User's Manual

Version: 1.0

Table of Contents

Terminology

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
CCK	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/ Collision Detection
DDNS	Dynamic Domain Name Server
DH	Diffie-Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FTP	File Transfer Protocol
GI	Guard Intervals
IAPP	Inter Access Point Protocol
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
MCS	Modulation Coding Scheme
MD5	Message Digest 5
NAT	Network Address Translation
NT	Network Termination
NTP	Network Time Protocol
PPTP	Point to Point Tunneling Protocol
PSD	Power Spectral Density
RF	Radio Frequency
SHA1	Secure Hash Algorithm

SNR	Signal to Noise Ratio
SSID	Service Set Identification
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UPNP	Universal Plug and Play
VPN	Virtual Private Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

1 Introduction

The Wireless LAN Broadband Router is an affordable IEEE 802.11ac/a/b/g/n of wireless LAN broadband router solution; setting SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN.

This document describes the steps required for the initial IP address assign and other WLAN router configuration. The description includes the implementation of the above steps.

1.1 Product Features

- Compatible with IEEE 802.11ac Specifications provides wireless speed up to 867Mbps data rate.
- Compatible with IEEE 802.11n Specifications provides wireless speed up to 300Mbps data rate.
- Compatible with IEEE 802.11g high rate standard to provide wireless Ethernet speeds of 54Mbps data rate.
- Maximizes the performance and ideal for media-centric applications like streaming video, gaming and Voice over IP technology.
- Supports WPS, WPA, WPA2, WPA3 encryption/decryption function to protect the wireless data transmission.
- Supports full duplex flow control on 10/100M Ethernet interface.
- Supports DHCP server to provide clients auto IP addresses assignment.
- Supports DHCP client, static IP, PPPoE of WAN Interface.
- Supports default firewall protection.
- Supports WEB based management and configuration.

Installation

2.1 Hardware Installation

Step 1: Place the Wireless LAN Broadband Router to the best optimum transmission location. The best transmission location for your WLAN Broadband Router is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.

Step 2: Connect the WLAN Broadband Router to your wired network. Connect the Ethernet WAN interface of WLAN Broadband Router by Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.

Step 3: Supply DC power to the WLAN Broadband Router. Use only the AC/DC power

adapter supplied with the WLAN Broadband Router; it maybe occur damage by using a different type of power adapter.

The hardware installation finished.

2.2 Software Installation

- There is no software drivers, patches or utilities installation needed, but only the configuration setting. Please refer to chapter 3 for software configuration.

Notice: It will take about 70 seconds to complete the boot up sequence after powered on the WLAN Broadband Router.

3 Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The WLAN Broadband Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Router/Repeater Mode

Default IP Address**:** ***192.168.1.1***

Default IP subnet mask**:** ***255.255.255.0***

WEB login User Name**:** ***root***

WEB login Password**:**

3.1 Prepare your PC to configure the WLAN Broadband Router

For OS of Microsoft Windows 95/ 98/ Me/XP:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
   Note: Windows Me users may not see the Network control panel. If so, *select* **View all Control Panel options** on the left side of the window
2. Move mouse and double-click the right button on ***Network*** icon. The ***Network*** window will appear.
3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.100**, any IP address within 192.168.1.2 to 192.168.1.254 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK and reboot your PC after completes the IP parameters setting.

For OS of Microsoft Windows 2000:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network and Dial-up Connections*** icon. Move mouse and double-click the ***Local Area Connection*** icon. The ***Local Area Connection*** window will appear. Click ***Properties*** button in the ***Local Area Connection*** window.
3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.100**, any IP address within 192.168.1.2 to 192.168.1.254 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to complete the IP parameters setting.

For OS of Microsoft Windows NT:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network*** icon. The ***Network*** window will appear. Click ***Protocol*** tab from the ***Network*** window.
3. Check the installed list of ***Network Protocol*** window. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.100**, any IP address within 192.168.1.2 to 192.168.1.254 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**

8. Click OK to complete the IP parameters setting.

For OS of Microsoft Windows Vista, Win7, Win8, Win8.1, Win10:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The Control ***Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network Connections*** item. The ***Network Connections*** window will appear. Double click ***Local Area Connection*** icon, then ***User Account Control*** window shown. Right click ***Continue*** button to set properties.
3. In ***Local Area Connection Properties*** window, Choose ***Networking*** tab, move mouse and click ***Internet Protocol Version 4 (TCP/IPv4)***, then click ***Properties*** button.
4. Move mouse and click ***General*** tab, Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.100**, any IP address within 192.168.1.2 to 192.168.1.254 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
5. Click OK to complete the IP parameters setting.

3.2 Connect to the WLAN Broadband Router

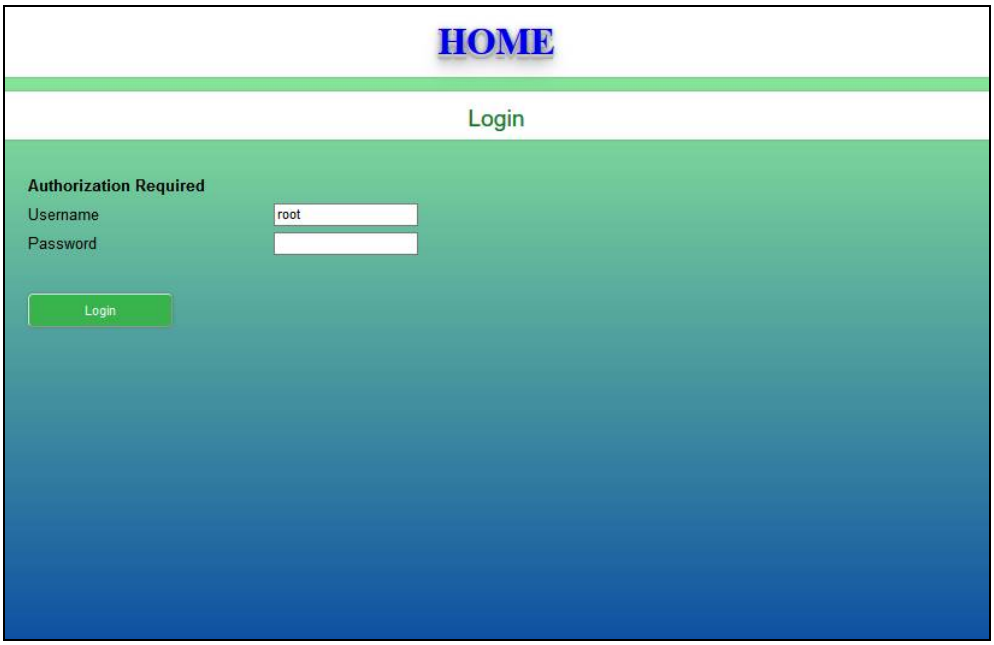
Open a WEB browser, i.e. Microsoft Internet Explore 6.1 SP1 or above, then enter 192.168.1.1 on the URL to connect the WLAN Broadband Router.

3.3 Management and configuration on the WLAN Broadband Router

3.3.1 Login

This page requests users to input User Name/ Password to login web home.

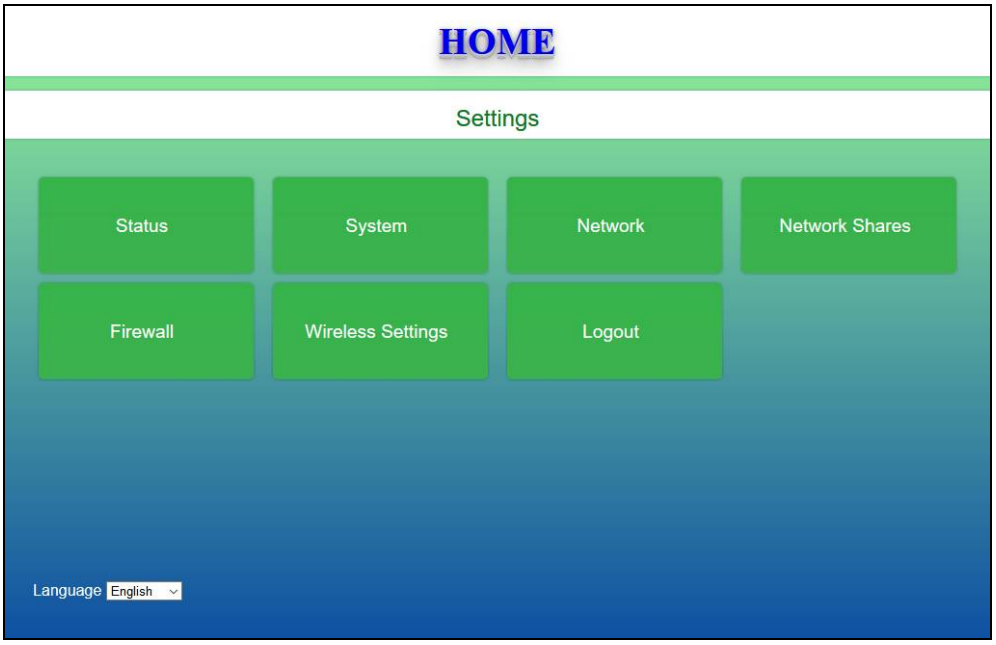
Default User Name/ Password is root/



Screen snapshot – Login

3.3.2 Web Home

This page is the first page after end user logs in.



Screen snapshot – Web Home

3.3.3 Status

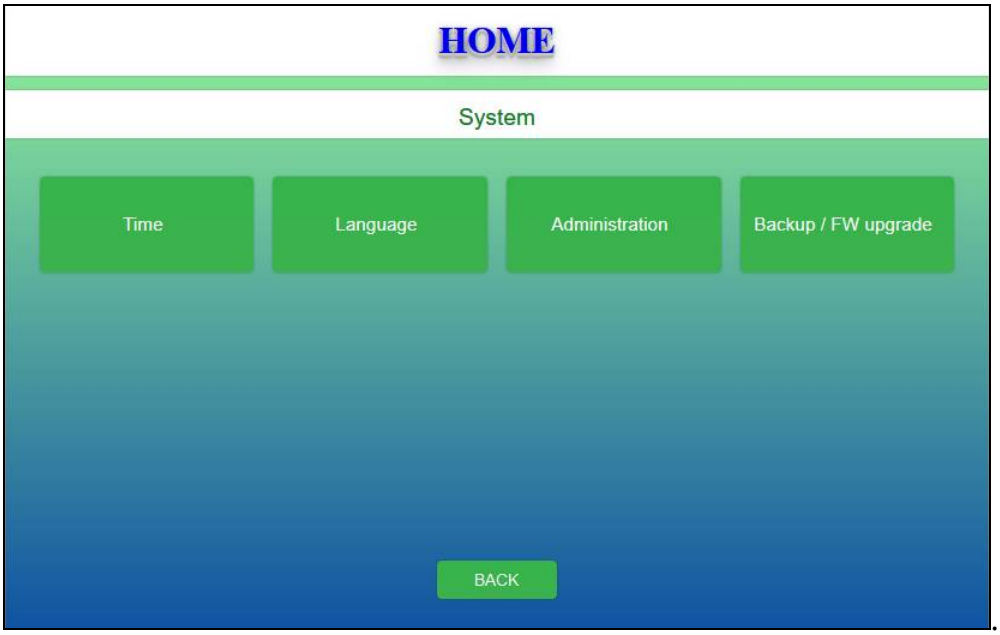
This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.

Screen snapshot – Status

Item	Description
System	
Firmware Version	It shows the firmware release version.
Local Time	It shows the timestamp of the local time zone
Up Time	It shows the duration since WLAN Broadband Router is powered on.
Internet Configuration	
Connected	It shows WAN connection status
Local Network Configuration	
Type	
Address	It shows the IP address of LAN interface of WLAN Broadband Router.
Netmask	It shows the IP subnet mask of LAN interface of WLAN Broadband Router.
MAC Address	It shows the MAC address of LAN interface of WLAN Broadband Router.
DHCP Lease	It shows the DHCP clients list
Wireless	
SSID	It shows 2G AP SSID name.
Mode	It shows the settings of wireless interface
Channel	It shows current AP which channel is occupied
Bitrate	It shows the current link data rate of wireless interface
BSSID	It shows current AP's mac address
Encryption	It shows current AP's security type.
Associated Stations	It shows the current wireless client connected list
BACK	Click the ***BACK*** button to go back previous page.

3.3.4 System

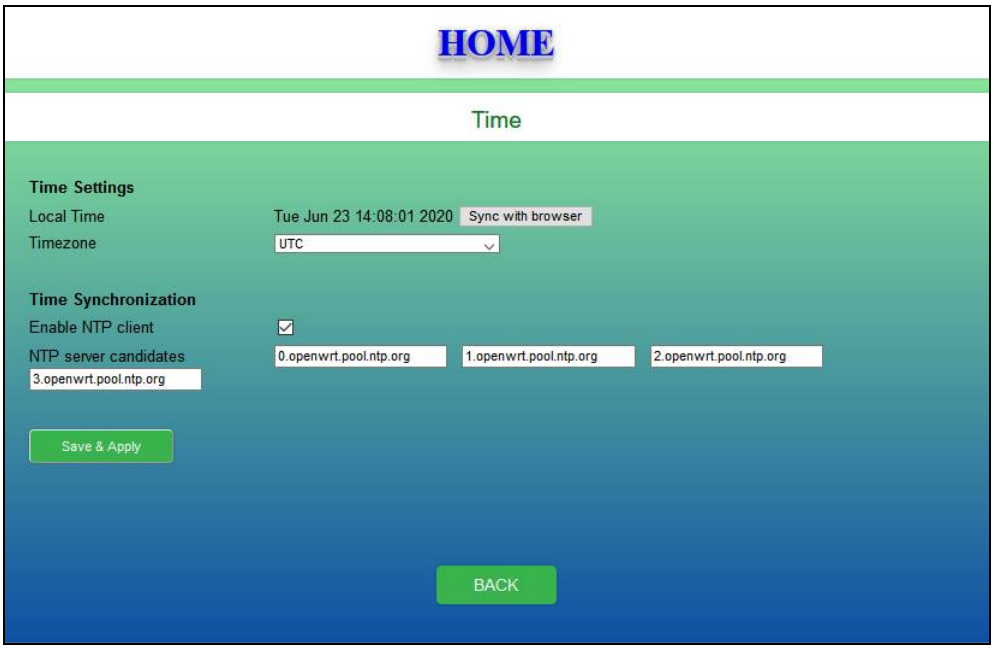
This page system `Time`, `Language`, `Administration` and `Back up/ FW upgrade settings page



Screen snapshot – System

I Time

This page is used to configure the time zone settings.



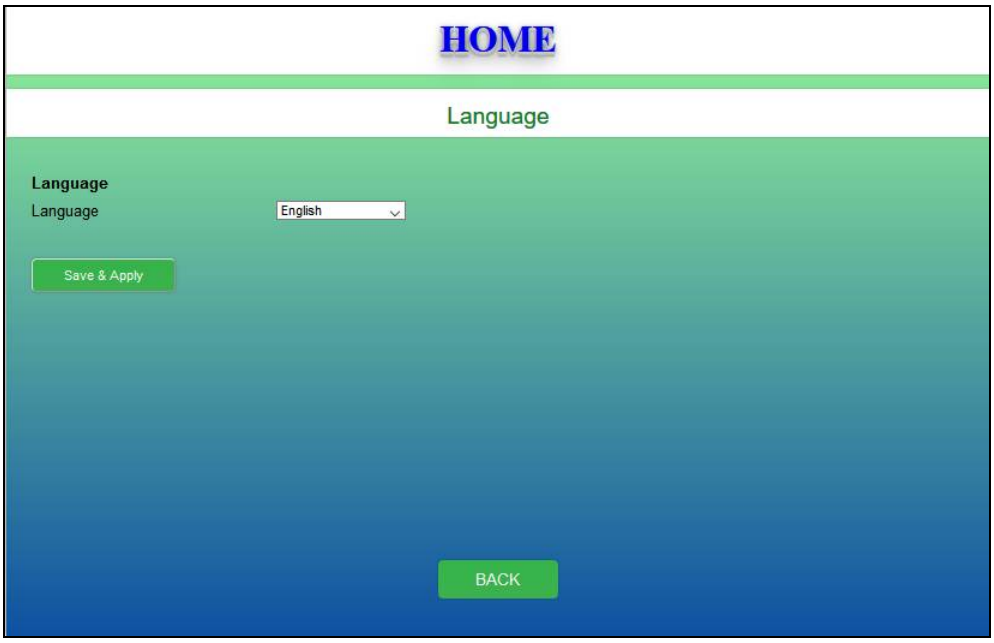
Screen snapshot – System– Time

Item	Description
Time Settings	

Local Tome	It shows current time.
Timezone	Click drop down menu to select the timezone area.
Time Synchronization	
Enable NTP client	Click checkbox to Enable/Disable NTP client function.
NTP Server candidates	It shows the available NTP servers.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

II Language

This page is used to set the language of web configuration pages are shown.

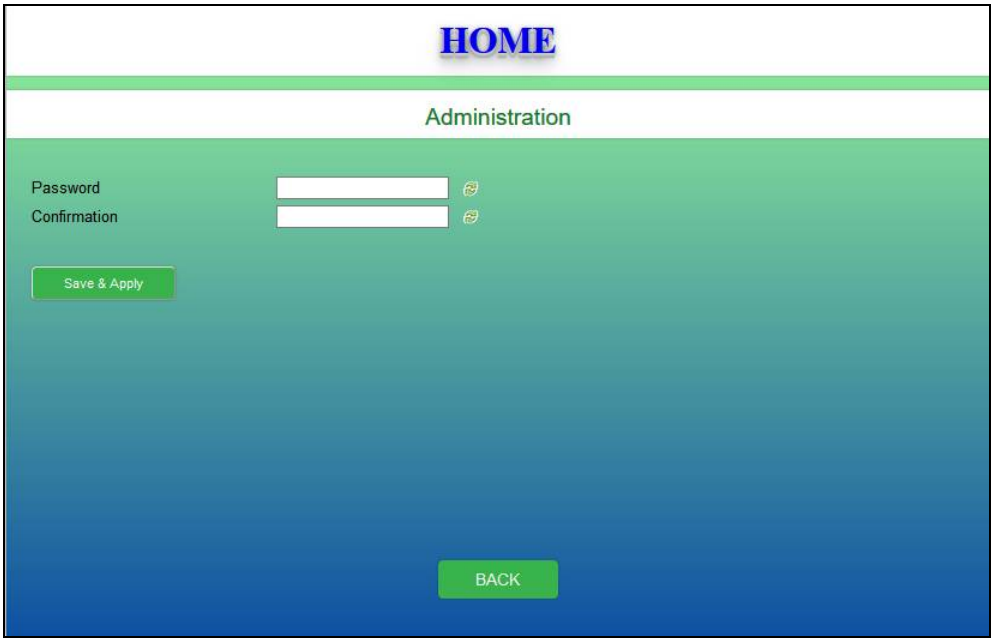


Screen snapshot – System– Language

Item	Description
Language	
Language	Click the drop down menu the set the available language.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

III Administration

This page is used to set the login password of current user.



Screen snapshot – System– Administration

Item	Description
Administration	
Password	To set/modify current user's password.
Confirmation	To confirm the above password.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

IV Backup / FW upgrade

This page is used to backup, restore, and reset configuration settings and firmware upgrade.

Screen snapshot – System– Backup / Firmware upgrade

Item	Description
Backup / Restore	
Download backup	Click **Generate archive** button and save current configuration.
Reset to defaults	Click **Perform reset** button to force current settings back to factory defaults.
Restore backup	Click **Browse** button to select the settings. Click **Upload archive** button to update current settings.
Firmware upgrade	Click **Browse** button to select the firmware that you want to upgrade. Click **Flash image** button to upgrade firmware.
BACK	Click the ***BACK*** button to go back previous page.

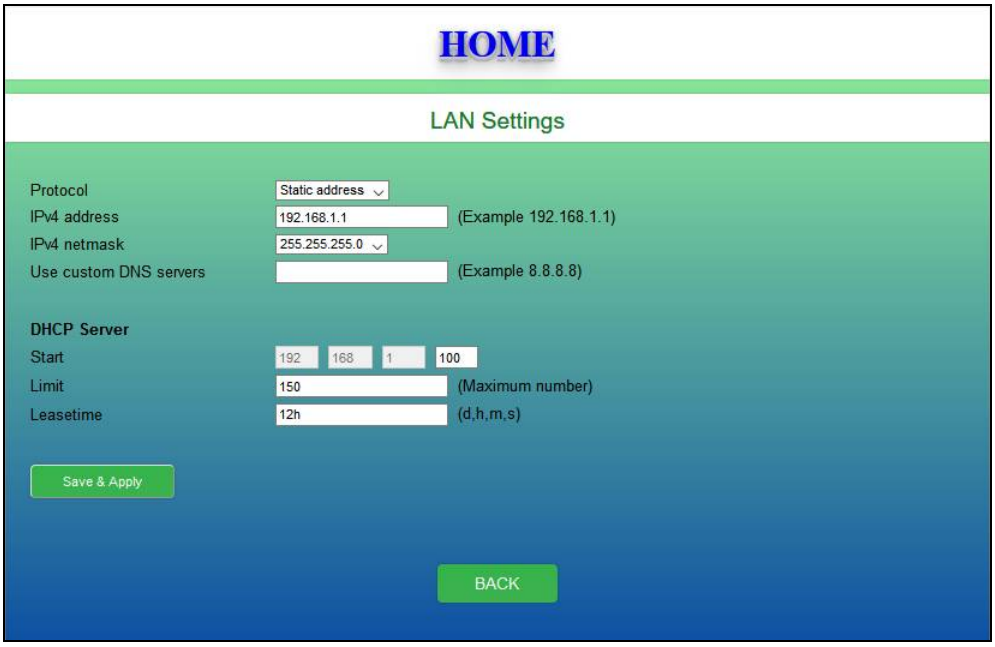
3.3.5 Network

This page is used to set LAN / WAN Settings.

Screen snapshot – Network

I LAN Settings

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN Broadband Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc.



Screen snapshot –Network – LAN Settings

Item	Description
Protocol	
IPv4 address	Fill in the IP address of LAN interfaces of this WLAN Access Point.
IPv4 netmask	Fill in the subnet mask of LAN interfaces of this WLAN Access Point.
DHCP Server	
Start	To set DHCP server leased start IP address.
Limit	To set DHCP clients connection limitation.
Lease Time	To set DHCP server leased time.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

II WAN Settings

This page is used to configure the parameters for wide area network that connects to the WAN port of your WLAN Broadband Router. Here you may change the access method to ***Static***, ***DHCP***, and ***PPPoE*** by click the item value of **WAN Access Type**.

■ Static address

Screen snapshot – Network – WAN Settings

Item	Description
WAN Settings	
Protocol	Click to select **Static address** support on WAN interface. There is IP address, subnet mask and default gateway settings need to be done.
IP v4 address	If you select the Static IP support on WAN interface, fill in the IP address for it.
IPv4 netmask	If you select the Static IP support on WAN interface, fill in the subnet mask for it.
IPv4 gateway	If you select the Static IP support on WAN interface, fill in the default gateway for it.
Use custom DNS sever	Fill in the IP address of Domain Name Server 1.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

- DHCP client

Item	Description
WAN Settings	
Protocol	Click to select **DHCP client** support on WAN interface for IP address assigned automatically from a DHCP server.
Hostname	Fill in the host name of Host Name. The default value is empty
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

- PPPoE

Item	Description
WAN Settings	
Protocol	Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.
Username	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Password	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

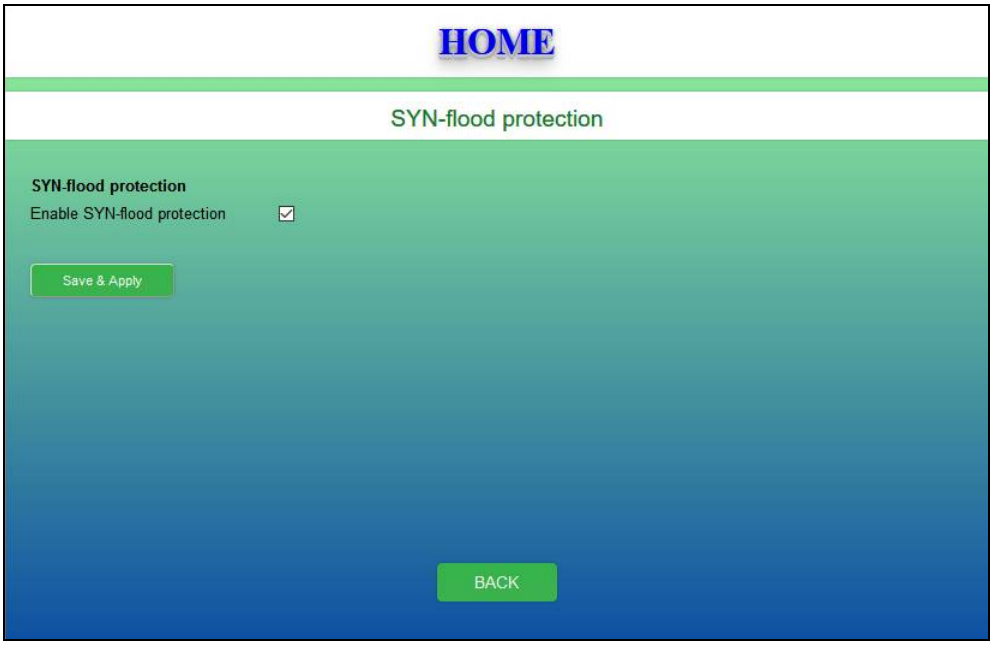
3.3.6 Firewall

This page is used to set LAN / WAN Settings

Screen snapshot – Network – WAN Settings

I SYN-flood protection

This page is to set up firewall syn-flood protection.

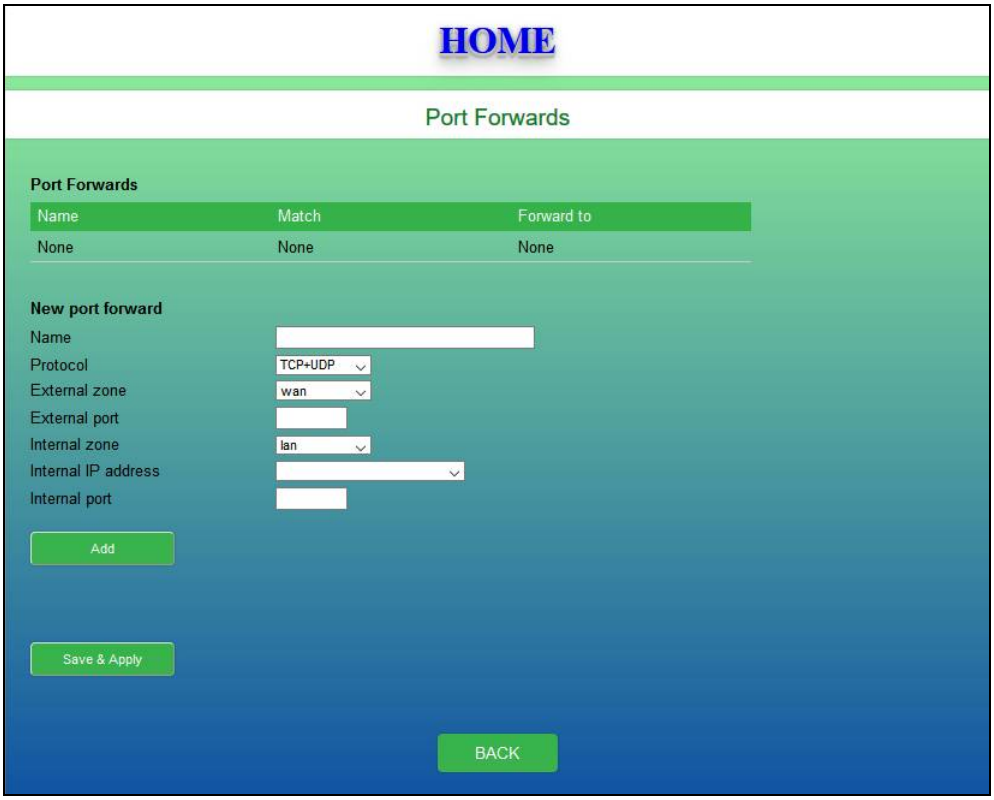


Screen snapshot –Firewall – SYN-flood protection

Item	Description
SYN-flood protection	
Enable SYN-flood protection	Click checkbox to Enable/Disable SYN-flood firewall function.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

II Port Forwarding

This page is to set up port forwarding rules.



Screen snapshot – Firewall – Port Forwards

Item	Description
Port Forwards	
Table	List port forwarding rules by **Add** button
New port forward	
Name	To setup rule name.
Protocol	Select TCP&UDP/TCP/UDP as protocol filter.
External zone	wan only
External port	To setup the port number of firewall wan.
Internal zone	lan only
Internal IP address	To setup firewall lan ip address.
Internal port	To setup port number of firewall lan.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

3.3.7 Wireless Settings

This page is used to configure the parameters for wireless LAN clients that may

connect to your Broadband Router. Here you may change wireless relative settings as well as wireless network parameters.

Screen snapshot – Wireless Settings

I 2G/5G Basic Settings

This page allows you setup WiFi mode and channel settings.

Screen snapshot – Wireless Settings – Basic Settings

Item	Description
Mode	Select the WiFi mode.
Channel	Select the WiFi channel.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

II SSID Security

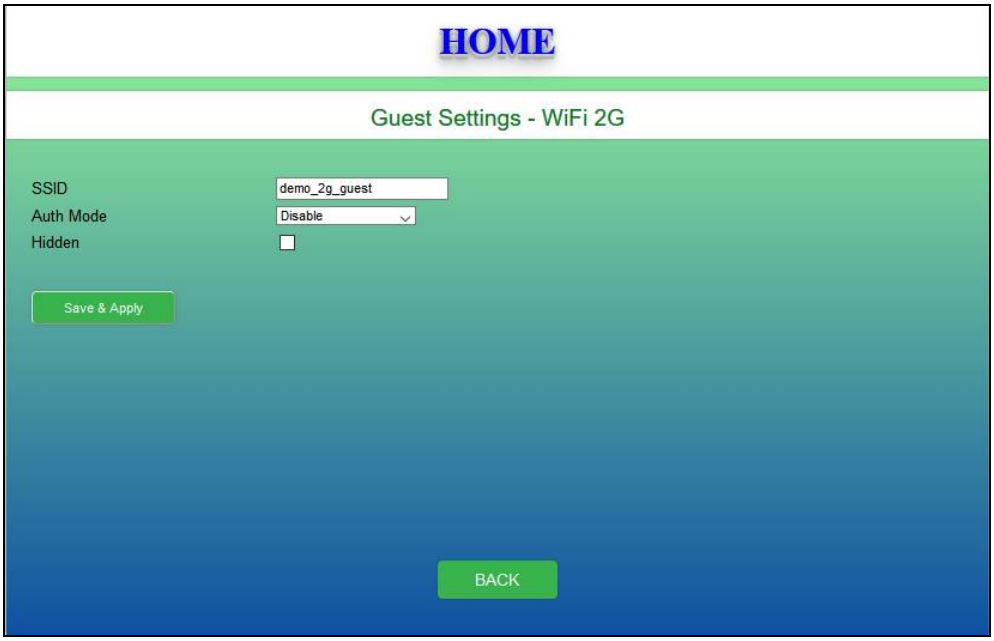
This page allows you setup the wireless security. Turn on WPA, WPA2 and WPA3 by using encryption keys could prevent any unauthorized access to your wireless network.

Screen snapshot – Wireless Settings - Security

Item	Description
Security Setup	
SSID	To set SSID
Auth Mode	Select the encryption supported over wireless access. The encryption method can be ***Disable, OPEN , WPA2-PSK, WPA3-PSK, WPAPSKWPA2PSK***
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

III Guest

This page is used to setup guest wifi SSID/ Security… settings.



Screen snapshot – Wireless Settings - Security

Item	Description
Guest Settings	
SSID	To set guest SSID
Auth Mode	Select the encryption supported over wireless access. The encryption method can be ***Disable, OPEN , WPA2-PSK, WPA3-PSK, WPAPSKWPA2PSK***
Hidden	Click checkbox to **Enable/Disable** hidden function.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

IV WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Screen snapshot –Wireless WPS

Item	Description
WPS Setup	
WPS	Click ***Enable*** to set up WPS settings and vice versa.
Save & Apply	Click the **Save & Apply** button to complete the new configuration setting.
BACK	Click the ***BACK*** button to go back previous page.

3.3.8 Logout

Item	Description
Logout	Click to sign out from configuration page.

4 Frequently Asked Questions (FAQ)

4.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- ✓ Open the Command program in the Microsoft Windows.
- ✓ Type in ***ipconfig /all*** then press the ***Enter*** button.

- ➢ Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

4.2 What is Wireless LAN?

A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

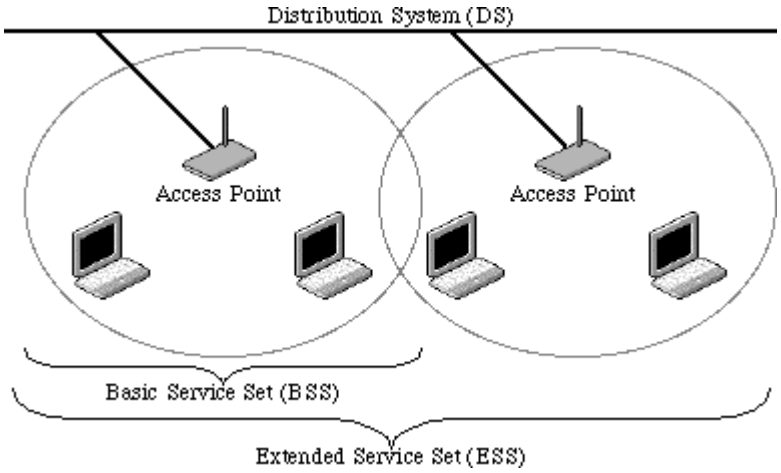
4.3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

4.4 How does wireless networking work?

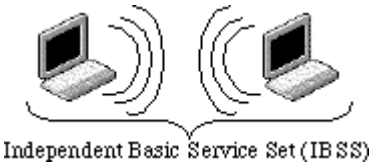
The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or

more BSSs forming a single sub network. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Example 2: wireless Ad Hoc Mode

4.5 What is BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just SSID. Serves as a network ID or name.

4.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It

is used to identify different wireless networks.

4.7 What are potential factors that may causes interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture… etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- ✓ Minimizing the number of walls and ceilings.
- ✓ Position the WLAN antenna for best reception.
- ✓ Keep WLAN devices away from other electrical devices, ex: microwaves, monitors, electric motors, … etc.
- ✓ Add additional WLAN Access Points if necessary.

4.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

4.9 What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

4.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11

to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

4.11 What is SSID stealth?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

4.12 What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team

developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

4.13 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

4.14 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

4.15 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

4.16 What is Universal Plug and Play (uPNP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

4.17 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1400.

4.18 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.

Since that all the clients will communicate outside world through the WLAN Broadband Router, so have the cloned MAC address set on the WLAN Broadband Router will solve the issue.

4.19 What is Privacy Seperator Between Clients?

An Infrastructure Basic Service Set is a BSS with a component called an *Access Point* (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS

4.20 What is WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

4.21 What is MIMO?

It's Multiple Input and Multiple Output. MIMO is a technology that uses multiple antennas to coherently resolve more information than possible using a single antenna

4.22 What is MU-MIMO?

It's Multiple User MIMO. Multi-user MIMO (MU-MIMO) can leverage multiple users as spatially distributed transmission resources, at the cost of somewhat more expensive signal processing. Multi-user MIMO can be generalized into two categories: MIMO broadcast channels (MIMO BC) and MIMO multiple access channels (MIMO MAC) for downlink and uplink situations, respectively.

FCC warning

Federal Communications Commission Statement

This device complies with FCC Rules Part 15. Operation is subject to the following two conditions:

• This device may not cause harmful interference.

• This device must accept any interference received, including interference that may cause undesired operation.

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

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.