

ECB-1220R Wireless Client Bridge /AP/Router/Client Router





4Gon www.4Gon.co.uk info@4gon.co.uk Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

Table of Contents

1	INTRODUCTION	5
	FEATURES & BENEFITS PACKAGE CONTENTS UNIT DESCRIPTION SYSTEM REQUIREMENTS APPLICATIONS NETWORK CONFIGURATION a) Ad-hoc (peer-to-peer) Mode b) Infrastructure Mode	5 7 8 8 9 9 9 10
2	UNDERSTANDING THE HARDWARE	.11
	HARDWARE INSTALLATION	.11
	IP ADDRESS CONFIGURATION	.11
3	CLIENT BRIDGE/ROUTER & ROUTER/ AP	13
	BRIDGE/BRIDGE ROUTER TO ACCESS POINT ACCESS POINT TO BRIDGE/BRIDGE ROUTER	13 13
4	ACCESS POINT/ROUTER MODE – CONFIG	14
	Logging In	14
	MANAGEMENT	16
	OPERATION MODE	17
	STATUS	19
	STATISTICS	20
	DYNAMIC DNS (ROUTER MODE)	21
	DENIAL OF SERVICE (DOS) (ROUTER MODE)	22
	Log	23
	UPGRADE FIRMWARE	24
	SAVE / RELOAD SETTINGS, RESET TO DEFAULT	25
	TCP/IP SETTINGS	20
	LAN INTERFACE	27
	4.3.2 SNMP Settings	27
	WLAN INTERFACE (ROUTER <i>MODE</i>)	28
	PPPUE PPTP (POINT-TO-POINT TUNNELING PROTOCOL) (ROUTER MODE)	30 31
	WIRELESS	33
	BASIC SETTINGS (INFRASTRUCTURE, ADHOC)	34
	ADVANCED SETTINGS	35
	SECURITY	30
	WEP 64-BIT / 128-BIT	38
	WPA / WPA2 PASSPHRASE	39
	WPA / WPA2 RADIUS AUTHENTICATION	40
	WIRELESS DISTRIBUTION SYSTEM	40 1
	MAC ADDRESS FILTER	43
	Port Forwarding	43
	WEB SITE FILTER	44
		45

4	CLIENT BRIDGE/ROUTER MODE – CONFIG	46
	Logging In	46
	Management	48
	OPERATION MODE	49
	Status	50
	Statistics	51
	Log	51
	UPGRADE FIRMWARE	52
	SAVE / RELOAD SETTINGS, RESET TO DEFAULT	52
	Password	53
	TCP/IP SETTINGS	54
	LAN INTERFACE	54
	STATIC IP Address	55
	DHCP CLIENT	55
	DHCP Server	56
	SNMP SETTINGS	57
	CLIENT BRIDGE ROUTER	58
		58
		59
		61
		61
	ADVANCED SETTINGS	62
	SECURITY	64
,		04 65
,	WER 04-BIT / 120-BIT	00
,	WIDELEON SITE SUDVEY	60
	WIRELESS SITE SURVEY	. 07
AP	PENDIX A – FCC INTERFERENCE STATEMENT	68
AP	PENDIX B – IC STATEMENT	69

Revision History

Version	Date	Notes
1.0	March 21, 2008	Created
1.1	March 22, 2008	Chapters added

1 Introduction

The Wireless Client Bri dge/AP/Router/Bridge Router device operates seamlessly in the 2.4 GH z fre quency spe ctrum s upporting the 802.11b (2.4GHz, 11Mbps) and faster 802 .11g (2.4GHz, 54Mbps) w ireless standards. It's the best w ay to add wireless ca pability t o your existing wired network, or to add b andwidth to your wireless installation.

ECB-1220R has high transmitted output power and high receivable sensitivity. High output power and high sensitivity can extend range and coverage to reduce the roaming between APs to get more stability wireless connection. It also can reduce the expense of equipment in the same environment.

To protect your wireless connectivity, it can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA/WPA2. The MAC address filter lets you select exactly which stations should have access to your network. User isolation function can protect the private network between client users.

This chapter describes the features & ben efits, package contents, applications, and network configuration.

Features	Benefits		
Client Bridge/AP/Router/Client Router			
High Speed Data Rate Up to 54Mbps	Capable of handling heavy data payloads such as MPEG video streaming		
High Output Power Solution	Excellent output power spreads the operation distance		
IEEE 802.11b/g Compliant	Fully Interoperable with IEEE 802.11b/IEEE802.11g compliant devices		

Features & Benefits

SNMP Remote Configuration	Help administrators to remotely
Management	configure or manage the Access Point
	easily.
Point-to-point, Point-to-multipoint	Let users transfer data between two
Wireless Connectivity	buildings or multiple buildings
DoS (Denial of Service) protection	Prevent from well-known DoS attack
Built-in 4-port Switch automatically detects cable type	Easy local connectivity
Web-based configuration	Simple and intuitive network management
Firmware change via the Web-based configuration screen	Allow easy upgrade/restore/dump system configuration via web interface
System log	Logging critical event according to network manager's criteria
WPA2/WPA/ IEEE 802.1x support	Powerful data security
DHCP Client/ Server	Simplifies network administration
Universal Repeater	The easiest way to expand your wireless
	network's coverage
Keep personal setting	Keep the latest setting when firmware
	upgrade
Route	/AP Mode
NAT Router	Multiple computer Internet Access, also act as natural firewall
UPnP(Universal Plug and Play)	Friendly to special application e.g. instant messenger, VoIP
Port forwarding	Set up application server (FTP, Web, Email,) on LAN
Access control	WLAN-to-WAN access control (allow/disallow), prevent users from access unwanted content
Firewall	Prevent malicious access from Internet
Hide SSID	Avoids unallowable users sharing
	bandwidth, increases efficiency of the
	network
WDS (Wireless Distributed System)	Make wireless AP and Bridge mode
	simultaneously as a wireless repeater
MAC address filtering	Ensures secure network connection

User isolation support	Protect the private network between client users.	
Client Router mode		
PPPoE function support	Easy to access internet via ISP service authentication	

Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do n ot discard the packing materials, in case of return; the unit must be shipped in its original package.

- > One Wireless Client Bridge Unit
- One Switching Power Adapter (12V/ 1.25A)
- > One CAT5 UTP Cable
- > One CD-ROM with User's Manual

Unit Description



System Requirements

The f ollowing are t he minim um s ystem requirements i n order c onfigure the device.

- > PC/AT compatible computer with Ethernet interface.
- Operating system that supports HTTP web-browser

Applications

The wireless LAN p roducts are easy to install and highly efficient. The following list describes some of the many applications made possible through the p ower and flexibility of wireless LANs:

a) Difficult-to-wire environments

There are many s ituations where wires cannot be laid e asily. Historic buildings, older buildings, open are as and across busy streets make the installation of LANs either impossible or very expensive.

b) Temporary workgroups

Consider situations in parks, athletic arenas, exhibition centers, disasterrecovery, temporary offices and construction si tes where on e wants a temporary WLAN established and removed.

c) The ability to access real-time information

Doctors/nurses, poin t-of-sale e mployees, a nd wa rehouse w orkers can access rea I-time information while d ealing w ith patients, se rving customers and processing information.

d) Frequently changed environments

Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) Small Office and Home Office (SOHO) networks

SOHO users need a cost-effective, easy and quick installation of a small

network.

f) Wireless extensions to Ethernet networks

Network managers in dynamic environments can minimize the overhead caused by moves, ex tensions t o ne tworks, and o ther c hanges with wireless LANs.

g) Wired LAN backup

Network manage rs implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

Training sites at corporations and s tudents at universities use wireless connectivity to ease access to information, information exchanges, and learning.

Network Configuration

To better u nderstand h ow the wireless LAN p roducts work toge ther to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

- a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
- b) I nfrastructure for enterprise LANs.

a) Ad-hoc (peer-to-peer) Mode

This is t he simples t network c onfiguration with s everal c omputers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, wo uld only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If use d in stand-alone, the AP can extend the range of independent w ireless L ANs b y a cting as a repeater, which effec tively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



2 Understanding the Hardware

Hardware Installation

- 1 Place the unit in an appropriate place after conducting a site survey.
- 2 Plug one end of the Ethernet cable into the RJ-45 port of the device and another end into your PC/Notebook.
- 3 Insert the DC-inlet of the power adapter into the port labeled "DC-IN" and the other end into the power socket on the wall.

This diagram depicts the hardware configuration



IP Address Configuration

This device can be configured as a Client Bridge or Access Point. The default IP address of the device is **192.168.1.1** or **192.168.1.2**. In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Net work Int erface C ard (NIC). You will then see the following screen.

ieneral Authentication Advanced	
Connect using:	
Intel 8255x-based PCI Ethemet Adapt	Configure
This connection uses the following items:	
Client for Microsoft Networks	
File and Printer Sharing for Microsoft Netwo	orks
QoS Packet Scheduler	
M Themet Protocol (TCP/IP)	
Instal Uninstal	Properties
Description	
Transmission Control Protocol/Internet Protocol, wide area network protocol that provides commu across diverse interconnected networks.	The default nication
Show icon in notification area when connected	
Notify me when this connection has limited or no	connectivity
OK	Cance

2. Selec t Internet Protocol (TCP/IP) and then click on the Properties button. This will allow you to configure the TCP/IP settings of your PC/Notebook.

Internet Protocol (TCP/IP) Prope	rties 🛛 🕐 🔀		
General			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network, administrator for the appropriate IP settings.			
Obtain an IP address automatical	y		
Use the following IP address:			
IP address:	192.168.1.10		
Subnet mask:	255 . 255 . 255 . 0		
Default gateway:			
O Obtain DNS server address automatically			
Use the following DNS server addresses:			
Preferred DNS server:	· · · ·		
Alternate DNS server:			
Advanced			
OK Cancel			

3. Selec t **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.

For Example:		Device IP address: 192.168.1.1	
	PC	IP address: 192.168.1.10	
	PC	subnet mask: 255.255.255.0	

4. C lick on the **OK** button to close this window, and once again to close LAN properties window.

3 Client Bridge/Router & Router/ AP

This device can be configured as a Bridge or Access Point. The default IP address of the device is **192.168.1.1** in Client Bridge /Client Router mode. The default IP address of the device is **192.168.1.2** in AP/Router mode. This chapter will describe the steps to switch from Bridge to Access Point and Access Point to Bridge.

Bridge/Bridge Router to Access Point

- 1 Enter the default IP address (192.168.1.2) of the bridge into the address bar of the web-browser.
- 2 By default, a user name and pas sword has not been configured. If you have configured a user name and password, please enter them into the field to continue
- 3 Once you have logge d in, click on the **Operation Mode** lin k un der the **Management** menu.
- 4 Since this device is currently in Bridge mode, the **Bridge** radio button will be selected by default.
- 5 Se lect the **AP** radio button to and then click on the **Apply Change** to switch the operation mode to Access Point.
- 6 Wait for about 1 minute and the device will auto matically restart into Access Point mode.

Access Point to Bridge/Bridge Router

- 1 Enter the default IP address (192.168.1.1) of the bridge into the address bar of the web-browser.
- 2 By default, a user name and pas sword has not been configured. If you have configured a user name and password, please enter them into the field to continue
- 3 Once you have logge d in, click on the **Operation Mode** lin k un der the **Management** menu.

- 4 Since this device is currently in Access Point mode, the **AP** radio button will be selected by default.
- 5 Se lect the **Bridge or Bridge Router** radio button to and then click on the **Apply Change** to switch the operation mode to Bridge.
- 6 Wait for about 1 minu te and t he device will auto matically restart into Bridge mode.

4 Access Point/Router Mode – Config

Logging In

• To configure the AP through the web-browser, type IP address (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.



- Make sure that the ECB-1220R and your computers are on the same subnet. Refer to Chapter 2 in order to configure the IP address of your computer.
- Username : admin; Password : admin



- After logging in you will graphical user interface (GUI) of the bridge. The navigation drop-down menu on left is divided into three main sections:
- 1. **Management**: This includes operation m ode, st atus, statistics, logs, u pgrade firmware, save/reload settings, and password.
- TCP/IP Settings: This includes the con figuration of the L AN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
- 3. **Wireless**: This includes the b asic, advanced, security and site-survey settings for the wireless interface.
- The Bridge status page is a lso d isplayed once you have l ogged in. This includes details about the system, wireless, and TCP/IP configuration.

Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:12h:43m:15s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	1
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:e0:4c:81:88:90
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP	Disabled
MAC Address	00:e0:4c:81:88:90

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

- System
 - **Uptime:** Duration of time since the device was last reset.
 - **Firmware version**: Version of the firmwar e that is currently loaded on the device.
- Wireless Configuration:

- **Mode**: Wireless configuration mode such as Client Bridge, AP, or WDS.
- o Band: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
- **SSID**: The name used to identify the wireless network.
- Channel Number: The channel us ed t o communicate o n the wirel ess network.
- Encryption: The type of security used on this net work. It may be disabled, WEP, WPA, etc.
- o BSSID: The MAC address of the SSID.
- **State**: The current state of the bridge. It may be scanning or associated or disabled.
- Signal Strength: The signal strength of the wireless device.
- Noise Level: The level of interference.
- TCP/IP Configuration:
 - Attain IP Protocol: The IP address setting may be fixed or static.
 - IP Address: Displays the current IP address of the LAN port.
 - o Subnet Mask: Displays the current subnet mask for the IP address.
 - **Default Gateway**: Displays the default gateway for the device.
 - o **DHCP**: Displays the DHCP setting.
 - MAC Address: Displays the MAC address of the device.

Management



 Click on the Management link on the navigation drop-down menu. You will then see fi ve options: operation mo de, sta tus, sta tistics, I og, u pgrade firmware, s ave/reload sett ings, a nd password. Each option is described below.

Management (Router mode)

	Management
	Operation Mode
	Status
	Statistics
	DDNS
	Time Zone Setting
	Denial-of-Service
	Log
	Upgrade Firmware
	Save/Reload Settings
	Password
	TCP/IP Settings
	LAN Interface
	SNMP Settings
	WAN Interface
	Wireless
	Basic Settings
	Advanced Settings
	Security
	Access Control
	WDS settings
	Firewall
	Port Filtering
	IP Filtering
	MAC Filtering
	Port Forwarding
	Web Site Filtering
	DMZ
2	Logout

Operation Mode

Click on the Operation Mode link under the Management menu. The Operation
 Mode allows you to switch from Client Bridge to Access Point mode/Router Mode.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

O Bridge:	Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.
O Bridge Router:	Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.
• AP:	Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.
O Router:	Router is connected to at least two networks, commonly two LANs or WANs. Routers are located at gateways, the places where two or more networks connect and support highly security.
Apply Change	Reset

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

O Bridge:	Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.
O Bridge Router:	Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.
○ AP:	Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.
● Router:	Router is connected to at least two networks, commonly two LANs or WANs. Routers are located at gateways, the places where two or more networks connect and support highly security.
Apply Change	Reset

- Select the AP, Bridge or Bridge Router and then click on the Apply Change button.
- Please wait and the n enter the specified IP address into the web-browser. The previous settings will be retained in AP mode.
- Refer to **Chapter 5** to learn how to configure this device in Access Point mode.

Status

 Click on the Status link under the Management menu. The Status page is the first page that is displayed once y ou have logged in. This in cludes d etails about the system, wireless, and TCP/IP configuration.

Client Bridge Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:17m:37s
Firmware Version	v1.39.06
Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	wireless_g
Channel Number	5
Encryption	Disabled
BSSID	00:00:00:00:00
State	Scanning
Signal Strength	0.00
Noise Level	0.00
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:02:6f:49:16:d6

Access Point Gateway Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:15h:6m:21s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	1
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:e0:4c:81:88:90
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:88:90
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:86:22

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

- System
 - **Uptime:** Duration of time since the device was last reset.
 - **Firmware version**: Version of the firmwar e that is currently loaded on the device.

Wireless Configuration:

- o Mode: Wireless configuration mode such as Client Bridge, AP, or WDS.
- **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
- o **SSID**: The name used to identify the wireless network.
- **Channel Number**: The channe I us ed t o communicate o n the wirel ess network.
- Encryption: The type of security used on this ne twork. It may be disabled, WEP, WPA, etc.
- **BSSID**: The MAC address of the SSID.
- State: The current state of the bridge. It may be scanning or associated or disabled.
- Signal Strength: The signal strength of the wireless device.
- **Noise Level**: The level of interference.
- TCP/IP Configuration:
 - Attain IP Protocol: The IP address setting may be fixed or static.
 - o IP Address: Displays the current IP address of the LAN port.
 - o Subnet Mask: Displays the current subnet mask for the IP address.
 - o **Default Gateway**: Displays the default gateway for the device.
 - o **DHCP**: Displays the DHCP setting.
 - o MAC Address: Displays the MAC address of the device.

Statistics

 Click on the Statistics link under the Management menu. This page displays the number of sent and received packets on the Ethernet and Wireless interface.

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

MIL-1	Sent Packets	56501		
WIREless LAIN	Received Packets	30676		
F-0 - 1 4 81	Sent Packets	2232		
Emernet LAN	Received Packets	1742		

Refresh

Additional WAN traffic information under Router Mode

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	Sent Packets	33
WIFeless LAIN	Received Packets	4139
Fah ann at I AN	Sent Packets	7769
Lthernet LAIN	Received Packets	6171
Eth ann at XVA N	Sent Packets	575
Luternet WAIN	Received Packets	0

Refresh

 Since the packet counter is not dynamic, you must click on the **Refresh** button for the most recent statistics.

Dynamic DNS (Router mode)

Allows you to host a ser ver (Web, FTP, Game Server, etc.) using a domain name that you h ave p urchased with your dynamically assigned IP a ddress. Most broadband In ternet Se rvice Pr oviders a ssign d ynamic (changing) IP a ddresses. When you use a Dy namic DNS service provider, your friends can enter y our host name to connect to your server, no matter what your IP address is.

- Enable Dynamic DNS: Place a check in this box to enable the DDNS feature.
- Service Address: S elect a DD NS service provide r from the d rop-down list. DynDNS is a free service while TZO offers a 30 day free trial.
- Host Name: Specify the website URL.
- User Name: Specify the user name for the DDNS service.
- **Password**: Specify the password for the DDNS service and verify it once again in the next field.

- **Timeout**: Specify the time between periodic updates to the Dynamic DNS, if the dynamic IP address has not changed. The timeout period is entered in hours.
- Cli ck on the Save Settings button once you have modified the settings.

Dynamic D	NS Setting
Dynamic DNS is a ser (an URL) to go with th	vice, that provides you with a valid, unchanging, internet domain name hat (possibly everchanging) IP-address.
Enable DDNS	
Service Provider :	DynDNS 🔽
Domain Name :	host.dyndns.org
User Name/Email:	akebrunos@dyndns.org
Password/Key:	•••••
Note: For IZO, you can ha For DynDNS, you ca	we a 30 days free trial <u>here</u> or manage your TZO account in <u>control pane.</u> m create your DynDNS account <u>here</u>
Apply Change	Reset

Time Zone Setting (Router *mode*)

Click on the **Time** link in the navig ation menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by synchronizing with a time server.

Note: If the device losses power for any reason, it will not be able to keep its clock running, and will not display the correct time on ce the device has be en restarted. Therefore, you must re-enter the correct date and time.

												_
¥r 2	2000	Mon	1	Day	1	Hr	8	Mn	52	Sec	34	
: (GI	MT+08:0	00)Ta	ipei									
lient 1	update											
۲	192.5.4	41.41	- Norti	n Am	erica	*						
0				M	anual I	IP Set	tting)					
	Yr 2 : (Gl :lient 1	Yr 2000 : (GMT+08:0 : (Iient update () 192.5.4	Yr 2000 Mon : (GMT+08:00)Ta : Image: Second secon	Yr 2000 Mon 1 : (GMT+08:00)Taipei	Yr 2000 Mon Day : (GMT+08:00)Taipei : itent update (Image: Second	Yr 2000 Mon 1 Day 1 : (GMT+08:00)Taipei	Yr 2000 Mon 1 Day 1 Hr : (GMT+08:00)Taipei	Yr 2000 Mon 1 Day 1 Hr 8 : (GMT+08:00)Taipei :lient update Image: State of the	Yr 2000 Mon 1 Day 1 Hr 8 Mn : (GMT+08:00) Taipei	Yr 2000 Mon 1 Day 1 Hr 8 Mn 52 : (GMT+08:00)Taipei :lient update Image: State of the state	Yr 2000 Mon 1 Day 1 Hr 8 Mn 52 Sec : (GMT+08:00)Taipei : itient update ● 192.5.41.41 - North America ▼ ● (Manual IP Setting)	Yr 2000 Mon 1 Day 1 Hr 8 Mn 52 Sec 34 : (GMT+08:00)Taipei :lient update Image: State of the state o

- **Current Time**: Displays the current time on the device.
- **Time Zone**: Select your time zone from the drop-down list.
- Enable NTP Server: Place a check in this box if you would like to synchronize the device's clock to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.
- NTP Server Used: Specify the NTP server or select one from the drop-down list.
- Click on the Apply Change button once you have modified the settings.

Denial of Service (DoS) (Router mode)

DoS attack is a n a ttempt by ha ckers to b lock services for le gitimate use rs of a PC/Network. Check the kind of specific protection you need.

Denial of Service

A "denial-of-service" (DoS) attack is chara egitimate users of a service from using tha	cterized by t service.	an explicit attempt by hackers to preve
Enable DoS Prevention		
Whole System Flood: SYN	0	Packets/Second
Whole System Flood: FIN	0	Packets/Second
Whole System Flood: UDP	0	Packets/Second
Whole System Flood: ICMP	0	Packets/Second
Per-Source IP Flood: SYN	0	Packets/Second
Per-Source IP Flood: FIN	0	Packets/Second
Per-Source IP Flood: UDP	0	Packets/Second
Per-Source IP Flood: ICMP	0	Packets/Second
TCP/UDP PortScan	Low	Sensitivity
ICMP Smurf		
IP Land		
IP Spoof		
IP TearDrop		
PingOfDeath		
TCP Scan		
TCP SynWithData		
UDP EchoChargen		
Select ALL Clear ALL		
Enable Source IP Blocking	0	Block time (sec)
Apply Changes		

Log

 C lick on the Log link under the Management menu. The Log page displays a list of events that are triggered on the E thernet and Wireless interface. This I og can be

referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

Enable Log		
✓ system all	✓ wireless	
✓ Enable Remote Log	Log Server IP Address:	
Apply Changes		

- In order for the log to record all the events, you must first place a check in the Enable
 Log or Enable Remote Log (Log Server required) check box.
- Se lect system all or wireless depending on the type of events you want recorded.
- Since the log is not d ynamic, you must click on the **Refresh** button for the most recent events, or click on the **Clear** button to clear the log.
- •

Upgrade Firmware

 Click on the Upgrade Firmware link under the Management menu. This page is used to up grade the firmware on the d evice. Make sure that d ownloaded the appropriate firmware from your vendor.

Upgrade Firmware								
This page allows you upgrade the Access Point firmware to new version. Please note, do no power off the device during the upload because it may crash the system.								
Reset to	default							
Seep las	st setting of IP, SSID, User Name, Password and WEP Key							
Select File:	Browse							
Upload	Reset							

- Click on the Browse button and then select the appropriate firmware and then clic k on the Upload button.
- Clic k on **Reset to Default** to restore the device to factory default settings.

<u>Note</u>: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

Save / Reload Settings, Reset to Default

- Click on the Save / Reload Setting link under the Management menu. This option is used to save the current settings of the device in a file on your local dis k or load settings on t o the device f rom a local disk. This feature is very handy for administrators who have several devices that need to be configured with the sam e settings.
- This page also allows you to reset the device to its factory default settings.

Save/Reload Settings								
This page allows you save co was saved previously. Besid	urrent settings to es, you could rese	a file or reload the settings from the file which et the current configuration to factory default.						
Save Settings to File:	Save							
Load Settings from File:		Browse Upload						
Reset Settings to Default:	Reset							
Restart the System:	Restart							

- Click on the Save button to save the current settings to a file on the local disk.
- Click on the Browse button to select the settings file and then click on the Upload button to load the previously saved settings.
- Click on the Reset b utton to reset the device to its factory default settings. Click Restart to reboot the device.

Password

 Click on the **Password** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password. For security reasons it is highly recommended that you create a user name and password.

Password Setu	p				
This page is used to set the	account to access t	he web server of Ac	cess Point. Empty	user name and passw	ord will disable the protection.
User Name:					
New Password:					
Confirmed Password:					
Apply Changes F	Reset				

- En ter a **user name** into the first field.
- Enter a password into the New Password field and then re-type the password into the Confirmed Password field. Then click on the Apply Changes button.
- By clicking on the Reset button, the user name and pa ssword fields will be come blank indicating that the username and password has been disabled.

TCP/IP Settings



 C lick on the TCP/IP Settings li nk on the navigation drop-down menu. You will then see the LA N Interface a nd SNM P o ption. The options are described in detail below.

LAN Interface

 Click on the LAN Interface link under the TCP/IP Settings menu. Using this option you may change the IP address of the device as well as toggle the DHCP setting.

LAN Interface Setup

This page is used to configue change the setting for IP add	e the parameters for local area network which con esss, subnet mask, DHCP, etc	nects to the LAN port of your Access Point. Here you may
IP Address:	192.168.1.254	
Subnet Mask:	255.255.255.0	
Default Gateway:	0.0.0.0	
DHCP:	Disabled 💌	
Apply Changes Re	set	

- **IP Address**: Enter the IP address.
- Subnet Mask: Enter the subnet mask for the IP address.
- Default Gateway: Enter the IP address for the default gateway.
- DHCP: If this device is a DHCP client and will receive its IP s ettings from a DHCP server, then select Enabled from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is disabled, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

4.3.2 SNMP Settings

SNMP Parameter Setup

This page is used to configure the parameters for simple network management protocol which connects to ye change the setting for SNMP demon , read-only and read-write community name, Trap demon, trap IP addres

SNMP Daemon:	C Disable	👁 Enable	
Read-Only Community Name:	public		
Read-Write Community Name:	private		
Send SNMP Trap:	C Disable	🖲 Enable	
Send Trap To:	IP address 1	92.168.1.66	Community public

- Read-Only Community Name: Specify the p assword f or access the S NMP community for read only access.
- Read-Write Community Name: Specify the passw ord f or access t o the S NMP community with read/write access.
- Send SNMP Trap: Select Enable if you would like to receive SNMP traps.
- Send Trap To: Specify the IP address that would receive the SNMP traps.
- Trap Community Name: Specify the password for the SNMP trap community.
- Click on the **Save Settings** button once you have modified the settings.

WLAN Interface (Router mode)

DHCP Connection (Dynamic IP address) – Choose this connection type if your ISP provides you the IP address. Most cable modems use this type of connection. PPPoE (Point-to-Point Protocol over Ethernet) – Ch oose this o ption if your internet connection requires a user name and password. Most DSL modems use this type of connection.

Static IP address – Choose this option if you have a dedicated IP address.

DHCP Client

WAN in terface can be configured as a DH CP Client in w hich the ISP provides the IP address to the device. This is also known as Dynamic IP.

• Se lect the DHCP and click on the Apply Changes button.

You have the option of cloning your PCs MAC address onto the device. Click on the **Clone Your PCs MAC Address** to automatically copy the MAC address. You may also specify a host name

WLAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WLAN port of your Access Point. Here you may change the access method to static IP or DHCP by click the item value of WLAN Access type.

WLAN Access Type:	DHCP Client 💌
Attain DNS Automat Attain Attain DNS Automat Attain Attai	cally
O Set DNS Manually	
DNS 1:	
DNS 2:	
DNS 3:	
Enable Ping Access	on WLAN
Enable Web Server	Access on WLAN
Apply Changes	Reset

(Router mode)

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:	DHCP Client	
Attain DNS Automatic	ally	
○ Set DNS Manually		
DNS 1:		
DNS 2:		
DNS 3:		
Clone MAC Address:	0000000000	
Enable uPNP		
Enable Ping Access on WAN		
Enable Web Server Access on WAN		
Enable IPsec pass through on VPN connection		
Enable PPTP pass through on VPN connection		
Enable L2TP pass through on VPN connection		
Apply Changes Reset		

Static IP

Static IP is a fixed IP configuration where a II p arameters including DN S if a ny shoul d explicitly configured. VPN pass through is configured here by defining exclusivity.

WLAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WLAN port of your Access Point. Here you may change the access method to static IP or DHCP by click the item value of WLAN Access type.

WLAN Access Type:	Static IP	
IP Address:	192.168.1.25	
Subnet Mask:	255.255.255.0	
Default Gateway:		
DNS 1:		
DNS 2:		
DNS 3:		
Enable Ping Access on WLAN		
Enable Web Server Access on WLAN		
Apply Changes	Reset	

(Router mode)

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:	Static IP 👻	
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	
MTU Size:	1500 (1400-1500 bytes)	
DNS 1:		
DNS 2:		
DNS 3:		
Clone MAC Address:	0000000000	
✓ Enable uPNP		
Enable Ping Access of	on WAN	
Enable Web Server A	Access on WAN	
Enable IPsec pass through on VPN connection		
Enable PPTP pass through on VPN connection		
Enable L2TP pass through on VPN connection		
Apply Changes Reset		

PPPoE

This type of connection is usually use d for a DS L service and req uires a username and password to connect.

(Router *mode*)

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:	PPPoE V	
User Name:		
Password:		
Service Name:		
Connection Type:	Continuous Connect Disconnect	
Idle Time:	5 (1-1000 minutes)	
MTU Size:	1500 (1360-1492 bytes)	
Attain DNS Autom:	atically	
○ Set DNS Manually		
DNS 1:		
DNS 2:		
DNS 3:		
Clone MAC Addre	ss: 0000000000	
Enable uPNP		
Enable Ping Access on WAN		
Enable Web Server Access on WAN		
✓ Enable IPsec pass through on VPN connection		
✓ Enable PPTP pass through on VPN connection		
✓ Enable L2TP pass through on VPN connection		
Apply Changes	Reset	

Username / Password & Connection type (PPPoE) should be input then click on the **Connect** button.

- Address Mode: P PPoE c an be u sed with a d ynamic or sta tic IP ad dress. If y ou select the Dynamic IP r adio b utton, then the IIP address in t he next field is not required.
- However, if you select the Static IP radio button, then the IP address in the next field is required.
- User Name: Specify the user name which is provided by your ISP.
- Password: Specify the password which is provided by your ISP, and then verify it once again in the next field.

PPTP (Point-to-Point Tunneling Protocol) (Router mode)

 The WAN inter face can be configured as PPTP. PPTP (Point to Point Tunneling Protocol) us es a virtual private network to connect to y our ISP. This me thod of connection is primarily u sed in E urope. This me thod of connect ion requires you to

enter a username and password (provided by your ISP) to gain access to the Internet. The supported authentication protocols are PAP and CHAP.

- S elect the Username / Password Connection (PPTP) radio button and then click on the Next button.
- Address Mode: PPTP can be used with a dynamic or static IP address. If you select the Dynamic IP radio button, then the IIP address in the n ext field is not required. However, if you select the Static IP radio button, then the IP address in the next field is required.
- PPTP Address: Specify the IP address
- PPTP Subnet Mask: Specify the subnet mask for the IP address.
- PPTP Server IP Address: If the PPTP Server's IP address is different from the default gateway, then you may specify it here.
- User Name: Specify the user name which is provided by your ISP.
- Password: Specify the password which is provided by your ISP, and then verify it once again in the next field.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:	РРТР	
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Server IP Address:	0.0.0.0	
User Name:		
Password:		
MTU Size:	1400 (1400-1460 bytes)	
Request MPPE Encry	ption	
Attain DNS Automatic	ally	
O Set DNS Manually		
DNS 1:		
DNS 2:		
DNS 3:		
Clone MAC Address:	0000000000	
Enable uPNP		
Enable Ping Access of	on WAN	
Enable Web Server Access on WAN		
✓ Enable IPsec pass through on VPN connection		
Enable PPTP pass through on VPN connection		
Énable L2TP pass the	rough on VPN connection	
Apply Changes	Reset	

Wireless



 Click on the Wireless link on the navigation drop-down menu. You will then see four options: b asic settings, a dvanced settings security and site survey. Each option is described below.

Basic Settings (Infrastructure, Adhoc)

Click on the Basic Settings link under the Wireless menu. Using this o ption you
may configure the 802.11b/g settings as well as the frequency, channel, and SSID.

Wireless Basic Settings				
This page is used to con your Access Point. Here network parameters.	figure the parameters for wireless LAN clients which may connect to e you may change wireless encryption settings as well as wireless			
Band:	2.4 GHz (B+G) 💌			
SSID:	Engenius			
Channel:	1 💌			
Associated Clients:	Show Active Clients			
Enable Universal	Repeater Mode (Acting as AP and client simultaneouly)			
SSID of Extended Interface:				
Apply Changes	Reset			

- Band: Depending on the type of wireless clients that are connected to the network, you m ay select B, G, or B+G. If y ou are not s ure about w hich c lients will be accessing the wireless networks, it is recommended that you select B+G for the best performance.
- SSID: The S SID is a un ique named shared amongst all the points of the wirel ess network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- Channel: Sel ect a c hannel from the dr op-down list. T he c hannels av ailable are based on the country's regulation. When selecting Infrastructure mode, a channel is not r equired, h owever, whe n s electing A dhoc mo de, you mu st select the same channel on all points.
- Enable Universal Repeater Mode: Select Enable to activate Universal Repeater Mode and type below SSID for extended wireless interface.

Advanced Settings

Wirel	ess Ad	lvanced	Settings
-------	--------	---------	----------

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○ Open System ○ Shared Key ④ Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Ack Timeout:	0 (0-255 x 4 us)
	Note: Ack Timeout default CCK:316 us OFDM:72 us.
Data Rate:	Auto 🐱
Preamble Type:	● Long Preamble ○ Long & Short Preamble
Broadcast SSID:	Enabled Obisabled
LAPP:	○Enabled
802.11g Protection:	Enabled Obisabled
User Isolation:	○Enabled
QoS(WMM):	○Enabled
Apply Changes Reset	

- Click on the Advanced Settings link under the Wireless menu. On this page you can configure the advanced s ettings to tweak the performance of y our wireless network. Options available a re: frag mentation th reshold, RTS threshold, beacon interval, data rate, preamble type, and 802.11g protection.
- Authentication Type: select an authentication method. Options a vailable are Open System, Shared Key or Auto. An open system allows any client to authenticate as long as it conforms to a ny MAC address filter policies that may have b een set. All authentication packets are transmitted w ithout encry ption. S hared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks.

- RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in n oisy ne tworks and preventing hidden no des from degrading the performance.
- Beacon Interval: Beacons will be sent out to devices at the specified intervals. This
 value is measured in milliseconds (ms).
- ACK Timeout: You may specify a value for the acknowledge timeout.
- Data Rate: Select a data rate from the drop-down list. However, it is recommended to select auto for the best performance.
- Preamble Type: For best performance, all de vices on the w ireless network should use the same p reamble type. However, the wireless network will still function even though the wrong preamble type is used.
- Enable/Disable: A few options to enable some Wireless settings.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

Security

Clic k on the Security link under the Wireless menu. On this page you can configure the authentication and encryption settings such as WEP, WPA, and 80.1x.

Version 1.1

Encryption Disabled

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: None	Set WEP Key	
Use 802.1x Authentication	• WEP 64bits • WEP 128bits	
WPA Authentication Mode:	O Enterprise (RADIUS) Personal (Pre-Shared Key)	
WPA Cipher Suite:	TKIP AES	
WPA2 Cipher Suite:	TKIP AES	
Pre-Shared Key Format:	Passphrase 😪	
Pre-Shared Key:		
Enable Pre-Authentication		
Authentication RADIUS Server:	Port 1812 IP address Shared Secret	
Note: When encryption WEP is selected, you must set WEP key value.		
Apply Changes Reset		

- Encryption: Select None from the drop-down list if your wireless network does not use any type of encryption.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

WEP 64-bit / 128-bit

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WEP	Set WEP Key	
Use 802.1x Authentication	• WEP 64bits O WEP 128bits	
WPA Authentication Mode:	O Enterprise (RADIUS) 💿 Personal (Pre-Shared Key)	
WPA Cipher Suite:	✓ TKIP AES	
WPA2 Cipher Suite:	TKIP AES	
Pre-Shared Key Format:	Passphrase 🗸	
Pre-Shared Key:		
Enable Pre-Authentication		
Authentication RADIUS Server:	Port 1812 IP address Shared Secret	
Note: When encryption WEP is selected, you must set WEP key value.		
Apply Changes Reset		

- Encryption: Select WEP from the drop-down list if your wireless network uses WEP encryption. WE P is an ac ronym for Wired Equivalent P rivacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- Set WEP Key: Click on this button to configure the WEP Key.

cey, and select ASCII (or Hex as the format of input value.	as the encryption
Key Length:	64-bit 💌	
Key Format:	Hex (10 characters)	
Default Tx Key:	Кеу 1 💌	
Encryption Key 1:	ADDREADEDDD	
Encryption Key 2:	Jadadadadadak	
Encryption Key 3:	3000000000k	
Encryption Key 4:		

- Key Length: Select a 64-bit or 128-bit from the drop-down list.
- Key Format: Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Default Tx Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- Encryption Key 1-4: You may enter four different WEP keys.
- Click on the Apply Changes button to confirm the changes and then click on the Close button to return to the pervious window.

WPA / WPA2 Passphrase

Wireless Security Setup This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.		
Encryption: WPA	Set WEP Key	
Use 802.1x Authentication	WEP 64bits OWEP 128bits	
WPA Authentication Mode:	🔘 Enterprise (RADIUS) 💿 Personal (Pr	e-Shared Key)
WPA Cipher Suite:	TKIP AES	
WPA2 Cipher Suite:	TKIP 🗹 AES	
Pre-Shared Key Format:	Passphrase 👻	
Pre-Shared Key:	senaosecure	
Enable Pre-Authentication		
Authentication RADIUS Server:	Port 1812 IP address	Shared Secret
Note: When encryption WEP is se	lected, you must set WEP key value.	
Apply Changes Res	et	

Encryption: Select WPA or WPA2 from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to wo rk with e xisting Wi- Fi products that h ave be en e nabled with WEP. WPA provides improved data enc ryption through the Te mporal Integrity Protocol (TK IP), which scrambles the keys u sing a has hing algorithm and by a dding an integrity checking feature which makes sure that keys haven't been tampered with.

- WPA Authentication Mode: Select the Personal (Pre-Shared Key) radio button.
- WPA/WPA2: Select TKIP or AES as the cipher suite.
- Pre-Shared Key Format: Select Passphrase from the drop-down list.
- Pre-Shared Key: E nter the pass phrase here; this should be b etween 8 and 63 characters.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

WPA / WPA2 RADIUS Authentication

- Encryption: Select WPA or WPA2 from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to wo rk with e xisting Wi- Fi products that h ave be en e nabled with WEP. WPA provides improved data enc ryption through the Te mporal Integrity Protocol (TK IP), which scrambles the keys using a has hing algorithm and by a dding an integrity checking feature which makes sure that keys haven't been tampered with.
- WPA Authentication Mode: Select the Enterprise (RADIUS) radio button.
- WPA/WPA2: Select TKIP or AES as the cipher suite.
- RADIUS Port: Enter the port number of the RADIUS server. The default is usually 1812.
- RADIUS IP Address: Enter the IP address of the RADIUS server.
- RADIUS Password: Enter the shared password of the RADIUS server.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

Wireless Distribution System

 Wireless Distribution Sy stem uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

WDS Settings		
Wireless Distribution System uses wireless m Ethemet does. To do this, you must set these of other APs which you want to communicate	edia to communica APs in the same cl with in the table an	te with other APs, like the hannel and set MAC address nd then enable the WDS.
✓ Enable WDS		
Add WDS AP: MAC Address	Commer	ıt
Apply Changes Reset	Set Security	Show Statistics
Current WDS AP List: MAC Address	Comment	Select
Delete Selected Delete All	Reset	

- Enable WDS choose to enable/disable
- Adding WDS AP: Enter MAC address.
- Set Security WEP/WPA/WPA2-mixed
- Show Statistics shows details of WDS AP
- Apply settings click to save settings.

Firewall



The d evice p rovides a tight firewall by virtue of the w ay NAT w orks. U nless you configure t he route r to the c ontrary, the NA T does n ot r espond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attacks. However, some n etwork applications cannot run with a tight firewall. Th ose applications need to sele ctively op en ports in the firewall to function correctly. The options on t his page c ontrol sev eral ways of opening the firewall to add ress the needs of specific types of applications.

Port Filtering			
Entries in this table are use to Internet through the Gat your local network.	d to restrict certain type eway. Use of such filter	s of data packets from you s can be helpful in securing	ır local network g or restricting
Enable Port Filtering			
Port Range:	Protocol: Bot	Comment:	
Apply Changes	Reset		
Current Filter Table:			
Port Range	Protocol	Comment	Select
Delete Selected	Delete All	Reset	

- The Access Control section allows you to control access in a nd out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.
- When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.			
Enable IP Filtering			
Loal IP Address:	Protocol:	Both V Comment:	
Apply Changes	Reset		
Current Filter Table:			
Local IP Address	Protocol	Comment	Select
Delete Selected	Delete All	Reset	

MAC Address Filter

- This feature is used to restrict certain MAC address from a ccessing the Internet.
 These filters can be used for securing and restricting your network.
- Configure MAC Filtering: Select one of the options from the drop-down list.
 - Turn MAC Filtering OFF: When "OFF" is selected, MAC addresses are not used to control network access.
 - Turn MAC Filtering ON and ALLOW computers listed to access the network: When "ALLOW" is selected, only computers with MAC addresses listed in the MAC Filtering Rules list are granted network access.
 - Turn MAC Filtering ON and DENY computers listed to access the network: When "DENY" is selected, any computer with a MAC address listed in the MAC Filtering Rules list is refused access to the network.
- MAC Address: Specify that MAC address that you would like to filter.
- Clic k Apply Changes button to store the changes.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.		
Enable MAC Filtering MAC Address: Comment:		
Apply Changes Reset		
Current Filter Table: MAC Address Comment Select		
Delete Selected Delete All	Reset	

Port Forwarding

Multiple connect ions a re required by some applications, such a s internet games, video confe rencing, Intern et teleph ony, an d othe rs. These a pplications ha ve difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a ran ge of ports in y our router and redirect data through those ports to a single PC on your network.

- **Enable**: Place a check in this box to enable the port forwarding rule.
- Name: Assign a me aningful n ame to t he virtual s erver, for example Web S erver. Several well-known types of virtual ser ver are available from the Application Name drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- IP Address: Specify the IP address for the virtual server entry.
- TCP/UDP Ports: Specify the TCP or UDP port numbers.

Dout Fourwording

rortrorwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
IP Address: Protocol: Both V Port Range: Comment:
Apply Changes Reset
Current Port Forwarding Table:
Local IP Address Protocol Port Range Comment Select
Delete Selected Delete All Reset

Web site Filter

- This is a type of parental control feature used to restrict certain websites form being accessed through your network. These filters can be used for securing and restricting your network.
- Website/URL/Domain: Specify the web address that you would like to filter. Do n ot use "http://"
- Click on the Apply changes button to store the changes.

Web Site Filtering

Web Site filter is used to deny LAN users from accessing the internet. Block those Web Sites which contain keywords listed below.

Enable Web Site Filtering	
Web Site: www.methree.com	
Apply Changes Reset Current Filter Table:	
URL Address	Select
Delete Selected Delete All Reset	

DMZ

- Place check in this box to enable DMZ host. DMZ host is a demilitarized zone used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web, FTP, email and DNS servers.
- DMZ IP Address: Specify the IP address of the DMZ host.
- Click on the Apply changes button to store the changes.

DMZ
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
✓ Enable DMZ
DMZ Host IP Address: 192.168.1.23
Apply Changes Reset

4 Client Bridge/Router Mode – Config

Logging In

 To configure the Access Point through the web-browser, enter the IP address of the Bridge (d efault: 192.168.1.1) i nto t he address bar of the w eb-browser and press Enter.



- Make sure that the Access Point and your computers are on the same subnet. Refer to Chapter 2 in order to configure the IP address of your computer.
- Log in User name : admin; Password : admin
- After logg ing in you will g raphical user interface (GUI) of the Access Point. The navigation drop-down menu on left is divided into three main sections:
- 4. **Management**: This includes operation m ode, st atus, statistics, logs, u pgrade firmware, save/reload settings, and password.
- TCP/IP Settings: This includes the con figuration of the L AN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
- 6. **Wireless**: This includes the b asic, advanced, security and site-survey settings for the wireless interface.
- The A ccess P oint status p age is also displayed once you h ave logg ed in . This includes details about the system, wireless, and TCP/IP configuration.

Client Bridge Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:13h:31m:47s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	4
Encryption	Disabled
BSSID	00:00:00:00:00
State	Scanning
Signal Strength	0.00
Noise Level	0.00
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP	Disabled
MAC Address	00:e0:4c:81:88:90

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

Bridge Router Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:14h:45m:2s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	Infrastructure Bridge Router
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	11
Encryption	Disabled
BSSID	00:00:00:00:00
State	Scanning
Signal Strength	0.00
Noise Level	0.00
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP	Server
MAC Address	00:e0:4c:81:88:90
WLAN Configuration	
Attain IP Protocol	Getting IP from DHCP server
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:88:90

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

- o System
- o Uptime: Duration of time since the device was last reset.
- **Firmware version**: Version of the firmwar e that is currently loaded on the device.
- Wireless Configuration:
 - **Mode**: Wireless configuration mode such as client bridge, AP, or WDS.
 - **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
 - **SSID**: The name used to identify the wireless network.
 - **Channel Number**: The channe I us ed t o communicate o n the wirel ess network.
 - **Encryption**: The type of security used on this ne twork. It may be disabled, WEP, WPA, etc.
 - **BSSID**: The MAC address of the SSID.
 - Associated Clients: Displays the number of clients currently associated to the Access Point.
- TCP/IP Configuration:
 - o Attain IP Protocol: The IP address setting may be fixed or static.
 - o **IP Address**: Displays the current IP address of the LAN port.
 - o Subnet Mask: Displays the current subnet mask for the IP address.
 - **Default Gateway**: Displays the default gateway for the device.
 - o **DHCP**: Displays the DHCP setting.
 - o MAC Address: Displays the MAC address of the device.

Management



 Click on the Management link on the navigation drop-down menu. You will then see fi ve options: operation mo de, sta tus, sta tistics, I og, u pgrade firmware, s ave/reload sett ings, a nd password. Each option is described below.

Operation Mode

 Click on the Operation Mode link under the Management menu. The Operation Mode allows you to switch from Access Point to Client Bridge mode.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Isridge:	Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.
O Bridge Router:	Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.
○ AP:	Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.
O Router:	Router is connected to at least two networks, commonly two LANs or WANs. Routers are located at gateways, the places where two or more networks connect and support highly security.
Apply Change	Reset

Se lect the AP, Bridge or Bridge Router and then click on the Apply Change button.

Apply Change	Reset
Please wait	

- Wait for about a minute until you see the Pop-Up message.
- Click on the **OK** button and then enter the specified IP address into the web-browser.
- Please wait and the n enter the spec ified IP address into the web- browser. The previous settings will be retained in AP mode.

Refer to Chapter 4 to learn how to configure this devic e in Bridge/Bridge Router mode.

Status

- Click on the Status link under the Management menu. The Status page is the first page that is displayed once y ou have logged in. This in cludes d etails about the system, wireless, and TCP/IP configuration.
- System
 - **Uptime:** Duration of time since the device was last reset.
 - **Firmware version**: Version of the firmwar e that is currently loaded on the device.
- Wireless Configuration:
 - **Mode**: Wireless configuration mode such as client bridge, AP, or WDS.
 - o **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
 - **SSID**: The name used to identify the wireless network.
 - **Channel Number**: The channe I us ed t o communicate o n the wirel ess network.
 - Encryption: The type of security used on this net work. It may be disabled, WEP, WPA, etc.
 - o **BSSID**: The MAC address of the SSID.
 - Associated Clients: Displays the number of clients currently associated to the Access Point.
- TCP/IP Configuration:
 - o Attain IP Protocol: The IP address setting may be fixed or static.
 - o IP Address: Displays the current IP address of the LAN port.
 - o Subnet Mask: Displays the current subnet mask for the IP address.
 - o Default Gateway: Displays the default gateway for the device.
 - o **DHCP**: Displays the DHCP setting.
 - MAC Address: Displays the MAC address of the device.

Statistics

 Click on the Statistics link under the Management menu. This page displays the number of sent and received packets on the Ethernet and Wireless interface.

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethemet networks.

Wireless LAN	Sent Packets	7754
	Received Packets	5847
Ethernet LAN	Sent Packets	5447
	Received Packets	4489

 Since the packet counter is not dynamic, you must click on the **Refresh** button for the most recent statistics.

Log

C lick on the Log link under the Management menu. The Log page displays a list of events that are triggered on the E thernet and Wireless interface. This lo g can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

System Log	
This page can be used to set ren	note log server and show the system log.
🗹 Enable Log	
system all	wireless
🗹 Enable Remote Log	Log Server IP Address:
Apply Changes	

- In order for the log to record all the events, you must first place a check in the Enable
 Log or Enable Remote Log (Log Server required) check box.
- Se lect system all or wireless depending on the type of events you want recorded.

 Since the log is not d ynamic, you must click on the Refresh button for the most recent events, or click on the Clear button to clear the log.

Upgrade Firmware

 Click on the Upgrade Firmware link under the Management menu. This page is used to up grade the firmware on the d evice. Make sure that d ownloaded the appropriate firmware from your vendor.

Upgrade Firmware			
This page allows you upgrade the Access Point firmware to new version. Please note, do no power off the device during the upload because it may crash the system.			
O Reset to default			
• Keep last setting of IP, SSID, User Name, Password and WEP Key			
Select File: Browse			
Upload Reset			

 Click on the Browse button and then select the appropriate firmware and then clic k on the Upload button.

Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

Save / Reload Settings, Reset to Default

- Click on the Save / Reload Setting link under the Management menu. This option is used to save the current settings of the device in a file on your local disk or load settings on t o the device f rom a local disk. This feature is very handy for administrators who have several devices that need to be configured with the sam e settings.
- This page also allows you to reset the device to its factory default settings.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:	Save
Load Settings from File:	Browse Upload
Reset Settings to Default:	Reset
Restart the System:	Restart

- Click on the Save button to save the current settings to a file on the local disk.
- Click on the Browse button to select the settings file and the n click on the U pload button to load the previously saved settings.
- Click on the Reset b utton to reset the device to its factory default settings. Click Restart to reboot the device.

Password

 Click on the **Password** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password. For security reasons it is highly recommended that you create a user name and password.

Password Set	սթ					
This page is used to set th	ne account to acce	ss the web server o	f Access Point. E	Impty user name and p	assword will disable t	he protection.
User Name:						
New Password:						
Confirmed Password:						
Apply Changes	Reset					

- En ter a **user name** into the first field.
- Enter a password into the New Password field and then re-type the password into the Confirmed Password field. Then click on the Apply Changes button.
- By clicking on the Reset button, the user name and pa ssword fields will become blank indicating that the username and password has been disabled.

TCP/IP Settings



 Clic k on the TCP/IP Settings lin k on the navigation drop-down m enu. You will then see t he LA N Interface a nd S NMP option. The options are described in detail below.

LAN Interface

 Click on the LAN Interface link under the TCP/IP Settings menu. Using this option you may change the IP add ress of the device as well as toggle the DH CP server/client and 802.1d spanning tree feature.

Static IP Address

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
DHCP:	Disabled 🚩
DHCP Client Banges	192.168.1.100 -
DHCF Chent Kange.	192.168.1.200 Show Clien

LAN Interface Setup

- **IP Address**: Enter the IP address.
- Subnet Mask: Enter the subnet mask for the IP address.
- Default Gateway: Enter the IP address for the default gateway.
- DHCP: Since a static IP address is used, this option must be set to Disabled. If this device is a DHCP client and will receive its IP settings from a DHCP server, then select Enabled from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is Disabled, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

DHCP Client

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
DHCP:	Client 🖌
DHCP Client Range	192.168.1.100 -
Difer chent Kange.	192.168.1.200 Show Client
Apply Changes Reset)

- DHCP: If this device is a DHCP client and will receive its IP s ettings from a DHCP server, the n select Client from the dro p-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is disabled, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

DHCP Server

LAN Interface Setup				
This page is used to configure the pa LAN port of your Access Point. Here mask, DHCP, etc	rameters for local area network which connects to the you may change the setting for IP addresss, subnet			
IP Address:	192.168.1.1			
Subnet Mask:	255.255.255.0			
Default Gateway:	192.168.1.1			
DHCP:	Server 💙			
DHCP Client Range	192.168.1.100 -			
Difer chent Kange.	192.168.1.200 Show Client			
Apply Changes Reset]			

- IP Address: Enter the IP address.
- Subnet Mask: Enter the subnet mask for the IP address.
- Default Gateway: Enter the IP address for the default gateway.
- DHCP: Select Server from the drop-down list since this d evice is the DHCP server. This device will distribute the IP addresses to the clients associated.
- DHCP Client Range: Enter the first and last IP address of the range. Make sure that the range is on the same subnet as the device. You may click on the Show Client button to view a list of IP addresses that were distributed.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

SNMP Settings

SNMP Parameter Setup

This page is used to configure the parameters for simple network management protocol which con change the setting for SNMP demon, read-only and read-write community name, Trap demon, trap

	SNMP Daemon:	C Disable ⓒ Enable			
	Read-Only Community Name:	public			
	Read-Write Community Name:	private			
	Send SNMP Trap:	C Disable © Enable			
SNMI	Send Trap To:	IP address 192.168.1.66	Community public		
Read				sS	NMP
comn	Apply Changes Reset				

- Read-Write Community Name: Specify the passw ord f or access t o the S NMP community with read/write access.
- Send SNMP Trap: Select Enable if you would like to receive SNMP traps.
- Send Trap To: Specify the IP address that would receive the SNMP traps.
- Click on the **Save Settings** button once you have modified the settings.

Client Bridge Router



WLAN Interface

DHCP Connection (Dynamic IP address) – Choose this connection type if your ISP provides you the IP address. Most cable modems use this type of connection.

PPPoE (Point-to-Point Protocol over Ethernet) – Ch oose this o ption if your internet connection requires a user name and password. Most DSL modems use this type of connection.

Static IP address – Choose this option if you have a dedicated IP address.

DHCP Client

WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.

Se lect the DHCP and click on the Apply Changes button.
 You have the option of cloning your PCs MAC address onto the device. Click on the Clone Your PCs MAC Address to automatically copy the MAC address. You may also specify a host name

WLAN Inter	face Setup
This page is used to conf of your Access Point. He value of WLAN Access t	igure the parameters for Internet network which connects to the WLAN port re you may change the access method to static IP or DHCP by click the item ype.
WLAN Access Type:	DHCP Client
Attain DNS Automat	ically
◯ Set DNS Manually	
DNS 1:	
DNS 2:	
DNS 3:	
Enable Ping Access	on WLAN
Enable Web Server	Access on WLAN
Apply Changes	Reset

Static IP

Static IP is a fixed IP configuration where a ll p arameters including DN S if a ny shoul d explicitly configured. VPN pass through is configured here by defining exclusivity.

WLAN Interf	face Setup
This page is used to confi of your Access Point. Her value of WLAN Access t	igure the parameters for Internet network which connects to the WLAN port re you may change the access method to static IP or DHCP by click the item ype.
WLAN Access Type:	Static IP
IP Address:	192.168.1.25
Subnet Mask:	255.255.255.0
Default Gateway:	
DNS 1:	
DNS 2:	
DNS 3:	
Enable Ping Access	on WLAN
Enable Web Server	Access on WLAN
Apply Changes	Reset

PPPoE

This type of connection is usually use d for a DS L service and req uires a username and password to connect.

Username / Password & Connection type (PPPoE) should be input then click on the **Connect** button.

- Address Mode: P PPoE c an be u sed with a d ynamic or sta tic IP ad dress. If y ou select the Dynamic IP r adio b utton, then the IIP address in t he next field is not required.
- However, if you select the Static IP radio button, then the IP address in the next field is required.
- User Name: Specify the user name which is provided by your ISP.
- Password: Specify the password which is provided by your ISP, and then verify it once again in the next field.

WLAN Inter	face Setup
This page is used to con of your Access Point. He value of WLAN Access	figure the parameters for Internet network which connects to the WLAN port ere you may change the access method to static IP or DHCP by click the item type.
WLAN Access Type:	PPPoE V
User Name:	senao
Password:	•••••
Service Name:	HINET
Connection Type:	Continuous Connect Disconnect
Idle Time:	5 (1-1000 minutes)
MTU Size:	1500 (1400-1492 bytes)
Attain DNS Automa	tically
○ Set DNS Manually	
DNS 1:	
DNS 2:	
DNS 3:	
Enable Ping Acces	s on WLAN
Enable Web Server	r Access on WLAN
Apply Changes	Reset

Wireless



 Click on the Wireless link on the navigation drop-down menu. You will then see five options: basic settings, advanced settings security, a ccess control and WDS. Each option is described below.

Basic Settings

Click on the Basic Settings link under the Wireless menu. Using this o ption you
may configure the 802.11b/g settings as well as the frequency, channel, and SSID.

Wireless Basic Settings

Band:	2.4 GHz (B+G) 🐱
:CII22	EnGenius
Channel:	1
Associated Clients:	Show Active Clients
Enable Univers	al Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended In	terface:

- Band: Select the IEEE 802.11 mode from the drop-down list. Options available are 2.4GHz (B), 2.4GHz (G), or 2.4GHz (B+G). Select the appropriate mode based on the type of wireless network. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select 2.4GHz (G) instead of 2.4GHz (B+G) which will reduce the performance of the wireless network.
- SSID: The S SID is a un ique named shared amongst all the points of the wirel ess network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- Channel: Sel ect a c hannel from the dr op-down list. T he c hannels av ailable are based on the country's regulation. When selecting Infrastructure mode, a channel is not r equired, h owever, whe n s electing A dhoc mo de, you mu st select the same channel on all points.
- Show Active Clients: Click on this button to view a list of associated clients.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.
- Enable Universal Repeater Mode: Select Enable to activate Universal Repeater Mode and type below SSID for extended wireless interface.

Advanced Settings

Click on the Advanced Settings link under the Wireless menu. On this page you can configure the advanced s ettings to tw eak the performance of y our wireless network. Options available a re: frag mentation th reshold, RTS thr eshold, b eacon interval, output power, preamble type, broadcast SSID, IAPP, and 802.11g protection.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	Open Syst	em 🔘 Shared Key 💿 Auto
Fragment Threshold:	2346	(256-2346)
RTS Threshold:	2347	(0-2347)
Beacon Interval:	100	(20-1024 ms)
Ack Timeout:	0	(0-255 x 4 us)
	Note: Ack Tim	eout default CCK:316 us OFDM:72 us.
Data Rate:	Auto 🔽	
Preamble Type:	O Long Prease	mble 🔵 Long & Short Preamble
Transparent Bridge:	O Enabled	Disabled
Apply Changes Rese	et	

- Authentication Type: select an authentication method. Options a vailable are Open System, Shared Key or Auto. An open system allows any client to authenticate as long as it conforms to a ny MAC address filter policies that may have b een set. All authentication packets are transmitted w ithout encry ption. S hared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in n oisy ne tworks and preventing hidden no des from degrading the performance.
- Beacon Interval: Beacons will be sent out to devices at the specified intervals. This
 value is measured in milliseconds (ms).
- ACK Timeout: You may specify a value for the acknowledge timeout.

- Data Rate: Select a data rate from the drop-down list. However, it is recommended to select **auto** for the best performance.
- Data Rate: If you would like to force a data rate, you may select one from the dropdown list. However, for best performance it is recommended to use the Auto setting.
- Preamble Type: For best performance, all de vices on the w ireless network should use the same p reamble type. However, the wireless network will still function even though the wrong preamble type is used.
- Transparent Bridge: Can be Enabled/Disabled
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

Security

 Clic k on the Security link under the Wireless menu. On this page you can configure the authentication and encryption settings such as WEP, WPA, and 802.1x.

Encryption Disabled

will cless beculley becup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

- Encryption: Select None from the drop-down list if your wireless network does not use any type of encryption.
- Click on t he Apply Changes b utton t o c onfirm t he changes. This d evice will automatically restart once these changes have been applied.

WEP 64-bit / 128-bit

Wireless Security Setup

Apply Changes Reset

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

WPA Cipher Suite:	• TKIP O AES
WPA2 Cipher Suite:	⊖ TKIP
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

- Encryption: Select WEP from the drop-down list if your wireless network uses WEP encryption. WE P is an ac ronym for Wired Equivalent P rivacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- Set WEP Key: Click on this button to configure the WEP Key.

Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length:	64-bit 🗸
Key Format:	Hex (10 characters) 💌
Default Tx Key:	Key 1 💌
Encryption Key 1:	****
Encryption Key 2:	****
Encryption Key 3:	*****
Encryption Key 4:	*****
Apply Changes	Close Reset

- Key Length: Select a 64-bit or 128-bit from the drop-down list.
- Key Format: Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- Default Tx Key: You may use up to four different keys for four different networks. Select the current key that will be used.
- Encryption Key 1-4: You may enter four different WEP keys.

 Click on the Apply Changes button to confirm the changes and then click on the Close button to return to the pervious window.

WPA / WPA2 / WPA2 Mixed Passphrase

Wireless Security	Setup
This page allows you setup the wir could prevent any unauthorized acc	eless security. Turn on WEP or WPA by using Encryption Keys cess to your wireless network.
Encryption: WPA 💌	Set WEP Key
WPA Cipher Suite:	⊙ TKIP ○ AES
WPA2 Cipher Suite:	⊖ TKIP [®] AES
Pre-Shared Key Format:	Passphrase 👻
Pre-Shared Key:	senaosecure
Note: When encryption WEP is sel	lected, you must set WEP key value. et

- Encryption: Select WPA, WPA2 or WPA2_Mixed from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to im prove up on the s ecurity fea tures of WEP (Wi red Equivalent P rivacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data e ncryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- WPA Authentication Mode: Select the Personal (Pre-Shared Key) radio button.
- WPA/WPA2: Select TKIP, AES or both as the cipher suite.
- Pre-Shared Key Format: Select Passphrase from the drop-down list.
- **Pre-Shared Key**: Enter the pass phrase; this should be between 8 and 63 characters.
- Click on t he Apply Changes b utton t o c onfirm t he changes. Th is d evice will automatically restart once these changes have been applied.

Wireless Security Setup This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network. Encryption: WPA2 v Set WEP Key WPA Cipher Suite: © TKIP © AES WPA2 Cipher Suite: © TKIP © AES Pre-Shared Key Senaosecure Note: When encryption WEP is selected, you must set WEP key value. Apply Changes Reset

Wireless Site Survey

 Clic k Refresh to see the WLAN AP's that was detected with modest details of each of them listed.

Wireless Site This page provides tool you could choose to co	to scan the wireless n nnect it manually when	etwork. If a n client mo	any Acc de is ena	ess Point o abled.	or IBSS is	found,
SSID	BSSID	Channel	Туре	Encrypt	Signal	Select
PUNSIDNET	00:50:f2:ce:78:8e	6 (B)	AP	WEP	90	0
	00:0f:ch:c1:4f:c2	11 (B+G)	ΔP	WPA-	76	0
3COM_11G	00.01.00.01.41.02	п (в о)		PSK	/0	\cup

Appendix A – FCC Interference Statement

Federal Communication Commission Interference Statement

This equipment has b een tested and found to comply with the limits for a Class B digital device, pursuant to P art 15 of the FCC Rules. T hese limits a redesigned to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction s, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can b e d etermined by turning the equipment of fland on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Cau tion: An y ch anges o r modifica tions not expressly a pproved by the party r esponsible for compliance could void the user's authority to operate this equipment.

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

IMPORTANT NOTE: FCC Radiation Exposure Statement:

This e quipment comp lies with F CC radiation ex posure lim its s et fo rth f or an un controlled environment.

This device complies with FCC RF Exposur e limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix B – IC Statement

IC statement

Operation is subject to the following two conditions:

This device may not cause interference and

This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 9 dBi. Antenna having a high er ga in is strictly pro hibited per regulations of Industry C anada. The required a ntenna impedance is 50 ohms.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must fo llow the sp ecific o perating in structions for sa tisfying RF exposure complia nce. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

Ce périphérique ne doit pas causer d'interférence et.

Ce périphérique doit acc epter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.