server IP will be in the same network segment as the device wireless Radio IP address. The DHCP Server needs to be configured to serve IP range of the wired side Ethernet IP. The DHCP Relay Agent is only available to hosts connected to the same LAN segment as the device wired-side Ethernet port.

Networking : DHCP Server Configuration

airClient TOTAL (sB3412) - [Router mode](#)

DHCP Server Configuration	
DHCP	<input type="radio"/> Enable DHCP Server <input checked="" type="radio"/> Enable DHCP Relay <input type="radio"/> Disable DHCP and DHCP Relay
DHCP Relay Agent	
DHCP Server IP	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="2"/>

[Apply Changes](#)

Figure 2-22 DHCP Relay Agent Configurations

2.8.5. Routing Table

The aCNPT Router web-interface provides viewing of the routes and allows for adding and deleting of the static routes for the aCNPT Router mode only.

To view the route entry in the aCNPT Router device, click on 'Networking' | 'Routing Table' from the menu bar to access the view routing table page.

Networking : Routing Table **airClient TOTAL (sB3412) - [Router mode](#)**

Routing Table						
Destination	Gateway	Mask	Flags	Metric	Interface	Type
192.168.1.0	*	255.255.255.0	U	0	Wireless	D
192.168.0.0	*	255.255.255.0	U	0	Ethernet	D
224.0.0.0	*	240.0.0.0	U	0	Ethernet	D

Add Static Route

Network IP Address	<input type="text" value="192 . 168 . 1 . 0"/>	Gateway	<input type="text" value="192 . 168 . 1 . 208"/>
Mask	<input type="text" value="255 . 255 . 255 . 0"/>	Interface	<input type="text" value="Select"/>
Metric	<input type="text" value="1"/>		<input type="button" value="Apply Changes"/>

Wireless
 Ethernet

Flags : **U** - route is up
G - use gateway
A - installed by addrconf
! - reject route

Type : **D** - Dynamic Route
S - Static Route

H - target is a host
R - reinstate route for dynamic routing
C - cache entry

Figure 2-23 Routing Table

Follow the steps below to add a static route entry in the aCNPT Router device.

1. Click on 'Networking' | 'Routing Table' from the menu bar to access the view routing table page.
2. Enter the Network IP, Mask, Gateway, Interface and Metric entry for the new route.
3. Click on 'Apply Changes' to add the new static route.

Follow the steps below to delete a static route entry in the aCNPT Router device.

1. Click on 'Networking' | 'Routing Table' from the menu bar to access the view routing table page.
2. Click on 'Del' on the right hand side of the route entry to be deleted.
3. Click on 'Apply Changes' to delete the route.

Note: Only static route can be deleted.

Networking : Routing Table

airClient TOTAL (sB3412) - [Router mode](#)

Routing Table						
Destination	Gateway	Mask	Flags	Metric	Interface	Type
192.168.1.0	*	255.255.255.0	U	0	Wireless	D
192.168.0.0	*	255.255.255.0	U	0	Ethernet	D
224.0.0.0	*	240.0.0.0	U	0	Ethernet	D

Please wait while your request is in progress

[Refresh](#)

Add Static Route			
Network IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/>	Gateway	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="210"/>
Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>	Interface	Wireless <input type="button" value="v"/>
Metric	<input type="text" value="1"/>	<input type="button" value="Apply Changes"/>	

Flags : **U** - route is up
G - use gateway
A - installed by addrconf
! - reject route

H - target is a host
R - reinstate route for dynamic routing
C - cache entry

Type : **D** - Dynamic Route

S - Static Route

Figure 2-24 Adding Static Route

2.8.6. Wireless Settings Management

The Radio Configuration Main page can be accessed from the **Radio** menu. The contents will be slightly different for each mode, Bridge, Router or NAT.

Radio Configuration : airClient Bridge - Main

airClient TOTAL (sB3412) - [Bridge mode](#)

Wireless Settings			
SSID	NEXUS_MASTER Associated		
MAC Address	00:30:1A:1F:4E:75		
Domain	FCC		
Radio Operating Mode	Mixed (802.11 a/b/g)		
Antenna Selection	Internal		
Channel	11 - (2462 MHz)		
Rates	1 Mbps 6 Mbps 24 Mbps	2 Mbps 9 Mbps 36 Mbps	5.5 Mbps 12 Mbps 48 Mbps 11 Mbps 18 Mbps 54 Mbps
Auto rate Fallback	Enabled		
Dial a Power	18 dBm	Antenna Gain (dBm):23	RF Cable Loss(dBm) :3
Status			

Figure 2-25 aCNPT Wireless Settings Page in Bridge Mode

2.8.7. Wireless Settings

The following table summarizes the information for the wireless settings.

Table 2-4 Wireless Settings

Page Items	Descriptions
SSID	This is the current SSID. User can change the SSID. The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. It is case sensitive and can contain up to 32 alphanumeric characters. Do not include special characters in the SSID.
Mac Address	When in aCNPT Bridge mode, this is the Radio MAC address of the Root Device
Domain	This is the current radio regulatory domain. User can choose the appropriate domain. The pull-down menu shows a list of domains supported by radio. Different domains will show different channel lists.
Radio Operating mode	sB Enhanced Mode gives better performance with the compression ON. For this reason, it does not support 802.11b and third party access point. Or The Radio Operating Mode can set to Mixed Mode i.e 802.11 a/b/g Or The Radio Operating Mode can be set to 802.11 b only or 802.11 g only
Channel	This is the current radio channel in the selected domain. This is settable when in aCNPT Bridge mode, user need to enter the same channel as the Access Point device from the pull-down list. The radio channel settings correspond to the frequencies available in the user regulatory domain.
Rates	This indicates the current rate at which the radio is operating, which can be set as desired by the user.
Auto Rate Fallback	Allows radio to fall back to lower data rate.
Dial-a-Power	Dial-a-Power is used to set the output power of the radio at the N Connector. The valid radio power range is from -5 dBm to 23 dBm
Antenna Gain	This is a gain of an antenna attached with the device. The gain input here is merely for the purpose of display and calculation of the EIRP. User can select anywhere between 2.2dBi to 30 dBi.
RF cable Loss	This refers to the loss of a RF cable connecting antenna to the device.
Status	Display associated link status.

2.8.8. Security

The different types of Security that can be configured on a Remote Router/NAT are as follows:

1. WEP Only
2. WPA –RADIUS
3. WPA –PSK
4. WPA2-RADIUS
5. WPA2-PSK

Note: Default Security is **None**.

WEP:

Wireless Equivalent Privacy (WEP) encryption is used for security between the aCNPT and the airPoint or any other access point. To enable/disable WEP or change the relevant settings, you need to access the security setting page on the web interface. The following table describes the information for the Security.

Table 2-5 Security Settings

Page Items	Descriptions
Authentication	Select authentication method between open system and shared key <u>Open system:</u> Open System is null authentication. With WEP enabled and valid WEP key on both ends, it provides data encryption. Clients without correct WEP key still can associate but can not send packet through. <u>Shared key:</u> Strict authentication for both authentication and data encryption. Clients must provide valid WEP key to associate
WEP	Enable /Disable WEP Encryption
WEP Key Type	HEX
WEP Key Size	Choose encryption key size between 64bits and 128bits <u>64 bits:</u> User has to input 10 HEX digits. <u>128 bits:</u> User has to input 26 HEX digits. Note: When key size is changed, all 4 keys are lost and user needs to re-enter.
Valid Key	Choose which key in key table is used for authentication: 1 – 4 This value must be matching between the aCNPT and access point.
Key Table	Display / Set WEP keys A maximum of four keys can be set.

Follow the steps below to configure the Data Encryption parameters.

1. Click the 'Security' link from the 'Radio Main' page.
2. Select the '**WEP Only**' from the drop down menu of Security mode.
3. Choose the Authentication as 'Open System' or 'Shared Key' by clicking on the radio button.

4. Choose a WEP Key Size (64 Bits or 128 Bits) from the pull-down list. WEP key length is 10 characters for 64 Bits and 26 characters for 128 Bits.
5. Choose a Valid Key from the pull-down list.
6. Enter the WEP key in the Key Table entries.
7. Click the 'Apply Changes' button to change the settings.

Note: The system will validate the key entries and provide error or warning notifications. The user must enter the key indicated by the Valid Key selection.

Radio : Security			
Security Mode		WEP Only <input type="button" value="v"/>	
WEP			
Authentication		<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key	
Wep Key Type		HEX	Wep Key Size: 64 Bits <input type="button" value="v"/>
Valid Key		First Key <input type="button" value="v"/>	
Key Table			
First Key		abcde12356	Second Key: ab23568adf
Third Key		abcd123dfa	Fourth Key: abcdf1235a
<input type="button" value="Apply Changes"/>			

Figure 2-26 WEP ONLY Configuration

WPA-PSK:

In order to configure WPA-PSK follow the steps as below:

1. Click the 'Security' link from the 'Radio Main' page.
2. Select the WPA-PSK from the drop down menu of the Security Mode.
3. Enter the WPA-Shared Key (ASCII) in the dialog box provided.
4. Select the Encryption Type between TKIP and AES.
5. Click on the Apply changes to save the configuration details.

Radio Configuration : - Security

airClient TOTAL (sB3412) - Router mode

Radio : Security	
Security Mode	WPA-PSK
WPA Shared Key Type	ASCII
WPA Shared Key	12345ABCDEF1235678ABABCDEF
Encryption Type :	TKIP TKIP AES

Figure: 2-27 Configuring WPA-PSK

Table 2-6 WPA Descriptions

Page Items	Descriptions
WPA-PSK	WPA-PSK is an extra-strong encryption where encryption keys are automatically changed (called rekeying) and authenticated between devices after a specified period of time, or after a specified number of packets has been transmitted. WPA-PSK is far superior to WEP and provides stronger protection for the home/SOHO user for two reasons. The process used to generate the encryption key is very rigorous and the rekeying (or key changing) is done very quickly. This stops even the most determined hacker from gathering enough data to break the encryption.
WPA-Shared Key	This is used by the clients to become authenticated with the Root Bridge/Remote Router/Remote NAT.

WPA-RADIUS:

WPA provides encryption via the Temporary Key Integrity Protocol (TKIP) using the RC4 algorithm. It is based on the 802.1X protocol and addresses the weaknesses of WEP by providing enhancements such as Per-Packet key construction and distribution, a message integrity code feature and a stronger IV (Initialization Vector).The length of a WPA key is between 8 and 63 characters.

Radio : Security	
Security Mode	WPA - RADIUS
Userid	smartBridges
Password	airclient
Validate certifiante	<input checked="" type="checkbox"/> <input type="text"/> Browse...

Apply Changes

Figure 2-28: WPA-RADIUS

Follow the steps below to configure the WPA-RADIUS:

1. Click the 'Security' link from the 'Radio Main' page.
2. Select the WPA-RADIUS from the drop down menu of the Security Mode.

3. Enter the User id and the Password in the dialog box provided
4. In order to validate the certificates, click on the validate certificate radio button (). A dialog box appears with a browser button, which you can use to browse for the certificates on your local machine.
5. Select the certificate by clicking the button.

WPA2-PSK:

Based on the 802.11i standard, WPA2 was released in 2004 and uses a stronger method of encryption – Like WPA, WPA2 offers two versions – Personal and Enterprise. Personal mode requires only an access point and uses a pre-shared key for authentication. Enterprise mode requires a RADIUS authentication server and uses EAP.

Note: Currently WPA2-PSK is using the TKIP as the encryption type.

Follow the steps below to configure the WPA2-PSK:

1. Click the 'Security' link from the 'Radio Main' page.
2. Select the WPA2-PSK from the drop down menu of the Security Mode.
3. Enter the WPA-Shared Key(ASCII) in the dialog box provided.
4. Select the Encryption Type between TKIP and AES.
5. Click on the Apply changes to save the configuration details.

Radio : Security	
Security Mode	WPA 2 - PSK <input type="button" value="v"/>
WPA Shared Key Type	ASCII
WPA Shared Key	12345ABCDEF1235678ABABCDEF
Encryption Type :	TKIP <input type="button" value="v"/>
<input type="button" value="Apply Changes"/>	

Figure 2-29: WPA2-PSK

WPA2-RADIUS:

The enterprise version of WPA2 is WPA2-RADIUS which uses an external RADIUS server for authentication which uses EAP (Extended Authentication Protocol).

When a user first attempts to connect to the network they are asked to enter their username and password. These are checked with the RADIUS server and access is granted accordingly. Every user has a unique key that is changed regularly to allow for better security. Hackers can crack the codes but it takes time. And with a new code being generated automatically every few minutes, when the hacker cracks the code it would have expired. 802.1X is essentially a simplified standard for passing EAP (Extensible Authentication Protocol) over a wireless (or wired) network.

Below is an image showing the 802.1X process.

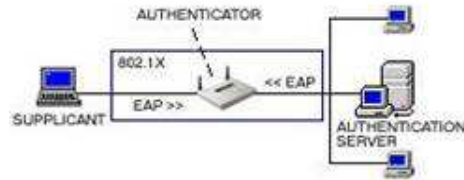


Figure 2-30 Authentications between the supplicant and the Authentication server

The wireless client (laptop) is known as the Supplicant. The access point is known as the Authenticator and the RADIUS server is known as the Authentication server.

Follow the steps below for Configuring the WPA2-RADIUS:

1. Click the '**Security**' link from the 'Radio Main' page.
2. Select the **WPA2-RADIUS** from the drop down menu of the Security Mode.
3. Enter the User id and the Password in the dialog box provided.
4. In order to validate the certificates, click on the validate certificate radio button (). A dialog appears with a browse button, which you can use to browse for the certificates on your local machine.

Radio : Security	
Security Mode	WPA 2 - RADIUS <input type="button" value="v"/>
Userid	<input type="text" value="smartBridges"/>
Password	<input type="text" value="airClient"/>
Validate certificate	<input checked="" type="checkbox"/> <input type="text"/> <input type="button" value="Browse..."/>

Figure 2-31: WPA2-RADIUS

3. Performance Parameters and Bandwidth Controller

This chapter gives instructions for editing the wireless radio protocol parameters to optimize radio performance and changing the Bandwidth Controller. These procedures are the same for all the three modes.

3.1. Link Performance Parameters and Features

The radio protocol parameters are:

- 1) Fragment Length (between 256 and 2346)
- 2) RTS/CTS (between 256 and 2346)
- 3) RSSI Threshold (between -90 and -20)
- 4) Throughput Optimizer
- 5) Frame Bursting
- 6) Piggy Back

Table 3-1 Radio Performance Parameters

Page Item	Descriptions
Fragment Length	a) Show current value b) Change to a value within its range This setting determines the size at which packets are fragmented. If the frame that the access point is transmitting is larger than the threshold, it will trigger the fragmentation function. The use of fragmentation can increase the reliability of frame transmissions. Because smaller frames are being sent, collisions are much less likely to occur. The range of its value is from 256 to 2346. The default value is 2346 bytes.
RTS/CTS Length	a) Shows current value b) Change value RTS: <u>R</u> equest <u>T</u> o <u>S</u> end CTS: <u>C</u> lear <u>T</u> o <u>S</u> end The RTS/CTS length determines the packet size at or larger than the set value. The radio issues a request to send (RTS) before sending the packet. The primary reason for implementing RTS/CTS is to minimize collisions among the hidden stations. The range of its value is from 256 to 2346. The default value is 2346 bytes.
RSSI Threshold	This function provides better performance in higher noise area. The device will ignore any signal below the set RSSI threshold. The default value is -90. The range of its value if from -90 to -20.

Throughput Optimizer	<p>The Throughput Optimizer is used to optimize the radio Link speed and performance.</p> <p>The Valid range is 0 to 10. The default value is 6.</p> <p>Setting a higher value will cause the radio to attempt to establish at the highest possible data rate in an aggressive way. A smaller "Throughput Optimizer" value means a more stable link.</p> <p>Note: The default value for the Throughput Optimizer is 6. Vary the Throughput Optimizer settings to achieve a more stable link.</p>
Frame Bursting	<p>Short 802.11g packets can be unwrapped and rebundled into a larger packet to reduce the impact of mandatory gaps between the packets. This increases the speed of 802.11g based wireless networks. Frame bursting is sometimes also called "packet bursting."</p>
Piggy Back	<p>Piggy back is a performance-boosting feature which increases the effective transmission speed with no intervention.</p> <p>According to the IEEE 802.11 standard specification, a single frame combining a plurality of information can be transmitted. For example, the frame may carry data+acknowledgement (ACK), data+poll, data+ACK+poll, or ACK+poll for transmission.</p> <p>Using the Piggy Back increases the communication efficiency depending on the transfer medium or size of data being transferred.</p>

Follow the steps below to change the performance parameters:

1. From the 'Radio Configuration' page click on the 'Performance' link.
2. Enter the 'Fragment Length', 'RTS/CTS Length' and RSSI Threshold in the appropriate boxes.
3. Select throughput from 'Throughput Optimizer'.
4. Click on the 'Apply Changes' button to effect the changes.

Performance	
Fragment Length (256 - 2346)	RTS / CTS Length (256 - 2346)
<input type="text" value="2346"/>	<input type="text" value="2346"/>
RSSI Threshold	<input type="text" value="-90"/>
Distance	<input type="text" value="91"/> Km
Frame bursting	Concatenation
<input type="button" value="On"/> ▼	<input type="button" value="Off"/> ▼
Piggy back	<input type="button" value="Off"/> ▼
Throughput Optimizer (0 - 10)	<input type="radio"/> 0 <input type="radio"/> 2 <input type="radio"/> 4 <input checked="" type="radio"/> 6 <input type="radio"/> 8 <input type="radio"/> 10
<input type="button" value="Apply Changes"/>	

Figure 3-1 aCNPT Bridge Performance Settings

3.2. Bandwidth Controller

Using the Bandwidth Controller on the aCNPT, the user can limit the wireless link bandwidth for the upload/download speed. The default is disabled and provides bandwidth up to 6Mbps. This is subject to the available upstream bandwidth, signal level and distance.

The user can key in the upload and download bandwidth for the wireless link.

Follow the steps below to change the bandwidth parameters:

1. From the menu bar click on '**Networking | Bandwidth Controller**' drop down menu item.
2. Click on the Bandwidth Controller '**Enable**' radio button.
3. Enter the desired value for upload and download.
4. Click on the "**Go to Advanced Settings**" to provide Bandwidth Control based on IP or MAC and click "**Add to list**" to save the defined settings.
5. In order to remove or delete the defined settings, Click on "**Delete Selected Rules**".
6. Click on the '**Apply Changes**' button to effect the changes.

Bandwidth Controller : airClient TOTAL (sB3412) - [Router mode](#)

Bandwidth Controller

Bandwidth Controller : Enable Disable Maximum Bandwidth available 6144 Kbps

Upload : Kbps Download : Kbps [Goto Advanced Settings](#)

Figure 3-2 aCNPT Bandwidth Controller

Bandwidth Controller

Bandwidth Controller : Enable Disable Maximum Bandwidth available 6144 Kbps

Upload : Kbps Download : Kbps [Goto Normal Settings](#)

IP / MAC : IP Address : . . .

Added Rules List

RULE - IP/192.168.0.205, Upload : 512, Download : 5632
--

[Delete Selected Rules](#)

Figure 3-3 Added list

4. Quality of Service (QoS)

The primary goal of QoS is to provide priority for certain applications by dedicating bandwidth, controlling jitter and latency (which are required by some real-time and interactive traffic), and improving loss characteristics. However, it is important to ensure that providing priority for one or more flows would not cause the other flows to fail.

QoS in 802.11 is defined by the IEEE 802.11e set of standards. Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification based on this IEEE 802.11e. WMM prioritizes traffic according to four AC (Access Categories) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

Though QoS is disabled by default, it can be enabled by clicking on “**QoS**” and selecting the “**Enable QoS**” option. A confirmation window appears as shown in Figure 4-1. Click **OK** to confirm and wait for the settings to be applied. After QoS is enabled, the page looks as shown in Figure 4-2.



Figure 4-1: Drop Down Menu for QoS.

QoS : Enabled

airClient TOTAL (sB3412) - Router mode

QoS Classes					
Sr.no	Min Bandwidth (Kbps)	Max Bandwidth (Kbps)	Priority	Enable	
1)	10	30720			
2)	10	30720	0	Enabled	Filters
3)	10	30720	0	Enabled	Filters
4)	10	30720	0	Enabled	Filters
5)	10	30720	0	Enabled	Filters
6)	10	30720	0	Enabled	Filters
7)	10	30720	0	Enabled	Filters
8)	10	30720	0	Enabled	Filters
9)	10	30720	0	Enabled	Filters

Note : class 1 indicates default value

Priority '0' indicates "Best Effort"

Figure 4-2: QoS front page

In total, there are 9 different classes which can be configured.

Note: Class 1 indicates the default value.

In order to define the filters for a class, follow the steps below:

1. Click on "**Filters**".
2. Select the application packet that has to be filtered.

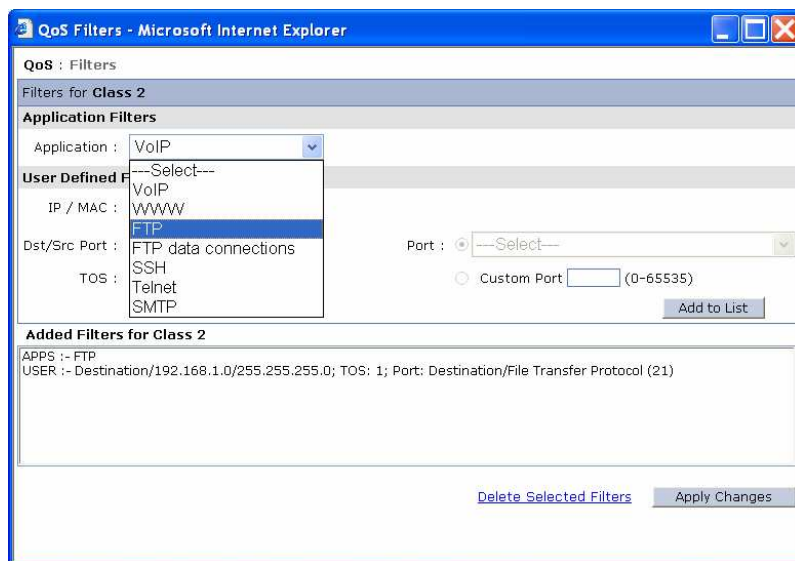


Figure 4-3: Selection Menu of Application Filter.

3. Select whether the packet has to be filtered based on the IP or MAC.

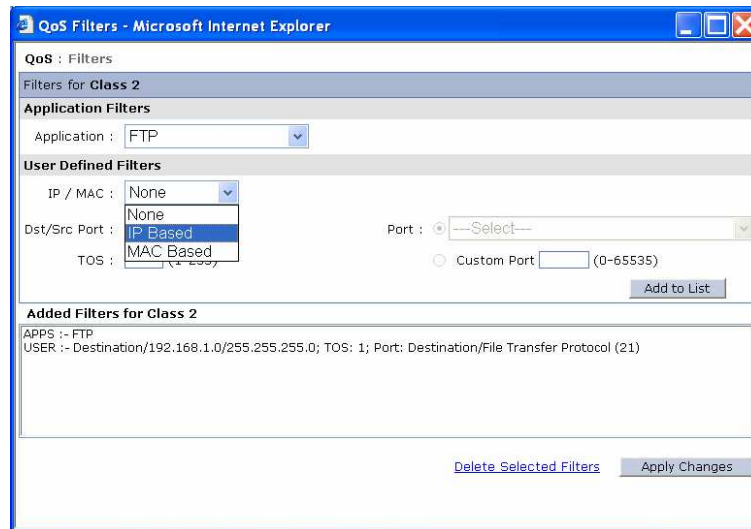


Figure 4-4: Selection Menu of IP/MAC based filter

4. Select whether the packet has to be filtered based on source address or the destination address. If the packet being filtered is based on IP, then enter the IP address. If it is based on MAC, then enter the MAC address.

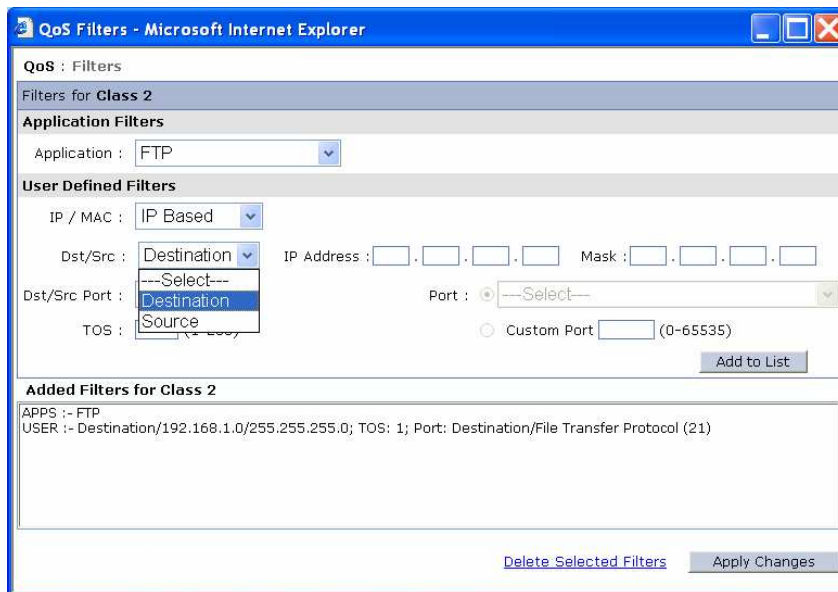


Figure 4-5: Selection Menu of Source/Destination based filter

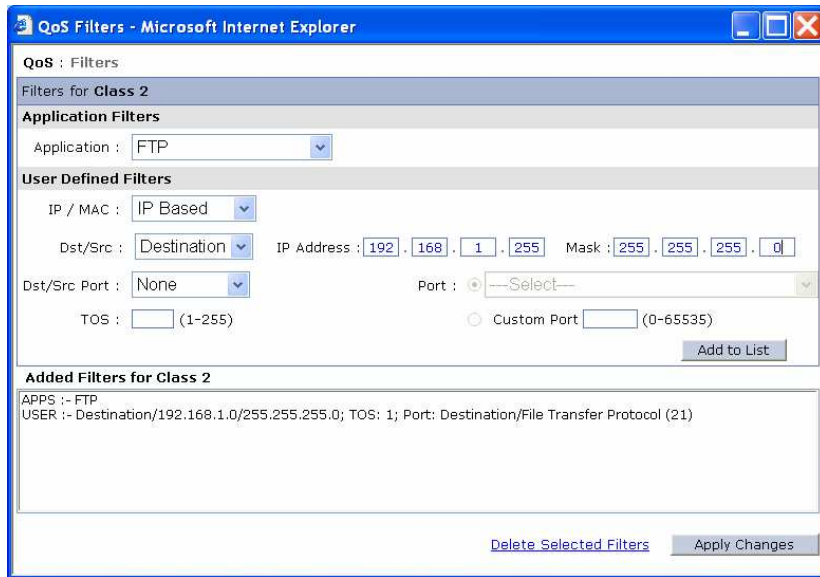


Figure 4-6: IP address dialog box.

5. Select the Port, either Destination or Source based and select the Port Number from the drop down menu. You can also select a customized the Port number.

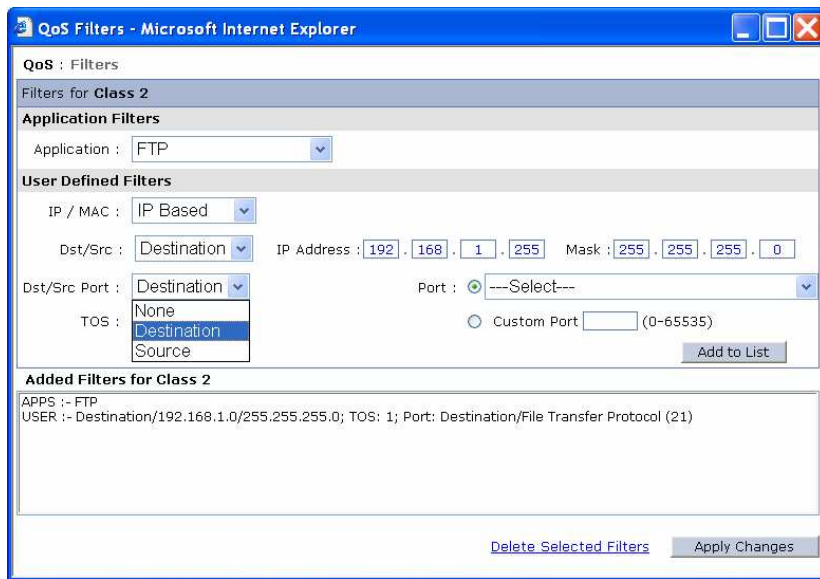


Figure 4-7: Selection of Destination /Source port

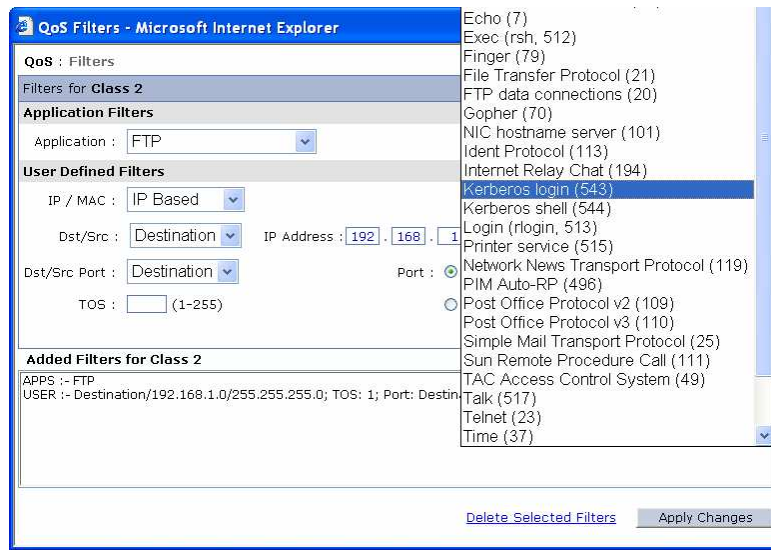


Figure 4-8: Selection menu of type of port (It can be customized by the user with the port number).

6. Assign a TOS value between 1 and 255.

Every IP packet sent over the network includes a TOS field in the header that indicates how the data should be prioritized and transmitted over the network.

The access point examines the TOS field in the headers of all packets that pass through the AP. Based on the value in a packet's TOS field, the AP prioritizes the packet for transmission by assigning it to one of the queues.

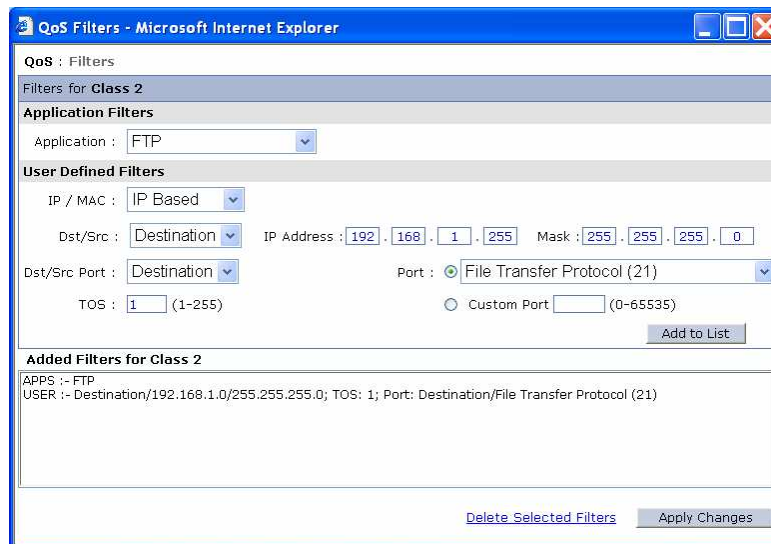


Figure 4-9: TOS value Dialog box.

7. After configuring the User defined filter, click on “Add to List” to add the selected filter.

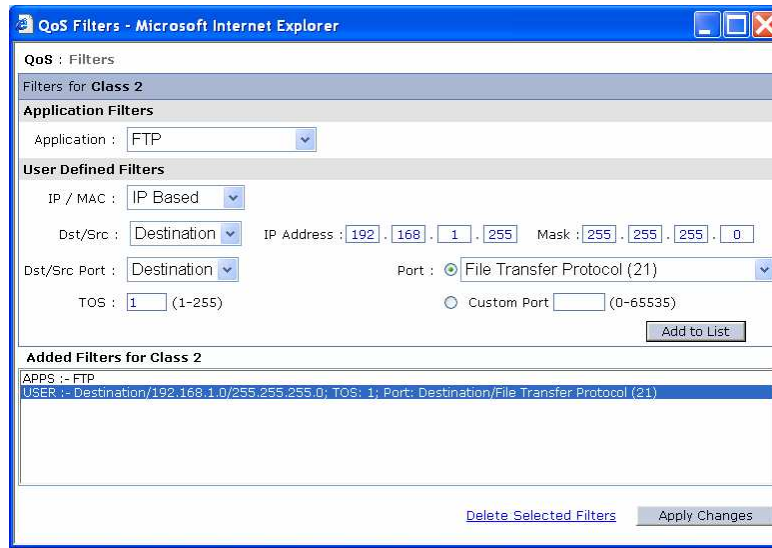


Figure 4-10: Selected filter list window

8. After adding the desired filters to the list, click on the **Apply Changes** to save the configuration of the filters. There will be a confirmation pop up window. Click **OK** to confirm or **Cancel** to discard the selection. Click on **Apply Changes** to save the selected list of filters.

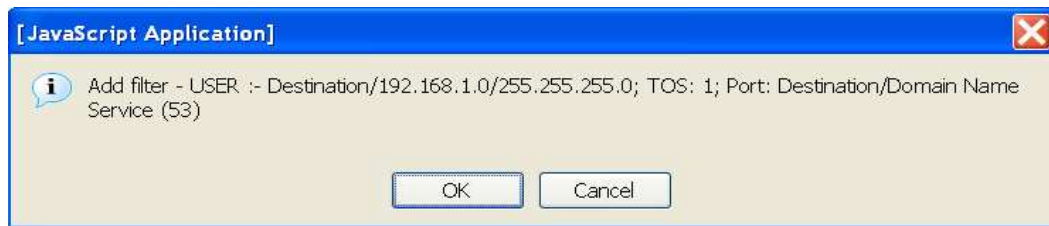


Figure 4-11: Add filter Confirmation POP UP WINDOW

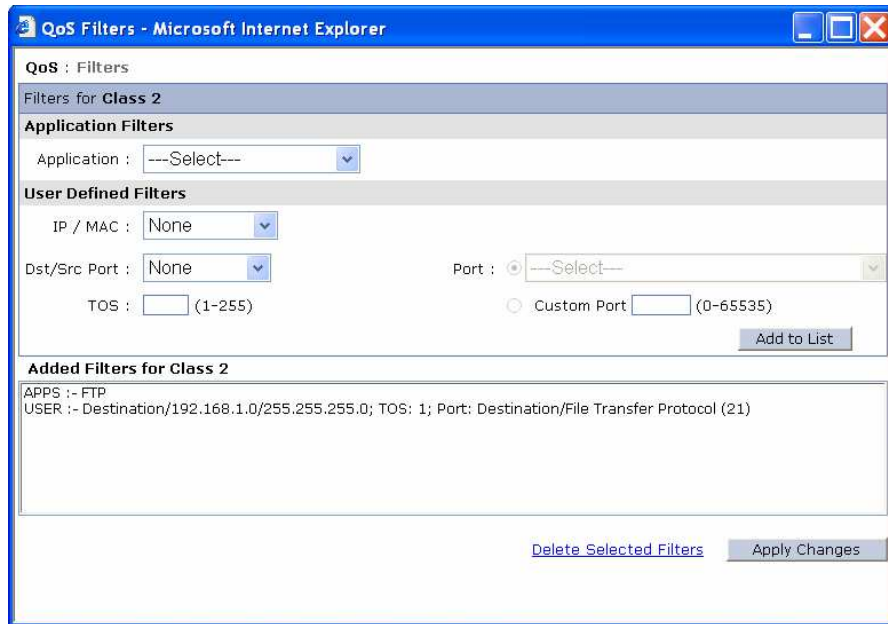


Figure 4-12: Added filters

9. The filters added can be deleted by first selecting the added filters from the list and then clicking on **Delete Selected filters** .

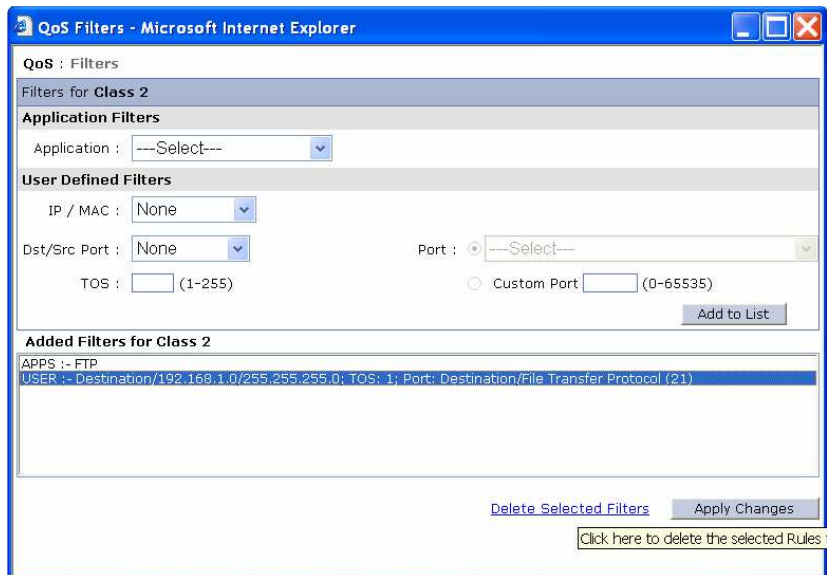


Figure 4-13: Delete Selected Filters.

10. In order to configure with the desired minimum and maximum bandwidth, priority across classes or disable certain classes, go to the QoS main page, click on the **QoS**. The page appears as shown in Figure 4-14.
11. Use the scroll bar to select the desired priority for a particular class.

12. In order to enable a particular class, click on the radio button. Tick mark indicates that the particular class is enabled. In order to disable, click on the radio button and the tick mark disappears, indicating that the class is disabled.

13. Click on the “**Apply changes**” to save the configuration

- Note:**
- 0 -> No Priority
 - 1 -> Highest Priority (Voice)
 - 2 -> High Priority (Video)
 - 3 -> Medium Priority (IP Traffic)
 - 4 -> Lowest Priority (File Transfer)

QoS :

airClient TOTAL (sB3412) - [Router mode](#)

QoS Classes					
Sr.no	Min Bandwidth (Kbps)	Max Bandwidth (Kbps)	Priority	Enable	
1)	<input type="text" value="10"/>	<input type="text" value="30720"/>			
2)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters
3)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters
4)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters
5)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters
6)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters
7)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters
8)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters
9)	<input type="text" value="10"/>	<input type="text" value="30720"/>	<input type="button" value="0"/> <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Filters

Note : class 1 indicates default value

Priority '0' indicates "Best Effort"

Figure 4-14: QoS Configuration Page

5. Site Survey Tool

To access the Site Survey page, go to the 'Tools' | 'Site Survey' drop down menu. The following figure shows the list of SSID from the site survey.

BSS List						
rows indicate airPoint devices						
Sr.no	MAC Address	Channel/Freq	RSSI(dBm)	SSID		
1	00:30:1A:0C:4C:75	6 - (2437 MHz)	-72	Res_AP		
2	00:30:1A:0C:4C:76	6 - (2437 MHz)	-73	VoIP_AP		
3	00:30:1A:07:A1:19	8 - (2447 MHz)	-81	RoofTop		
4	00:30:1A:09:4E:E6	6 - (2437 MHz)	-74	airPoint-PROOutdoor		
5	00:02:8A:42:2D:2B	9 - (2452 MHz)	-80	Cisco1100		
						Associate
Current Configuration						
SSID		airPoint-PROOutdoor				
						Refresh
<small>(Data will refresh automatically after every 30 seconds)</small>						

Figure 5-1 Site Survey showing associated devices

To associate to a particular SSID, click the 'Associate' button or double click the desired SSID to establish the wireless link to the access point. If WEP or any security option is used on the access point, then WEP needs to be enabled and the WEP key defined prior to association.

6. Antenna Alignment

Antenna alignment can be used to optimize the radio performance and check the RSSI. To access the antenna alignment, go to the menu bar under **Tools** and choose '**Antenna Alignment**'. In order to view this information (Link Status), from the Radio page, use the Wireless Settings to associate the aCNPT with an access point.

Click on the '**Status**' link to go to the Antenna Alignment page. The Link Status page will be displayed as below.

RSSI Audio Tones are provided to help the user to align the antenna without looking at the link status display. Click on the '**Antenna Alignment Tone**' to ON button to hear the alignment tones. You will need to insert the earphones provided into the earphone jack in the unit. For more information on antenna alignment, please refer to the Quick Installation Guide.

To perform the antenna alignment:

1. Go to the menu bar and choose '**Radio**' menu item.
2. From the Radio page, use the Wireless Settings to associate the aCNPT with a root device or access point.
3. Click on the '**Status**' link to go to the Antenna Alignment page. The Link Status page will be displayed as below.
4. A set of tones are provided to help the user align the antenna without looking at the link status display. Click on the '**Antenna Alignment Tone**' to ON button to hear the alignment tones.

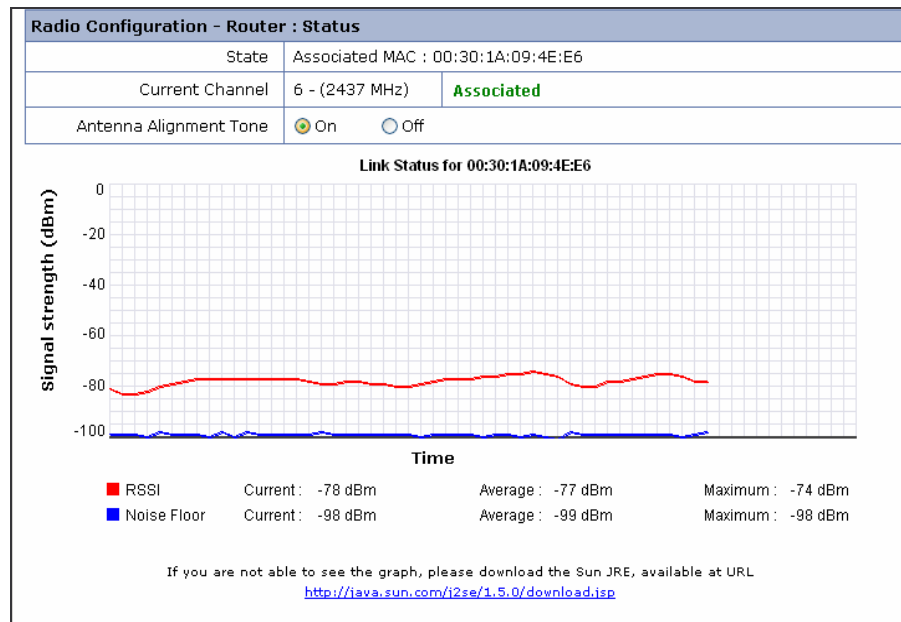


Figure 6-1 Antenna Alignment

Note: A jump in the audio frequency from low to high indicates that the RSSI is increasing and vice versa.

7. Traffic Statistics

Wireless and Ethernet Traffic Statistics can be displayed by clicking on the 'Networking' | 'Statistics' drop down menu. The following figure shows the statistics page. This page is refreshed after every 10 seconds.

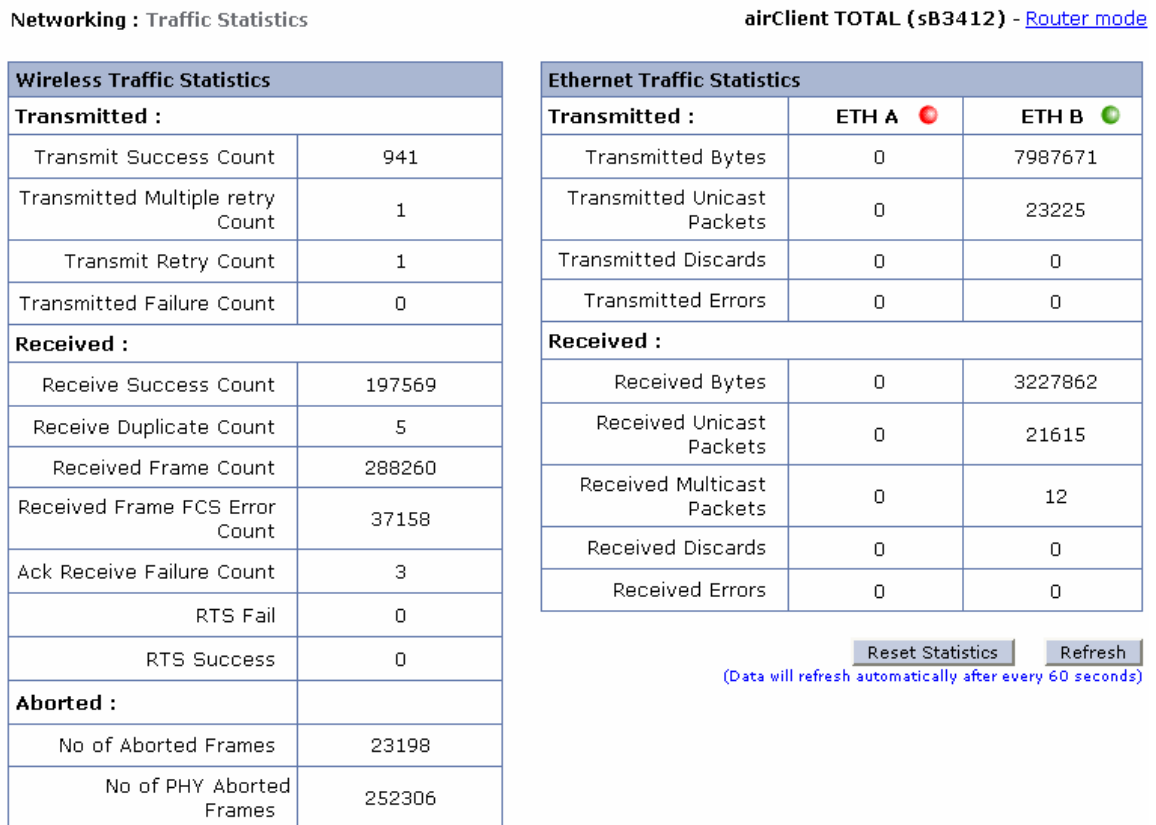


Figure 7-1 Traffic Statistics

Table 7-1 Ethernet Traffic Statistics

Ethernet Traffic Statistics	
Transmitted Bytes	Total number of packets transmitted from the particular interface
Transmitted Unicast packets	Total number of successfully transmitted unicast packets to a specified destination
Transmitted Discards	The number of unicast and multicast packets dropped before a transmission attempt was made because of congestion or an error along the path. In most cases, packet loss is due to network congestion. Packets are discarded to avoid the very large delays that can arise when too much traffic is queued up.

Transmitted error	The number of unicast and multicast packets that could not be or were not successfully transmitted by the device.
Received Bytes	Total number of packets received through the particular interface
Received Unicast packets	Total number of packets received successfully with a specified destination.
Received Multicast Packets	Total number of packets received successfully belonging to a multicast destination address or group.
Received Discards	Total number of dropped unicast and multicast packets due to resource limitation.
Received Errors	Total number of partially or erroneously received unicast and multicast packets because of format error.

The wireless statistics is also available from the 'Radio Configuration' Main Page.

Wireless Traffic Statistics			
Transmitted :		Received :	
Transmit Success Rate	2528	Receive Success Rate	26
Transmitted Multiple retry Count	0	Receive Duplicate Rate	0
Transmit Retry Rate	0	Received Frame Count	27
Transmitted Failure Count	0	Received Frame FCS Error Count	6
Aborted :		Ack Receive Failure Count	0
No of Aborted Frames	1	RTS Fail	0
No of PHY Aborted Frames	2	RTS Success	0
<input type="button" value="Refresh"/>			
<small>(Data will refresh automatically after every 10 seconds)</small>			

Figure 7-2 Wireless Statistics from Radio Main Page

Table 7-2 Wireless Traffic Statistics

Wireless Traffic Statistics	
Transmit Success Rate	Total number of successfully transmitted unicast and multicast MPDU's.
Transmit Multiple Retry count	Total number of unicast MPDU's successfully transmitted after two or more retries.
Transmit One Retry count	Total number of unicast MPDU's successfully transmitted after one retry.
Transmitted Failure count	Total number of unicast MPDU's for which the maximum number of retries exceeded and so were dropped.
Received Success count	Total number of successfully received unicast MPDU's
Received Duplicate Count	Total number of successfully received unicast MPDU's that were a duplicate of earlier frames.
Received Frame FCS Error Count	Total number of unsuccessfully received frames in which checksum error was detected.
ACK Receives Failure Count	Total of frame transmissions for which an acknowledgement response frame was expected but not received.

RTS Fail	Total number of transmitted RTS frames for which no response CTS frame was received.
RTS Success	Total number of CTS frames received in response to the RTS frames.
No of Aborted Frames	Total number of frames that are aborted by the radio. An aborted frame occurs when it experiences a brief or permanent internal error that interrupts the transmission of the frame.
No of PHY Aborted Frames	No of PHY aborted frames when lmac drops frames. This can happen only when PLCP checksum failure occurs.

Note: The wireless statistics is also accessible from the 'Radio Configuration' bottom page.

8. Tools

Here you will find the relevant information for conducting the different reset options, using the Profile Manager and doing a Link Test as well as estimating the Link Budget.

8.1 System Configuration

The System Configuration page provides a one page tool to configure the aCNPT device. To access the System Configuration page go to 'Tools' | 'System Configuration' drop down menu. The following figure displays the System Configuration page.

Home	Networking	Radio	Tools	Help	Logout
System Configuration :			airClient TOTAL (sB3412) - NAT mode		
System Configuration					
System Name	Nexus				
System Description	Nexus				
SNMP Security	SNMP Security				
Reset	Reset				
Delayed Reset	Delayed Reset				
NTP Server	NTP Server Settings Time Server Not available				
Firmware Version	v0.00.04 Release Notes				
Radio Firmware Version	1.1.2.16				
Edit Configuration	IP Configuration Radio : Performance				
Reset To Factory Defaults	Reset To Defaults				
Ethernet MTU Size	1512 bytes				
Syslog server IP Address	0.0.0.0				Log level : -
SNMP Trap server IP Address	0.0.0.0				
Watch Guard	Enabled				Suspend
LED Control	On				
Current Operational Mode					
<input type="radio"/> Bridge <input type="radio"/> Router <input checked="" type="radio"/> NAT					

Figure 8-1 System Configuration

The following page summarizes the page contents of the System Configuration page.

Table 8-1 System Configuration Page Items

Page Item	Descriptions.
System Name	Displays name of aCNPT unit Allows user to change aCNPT unit name
System Description	Displays description of aCNPT unit Allows user to change aCNPT unit description
SNMP Security	Access the SNMP security settings
Reset	Reset device
Reset To Factory Defaults	Reset device to factory defaults
Delayed Reset	Schedule a reset
NTP Server	NTP server setup, as well as NTP time if server is setup
Software Version	Display the installed firmware version
Radio Firmware Version	Display the installed radio firmware version
Edit Configuration	Provide links to edit IP, radio, configurations
Ethernet MTU Size	Set the Ethernet MTU Size
Syslog server IP Address	Display the current message Syslog server IP Address. User can change the IP address.
SNMP Trap IP	Display the current SNMP trap IP address. User can change the IP address.
Log Level	Display the current Log Level
WatchGuard	Suspends/Enables the radio defenders. If the WatchGuard is suspended, the defenders will stop for 2 hours and start again thereafter. If the WatchGuard is enabled the radio defender's will start immediately. Note: The Radio Defenders will monitor the Wireless Association Status (automatically) and traffic and take corrective action if needed.
LED Control	Displays the current LED status. The user can change the LED status to on/off
Current Operational mode	Display the current operational mode. User can change the current operational mode.

8.1.1 SNMP Security

The user can edit the SNMP Community String and SNMP Access filters. The SNMP community needs to match with the SNMP monitoring software used. The SNMP Access Filters allows you to determine which host(s) is authorized to monitor the device using SNMP. It is recommended that you set this for security reason and to prevent an attack. To change the SNMP security settings, click on the SNMP security link in the System Configuration page. Figure 7-2 shows the SNMP Security Configuration page.

Follow the steps below to change the SNMP security settings.

1. Enter New Community and Confirm Community with the same string.
2. Check the 'SNMP Access Filters' Enable box.
3. Enter Access Filters IP Address and Mask. Up to three IP's settings can be entered.
4. Click the 'Apply Changes' button.

System Configuration : SNMP Security
airClient TOTAL (sB3412) - [Router mode](#)

SNMP Security

SNMP Community :

New Community : Confirm Community :

SNMP Access Filters Enable

1) IP : . . . Mask : . . .

2) IP : . . . Mask : . . .

3) IP : . . . Mask : . . .

Figure 8-2 SNMP Security Configuration

Table 8-2 Description of SNMP Page Items

Page Items	Descriptions
SNMP Community	Display SNMP Community String that is currently used to communicate to the device through SNMP
New Community	User can change the SNMP Community String by entering a new Community string
Confirm Community	User must enter the same community string as a new community string to confirm.
Access Filters	Display the Current Access Filter status User can change the Access Filter status.
IP	List of 3 IP filters. User can enter the IP address and mask.

8.1.2 Reset Options

All reset options power cycles the device and restarts the whole system.

Reset: To reset the device. The device will reboot with the current configuration/values.

Reset to Defaults: To reset the device to factory default configuration values.

Delayed Reset: To reset the device at a particular time and can be programmed to do so on a daily/weekly/monthly basis. The current time can be set by specifying a NTP server (there is one already specified by default) and the time zone. After enabling the delayed reset, specify a time which is valid in reference to current time. When recurrence is set to weekly, monthly or daily, the reference is made with the first set time i.e. Reset time.

Tools : Delayed Reset

airClient TOTAL (sB3412) - Router mode


Delayed Reset	
<input type="checkbox"/> Disable Delayed reset	
(dd-mm-yyyy)	Hour Minutes
Reset time : <input type="text" value="07-09-2005"/> 	<input type="text" value="2"/> : <input type="text" value="15"/>
Recurrence : <input type="radio"/> Daily <input type="radio"/> Weekly <input checked="" type="radio"/> Monthly <input type="radio"/> Only once	
<input type="button" value="Apply Changes"/>	
NTP Server Settings	
IP address of the NTP server	<input type="text" value="128"/> . <input type="text" value="250"/> . <input type="text" value="36"/> . <input type="text" value="2"/>
Time Zone	<input type="text" value="(GMT+08:00)Kuala Lumpur,Singapore"/>
Current Time	Time Server Not available
<input type="button" value="Apply Changes"/>	

Figure 8-3 Delayed Reset Settings

For delayed reset, follow the steps below:

1. Select date from the calendar that has been provided.
2. Select the recurrence.
3. Click 'Apply Changes' button to change the settings.
4. To disable 'Delayed Reset', check the box provided.

8.1.3 NTP Time Server Setup

The device time comes from the network time information source. The device needs access to a network timer (NTP time server) source. The NTP time server IP can be configured as follows:

1. From the 'System Configuration' page, click on the 'NTP Server Setting' link.
2. A 'Time Settings' page will be displayed. Click on the 'NTP Server Settings' link to enable timer settings input.
3. Enter a valid NTP server IP address and select the Time Zone. The default NTP server is 128.250.36.2 and the default Time Zone is Singapore.
4. Click on the 'Apply Changes' button to configure the NTP. The network time will appear on the browser if NTP server is contactable.

Note: Please ensure that the NTP server IP is accessible from the device. Use the ping test tool from the 'Tools | Link Test' to check if the NTP server can be pinged from the device. The device can still operate without the Time Server configuration but you will not be able to perform the Delayed Reset function.

Tools : Time Settings

airClient TOTAL (sB3412) - Router mode

NTP Server Settings	
IP address of the NTP server	<input type="text" value="128"/> . <input type="text" value="250"/> . <input type="text" value="36"/> . <input type="text" value="2"/>
Time Zone	<input type="text" value="(GMT+08:00)Kuala Lumpur,Singapore"/> ▼
Current Time	Time Server Not available
<input type="button" value="Apply Changes"/>	

Figure 8-4 NTP Time Settings

8.2 Profile Manager

The aCNPT Nexus configuration parameters can be saved as profiles in the system. There are four profiles available in the system:

1. Installation profile
2. Profile1
3. Profile1
4. Profile3

All the four profiles contain the same default parameters. You can save the current configurations to any of the four profiles and re-load the profiles later on or create different configurations and save them under different profiles. These can be loaded at different times based on a pre-defined calendar schedule.

The Profile Manager Configuration page can be accessed from the navigation menu bar 'Tools | Profile Manager' dropdown menu. The following figure displays the Profile Manager page.

8.2.1 Save Profile

Follow the steps below to save the current configuration to a profile:

-
1. Select a profile name from 'Save As'.
 2. Enter a description of the profile.
 3. Click the 'Save Profile' button to effect the changes.
-

Note: Existing configuration parameters in the selected profile name will be replaced with current configuration parameters.

8.2.2 Load Operating Profile

To load the desired operating profile, follow these steps:

-
1. Select a profile to load from the Profile Table.
 2. Click the Load button to load the selected profile.
-

Note: Current configuration parameters will be replaced by the new loaded profile. User will be asked to wait while the new profile loads.

8.2.3 Profile Calendar

The Profile Calendar allows the user to manage profiles based on different calendar times. With it the different profiles and scheduled activities can be configured based on the profiles set for a pre-defined time.

A typical situation is when an operator has two profiles for day and night. The two different profiles can be created and saved as Profile Day and Profile Night. The Profile Calendar can then be scheduled to activate each profile at the correct time.

Follow the steps below to schedule the activation of a saved profile:

-
1. Select a profile to schedule.
 2. Uncheck the 'Disable Profile Calendar' check box. A profile calendar will be displayed.
 3. Select the date and time from the load time calendar. Choose a start date with the calendar icon.
 4. Select the recurrence (daily, weekly, monthly, only once).
 5. Click the 'Apply Changes' button. The schedule will be loaded either daily, weekly monthly or only once at the specified start date and time.
 6. To disable the scheduled profile, check the box 'Disable Profile Calendar'.
-

The screenshot shows a web-based configuration window titled "Profile Calendar :". At the top, there is a "Select Profile" dropdown menu set to "Profile 1", followed by a link "Time Server Not available" and a checkbox "Disable Profile Calendar - Profile 1". Below this, the "Load time" is set to "14-03-2005" with a calendar icon. To the right, "Hour" is set to "10" and "Minutes" to "20". The "Recurrence" section has four radio buttons: "Daily", "Weekly", "Monthly", and "Only once", with "Only once" selected. An "Apply Changes" button is located at the bottom right of the form.

Figure 7-6 Scheduling a Profile

Link Test

The Link Test utility is available from the navigation menu bar in the 'Tools | Link Test' drop down menu. From the Link Test tools, the user can test Throughput and perform Ping Test. You can run Radio Transmit or Radio Receive. The remote device will automatically start receiving /transmitting (provided an airPoint Nexus is used).

The remote radio IP address has to be specified for the test.

Follow the steps below to do a Ping Test:

1. Enter a valid IP address for Far-end Radio IP Address.
2. Click on the 'Start' button under 'Ping'. The Ping result will be displayed.
3. Click on the 'Stop' button to stop the test.

Tools : Link Test

airClient TOTAL (sB3412) - [Router mode](#)

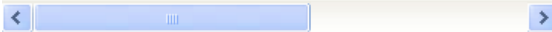
SSID : airPointS83210	Channel : 11 - (2462 MHz)
Association Status : Associated	RSSI (dBm): -14

Far-end Radio IP Address . . .

Ping Test	Throughput Test
<input type="button" value="Start"/> <input type="button" value="Stop"/>	<input type="button" value="Radio Transmit"/> <input type="button" value="Radio Receive"/> <input type="button" value="Stop"/>

Showing Ping Request

Packet 1: 64 bytes from 192.168.1.10: icmp_seq=0 ttl=64
 Packet 2: 64 bytes from 192.168.1.10: icmp_seq=0 ttl=64
 Packet 3: 64 bytes from 192.168.1.10: icmp_seq=0 ttl=64
 Packet 4: 64 bytes from 192.168.1.10: icmp_seq=0 ttl=64
 Packet 5: 64 bytes from 192.168.1.10: icmp_seq=0 ttl=64
 Packet 6: 64 bytes from 192.168.1.10: icmp_seq=0 ttl=64
 Packet 7: 64 bytes from 192.168.1.10: icmp_seq=0 ttl=64

**Figure 8-7 Ping Test Result**

When the aCNPT is associated with an airPoint Nexus, you can do a Throughput Test to test the speed of the link.

Follow the steps below to do a Throughput Test:

1. Enter a valid IP address of the far Radio.
2. Click on the 'Radio Receive' button on the near radio under the Throughput Test and the 'Radio Transmit' button at the far radio.
3. The Throughput test will start and the result will be displayed.
4. Click on the 'Stop' button if you want to stop the test.

Note: The Throughput Test can be done only between Nexus units.

Tools : Link Test

airClient TOTAL (sB3412) - Router mode

SSID : airPointSB3210	Channel : 11 - (2462 MHz)
Association Status : Associated	RSSI (dBm): -17

Far-end Radio IP Address . . .

Ping Test	Throughput Test
<input type="button" value="Start"/> <input type="button" value="Stop"/>	<input type="button" value="Radio Transmit"/> <input type="button" value="Radio Receive"/> <input type="button" value="Stop"/>

Throughput Test - Receive

Test 1 :Successfully downloading @6 Mbits/sec
 Test 2 :Successfully downloading @6 Mbits/sec
 Test 3 :Successfully downloading @6 Mbits/sec
 Test 4 :Successfully downloading @6 Mbits/sec
 Test 5 :Successfully downloading @6 Mbits/sec
 Test 6 :Successfully downloading @6 Mbits/sec

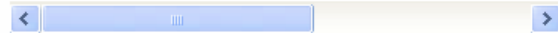


Figure 8-8 Throughput Test Result

8.4 Link Budget Planning

Link Budget Planning is a very useful tool for link budget estimation. The Link Budget Planning Calculator can be accessed from the navigation menu bar 'Tools | Link Budget Planning Calculator' drop down menu.

A GPS Calculator is provided in the Link Budget Planning Calculator page to calculate the distance between two aCNPT and the access point stations.

To calculate the distance, follow the steps below:

1. Enter the GPS co-ordinates of Station 1 (Latitude1 and Longitude1) and Station 2 (Latitude 2 and Longitude 2). GPS co-ordinates may be entered in DD: MM:MM or DD: MM: SS.SS formats.
2. Select the distance units (miles or kilometers).
3. Click the 'Compute Distance' button to calculate the distance between the two stations.
4. The distance will be displayed in the Distance text box.

GPS Calculator					
Latitude1	Longitude1	Latitude2	Longitude2		
<input type="text" value="00:03.00"/>	<input type="text" value="00:00.00"/>	<input type="text" value="00:00.05"/>	<input type="text" value="00:00.00"/>		
<input type="button" value="N"/>	<input type="button" value="W"/>	<input type="button" value="N"/>	<input type="button" value="W"/>		
					<input type="button" value="Compute Distance"/>
Course 1-2 (Degrees)	Course 2-1 (Degrees)	Distance			
<input type="text" value="180"/>	<input type="text" value="0"/>	<input type="text" value="3"/> miles			

Figure 8-9 Link Budget Planning Calculator GPS Calculator

Once the distance is computed follow the steps below for the link budget calculations:

1. Select the radio mode for station 1 and 2.
2. Enter the transmit output power in dBm for station 1 and 2.
3. Enter the antenna Gain in dB for station 1 and 2.
4. Enter the Cable Losses in dB for station 1 and 2.
5. Click the 'Compute Link Budget' button to calculate the link budget information.
6. The link budget information will be displayed in the following figure.

The link budget information includes the EIRP, Free Space Loss and Theoretical RSSI.

The Receive Sensitivity, Maximum Transmit Power, System Gain and Available Fade Margin at various Link Speeds are also computed and displayed in a table.

The Ideal fade margin for a link is between 10 dB to 20 dB for a stable link base on the environmental condition of a region.

Fresnel Zone Clearance Required will also be displayed.

Distance from Root Device to Remote Device is miles (Please Select)

Root Device	Remote Device
Device : <input type="text" value="airPoint Nexus"/> <input type="button" value="v"/>	Device : <input type="text" value="airClient Nexus"/> <input type="button" value="v"/>
Radio Mode : <input type="text" value="High Band"/> <input type="button" value="v"/>	Radio Mode : <input type="text" value="High Band"/> <input type="button" value="v"/>
Tx Output Power (dBm) : <input type="text" value="18 dBm"/> <input type="button" value="v"/> (-5 to 23)	Tx Output Power (dBm) : <input type="text" value="18 dBm"/> <input type="button" value="v"/> (-5 to 23)
Antenna Gain : <input type="text" value="18"/> <input type="button" value="v"/>	Antenna Gain : <input type="text" value="18"/> <input type="button" value="v"/>
RF Cable Loss : <input type="text" value="3"/>	RF Cable Loss : <input type="text" value="3"/>
<input type="button" value="Compute Link Budget"/>	
EIRP : 33	33
Free Space Loss : 120.4	120.4
Theoretical RSSI (dBm) : -72	-72 (Recommended minimum -75dBm)
Available Fade Margin (dBm) : 20	20
Fresnel Zone Clearance Required : 17 feet	
<input type="button" value="Save"/> <input type="button" value="Clear"/>	

Figure 8-10 Link Budget Planning Calculator Link Budget

9. Firmware Upgrade

The latest firmware for aCNPT Nexus is available for download from the smartBridges Support website at <http://www.smartbridges.com/support/>

The aCNPT Nexus unit firmware can be upgraded from the web management interface.

Follow the steps below to upgrade the aCNPT Nexus firmware:

1. Download the latest (or a particular release version) of the aCNPT Nexus firmware from the website <http://www.smartbridges.com/support/>
2. Login to the device web interface. Go to Tools | Firmware Upgrade drop down menu. The Firmware Upgrade page will be displayed as shown below.
3. Enter the firmware tar-ball file name downloaded in Step 1.
4. Click on the Upgrade button to upgrade the firmware.
5. When the firmware tar-ball file transfer is completed, a message will be displayed on the web-page.
6. Wait for about 10 minutes or so for the device firmware to be upgraded. Once the upgrade completes, a pop-up window displaying the upgraded firmware version will appear.

Note: During the upgrade period (about 10-15 minutes), the aCNPT unit must NOT be reset or power-cycled.

Tools : Firmware Upgrade

airClient TOTAL (sB3412) - [Router mode](#)

Firmware Upgrade	
Current Firmware Version	v0.00.02
Upgrade System Software Tar File	<input type="text" value="C:\SB3412_IXP_v0.00.02.tar"/> <input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/>	

Figure 9-1 aCNPT Nexus Firmware Upgrade page

Tools : Firmware Upgrade

**System Software Tar File has been transferred.
The device is being upgraded and will be unavailable for 10-15 minutes.**

DO NOT Reset or Reboot during this time.....

Time elapsed : 00:28 (MM:SS)

Figure 9-2 aCNPT Nexus Firmware Upgrade (Firmware transferred)



Figure 9-3 Successful upgrade pop-up window

Appendix A – SNMP Trap

aCNPT Nexus generates a SNMP trap that can be forwarded to the SNMP Trap server. The SNMP Trap server IP address is set in section.

The following table provides a list of SNMP traps generated.

Trap	Message
IP address	Object Identifier: 1.3.6.1.4.1.14882.2.1.1 Value: <changed IP address>
IP netmask	Object Identifier: 1.3.6.1.4.1.14882.2.1.2 Value: <changed IP netmask>
Gateway	Object Identifier: 1.3.6.1.4.1.14882.2.1.3 Value: <changed Gateway>
SSID	Object Identifier: 1.3.6.1.4.1.14882.5.1.3.3 Value: <changed SSID>
Radio Mode	Object Identifier: 1.3.6.1.4.1.14882.5.1.18 Value: <changed Radio Mode>
	Note: Possible values for radio mode are given in the table below:

Value	airHaul	airPoint	aCNPT
0	Remote Router		Router
1	Remote Bridge		Bridge
2			
3	Root Bridge	Bridge	
4			NAT

Appendix B – Useful terms and definitions

Acronyms and Abbreviations	
MAC	Media Access Control
aCNPT	aCNPT Nexus PRO TOTAL
RSSI	Receive Signal Sensitivity Indication
SSID	Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
ACL	Access Control List
SNMP	Simple Network Management Protocol
NTP	Network Time Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol

802.11h

The 802.11h specification is an addition to the 802.11 family of standards for wireless local area networks (WLANs). 802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military radar systems and medical devices.

802.11Q

IEEE **802.11Q** defines a mechanism for tagging frames so that they can be segregated into separate **VLANs**.

802.11i

An upcoming security standard currently being developed by IEEE that features 802.1x authentication protections and adds AES (Advanced Encryption Standard) technology, a stronger level of security than used in WPA for encryption protection along with other enhancements.

IEEE 802.1x

A security standard featuring a port-based authentication framework and dynamic distribution of session keys for WEP encryption. A RADIUS server is required.

SSID

Each **ESS** has a Service Set Identifier (**SSID**) used to identify the **Radio** that belong to the **ESS**. **Radios** can be configured with the **SSID** of the **ESS** to which they should associate. By default, radios broadcast their **SSID** to advertise their presence.

VLAN

A **VLAN** is a switched network that is logically rather than physically segmented. **VLANs** enable workstations and other devices to have a virtual association - independent of geographic location or physical attachment to the network. These groupings can be based upon organizational unit, application, role, or any other logical grouping.

WEP

According to the IEEE 802.11 standard, **Wired Equivalent Privacy (WEP)** is intended to provide “confidentiality that is subjectively equivalent to the confidentiality of a wired local area network medium and that does not employ cryptographic techniques to enhance privacy.”

WEP relies on a secret key that is shared between a mobile station and an access point. **WEP** uses the RC4 stream cipher invented by RSA Data Security. RC4 is a symmetric stream cipher that uses the same variable length key for encryption and decryption. With **WEP** enabled, the sender encrypts the data frame payload and replaces the original payload with the encrypted payload. The sender then forwards the encrypted frame to its destination. The encrypted data frames are sent with the MAC header **WEP** bit set. Thus, the receiver knows to use the shared **WEP** key to decrypt the payload and recover the original frame. The new frame, with an unencrypted payload can then be passed to an upper layer protocol.

WEP keys can be either statically configured or dynamically generated. In either case, **WEP** has been found to be easily broken.

WPA

Wi-Fi Protected Access (**WPA**) is a replacement security standard for **WEP**. It is a subset of the IEEE 802.11i standard being developed. **WPA** makes use of **TKIP** to deliver security superior to **WEP**. 802.1X access control is still employed. The **Authentication Server** provides the material for creating the keys.

Packet Concatenation

Packet concatenation will increase the throughput of the equipment by simply buffering the packets at the transmitter and convert them into superframe for the transmission over the wireless interface.

Packet Bursting

Packet bursting is for increasing the throughput by increasing the window size and reducing the time for acknowledgement.

Packet Compression

LZO compression is being used to achieve more throughputs.

COFDM

COFDM involves modulating the data onto a large number of carriers using the FDM technique. The Key features which makes it work, in a manner is so well suited to terrestrial channels, includes:

- Orthogonality (the “O” of COFDM);
- The addition of Guard interval;
- The use of error coding (the “C” of COFDM), interleaving and channel-state information

COFDM is resistant to multipath effects because it uses multiple carriers to transmit the same signal.

Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or to a LAN of multiple segments.

RIP

The most popular of the TCP/IP interior routing protocols is the *Routing Information Protocol (RIP)*. RIP is used to dynamically exchange routing information. RIP routers broadcast their routing tables every 30 seconds by default. Other RIP equipments will listen for these RIP broadcasts and update their own route tables.

DHCP

DHCP stands for 'Dynamic Host Configuration Protocol' and is a means for networked computers to get their TCP/IP networking settings from a central server. Importantly, DHCP assigns IP addresses and other TCP/IP configuration parameters automatically.

SNMP

Short for ***Simple Network Management Protocol***, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called *protocol data units (PDUs)*, to different parts of a network. SNMP-compliant devices, called *agents*, store data about themselves in *Management Information Bases (MIB)* and return this data to the SNMP requesters.

SYSLOG

In order to track information on events, device jobs, and packets flows, most security devices out put these events using the syslog information model. This output uses a specific format and protocol defined in RFC 3164.

Appendix C – License

aCNPT Nexus is Copyright © 2004-2005 by smartBridges. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Please refer to the URL below for latest updates to the Software Warranty Statement
<http://www.smartbridges.com/support/>