DLB70XX
WLAN Dual Outdoor Radio

User Manual

Version 1.0.0 (11.08.2006)

Table of Contents

Preface 4

FCC Information 4

Electronic Emission Notices 4

FCC Frequency Interference Statement 4

FCC Radiation Exposure Statement 4

Antenna Installation 4

Installation Requirements 4

Packing List 5

Quick Start Guides 6

Access Point Client Mode 6

Configuring Universal Repeater 10

Wireless Setup 11

Initial Configuration 11

Operation Mode 11

Router 12

Bridge 12

WISP (Wireless ISP) 12

WLAN 1 Wireless Configuration 14

Basic Settings 14

Disable Wireless LAN Interface 14

Band 14

Mode 14

Network Type 15

SSID 15

Channel Number 15

Advanced Settings 17

Authentication Type 17

Fragment Threshold 17

RTS Threshold 17

Beacon Interval 17

ACK Timing 18

Client Expired Time 18

MTU Size 18

Data Rate 18

Preamble Type 18

Broadcast SSID 18

IAPP 18

802.11g Protection 18

Block WLAN Relay (Isolate Client) 18

Turbo Mode 18

Aggregation Mode 18

Tx Burst Mode 19

Transmit Power 19

Security 20

Encryption 20

WPA Authentication Mode 22

Access Control 22

WDS Settings 22

WDS Network Topology 23

Wireless Repeater 25

Wireless Bridge 26

Site Survey 26

Connecting Profile 26

WLAN 2 Wireless Configuration 28

Basic Settings 28

Disable Wireless LAN Interface 28

Band 28

Mode 28

Network Type 29

SSID 29

Channel Number 29

Advanced Settings 31
Authentication Type *31*
Fragment Threshold *31*
RTS Threshold *31*
Beacon Interval *32*
ACK Timing *32*
Client Expired Time *32*
MTU Size *32*
Data Rate *32*
Preamble Type *32*
Broadcast SSID *32*
IAPP *32*
802.11g Protection *32*
Block WLAN Relay (Isolate Client) *32*
Turbo Mode *33*
Aggregation Mode *33*
Tx Burst Mode *33*
Transmit Power *33*
Security 34
Encryption *34*
WPA Authentication Mode *36*
Access Control 37
WDS Settings 37
Site Survey 37
Connecting Profile 38

TCP/IP Configuration 40

Configuring LAN Interface 40
Configuring DHCP Server *40*
Configuring WAN Interface 40
Static IP *41*
PPPoE *43*
PPTP *44*
Configuring Clone MAC Address *45*
VPN Pass-through *48*
Static Route Setup 48
Dynamic Route Setup 49

Firewall Configuration 51

Configuring LAN to WAN Firewall 51
Port Filtering 51
IP Filtering 51
MAC Filtering 51
Configuring Port Forwarding (Virtual Server) 52
Multiple Servers behind NAT Example: 52
Configuring DMZ 53
Configuring VPN 54

Management Configuration 55

Quality of Service (QoS) 55
QoS Rule settings *56*
Current QoS setting table *56*
Bandwidth Control 57
SNMP Agent 58
Upgrade Firmware 61
Firmware Types *61*
Upgrading Firmware *61*
Save/Reload Settings 61
Reset Setting to Factory Default Value *61*
Password 62

Using CLI Menu 63

Start a SSH(Secure Shell) client session to login to the device *63*
Execute CLI program *63*
Menu Tree List *64*
Password *64*

Auto Discovery Tool 66
Discover 66
Setup IP 66
Detail 67
WDS 68
Active Clients 68
Connect to Web Server 68

Preface

FCC Information

Electronic Emission Notices

This device complies with CFR 47 Part 15 of the FCC rules.

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.

FCC Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to CFR47 Part 15. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment, not withstanding use in commercial, business and industrial environment.

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. There is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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 where the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications to this equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Radiation Exposure Statement

To comply with FCC RF exposure requirements in section 1.1307, a minimum separation distance of 0.4-meters (15.75-inches) is required between the antenna and all persons.

Antenna Installation

WARNING: It is installer's responsibility to ensure that when using the outdoor antenna in the United States (or where FCC rules apply), only those antennas certified with the product are used. The use of any antenna other than those certified with the product is expressly forbidden in accordance to FCC rules CFR47 part 15.204. The installer should configure the output power level of antennas, according to country regulations and per antenna type. Professional installation is required of equipment with connectors to ensure compliance with health and safety issues.

Installation Requirements

This guide is for the networking professional who installs and manages the Deliberant DLB70xx line of outdoor products hereafter referred to as the "device". To use this guide, you should have experience working with the TCP/IP configuration and

be familiar with the concepts and terminology of wireless local area networks.

NOTE: Only those antennas that are of the same type and with lesser gain than those that are certified with this device may be used legally by the installer.

23 dBi gain antenna - Arc Wireless Solutions antenna PN ANT-S-2126-01

Packing List

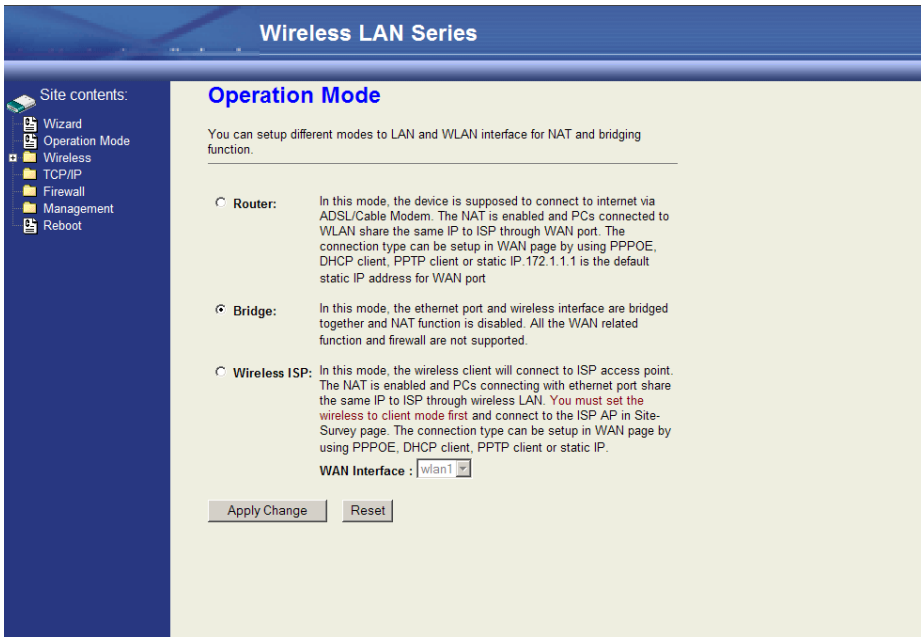
Before you start to install the device, make sure the package contains the following items：

- Wireless Outdoor Bridge unit * 1
- Mounting Kit * 1
- Power Over Ethernet Kit * 1

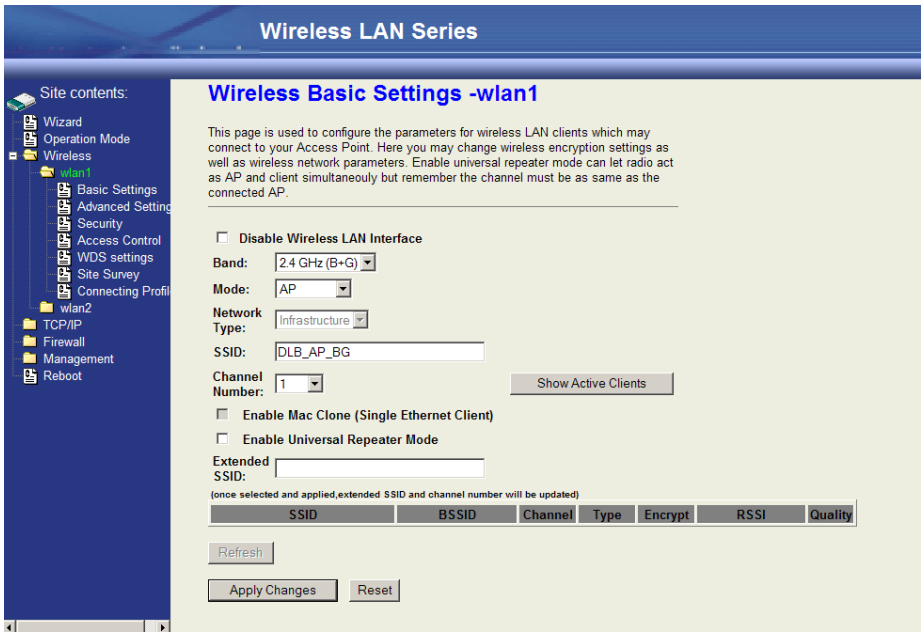
Quick Start Guides

Simple Access Point (Dual AP)

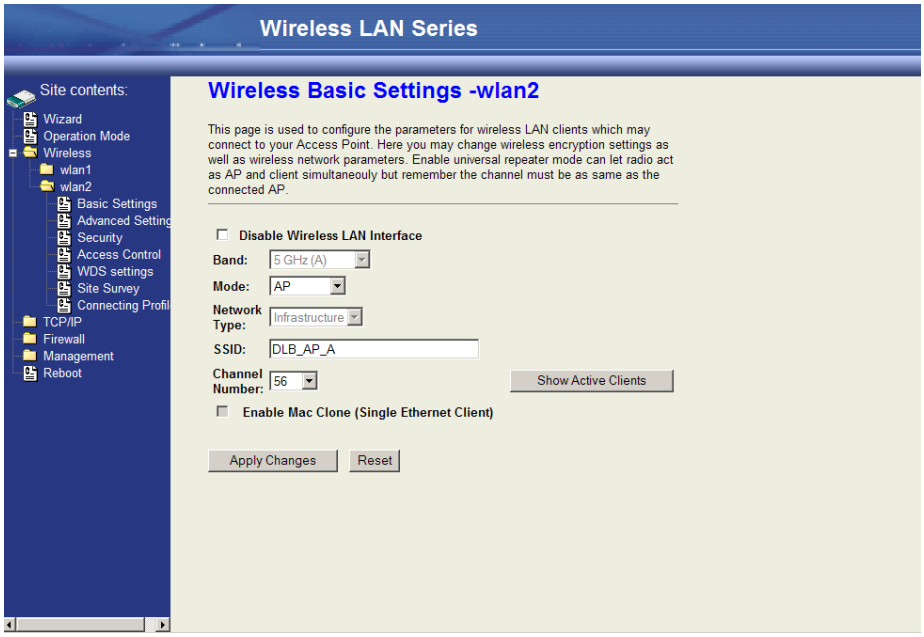
The DLB70XX series have two wireless radios: one 802.11A and one 802.11B/G. Sometimes it is desirable to provide customers with all three wireless standards, so this example shows how to create a bridged Access Point using both the 802.11A radio and the 802.11B/G radio.



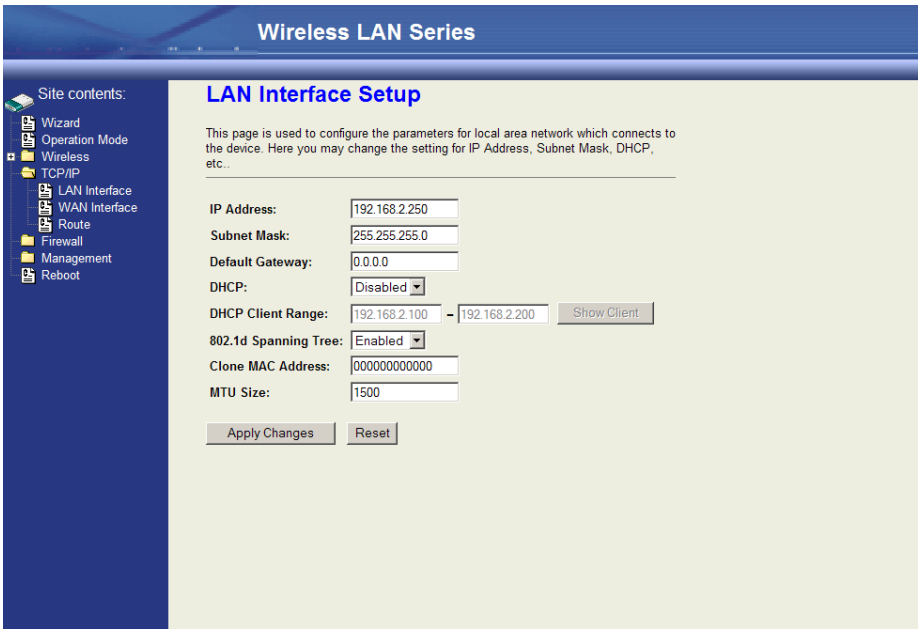
The Operation Mode needs to be set to Bridge. This bridges both wireless interfaces and the ethernet interface.



In the Wireless > wlan1 > Basic Settings section: uncheck “Disable Wireless LAN Interface” checkbox. Set the Mode to “AP”. Assign the SSID. For this example we used DLB_AP_BG since this is the 802.11B/G interface.



Follow the same steps for wlan2. In the Wireless > wlan2 > Basic Settings section: uncheck “Disable Wireless LAN Interface” checkbox. Set the Mode to “AP”. Assign the SSID. For this example we used DLB_AP_A since this is the 802.11A interface.



For ease of management, it might be beneficial to change the LAN IP address to reside on the same subnet as the other PCs in your bridged network.

5G Backhaul (WDS) / 2.4G AP (Bridged)

5G Backhaul (WDS) / 2.4G AP (Routed)

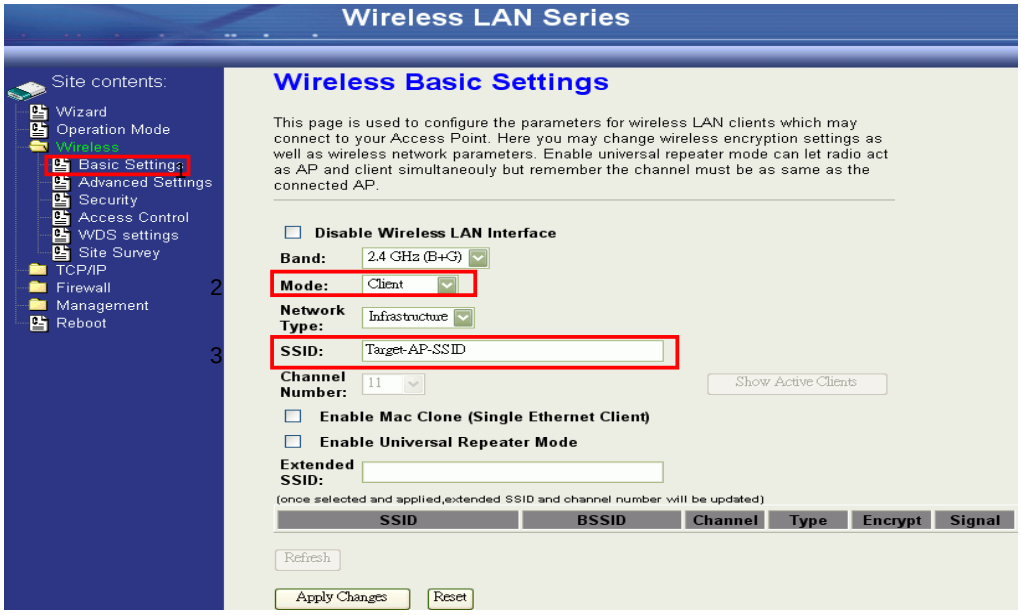
5G AP Client / 2.4G AP

Dual Backhaul with STP

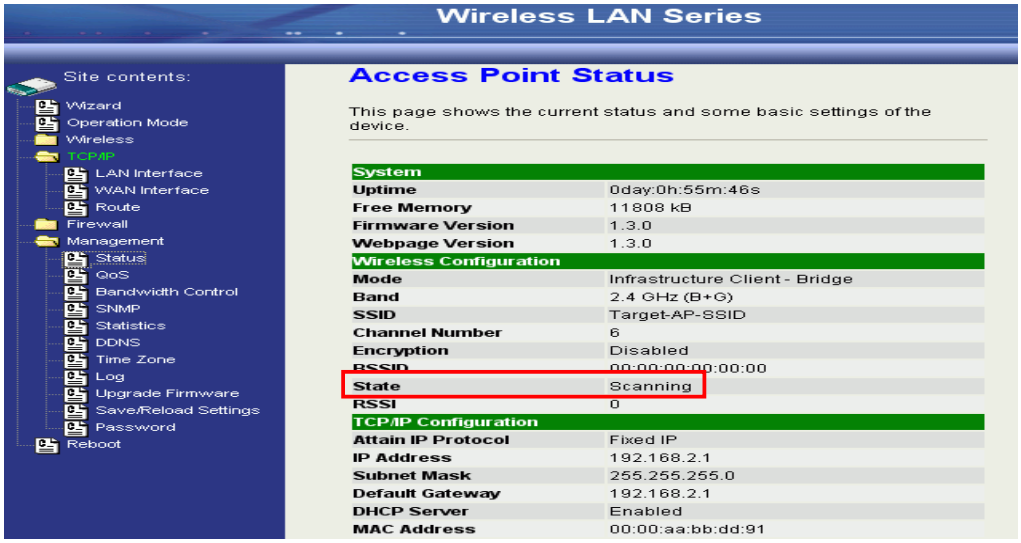
Access Point Client Mode

This device can be configured as a wireless Ethernet adapter. In this mode, the device can connect to the other wireless stations (Ad-Hoc network type) or Access Point (Infrastructure network type) and you don't need to install any driver.

In "Basic Settings" page, change the Mode to "Client" mode. And key in the SSID of the AP you want to connect then press "Apply Changes" button to apply the change.

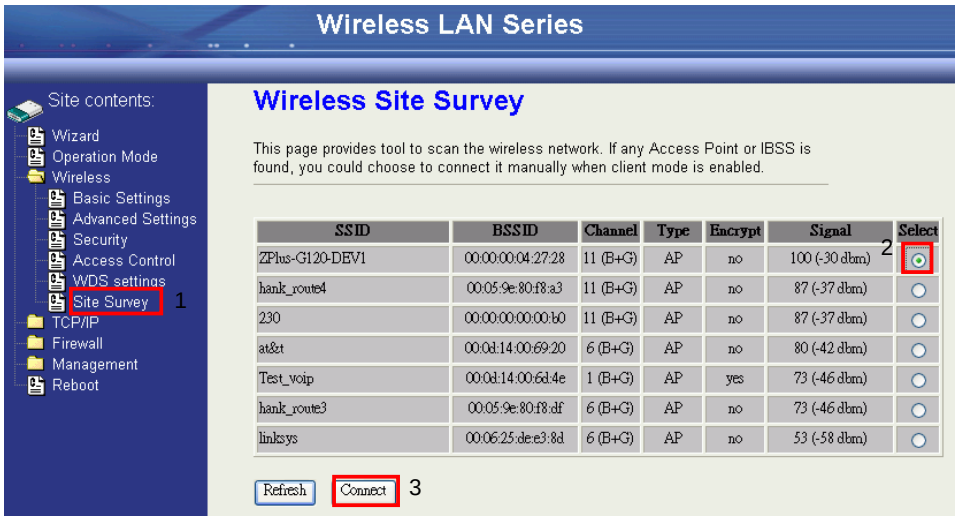


Check the status of connection in the "Status" web page



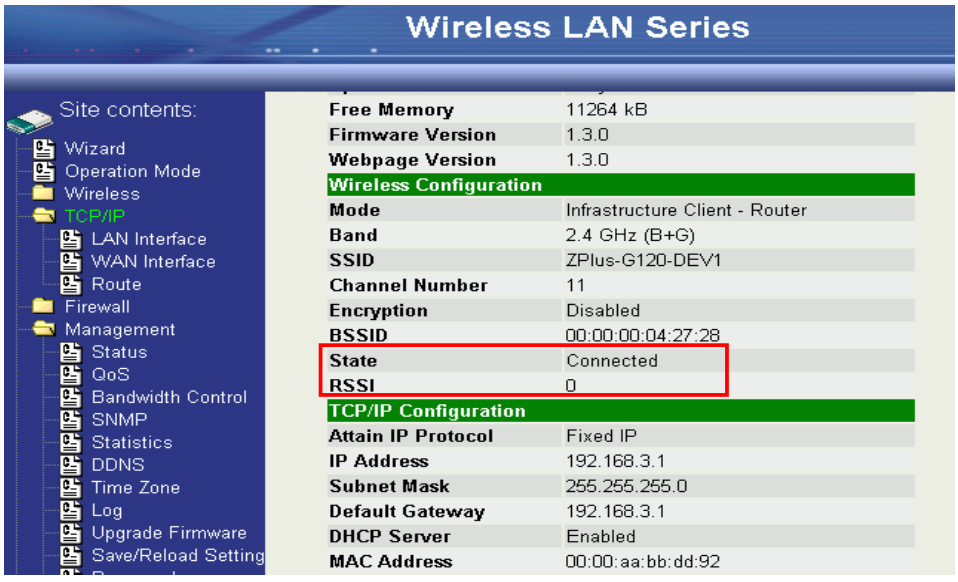
The alternative way to configure is as follows:

In the “Wireless Site Survey” page, select one of the SSIDs you want to connect and then press “Connect” button to establish the link.



If the link is established successfully it will show the message “Connect successfully”. Then press “OK”.

Then you can check the linking information in “Status” page.



NOTE: If the available network requires authentication and data encryption, you need to setup the authentication and

encryption before step1 and all the settings must be as same as the Access Point or Station. For more information about the detail authentication and data encryption settings, please refer the security section.

Authentication Type

In client mode, the device also supports two Authentication Types “Open system” and “Shared Key”. Although the default setting is “Auto”, not every Access Points can support “Auto” mode. If the authentication type on the Access Point is known by the user, we suggest setting the authentication type the same as the Access Point.

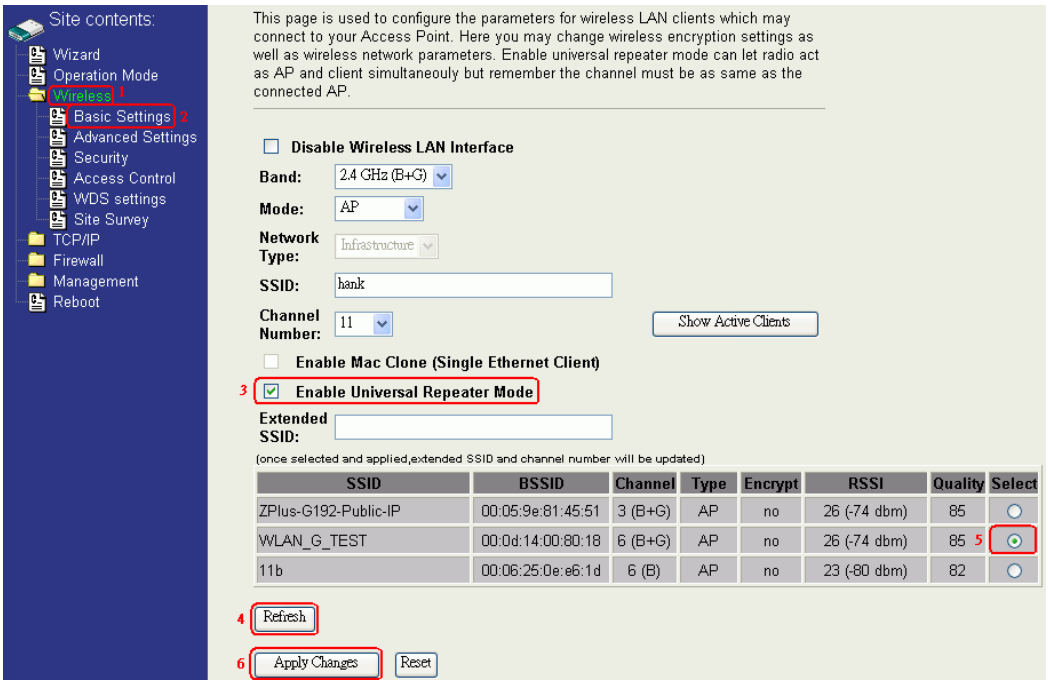
Data Encryption

In client mode, the device supports WEP and WPA Personal/Enterprise except WPA2 mixed mode data encryption. For more information about the detail data encryption settings, please refer the security section.

Configuring Universal Repeater

This device can be configured as a Repeater. In this mode, the device can extend the available wireless range of other AP and let the user link to the network that they want. (The device is working as an AP and Repeater at the same time.)

Enable Universal Repeater Mode and then select an SSID in the Table that you want. Then click the Apply Changes button. (Click the Refresh button to refresh the table.)



NOTE: Universal Repeater Mode is only available under AP, WDS and AP+WDS mode.

Enter specific SSID in the Extended SSID field and then click the Apply Changes button.

Wireless Setup

Initial Configuration

There are two ways to configure the device, one is through web-browser, and the other is through Secure Shell CLI interface. To access the configuration interfaces, make sure you are using a computer connected to the same network as the device. The default IP address of the device is 192.168.2.254, and the subnet-mask is 255.255.255.0.

The device has three operation modes (Router/Bridge/WISP). In bridge mode, also known as AP Client, you can access the device by both WLAN (Wireless Local Area Network) and wired LAN. And in router/WISP modes, the device can be accessed by both WLAN and WAN. The default IP addresses for the device are 192.168.2.254(for LAN), 172.1.1.1(for WAN), so you need to make sure the IP address of your PC is in the same subnet as the device, such as 192.168.2.X (for LAN), 172.1.1.X (for WAN).

NOTE: By default the DHCP server is enabled. Do not have multiple DHCP servers in your network environment; otherwise it will cause an abnormal situation.

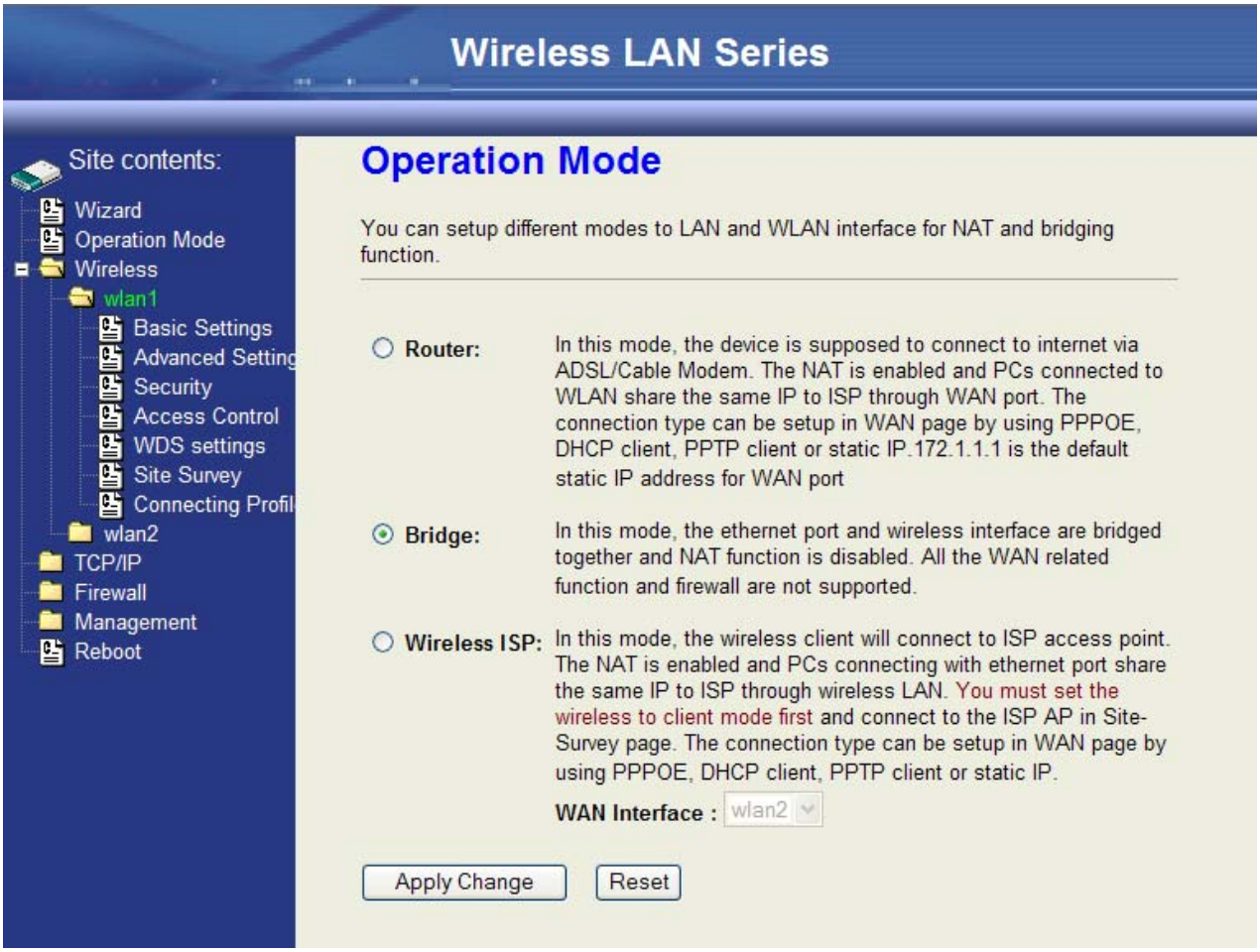
We also provide an auto-discovery tool which is used for finding out the IP of the device. In case you have forgotten the IP of the device or the IP of the device has been changed, you can use the tool to find out the IP of the device even if your PC is not in the same subnet as the device.

Operation Mode

This device can act in the following roles, and supports WDS (Wireless Distribution System) function:

- Access Point
- WDS (Wireless Repeater)
- Bridge/Router
- WISP
- AP Client

The device provides 3 different operation modes and the wireless radio of the device can act as AP/Client/WDS. The operation mode determines the communication mechanism between the wired Ethernet NIC and wireless NIC. The following are the available operation modes:



Router

In this operation mode, the wired Ethernet (WAN) port is used to connect with an ADSL/Cable modem and the wireless NIC is used for your private WLAN. The NAT is enabled between the 2 NICs, and all the wireless clients share the same public IP address through the WAN port to the ISP. The default IP configuration for the WAN port is static IP. You can access the web server of device through the default WAN IP address 172.1.1.1 and modify the setting base on your ISP requirement.

Bridge

The wired Ethernet and wireless NIC are bridged together. Once Bridge mode is selected, all the WAN related functions will be disabled.

WISP (Wireless ISP)

This mode allows the wireless NIC to act as the WAN port and the wired NIC to act as the LAN port with NAT enabled between them. To use this mode, you must first set the wireless radio to be in client mode and connect to the AP of your ISP, then you can set the WAN IP configuration to meet your ISP requirement.

The wireless radio of the device acts in the following roles.

AP (Access Point)

The wireless radio of the device serves as a communications “hub” for wireless clients and provides a connection to a wired LAN.

AP Client

This mode provides the capability to connect with another AP using infrastructure/Ad-hoc networking types. With bridge operation mode, you can directly connect the wired Ethernet port to your PC and the device becomes a wireless adapter. And with WISP operation mode, you can connect the wired Ethernet port to a hub/switch and all the PCs connecting with the hub/switch can share the same public IP address from your ISP.

WDS (Wireless Distribution System)

This mode serves as a wireless repeater; the device forwards the packets to another AP with WDS function. When this mode is selected no wireless clients can survey or connect to the device. The device only allows the WDS connection.

WDS+AP

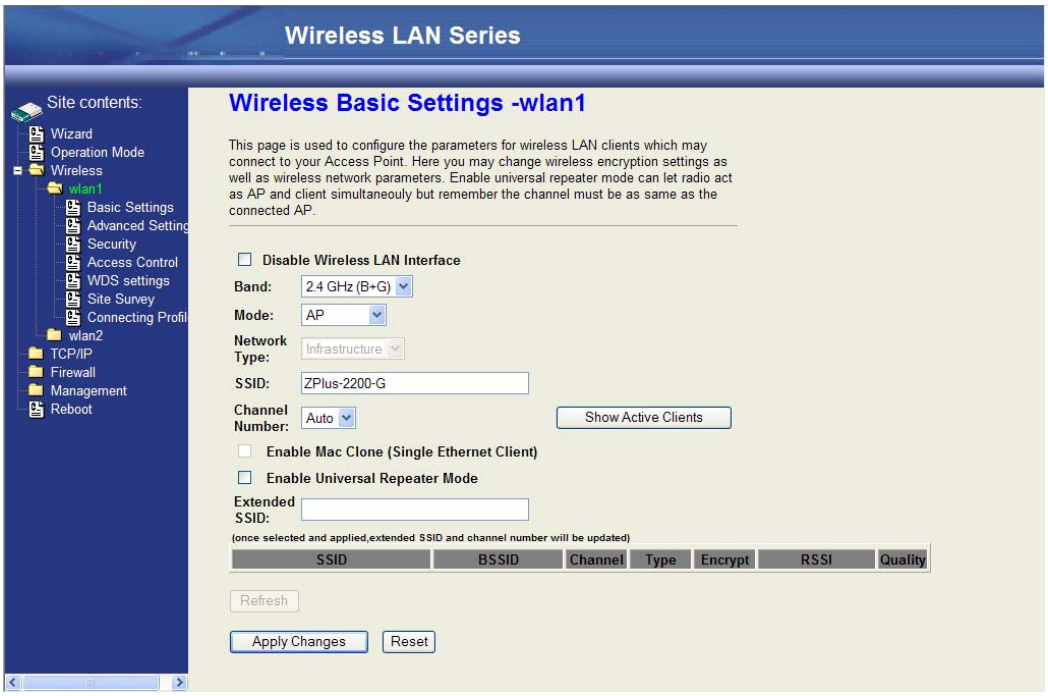
This mode combines WDS plus AP modes, it not only allows WDS connections but also allows the wireless clients to survey and connect to the device.

The following table shows the supporting combination of operation and wireless radio modes:

	Bridge	Router	WISP
AP	✓	✓	✗
WDS	✓	✓	✗
Client	✓	✗	✓
AP+WDS	✓	✓	✗

WLAN 1 Wireless Configuration

Basic Settings



Disable Wireless LAN Interface

Disable the wireless interface of device

Band

The device supports 2.4GHz(B), 2.4GHz(G) and 2.4GHz(B+G) mixed modes.

Mode

The radio of the device supports different modes as follows:

AP

The radio of the device acts as an Access Point to serves all wireless clients to join a wireless local network.

Client

Support Infrastructure and Ad-hoc network types to act as a wireless adapter.

WDS

This mode serves as a wireless repeater; the device forwards the packets to another AP with WDS function. When this mode is selected no wireless clients can survey or connect to the device. The device only allows the WDS connection.

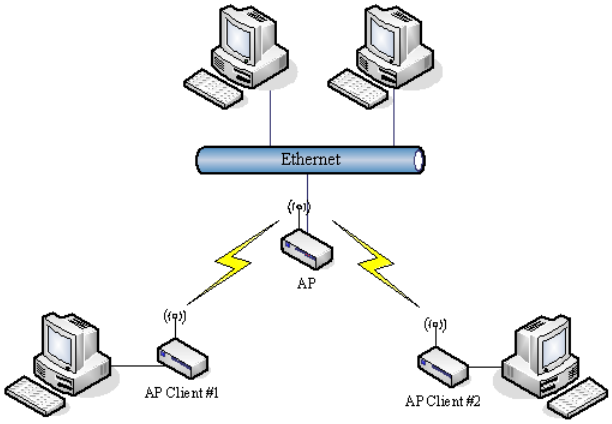
AP+WDS

This mode combines WDS plus AP modes, it not only allows WDS connections but also allows the wireless clients to survey and connect to the device.

Network Type

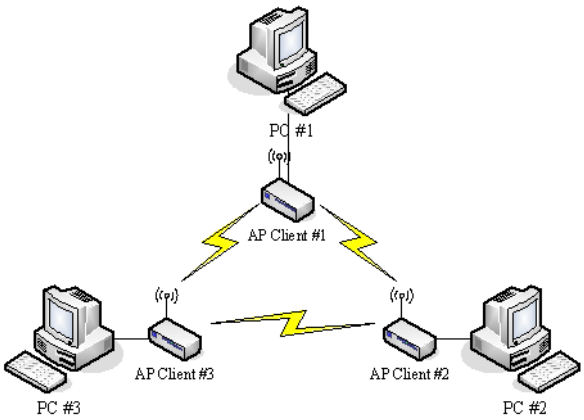
Infrastructure

This type requires the presence of 802.11b/g Access Point. All communication is done via the Access Point.



Ad Hoc

This type provides a peer-to-peer communication between wireless stations. All the communication is done from Client to Client without any Access Point involved. Ad Hoc networking must use the same SSID and channel for establishing the wireless connection.



In client mode, the device can not support the Router mode functions including Firewall and WAN settings.

SSID

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID.

Channel Number

The following table is the available frequencies (in MHz) for the 2.4-GHz radio:

Channel No.	Frequency	Country Domain
1	2412	Americas, EMEA, Japan, and China

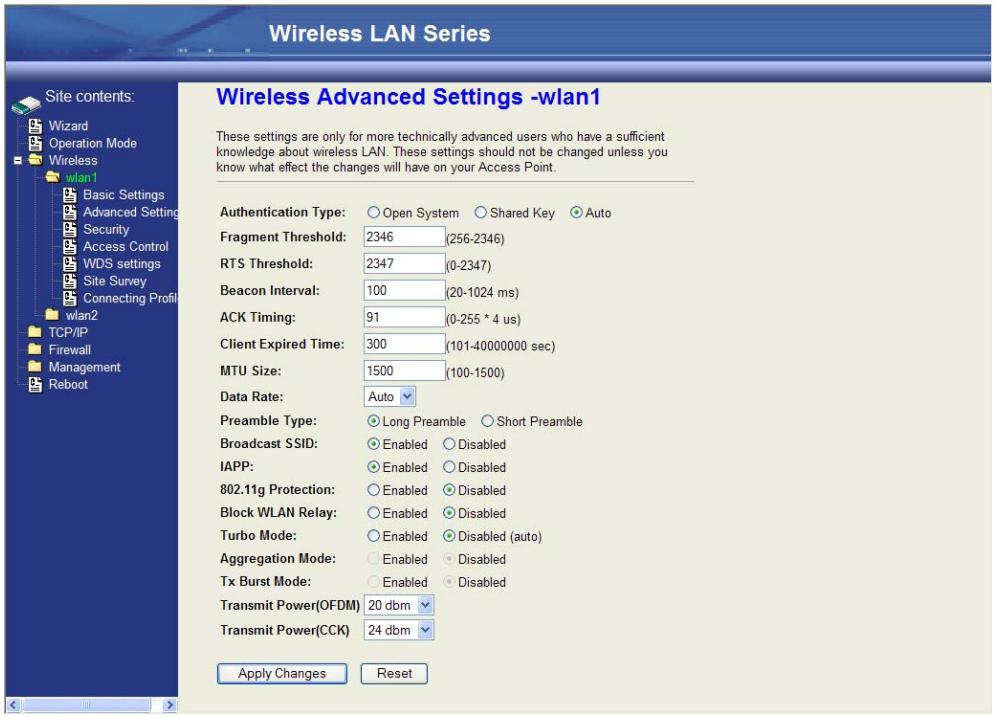
2	2417	Americas, EMEA, Japan, and China
3	2422	Americas, EMEA, Japan, Israel, and China
4	2427	Americas, EMEA, Japan, Israel, and China
5	2432	Americas, EMEA, Japan, Israel, and China
6	2437	Americas, EMEA, Japan, Israel, and China
7	2442	Americas, EMEA, Japan, Israel, and China
8	2447	Americas, EMEA, Japan, Israel, and China
9	2452	Americas, EMEA, Japan, Israel, and China
10	2457	Americas, EMEA, Japan, and China
11	2462	Americas, EMEA, Japan, and China
12	2467	EMEA and Japan only
13	2472	EMEA and Japan only
14	2484	Japan only

When set to “Auto”, the device will find the least-congested channel for use.

Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LANs. These settings should not be changed unless you know what effect the changes will have on your device. The default setting is optimized for the normal operation.

NOTE: Any unreasonable value change from the default settings will reduce the throughput of the device.



Authentication Type

The device supports two Authentication Types “Open system” and “Shared Key”. When you select “Shared Key”, you need to setup the “WEP” key in the “Security” page (See the next section). The default setting is “Auto”. The wireless client can associate with the device by using one of the two types.

Fragment Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help you to improve the network performance.

RTS Threshold

The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347 bytes.

Beacon Interval

The beacon interval is the amount of time between access point beacons in milliseconds. The default beacon interval is 100.

ACK Timing

This is the amount of time that a station will wait for the ACK response after sending a wireless frame to a remote station. This is roughly transmission time (round-trip) + processing time on the remote station and can vary depending on environment. Generally a trial and error approach is best for finding optimum timing and should only be changed on longer wireless links.

Client Expired Time

This is the amount of time that a station can be out of contact with the access point before it is removed from the association table.

MTU Size

Maximum Transmission Unit (MTU) is the largest packet size (in bytes) that a network can transmit. Any packet of larger size will be fragmented into smaller packets.

Data Rate

The standard IEEE 802.11b/11g supports 1, 2, 5.5, 11 / 6, 9, 12, 18, 24, 36, 48 and 54 Mbps data rates. You can choose the rate that the device uses for data transmission. The default value is “auto”. The device will use the highest possible selected transmission rate.

Preamble Type

The preamble is part of the 802.11 frame and is PHY dependant. All 802.11b/g systems support the long preamble. The short preamble (optional) maybe used to improve throughput when all stations on the network support the short preamble.

Broadcast SSID

Broadcasting the SSID will let your wireless clients find the device automatically. If you are building a public Wireless Network, disabling this function can provide better security. Every wireless station located within the coverage of the device must connect to this device by manually configuring the SSID in your client settings.

IAPP

(802.11f) This provides a mechanism for association data (e.g. encryption settings, station information, etc.) to be handed off to a new AP when a station roams between APs.

802.11g Protection

This ensures that 802.11g stations are backwards compatible with legacy 802.11b stations. With 802.11g protection enabled, a CTS will be used to lock out 802.11b stations while the 802.11g station is transmitting. While this does allow backwards compatibility with legacy 802.11b stations, it should be disabled in a pure 802.11g environment, as it will have a significant impact on 802.11g performance (as high as 50% decrease in throughput).

Block WLAN Relay (Isolate Client)

The device supports an isolation function. If you are building a public Wireless Network, enabling this function can provide better security. The device will block packets between wireless clients (relay). The wireless clients connected to the device cannot see each other.

Turbo Mode

This allows two Realtek (802.11b/g chipset in the DLB70xx) stations to transmit at 72Mbps between each other. Note this is Realtek proprietary and will only function between Realtek stations.

Aggregation Mode

Not applicable for WLAN 1.

Tx Burst Mode

Not applicable for WLAN 1.

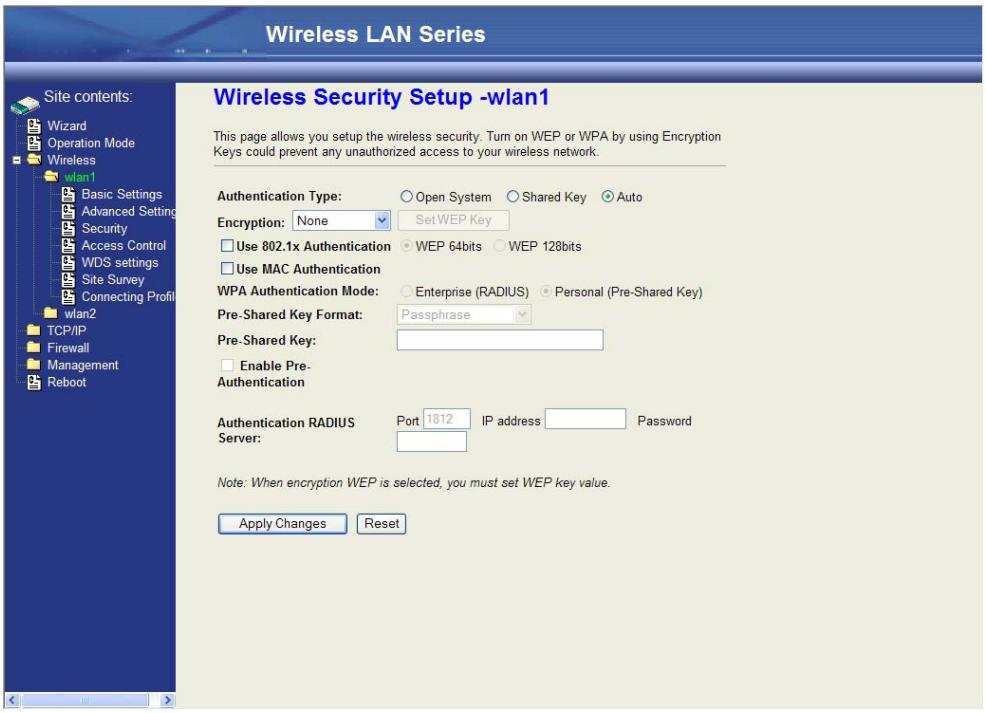
Transmit Power

The device supports four transmission output power levels 250, 200, 150 and 100mW for CCK (802.11b) mode and two transmission output power levels 100 and 50mW for OFDM (802.11g) mode. You can adjust the power level to change the coverage of the device. Every wireless station located within the coverage of the device also needs to have the high power radio. Otherwise the wireless station can only survey the device and cannot establish a connection with device.

Security

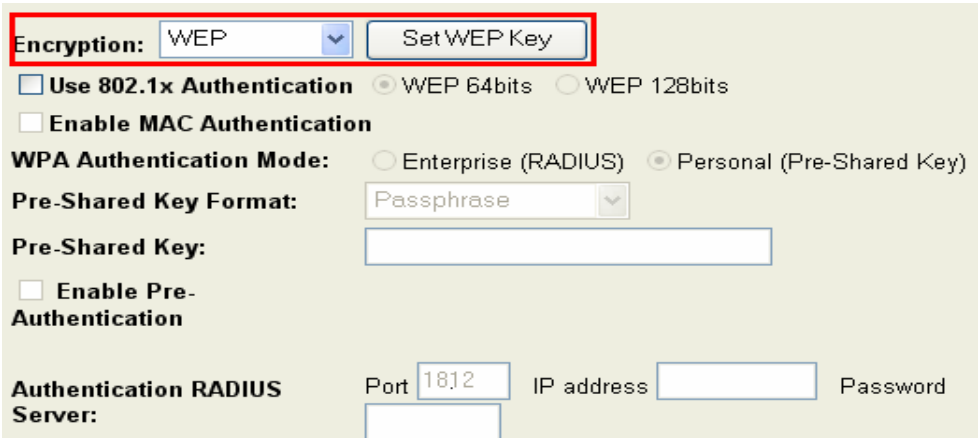
This device provides complete wireless security function include WEP, 802.1x, WPA-TKIP, WPA2-AES and WPA2-Mixed in different mode (see the Security Support Table).

The default security setting of the encryption function is disabled. Choose your preferred security setting depending on what security function you need.



Encryption

Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be the same as each client in your wireless network. For more secure data transmission, you can change the encryption type to “WEP” and click the “Set WEP Key” button to open the “Wireless WEP Key setup” page.

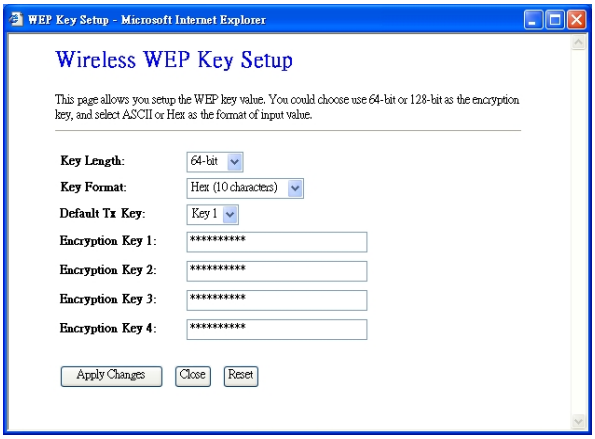


When you decide to use the WEP encryption to secure your WLAN, please refer to the following settings of the WEP encryption:

- 64-bit WEP Encryption: 64-bit WEP keys are as same as the encryption method of 40-bit WEP. You can input 10 hexadecimal digits (0~9, a~f or A~F) or 5 ACSII chars.

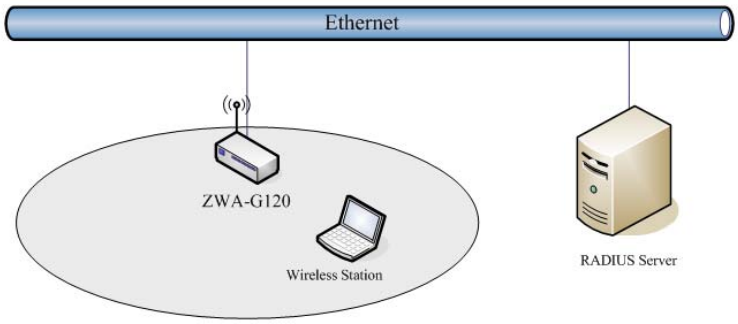
- 128-bit WEP Encryption:128-bit WEP keys are as same as the encryption method of 104-bit WEP. You can input 26 hexadecimal digits (0~9, a~f or A~F) or 10 ACSII chars.

The Default Tx Key field determines which of the four keys you want to use in your WLAN environment.

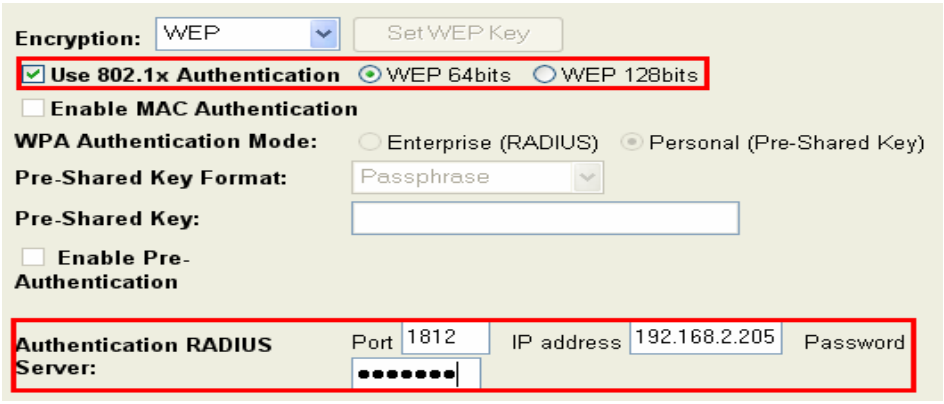


WEP Encryption with 802.1x Setting

The device supports an external RADIUS Server that can secure networks against unauthorized access. If you use the WEP encryption, you can also use the RADIUS server to check the admission of the users. In this way every user must use a valid account before accessing the Wireless LAN and requires a RADIUS or other authentication server on the network. An example is shown as follows:



You should choose WEP 64 or 128 bit encryption based on your current network requirements. Then add user accounts and the target device to the RADIUS server. In the device, you need to specify the IP address, Password (Shared Secret) and Port number of the target RADIUS server.



WPA Authentication Mode

The WPA feature provides a high level of assurance for end-users and administrators that their data will remain private and that access to their network is restricted to authorized users. You can choose the WPA encryption and select the Authentication Mode. This device supports two WPA modes:

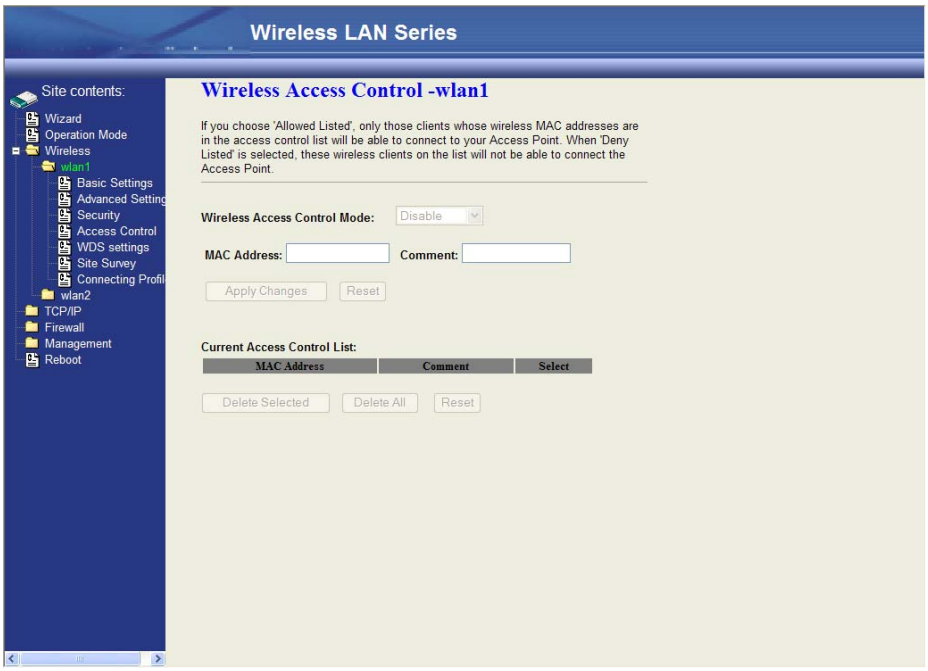
Enterprise (RADIUS)

In this mode authentication is achieved via a WPA RADIUS Server. You need a RADIUS or other authentication server on the network. When WPA Authentication mode is Enterprise (RADIUS), you have to add user accounts and the target device to the RADIUS Server. In the device, you need to specify the IP address Password (Shared Secret) and Port number of the target RADIUS server.

Pre-Share Key

In this mode you can use the Pre-shared Key to enhance your security setting. This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be the same as each wireless client in your wireless network. When the Key format is Passphrase, the key value should have 8~63 ACSII chars. When Key format is Hex, the key value should have 64 hexadecimal digits (0~9, a~f or A~F).

Access Control



WDS Settings

Wireless Distribution System (WDS) uses wireless media to communicate with the other devices, like the Ethernet does. This function allows one or more remote LANs to connect with the local LAN. To do this, you must set these devices in the same channel and set the MAC address of other devices you want to communicate with in the WDS AP List and then enable the WDS.

When you decide to use the WDS to extend your WLAN, please refer to the following instructions for configuration:

- The bridging devices by WDS must use the same radio channel.
- When the WDS function is enabled, no wireless stations can connect to the device.

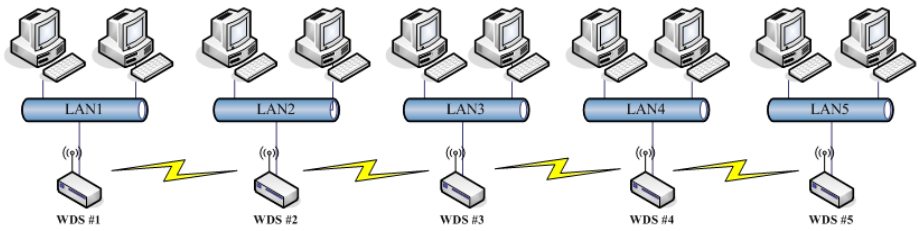
- If your network topology has a loop, you need to enable the 802.1d Spanning Tree function.
- You don't need to add all MAC address of devices existing in your network to the WDS AP List. The WDS AP List only needs to specify the MAC address of devices you need to directly connect to.
- The bandwidth of the device is limited. Bandwidth will be shared between bridging devices.

WDS Network Topology

In this section, we will demonstrate the WDS network topologies and WDS AP List configuration. You can setup four kinds of network topologies: bus, star, ring and mesh.

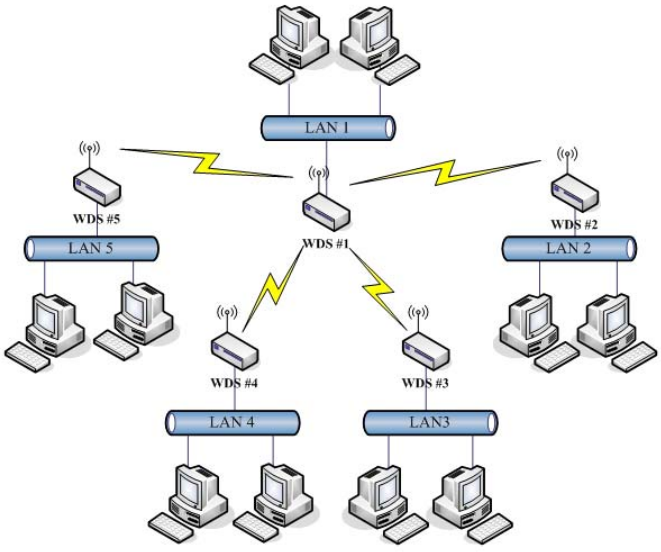
In this case, there are five devices with WDS enabled: WDS1, WDS2, WDS3, WDS4 and WDS5.

Bus topology



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Address of WDS2	No
WDS2	The MAC Addresses of WDS1 and WDS3	No
WDS3	The MAC Addresses of WDS2 and WDS4	No
WDS4	The MAC Addresses of WDS3 and WDS5	No
WDS5	The MAC Address of WDS4	No

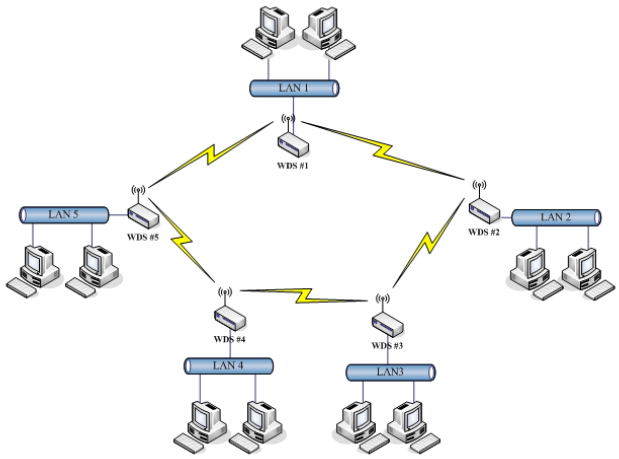
Star topology



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	No

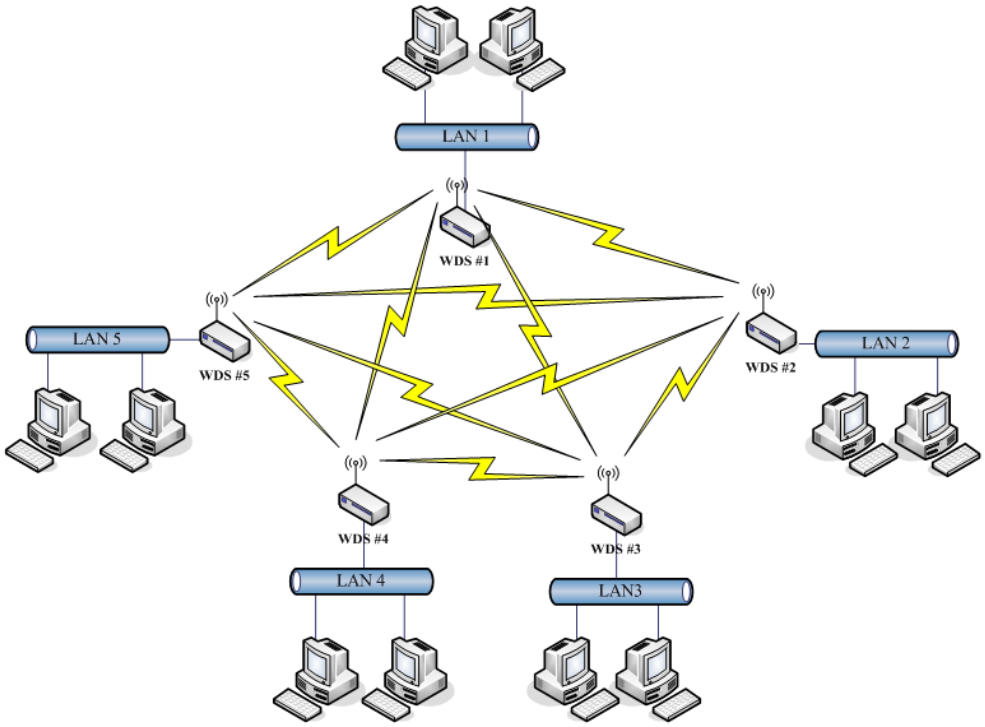
WDS2	The MAC Address of WDS1	No
WDS3	The MAC Address of WDS1	No
WDS4	The MAC Address of WDS1	No
WDS5	The MAC Address of WDS1	No

Ring topology



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2 and WDS5	Yes
WDS2	The MAC Addresses of WDS1 and WDS3	Yes
WDS3	The MAC Addresses of WDS2 and WDS4	Yes
WDS4	The MAC Addresses of WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS4 and WDS1	Yes

Mesh topology



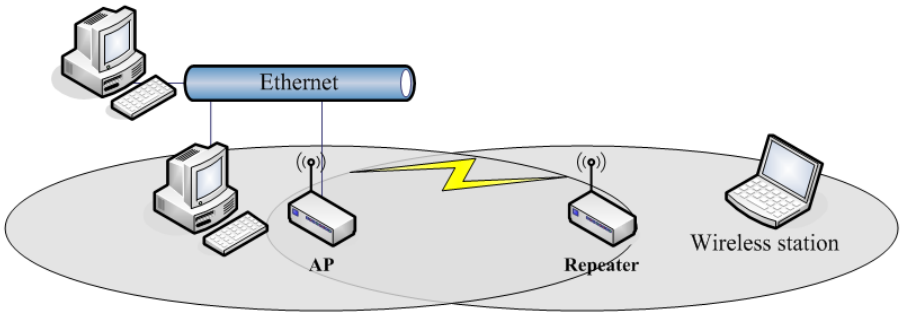
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	Yes
WDS2	The MAC Addresses of WDS1, WDS3, WDS4 and WDS5	Yes
WDS3	The MAC Addresses of WDS1, WDS2, WDS4 and WDS5	Yes
WDS4	The MAC Addresses of WDS1, WDS2, WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS1, WDS2, WDS3 and WDS4	Yes

Wireless Repeater

A Wireless Repeater can be used to increase the coverage area of another device (Parent AP). Between the Parent AP and the Wireless Repeater, wireless stations can move among the coverage areas of both devices. When you decide to use the WDS as a Repeater, please refer to the following instructions for configuration.

In AP mode, enable the WDS function. You must set these connected devices with the same radio channel and SSID. Choose “WDS+AP” mode.

Using the bus or star network topology:



Description	Entries of WDS AP List	Spanning Tree Protocol Required
Access Point	The MAC Address of Repeater	Yes
Repeater	The MAC Address of Access Point	Yes

Wireless Bridge

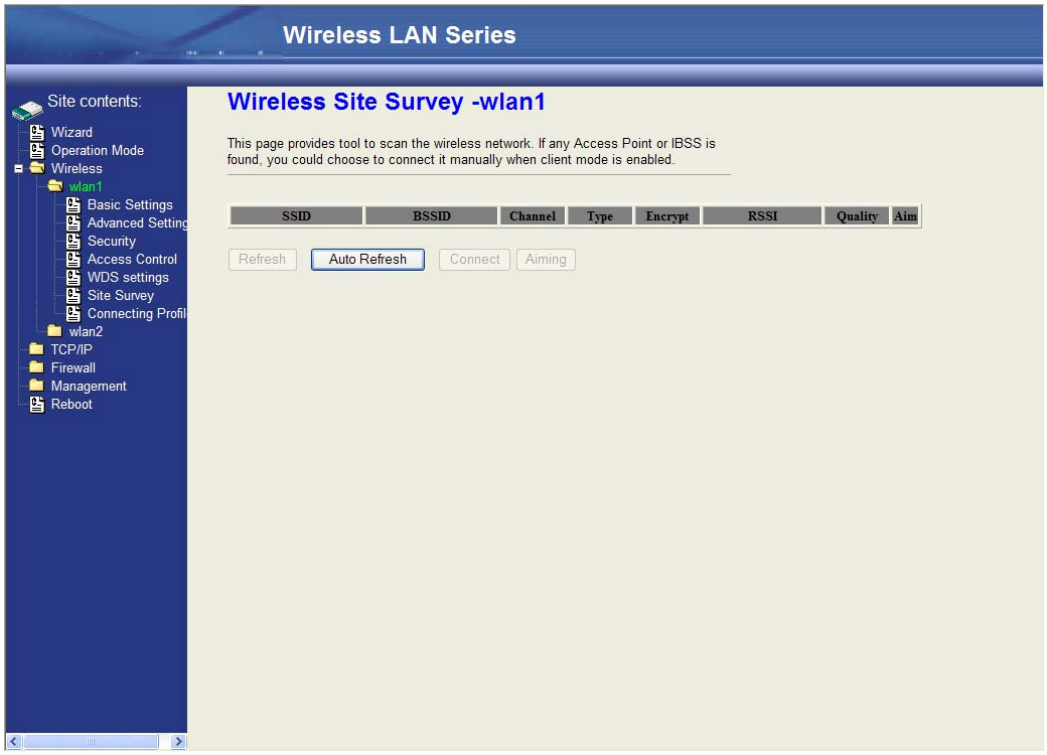
As a Wireless Bridge the device can establish a wireless connection between two or more Wired LANs. When you decide to use the WDS as a Wireless Bridge, please refer the following instructions for configuration.

In AP mode, enable the WDS function. You must set these connected devices to the same radio channel, but you may use different SSID.

Choose “WDS” mode for only wireless backbone extension purpose. You can use any network topology, please refer the WDS topology section.

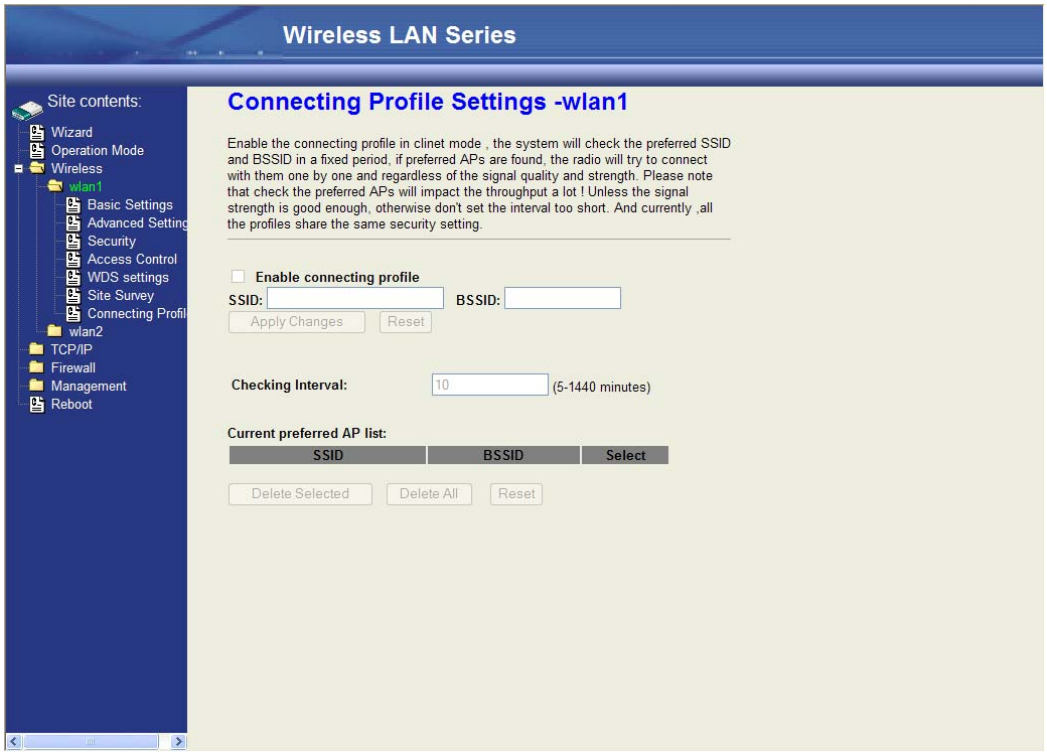
Site Survey

This tool allows you to scan for nearby wireless networks. If any Access Point or IBSS is found, you can choose to connect it manually when client mode is enabled.



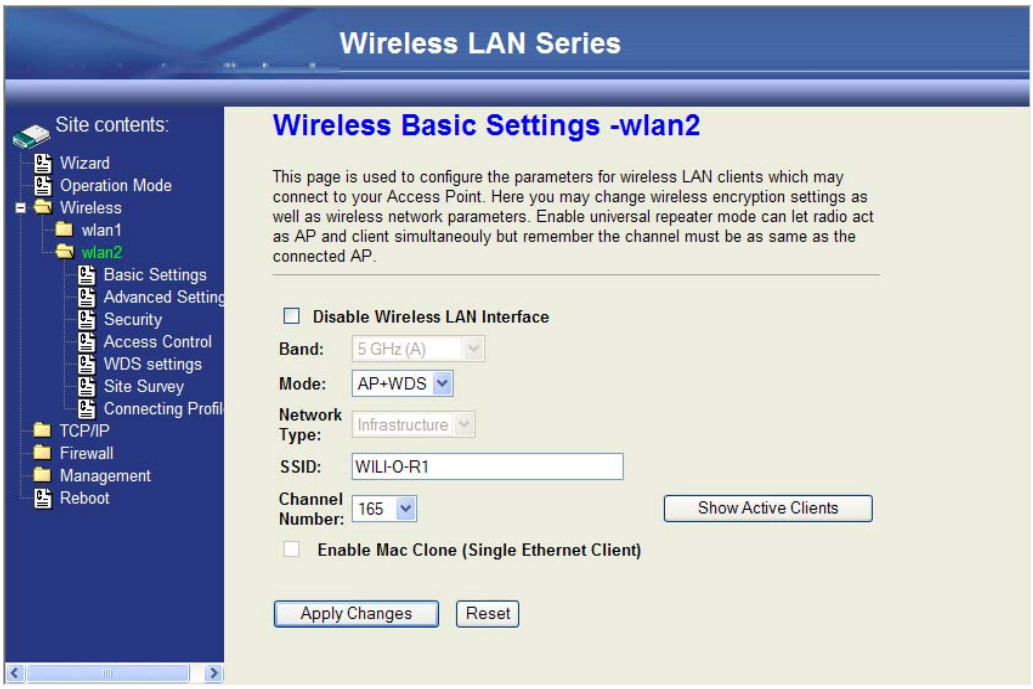
Connecting Profile

If you enable the connecting profile in client mode, the system will check the preferred SSID and BSSID in a fixed period. If preferred APs are found, the radio will try to connect to them one by one regardless of the signal quality and strength. Please note that checking the preferred APs will have a significant impact on throughput. All the profiles share the same security settings.


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
wlan1
Basic Settings
Advanced Setting
Security
Access Control
WDS settings
Site Survey
Connecting Profil
wlan2
TCP/IP
Firewall
Management
Reboot
Connecting Profile Settings -wlan1
Enable the connecting profile in clinet mode , the system will check the preferred SSID and BSSID in a fixed period, if preferred APs are found, the radio will try to connect with them one by one and regardless of the signal quality and strength. Please note that check the preferred APs will impact the throughput a lot ! Unless the signal strength is good enough, otherwise don't set the interval too short. And currently ,all the profiles share the same security setting.
Enable connecting profile
SSID:
BSSID:
Apply Changes
Reset
Checking Interval:
10
(5-1440 minutes)
Current preferred AP list:
SSID
BSSID
Select
Delete Selected
Delete All
Reset

WLAN 2 Wireless Configuration

Basic Settings



Disable Wireless LAN Interface

Disable the wireless interface of device

Band

The device supports 2.4GHz(B), 2.4GHz(G) and 2.4GHz(B+G) mixed modes.

Mode

The radio of the device supports different modes as follows:

AP

The radio of the device acts as an Access Point to serves all wireless clients to join a wireless local network.

Client

Support Infrastructure and Ad-hoc network types to act as a wireless adapter.

WDS

This mode serves as a wireless repeater; the device forwards the packets to another AP with WDS function. When this mode is selected no wireless clients can survey or connect to the device. The device only allows the WDS connection.

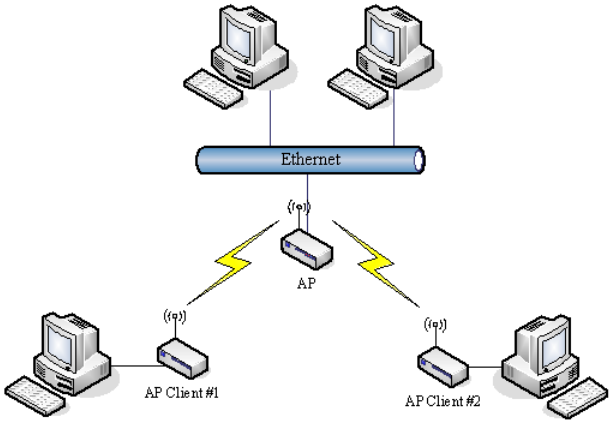
AP+WDS

This mode combines WDS plus AP modes, it not only allows WDS connections but also allows the wireless clients to survey and connect to the device.

Network Type

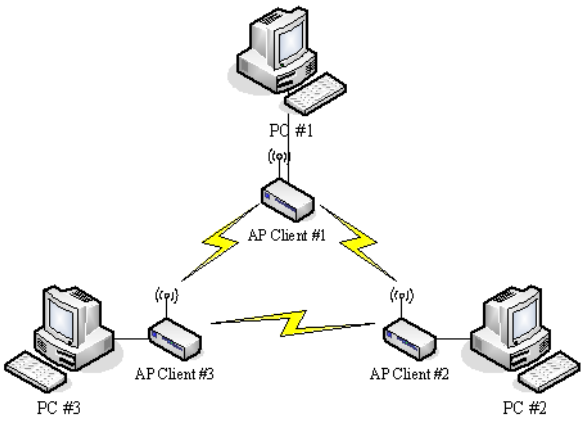
Infrastructure

This type requires the presence of 802.11b/g Access Point. All communication is done via the Access Point.



Ad Hoc

This type provides a peer-to-peer communication between wireless stations. All the communication is done from Client to Client without any Access Point involved. Ad Hoc networking must use the same SSID and channel for establishing the wireless connection.



In client mode, the device can not support the Router mode functions including Firewall and WAN settings.

SSID

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID.

Channel Number

The following table is the available frequencies (in MHz) for the 5-GHz radio:

Channel Identifier	Frequency in MHz	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)

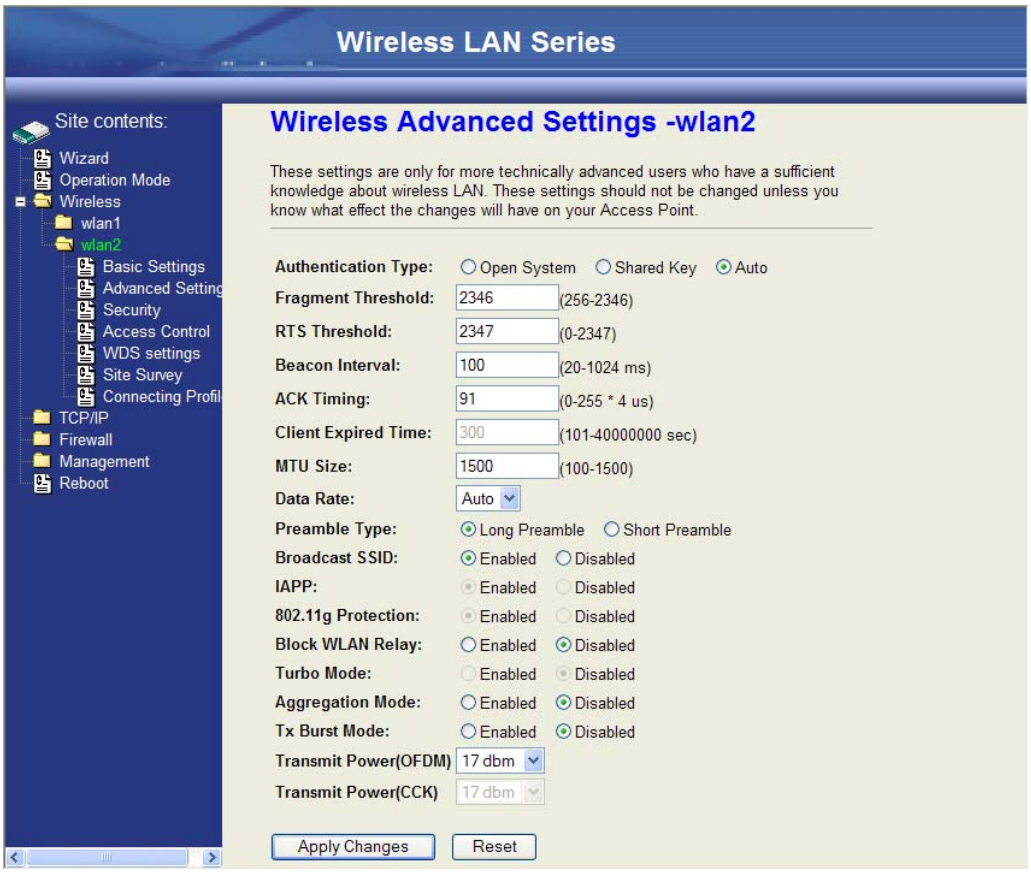
34	5170		✓		
36	5180	✓		✓	
38	5190		✓		
40	5200			✓	
42	5210		✓		
44	5220	✓		✓	
46	5230		✓		
48	5240	✓		✓	
52	5260	✓			✓
56	5280	✓			✓
60	5300	✓			✓
64	5320	✓			✓
149	5745	✓			
153	5765	✓			
157	5785	✓			
161	5805	✓			

When set to “Auto”, the device will find the least-congested channel for use.

Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LANs. These settings should not be changed unless you know what effect the changes will have on your device. The default setting is optimized for the normal operation.

NOTE: Any unreasonable value change from the default settings will reduce the throughput of the device.



Authentication Type

The device supports two Authentication Types “Open system” and “Shared Key”. When you select “Shared Key”, you need to setup the “WEP” key in the “Security” page (See the next section). The default setting is “Auto”. The wireless client can associate with the device by using one of the two types.

Fragment Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help you to improve the network performance.

RTS Threshold

The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347

bytes.

Beacon Interval

The beacon interval is the amount of time between access point beacons in milliseconds. The default beacon interval is 100.

ACK Timing

This is the amount of time that a station will wait for the ACK response after sending a wireless frame to a remote station. This is roughly transmission time (round-trip) + processing time on the remote station and can vary depending on environment. Generally a trial and error approach is best for finding optimum timing and should only be changed on longer wireless links.

Client Expired Time

This is the amount of time that a station can be out of contact with the access point before it is removed from the association table.

MTU Size

Maximum Transmission Unit (MTU) is the largest packet size (in bytes) that a network can transmit. Any packet of larger size will be fragmented into smaller packets.

Data Rate

The standard IEEE 802.11b/11g supports 1, 2, 5.5, 11 / 6, 9, 12, 18, 24, 36, 48 and 54 Mbps data rates. You can choose the rate that the device uses for data transmission. The default value is “auto”. The device will use the highest possible selected transmission rate.

Preamble Type

The preamble is part of the 802.11 frame and is PHY dependant. All 802.11b/g systems support the long preamble. The short preamble (optional) maybe used to improve throughput when all stations on the network support the short preamble.

Broadcast SSID

Broadcasting the SSID will let your wireless clients find the device automatically. If you are building a public Wireless Network, disabling this function can provide better security. Every wireless station located within the coverage of the device must connect to this device by manually configuring the SSID in your client settings.

IAPP

(802.11f) This provides a mechanism for association data (e.g. encryption settings, station information, etc.) to be handed off to a new AP when a station roams between APs.

802.11g Protection

This ensures that 802.11g stations are backwards compatible with legacy 802.11b stations. With 802.11g protection enabled, a CTS will be used to lock out 802.11b stations while the 802.11g station is transmitting. While this does allow backwards compatibility with legacy 802.11b stations, it should be disabled in a pure 802.11g environment, as it will have a significant impact on 802.11g performance (as high as 50% decrease in throughput).

Block WLAN Relay (Isolate Client)

The device supports an isolation function. If you are building a public Wireless Network, enabling this function can provide better security. The device will block packets between wireless clients (relay). The wireless clients connected to the device cannot see each other.

Turbo Mode

Not applicable for WLAN 2.

Aggregation Mode

This is a proprietary Ralink (802.11a chipset in the DLB70xx) aggregation setting that allows for jumbo frames consisting of multiple smaller frames that increases throughput between Ralink stations.

Tx Burst Mode

This is a proprietary Ralink (802.11a chipset in the DLB70xx) burst setting and allows very small networks (1~3 clients) to transmit at higher speeds. In larger networks, this will result in degraded performance.

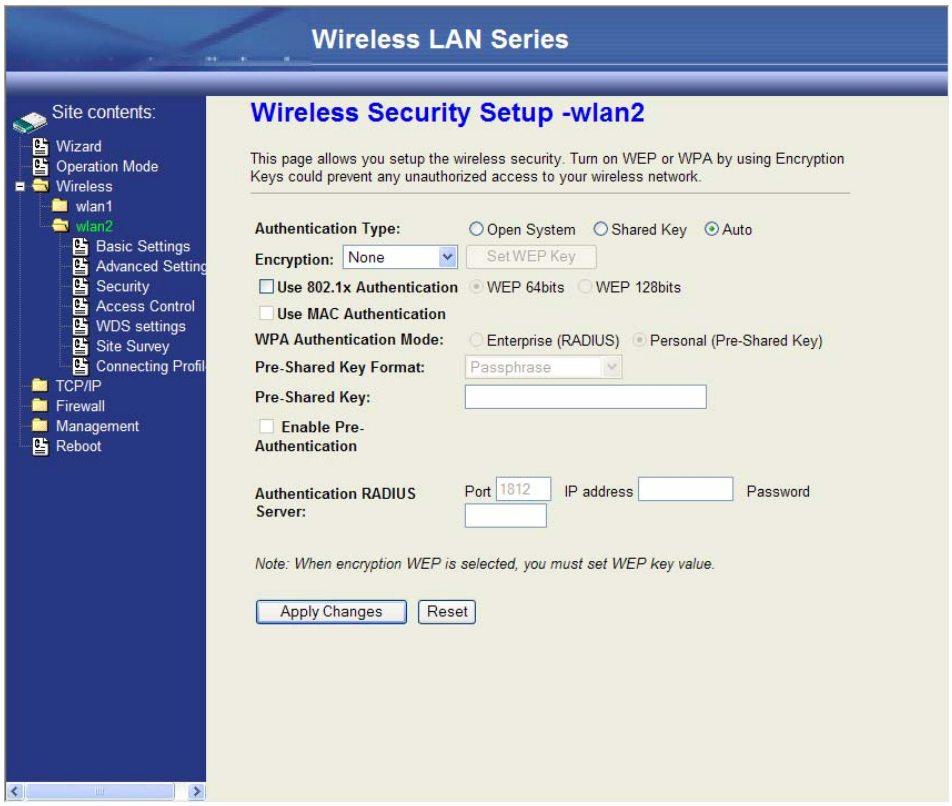
Transmit Power

The device supports four transmission output power levels 250, 200, 150 and 100mW for CCK (802.11b) mode and two transmission output power levels 100 and 50mW for OFDM (802.11g) mode. You can adjust the power level to change the coverage of the device. Every wireless station located within the coverage of the device also needs to have the high power radio. Otherwise the wireless station can only survey the device and cannot establish a connection with device.

Security

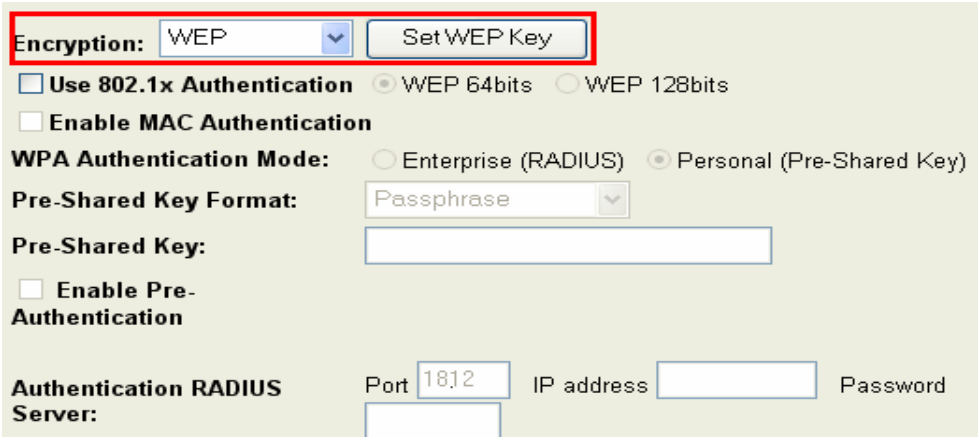
This device provides complete wireless security function include WEP, 802.1x, WPA-TKIP, WPA2-AES and WPA2-Mixed in different mode (see the Security Support Table).

The default security setting of the encryption function is disabled. Choose your preferred security setting depending on what security function you need.



Encryption

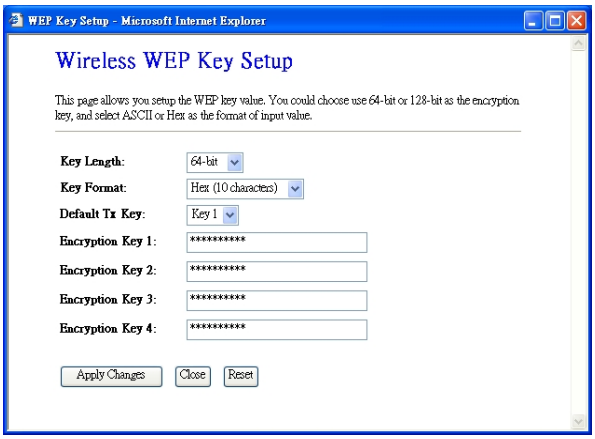
Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be the same as each client in your wireless network. For more secure data transmission, you can change the encryption type to “WEP” and click the “Set WEP Key” button to open the “Wireless WEP Key setup” page.



When you decide to use the WEP encryption to secure your WLAN, please refer to the following settings of the WEP encryption:

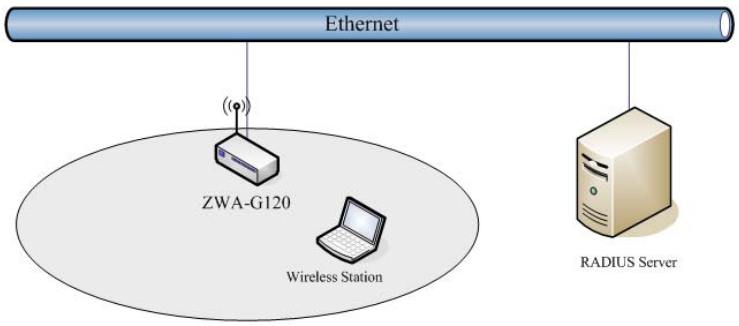
- 64-bit WEP Encryption: 64-bit WEP keys are as same as the encryption method of 40-bit WEP. You can input 10 hexadecimal digits (0~9, a~f or A~F) or 5 ACSII chars.
- 128-bit WEP Encryption:128-bit WEP keys are as same as the encryption method of 104-bit WEP. You can input 26 hexadecimal digits (0~9, a~f or A~F) or 10 ACSII chars.

The Default Tx Key field determines which of the four keys you want to use in your WLAN environment.

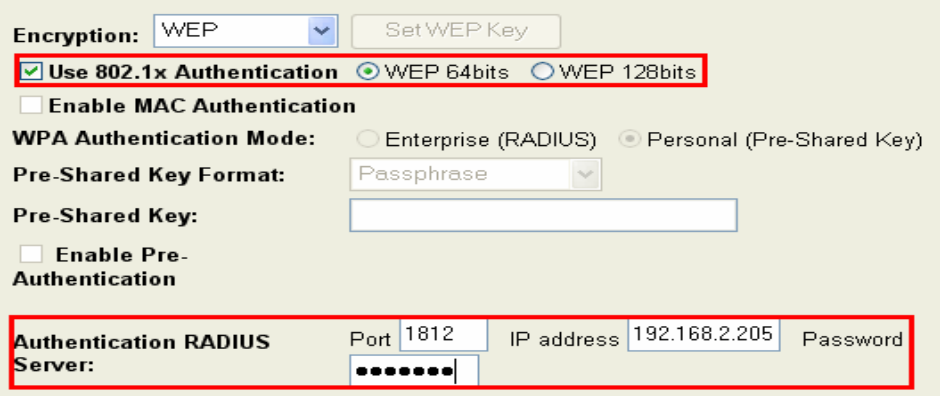


WEP Encryption with 802.1x Setting

The device supports an external RADIUS Server that can secure networks against unauthorized access. If you use the WEP encryption, you can also use the RADIUS server to check the admission of the users. In this way every user must use a valid account before accessing the Wireless LAN and requires a RADIUS or other authentication server on the network. An example is shown as follows:



You should choose WEP 64 or 128 bit encryption based on your current network requirements. Then add user accounts and the target device to the RADIUS server. In the device, you need to specify the IP address, Password (Shared Secret) and Port number of the target RADIUS server.



WPA Authentication Mode

The WPA feature provides a high level of assurance for end-users and administrators that their data will remain private and that access to their network is restricted to authorized users. You can choose the WPA encryption and select the Authentication Mode. This device supports two WPA modes:

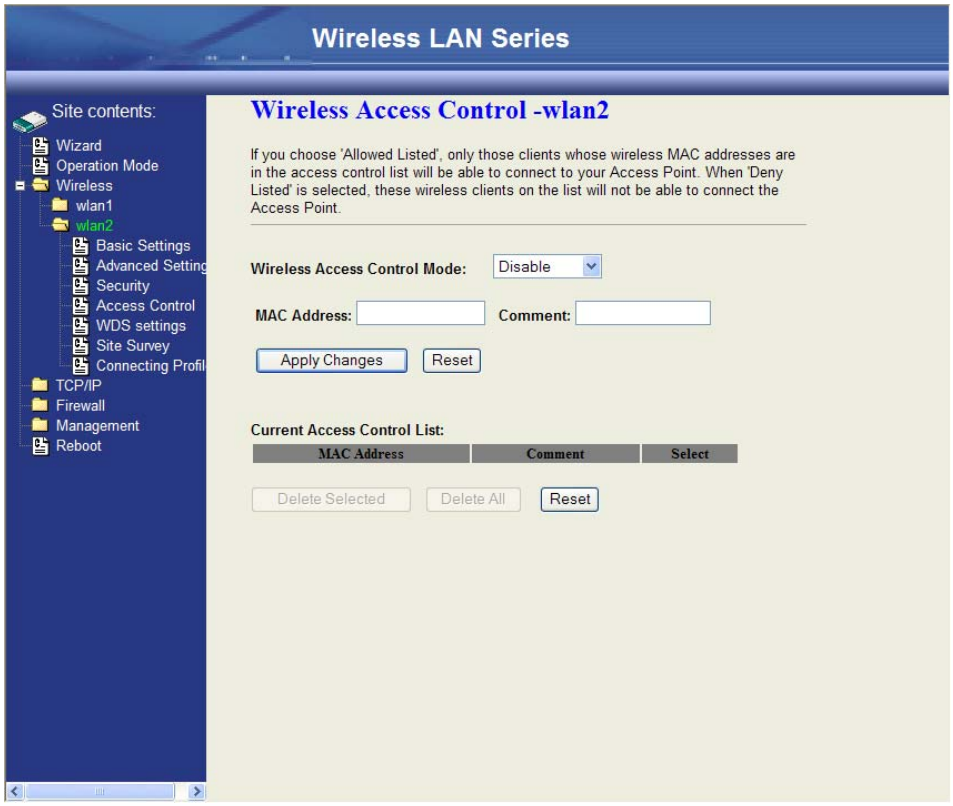
Enterprise (RADIUS)

In this mode authentication is achieved via a WPA RADIUS Server. You need a RADIUS or other authentication server on the network. When WPA Authentication mode is Enterprise (RADIUS), you have to add user accounts and the target device to the RADIUS Server. In the device, you need to specify the IP address Password (Shared Secret) and Port number of the target RADIUS server.

Pre-Share Key

In this mode you can use the Pre-shared Key to enhance your security setting. This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be the same as each wireless client in your wireless network. When the Key format is Passphrase, the key value should have 8~63 ACSII chars. When Key format is Hex, the key value should have 64 hexadecimal digits (0~9, a~f or A~F).

Access Control



WDS Settings

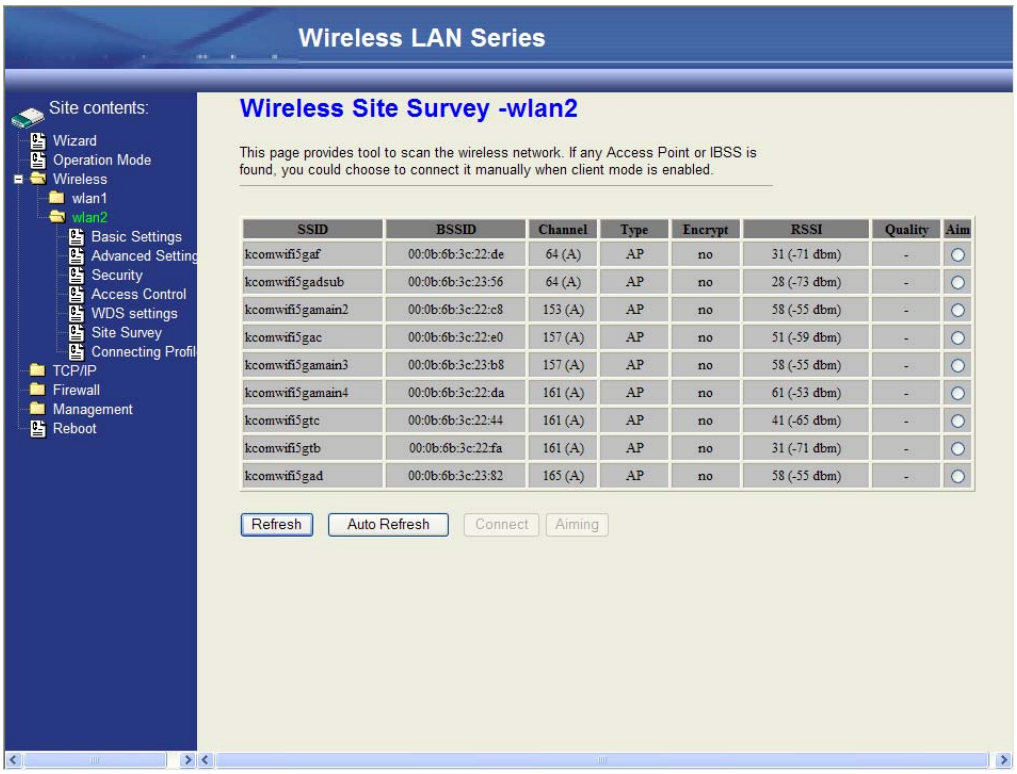
Wireless Distribution System (WDS) uses wireless media to communicate with the other devices, like the Ethernet does. This function allows one or more remote LANs to connect with the local LAN. To do this, you must set these devices in the same channel and set the MAC address of other devices you want to communicate with in the WDS AP List and then enable the WDS.

When you decide to use the WDS to extend your WLAN, please refer to the following instructions for configuration:

- The bridging devices by WDS must use the same radio channel.
- When the WDS function is enabled, no wireless stations can connect to the device.
- If your network topology has a loop, you need to enable the 802.1d Spanning Tree function.
- You don't need to add all MAC address of devices existing in your network to the WDS AP List. The WDS AP List only needs to specify the MAC address of devices you need to directly connect to.
- The bandwidth of the device is limited. Bandwidth will be shared between bridging devices.

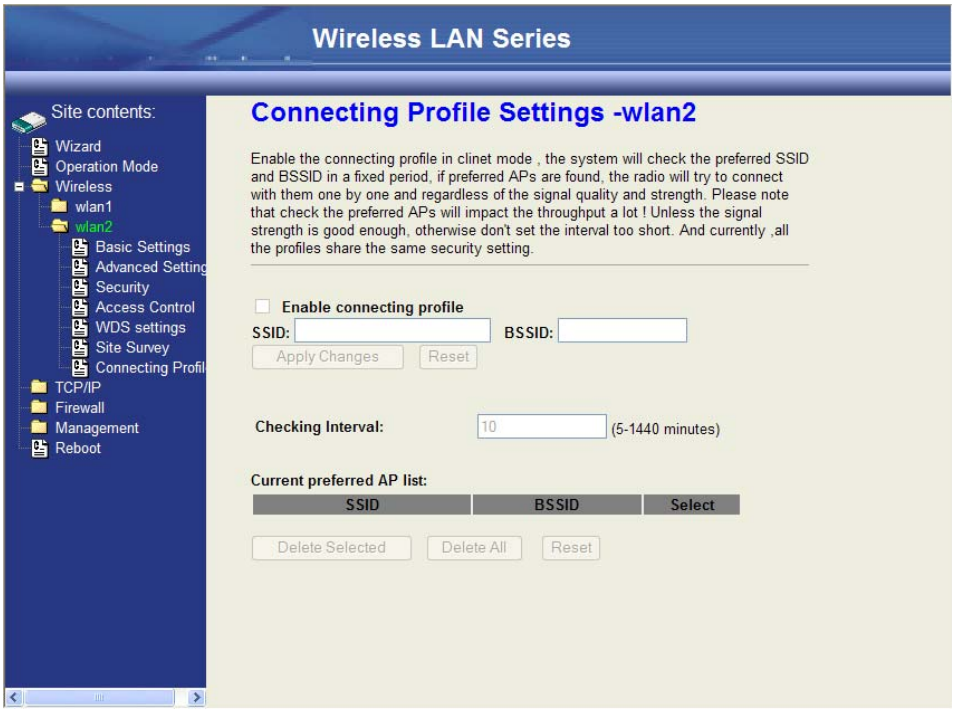
Site Survey

This tool allows you to scan for nearby wireless networks. If any Access Point or IBSS is found, you can choose to connect it manually when client mode is enabled.



Connecting Profile

If you enable the connecting profile in client mode, the system will check the preferred SSID and BSSID in a fixed period. If preferred APs are found, the radio will try to connect to them one by one regardless of the signal quality and strength. Please note that checking the preferred APs will have a significant impact on throughput. All the profiles share the same security settings.



TCP/IP Configuration

Configuring LAN Interface

Configuring DHCP Server

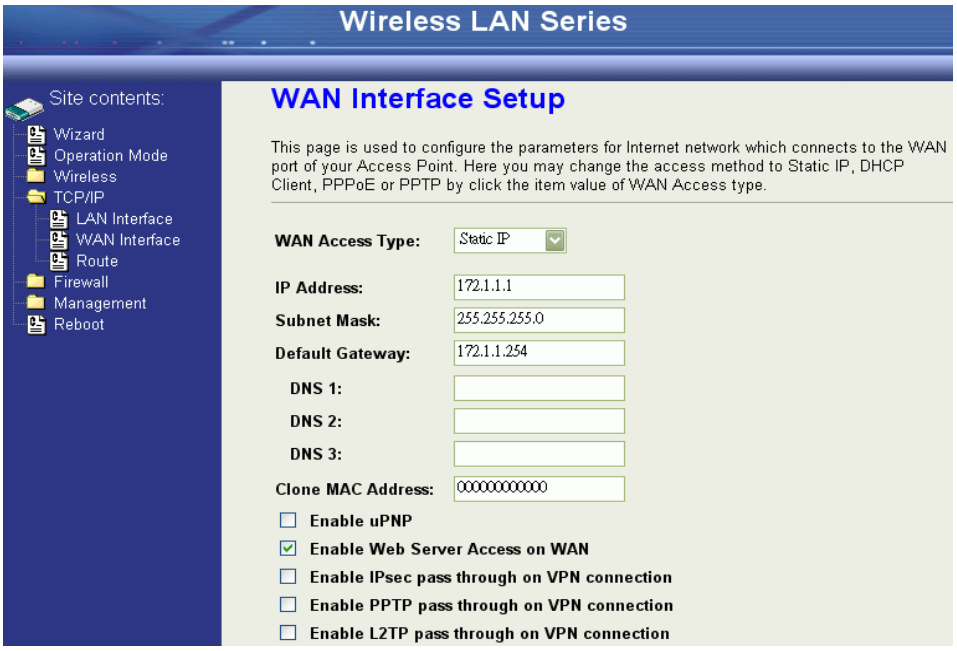
To use the DHCP server inside the device, please make sure there is no other DHCP server that exists in the same network as the device.

Enable the DHCP Server option and assign the client range of IP addresses as shown in the following page.

When the DHCP server is enabled and also the device router mode is enabled then the default gateway for all the DHCP client hosts will be set to the IP address of device.

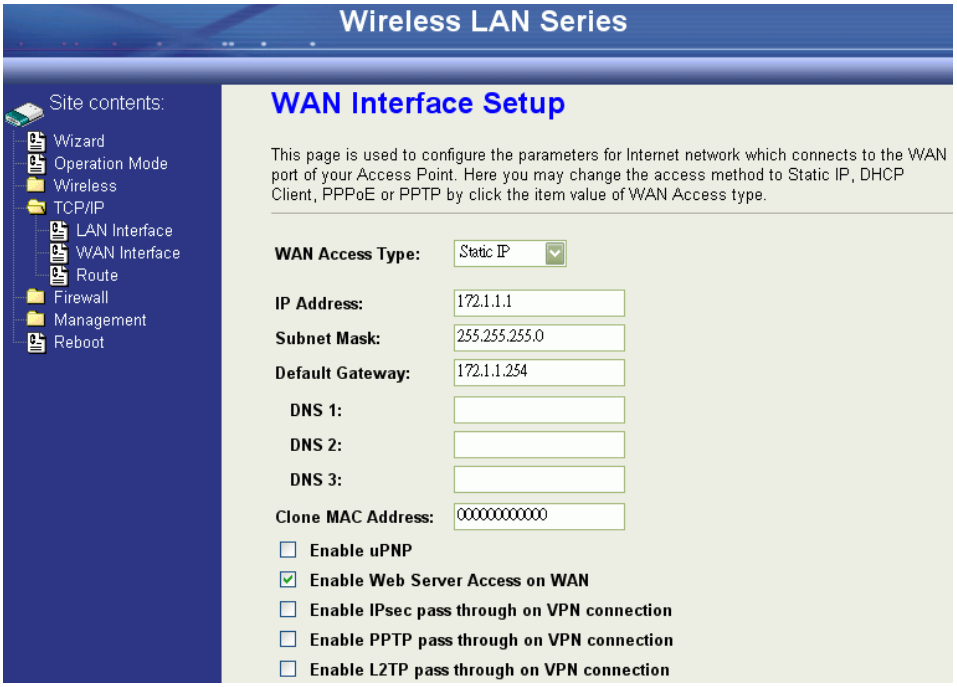
Configuring WAN Interface

The device supports four kinds of IP configuration for WAN interface, including Static IP, DHCP Client, PPPoE and PPTP. You can select one of the WAN Access Types depending on the requirements of your ISP. The default WAN Access Type is “Static IP”.



Static IP

You can get the IP configuration data of the Static-IP from your ISP. You will need to fill in IP address, subnet mask, gateway address, and one of the DNS addresses.

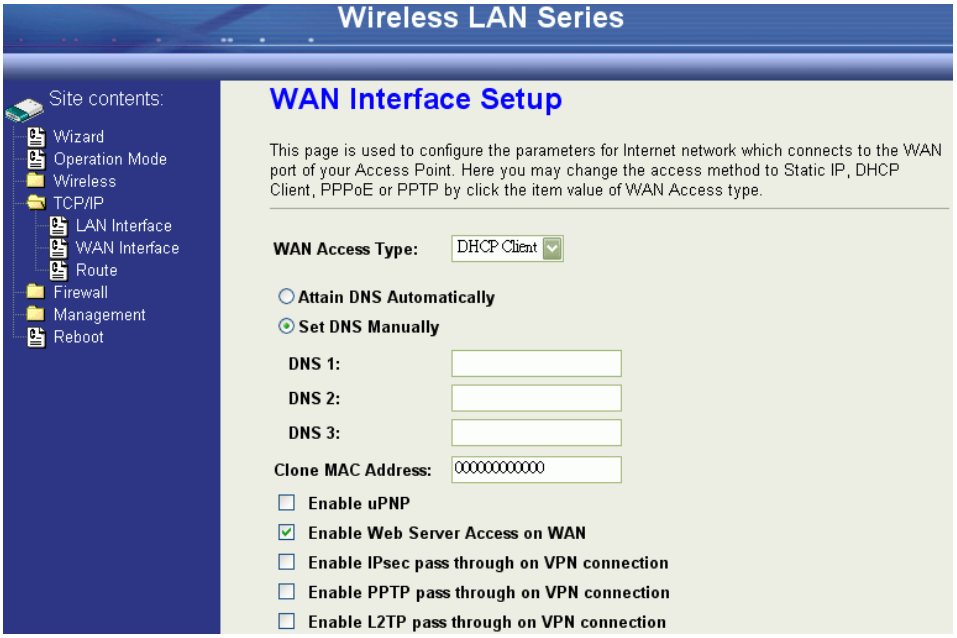


IP Address	The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier outside of your local network.
Subnet Mask	The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

Default Gateway	The IP address of Default Gateway provided by your ISP or MIS. The Default Gateway is the intermediate network device that has knowledge of the network IDs of the other networks in the Wide Area Network, so it can forward the packets to other gateways until they are delivered to the one connected to the specified destination.
DNS 1~3	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. The DNS maintains central lists of domain name/IP addresses and maps the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address	Clone device MAC address to the specific MAC address required by your ISP.
Enable uPnP	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

DHCP Client (Dynamic IP)

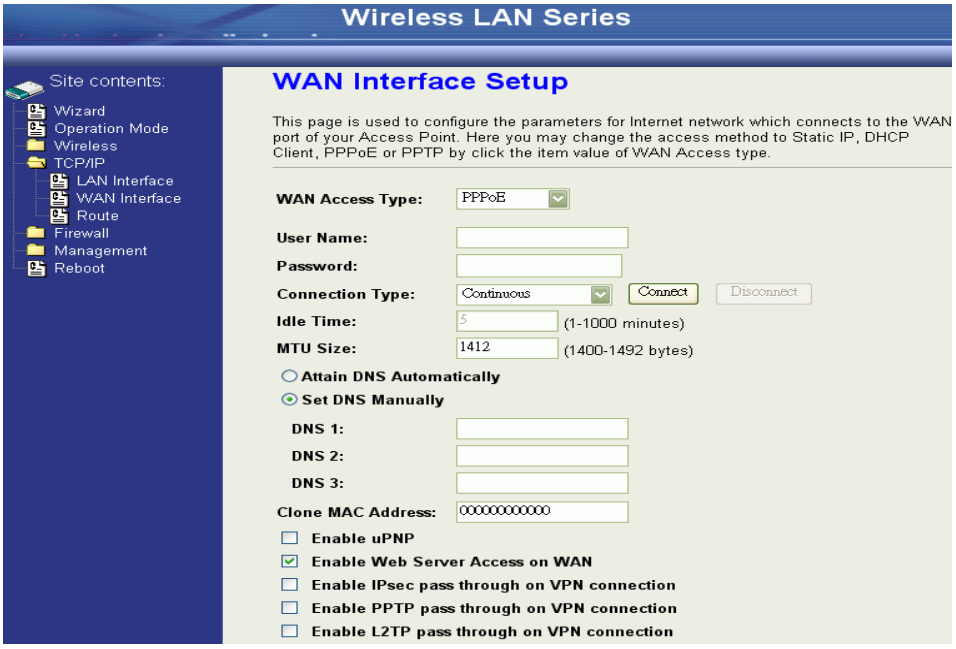
All IP configuration data besides DNS will be obtained from the DHCP server when DHCP-Client WAN Access Type is selected.



DNS 1~3	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. The DNS maintains central lists of domain name/IP addresses and maps the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address	Clone device MAC address to the specific MAC address required by your ISP.
Enable uPnP	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

PPPoE

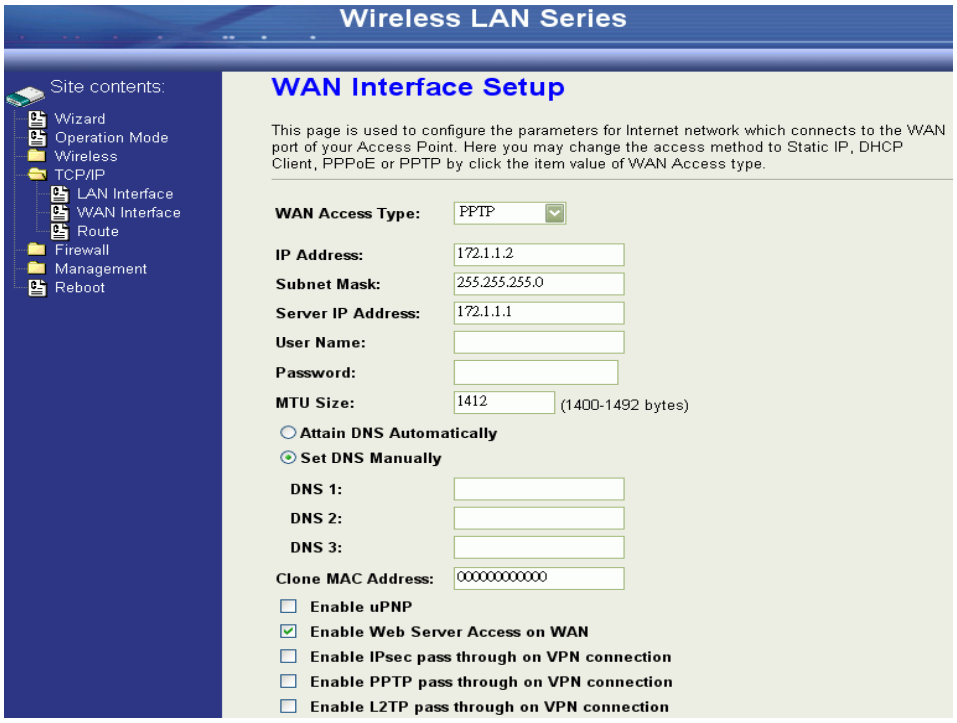
When the PPPoE (Point to Point Protocol over Ethernet) WAN Access Type is selected, you must fill the fields of User Name, Password with the username and password provided by your ISP. The IP configuration will be done when the device successfully authenticates with your ISP.



User Name	The account provided by your ISP
Password	The password for your account.
Connect Type	“Continuous “: connect to ISP permanently “Manual”: Manually connect/disconnect to ISP “On-Demand”: Automatically connect to ISP when the user needs to access the Internet.
Idle Time	The number of minutes of inactivity before disconnecting from ISP. This setting is only available when “Connect on Demand” connection type is selected.
MTU Size	Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.
DNS 1~3	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. The DNS maintains central lists of domain name/IP addresses and maps the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address	Clone device MAC address to the specific MAC address required by your ISP.
Enable uPnP	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only

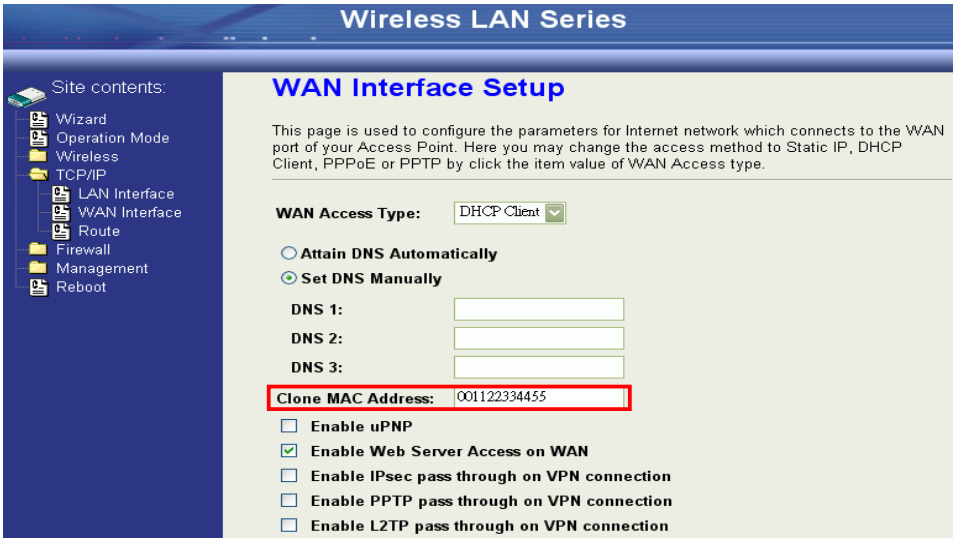


IP Address	The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier outside of your local network.
Subnet Mask	The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
Server IP Address (Default Gateway)	The IP address of PPTP server
User Name	The account provided by your ISP
Password	The password of your account
MTU Size	Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.
DNS 1~3	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. The DNS maintains central lists of domain name/IP addresses and maps the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address	Clone device MAC address to the specific MAC address required by your ISP.
Enable uPnP	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

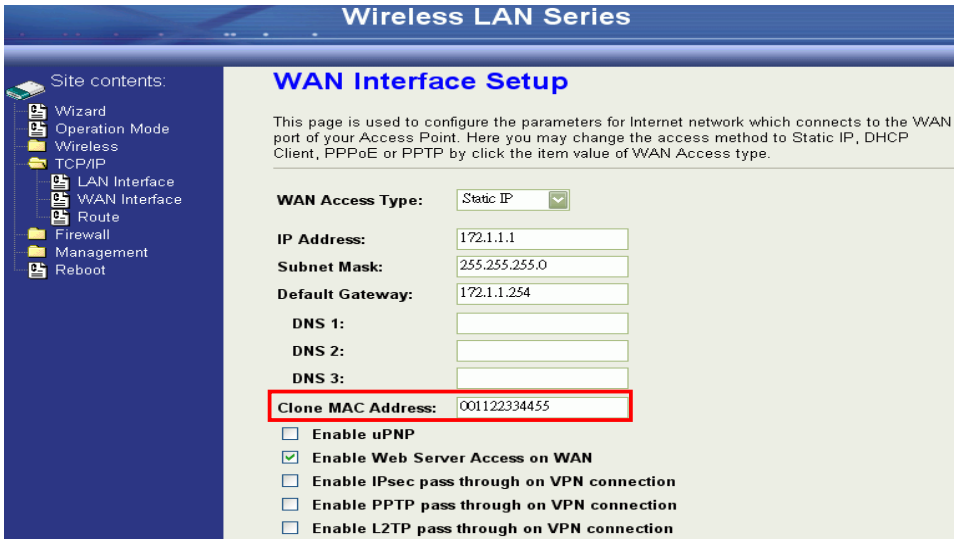
Configuring Clone MAC Address

The device provides a MAC address clone feature to fit the requirements of some ISP need to specify the client MAC address.

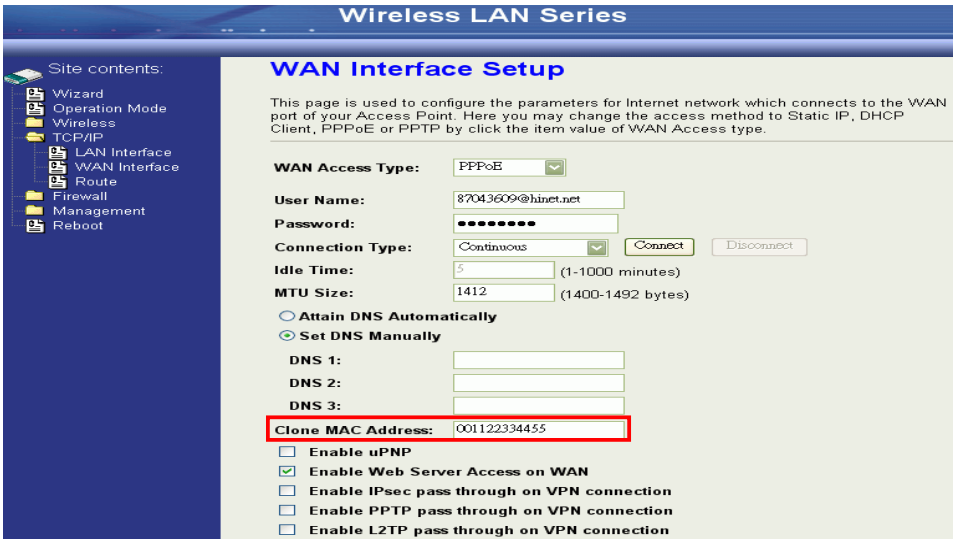
Clone MAC address for DHCP Client WAN access type:



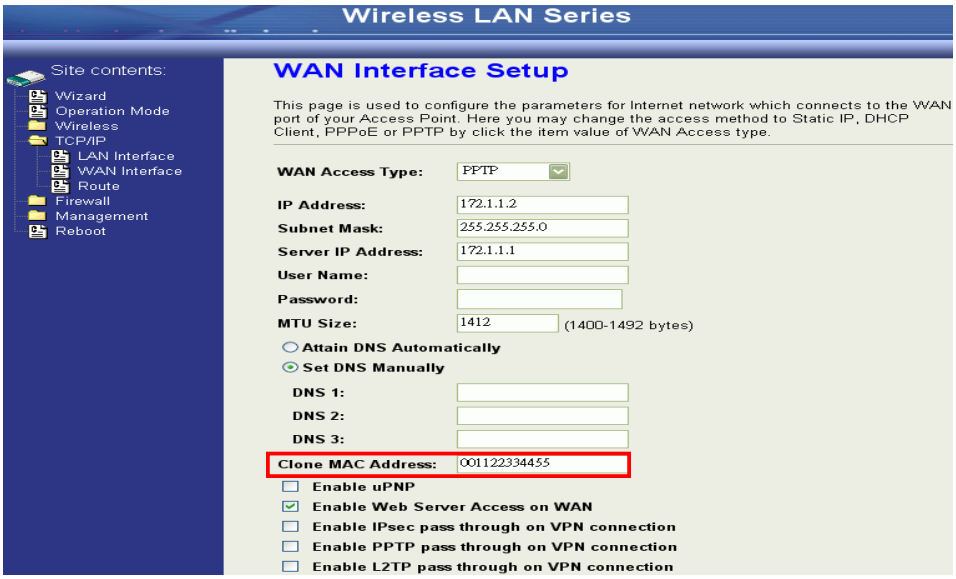
Clone MAC address for Static IP WAN access type:



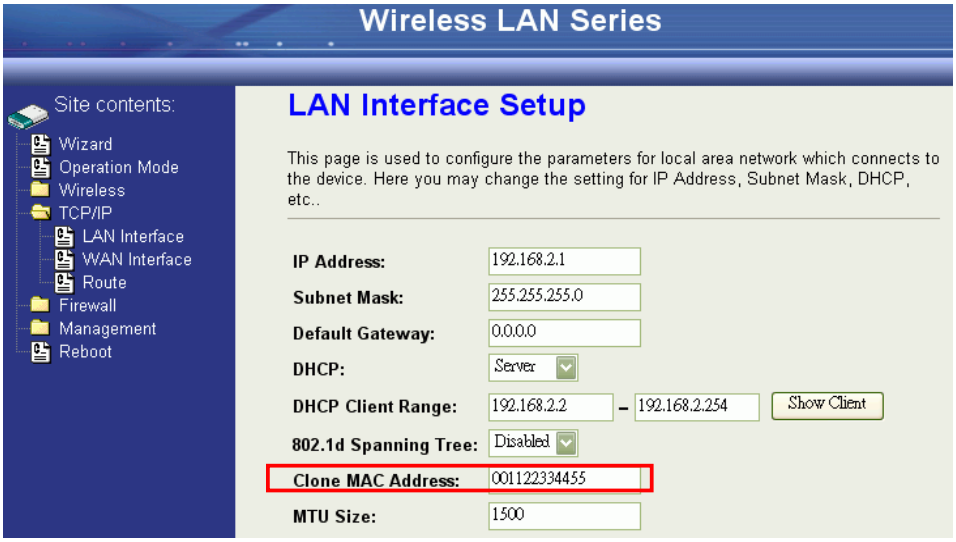
Clone MAC address for PPPoE WAN access type:



Clone MAC address for PPTP WAN access type:

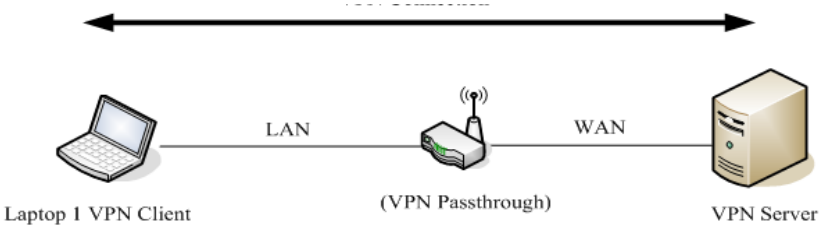


Physical LAN interface MAC address clone:

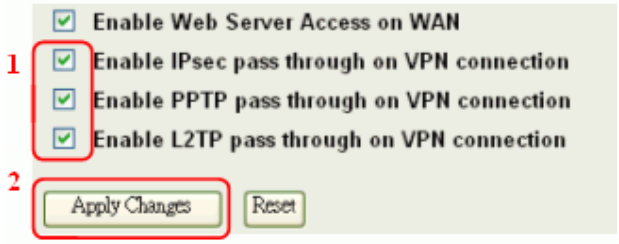


VPN Pass-through

This functionality lets the device Pass-through the VPN packets including PPTP/ L2TP/IPsec VPN Connection.

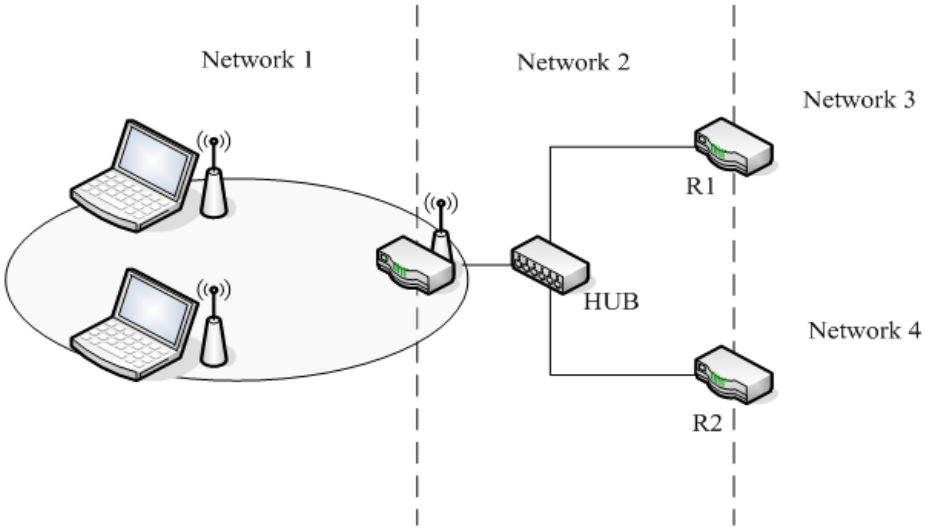


Check the VPN Pass-through in WAN Interface of TCP/IP Page that you want and then click Apply Changes button.



Static Route Setup

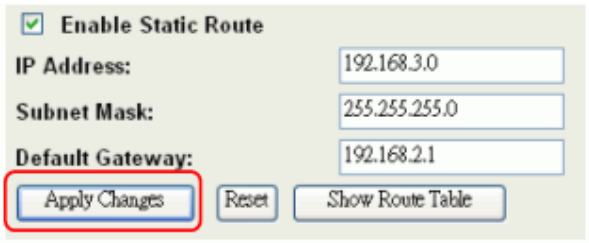
You can set the routing information to let the Router know what routing is correct if it cannot learn automatically through other means.



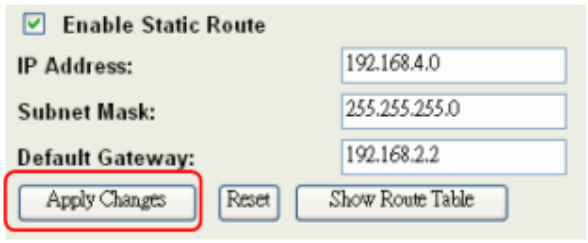
For example, if the user wants to link the Network 3 and Network 4 separately from Network 1, the Routing Table configuration would be as shown below:

Enable Static Routing in Route Setup of TCP/IP page and then enter IP Address of Network 3, Subnet Mask and IP Address of

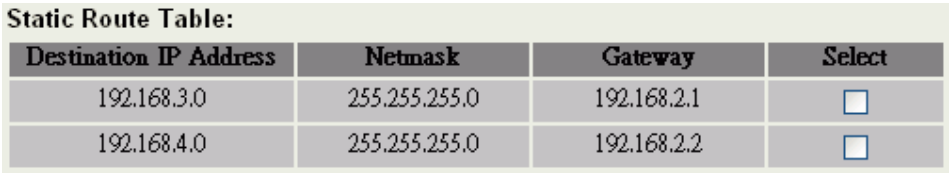
Router (R1) in Default Gateway field then click Apply Change button.



Enter IP Address of Network 4, Subnet Mask and IP Address of Router (R2) in Default Gateway field then click Apply Change button.



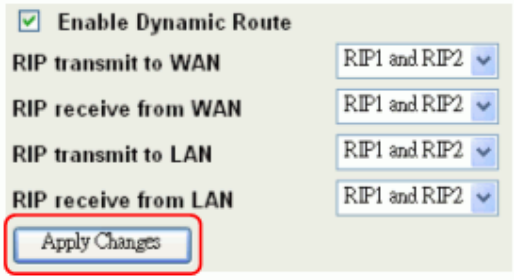
In Static Route Table there have two routings for Network 3 and Network 4



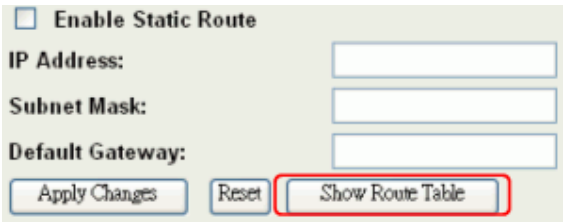
Dynamic Route Setup

The Dynamic Route utilizes RIP1/2 to transmit and receive the route information with other Routers.

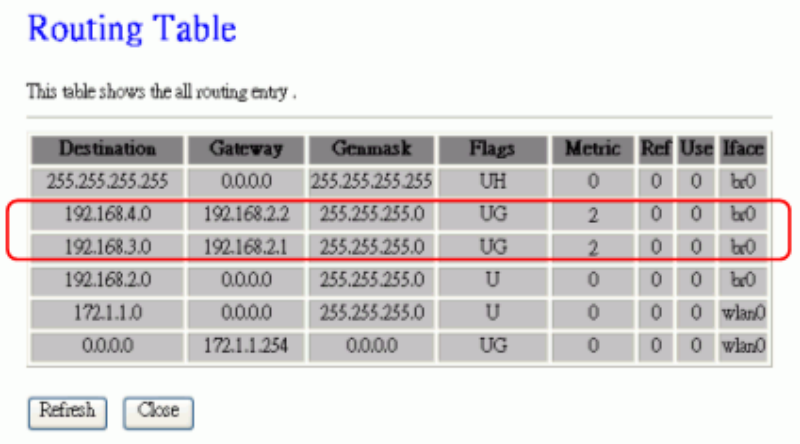
Enable Dynamic Route and then select RIP 1, RIP2 or Both to transmit/receive packets then click the Apply Change button.



Click the Show Route Table button to show Dynamic Route Table.



In the Dynamic Routing Table there are two routings for Network 3 and Network 4



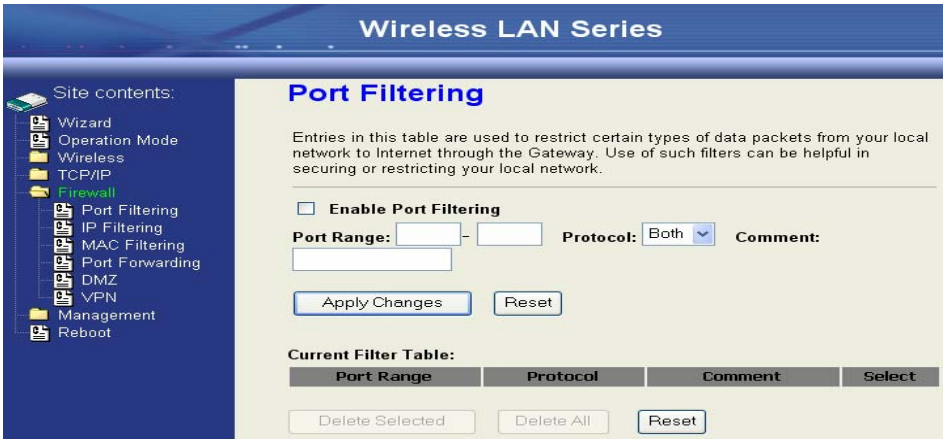
Firewall Configuration

Configuring LAN to WAN Firewall

The device supports three kinds of filter Port Filtering, IP Filtering and MAC Filtering. All the entries in current filter table are used to restrict certain types of packets from your local network through the device. Use of such filters can be helpful in securing or restricting your local network.

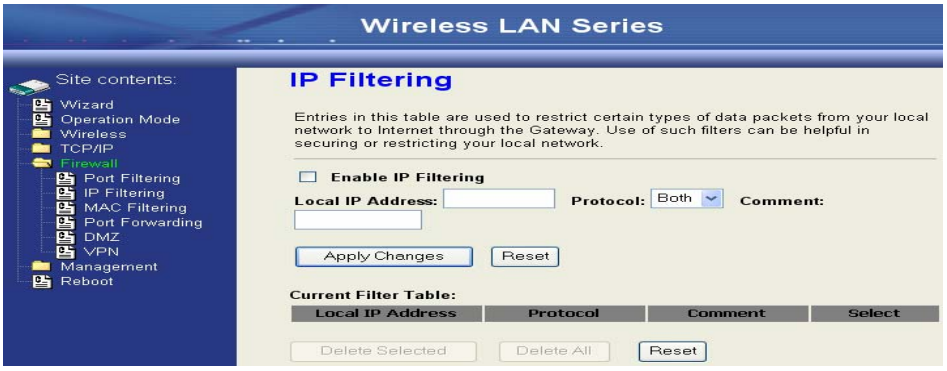
Port Filtering

When you enable the Port Filtering function, you can specify a single port or port ranges in the current filter table. When the source port of outgoing packets matches the port definition or falls within the port ranges in the table, the firewall will block those packets from LAN to WAN.



IP Filtering

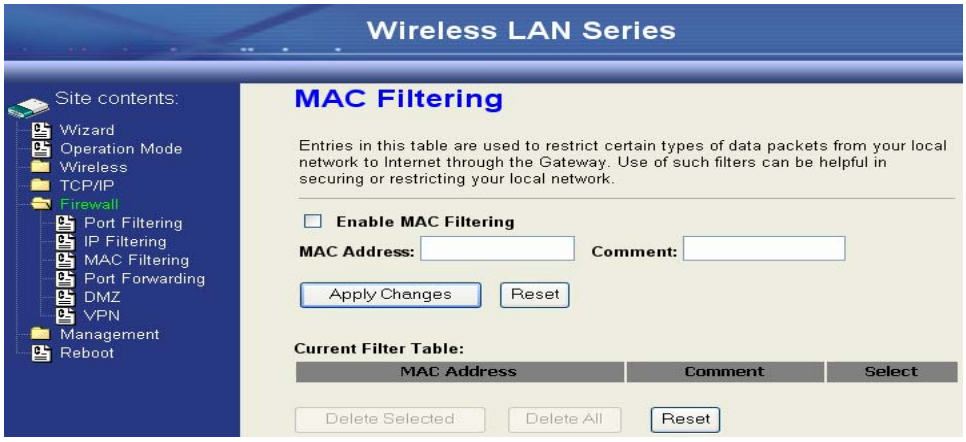
When you enable the IP Filtering function, you can specify local IP Addresses in the current filter table. When the source IP address of outgoing packets matches the IP Addresses in the table the firewall will block this packet from LAN to WAN.



MAC Filtering

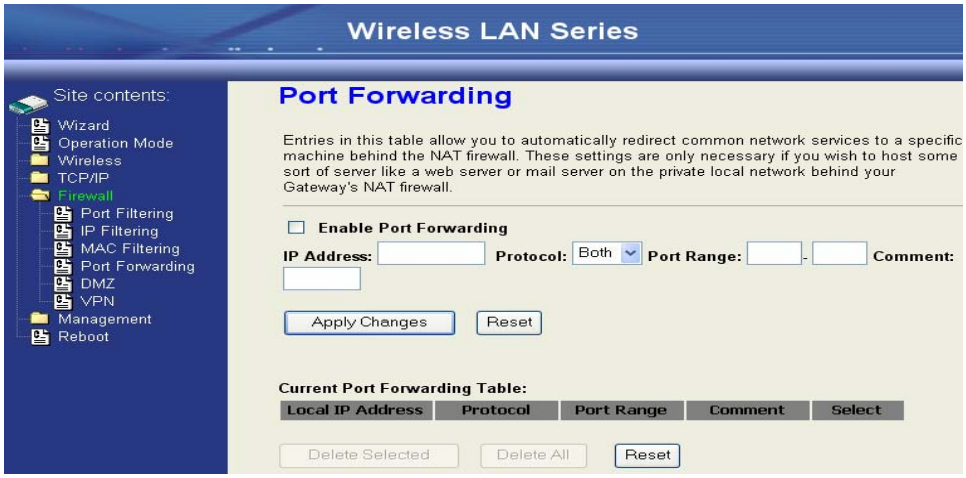
When you enable the MAC Filtering function, you can specify the MAC Addresses in the current filter table. When the source MAC Address of outgoing packets matches the MAC Addresses in the table the firewall will block this packet from LAN to

WAN.



Configuring Port Forwarding (Virtual Server)

This function allows 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 the device's NAT firewall.

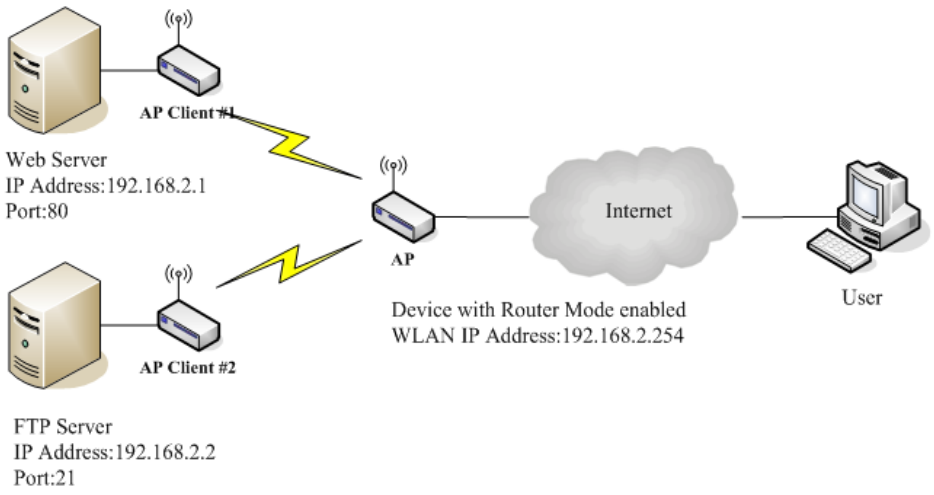


The most often used port numbers are shown in the following table.

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer Protocol)	80
POP3 (Post Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
SIP (Session Initiation Protocol)	5060
PPTP (Point-to-Point Tunneling Protocol)	1723

Multiple Servers behind NAT Example:

In this case, there are two PCs in the local network accessible for outside users.



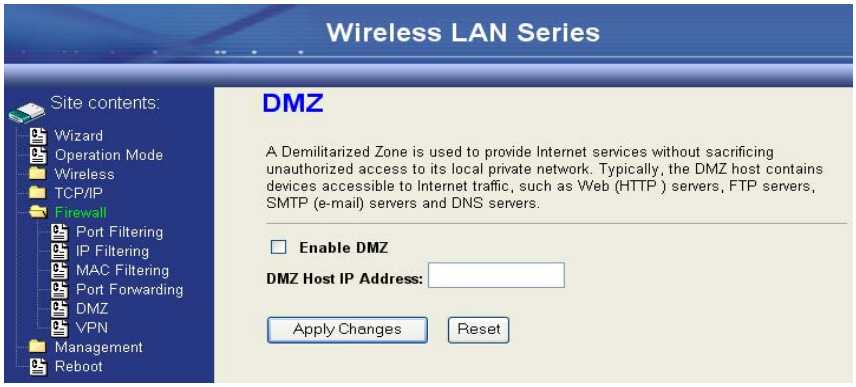
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.2.1	TCP+UDP	80	Web Server	☐
192.168.2.2	TCP+UDP	21	FTP Server	☐

Delete Selected | Delete All | Reset

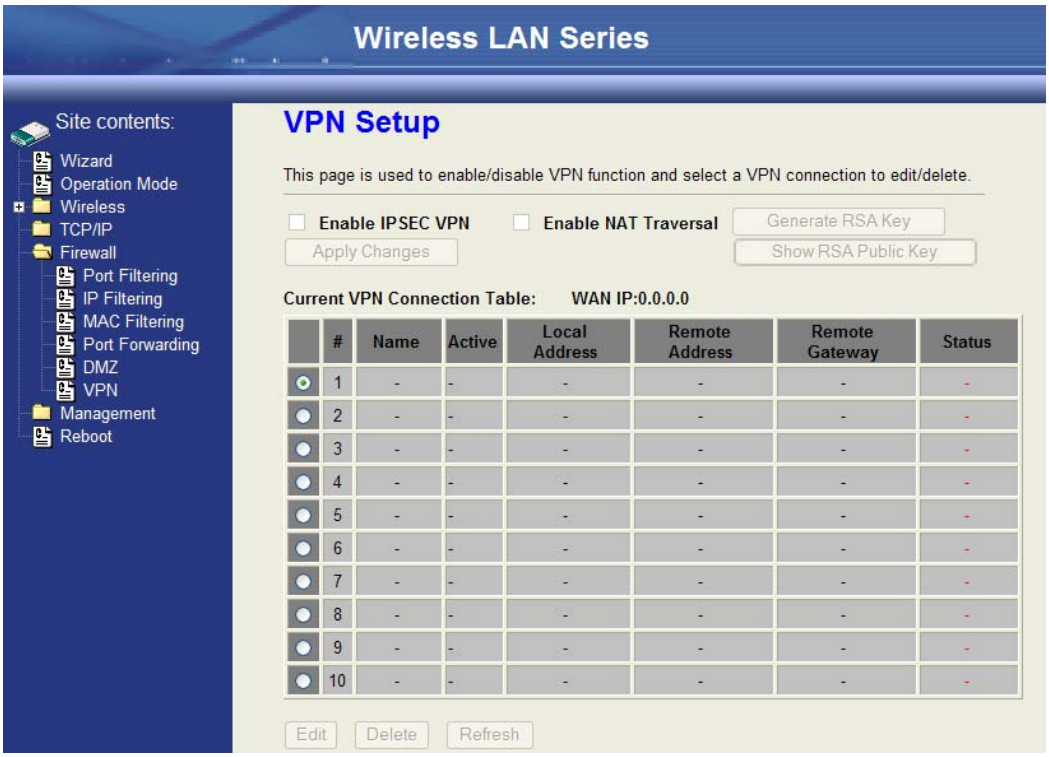
Configuring DMZ

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. All inbound packets will be redirected to the computer you set. It also is useful if you run some applications (e.g. Internet games) that use uncertain incoming ports.



Enable DMZ	Enables the DMZ.
DMZ Host IP Address	Input the IP Address of the computer that you want to expose to the Internet.

Configuring VPN

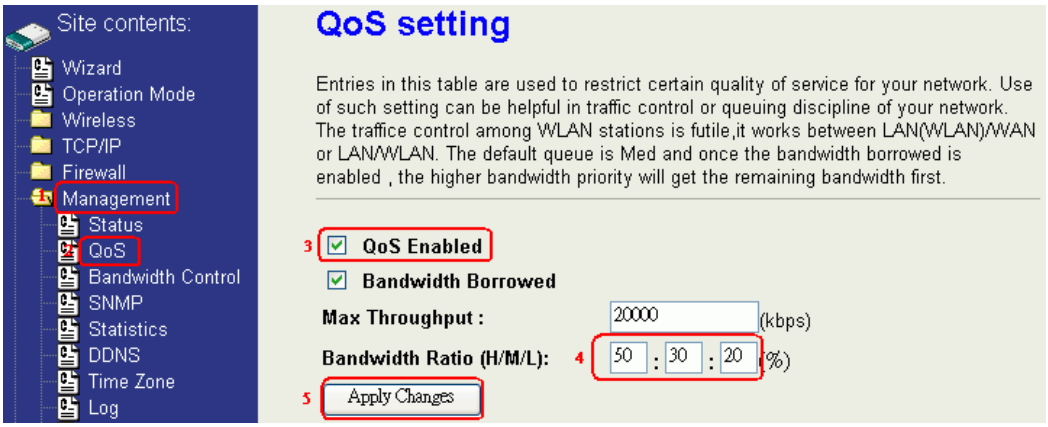


Management Configuration

Quality of Service (QoS)

QoS allows you to specify some rules, to ensure the quality of service in your network, such as Bandwidth Priority to allocate bandwidth. This function can be helpful in shaping and queuing traffic from LAN (WLAN) to WAN or LAN to WLAN, but not WLAN to WLAN.

Enable the QoS and then fill in the Bandwidth Ratio (H/M/L). The device has three Bandwidth Priorities High, Medium and Low. The user can allocate Bandwidth among these and the default is High:50%, Medium:30% and Low:20%.

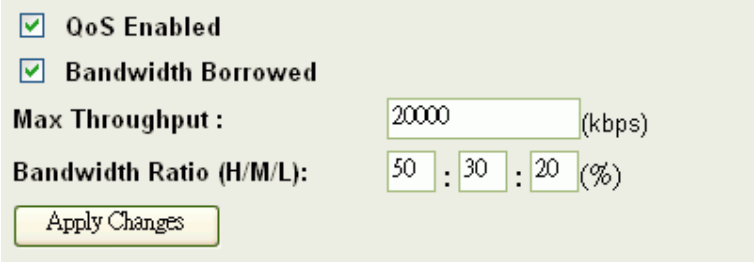


The following table describes the priorities that you can apply to bandwidth.

Priority Level	Description
High	Typically used for voice or video applications that is especially sensitive to the variations in delay.
Medium	Typically used for important traffic that can tolerate some delay.
Low	Typically used for non-critical traffic such as a large number of transfers but that should not affect other application.

Click the QoS link under Management to open the QoS Setting page. This page is divided into three parts: basic settings, QoS rule settings, and current QoS setting table.

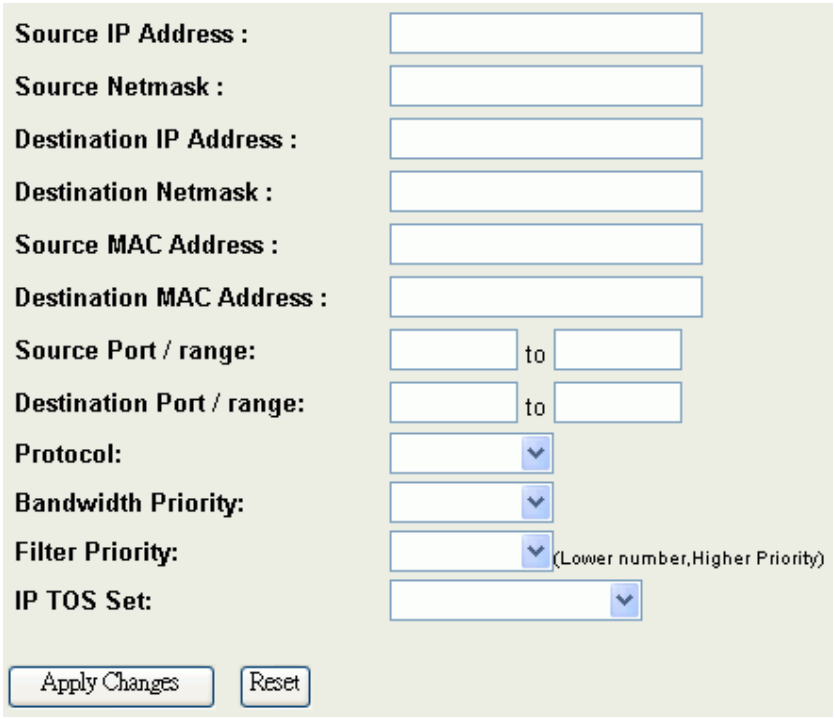
Enable QoS and enter Max Throughput (default 20Mbps) 、 Bandwidth Ratio (default H:50%, M:30%, L:20%)



Label	Description

QoS Enabled	Select this check box to enable quality of service.
Bandwidth Borrowed	Select this check box to allow a rule to borrow unused bandwidth. Bandwidth borrowing is decided by priority of the rules. Higher priority will get the remaining bandwidth first.
Max Throughput	Enter the value of max throughput in kbps that you want to allocate for one rule. The value should between 1200 kbps and 24000 kbps.
Bandwidth Ratio (H/M/L)	You can specify the ratio of priority in these fields. The range from 1 to 99. The High priority's ratio should higher than Medium priority's ratio and Medium priority's ratio should higher than Low priority's ratio.
Apply Changes	Click this button to save and apply your settings.

QoS Rule settings



Label	Description
IP Address	Enter source/destination IP Address in dotted decimal notation.
Netmask	Once the source/destination IP Address is entered, the subnet mask address must be filled in this field.
MAC Address	Enter source/destination MAC Address.
Port / range	You can enter specific port number or port range of the source/destination
Protocol	Select a protocol from the drop down list box. Choose TCP/UDP, TCP or UDP.
Bandwidth Priority	Select a bandwidth priority from the drop down list box. Choose Low, Medium or High.
Filter Priority	Select a filter priority number from the drop down list box. Lower number gets higher priority while two rules have the same bandwidth priority.
IP TOS Match	Select an IP type-of-service value from the drop down list box. Choose Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, or Minimize Delay.
Apply Changes	Click this button to save and apply your settings.
Reset	Click this button to begin re-input the parameters.

Current QoS setting table

In this part, you can see how many rules have been specified. In addition you can see the detail about the rules and manage

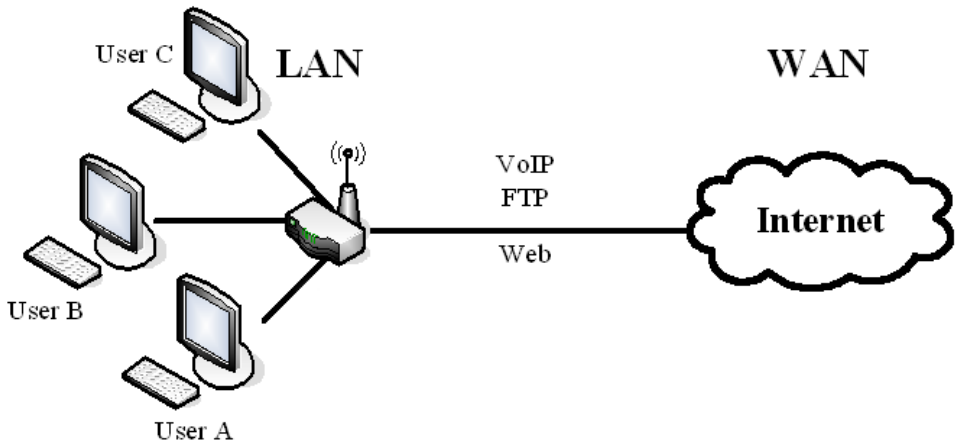
the rules. This table can handle 50 rules at most.

Current QoS Setting:
(Mask 255.255.255.255 means single host)

Src Adr	Dst Adr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	140.113.27.181/24	00:05:9e:80:aa:ee	-	21-21	21-21	TCP	LOW	0	Normal	☐
anywhere	anywhere	-	-	80-80	-	TCP/UDP	MED	0	Normal	☐
192.168.2.13/24	anywhere	-	-	50000-50050	-	TCP/UDP	LOW	2	Normal	☐
anywhere	192.168.2.12/24	-	-	-	-	TCP/UDP	MED	1	Normal	☐
192.168.2.15/24	anywhere	00:05:9e:80:aa:cc	-	-	-	TCP/UDP	HIGH	0	Normal	☐

Delete Selected | Delete All | Reset

An example for usage



For example, there are three users in your network.

User A wants to browse the websites to retrieve information.

User B wants to use FTP connection to download a large file.

User C wants to use software phone to connect with customer.

Since VoIP traffic is sensitive to variations in delay (jitter), you can set High priority for User C. However, because the FTP transmission may take a long time, you can set Low priority for User B.

Current QoS Setting:
(Mask 255.255.255.255 means single host)

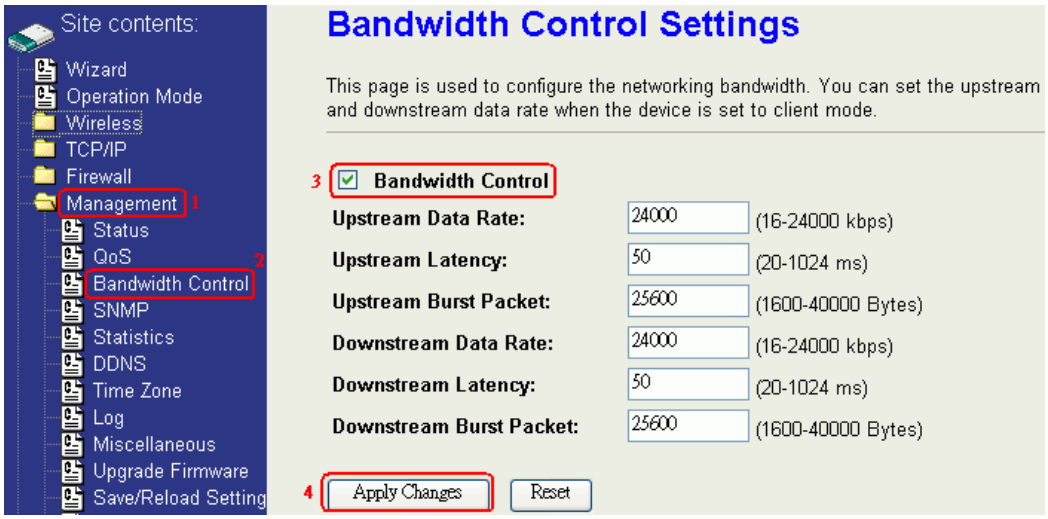
Src Adr	Dst Adr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	anywhere	-	-	5060-5061	-	TCP/UDP	HIGH	0	Normal	☐
192.168.2.12/24	anywhere	-	-	21-21	-	TCP	LOW	0	Normal	☐
192.168.2.13/24	anywhere	-	-	80-80	-	TCP	MED	0	Normal	☐

Delete Selected | Delete All | Reset

Bandwidth Control

This functionality can control the upstream and downstream bandwidth.

Enable Bandwidth Control and then enter Data Rate、Latency and Burst Packet in the specific field.



NOTE: Only device on Client mode or WISP mode this functionality can take effective.

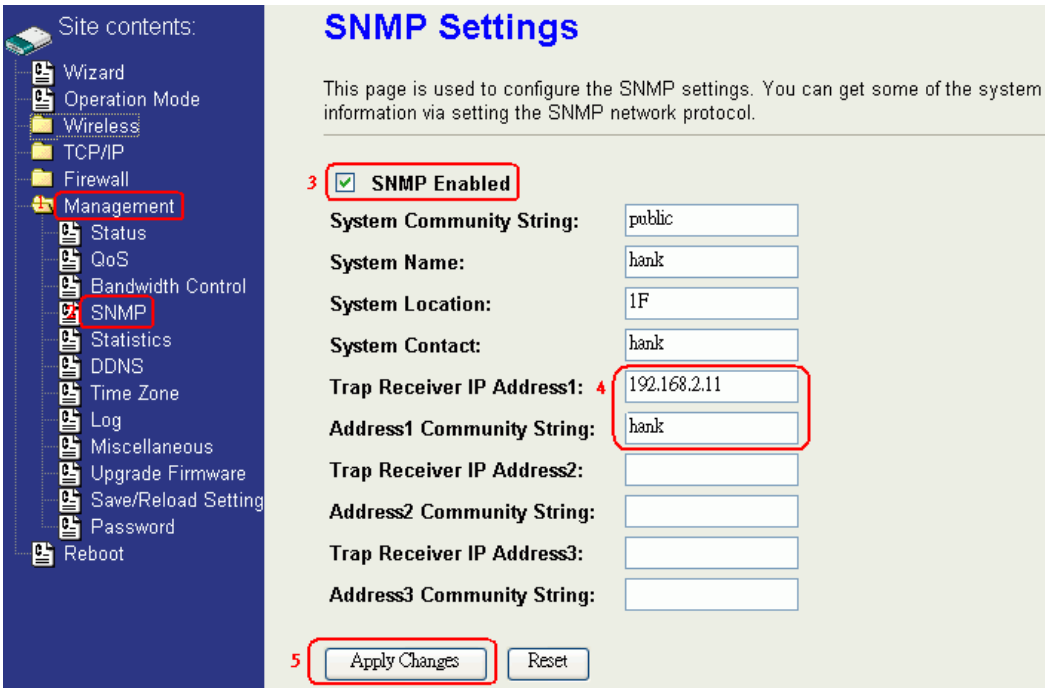
Parameter Definition

Label	Description
Upstream Data Rate	Speed of transmit data that from Ethernet interface to Wireless interface.
Upstream Latency	Similar a waiting time the data queuing- time.
Upstream Burst Packet	Similar a buffer the data will into the buffer while the data is transmit or receive.
Downstream Data Rate	Speed of transmit data that from Wireless interface to Ethernet interface.
Downstream Latency	Similar a waiting time the data queuing- time.
Downstream Burst Packet	Similar a buffer the data will into the buffer while the data is transmit or receive.

SNMP Agent

This device is compatible with SNMP v1/v2c and provides standard MIB II. Currently only the “public” community string is available and any setting modified by SNMP SET requests will be lost after rebooting the device.

Enable SNMP and then enter IP Address of SNMP Manager in Trap Receiver IP Address field and Community String in System Community String field then click the Apply Changes button.



Following Table describes the SNMP configuration parameters

Label	Description
System Community String	This is password sent with each trap to the SNMP Manager.
System Name	Type the Name which is name of device.
System Location	Type the Location which is location of device
System Contact	Type the Name which is person or group when the device has problem can find they.
Trap Receiver IP Address	Type the IP Address which is address of SNMP Manager.
Trap Receiver Community String	This is password receive with trap from the device (SNMP Agent).

SNMP Traps

Traps	Description
coldStart(0)	The trap from device after reboot the device
linkDown(2)	The trap is sent when any of the links are down. See the following table.
linkup(3)	The trap is sent when any of the links are UP. See the following table.
authenticationFailure(4)	The trap is sent when the device receiving gets or sets requirement with wrong community.

Private MIBs

OID	Description
1.3.6.1.4.1.99.1	Mode, Operation Mode in device.
1.3.6.1.4.1.99.2	SSID, SSID of the device
1.3.6.1.4.1.99.3	Channel, Channel of the device in WLAN
1.3.6.1.4.1.99.4	Band, 802.11g / 802.11b only
1.3.6.1.4.1.99.5	RSSI, Receive Signal Strength Index (Support AP and Client RSSI)
1.3.6.1.4.1.99.6	Active_Clients, The number of associate clients
1.3.6.1.4.1.99.7	Active_Clients_List, Client's Information (MAC Address, Data Rate, RSSI…etc)
1.3.6.1.4.1.99.8	Encryption, Encryption type of device in Wireless Network

1.3.6.1.4.1.99.1 - Mode

.1.3.6.1.4.1.99.1.2.1	MODE
.1.3.6.1.4.1.99.1.3.1	/bin/flash snmpget MODE
.1.3.6.1.4.1.99.1.100.1	0
.1.3.6.1.4.1.99.1.101.1	AP - Bridge

1.3.6.1.4.1.99.2 - SSID

.1.3.6.1.4.1.99.2.2.1	SSID
.1.3.6.1.4.1.99.2.3.1	/bin/flash snmpget SSID
.1.3.6.1.4.1.99.2.100.1	0
.1.3.6.1.4.1.99.2.101.1	hank

1.3.6.1.4.1.99.3 - Channel

.1.3.6.1.4.1.99.3.1.1	1
.1.3.6.1.4.1.99.3.2.1	CHANNEL
.1.3.6.1.4.1.99.3.3.1	/bin/flash snmpget CHANNEL
.1.3.6.1.4.1.99.3.100.1	0
.1.3.6.1.4.1.99.3.101.1	11

1.3.6.1.4.1.99.4 - Band

.1.3.6.1.4.1.99.4.2.1	BAND
.1.3.6.1.4.1.99.4.3.1	/bin/flash snmpget BAND
.1.3.6.1.4.1.99.4.100.1	0
.1.3.6.1.4.1.99.4.101.1	802.11bg

1.3.6.1.4.1.99.5 - RSSI

.1.3.6.1.4.1.99.5.2.1	RSSI
.1.3.6.1.4.1.99.5.3.1	/bin/flash snmpget RSSI
.1.3.6.1.4.1.99.5.100.1	0
.1.3.6.1.4.1.99.5.101.1	100

1.3.6.1.4.1.99.6 - Active_Clients

.1.3.6.1.4.1.99.6.2.1	ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.3.1	/bin/flash snmpget ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.100.1	0
.1.3.6.1.4.1.99.6.101.1	1

1.3.6.1.4.1.99.7 - Active_Clients_List

.1.3.6.1.4.1.99.7.2.1	ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.3.1	/bin/flash snmpget ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.100.1	0 MAC Data Rate RSSI
.1.3.6.1.4.1.99.7.101.1	00:13:02:03:51:5e,102,125,54,no,300,57(-55 dbm)

1.3.6.1.4.1.99.8 - Encryption

.1.3.6.1.4.1.99.8.2.1	ENCRYPTION
.1.3.6.1.4.1.99.8.3.1	/bin/flash snmpget ENCRYPTION
.1.3.6.1.4.1.99.8.100.1	0 AP-WEP
.1.3.6.1.4.1.99.8.101.1	WEP(AP),Disabled(WDS)

Upgrade Firmware

Firmware Types

The firmware for this device is divided into 2 parts, one is web pages firmware the other is application firmware, usually named g120webpage.bin and g120linux.bin. To upgrade the firmware, we suggest the user first upgrade the application firmware then the web pages firmware.

Upgrading Firmware

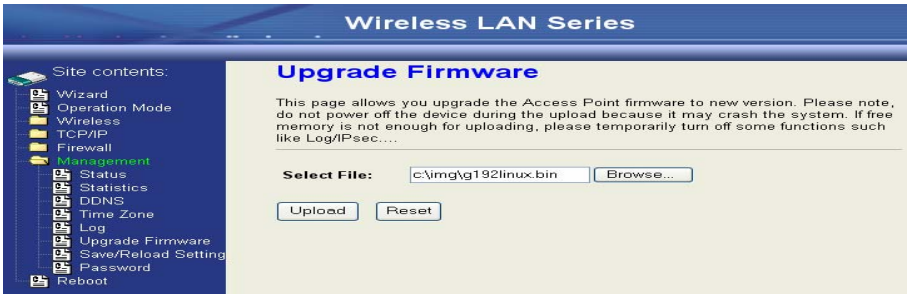
The Web-Browser upgrading interface is the simplest and safest way to upgrade the firmware. It will check the firmware checksum and signature, and the wrong firmware won't be accepted. After upgrading, the device will reboot.

WARNING: Older versions of the firmware may cause the device configuration to be restored to the factory default setting upon rebooting and the original configuration data will be lost!

To upgrade the firmware, just enter the file name with full path and click the "Upload" button.

Memory Limitation

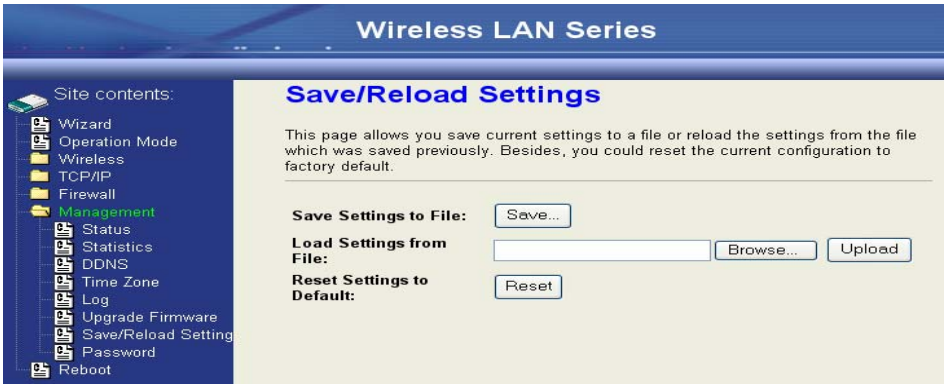
To make sure the device has enough memory to upload firmware, the system will check the capacity of free memory. If the device lacks enough memory to upload the firmware, please temporarily turn-off some functions then reboot the device to get enough memory for firmware uploading.



Save/Reload Settings

Reset Setting to Factory Default Value

Since the device is designed for outdoor use, there is no interface outside the housing to reset the configuration value to the factory default value. The device provides the Web-Browser interface to reset the configuration data. After resetting it, the current configuration data will be lost and restored to factory default value.



To save & restore configuration data of device, just enter the target filename with full path to your local host then you can back up the configuration data to local host or restore configuration data to the device.

Password

The Web-Browser interface has password protection.

To disable the Web-Browser password protection just leave the “User Name” field to blank then click the “Apply Changes” button.

Using CLI Menu

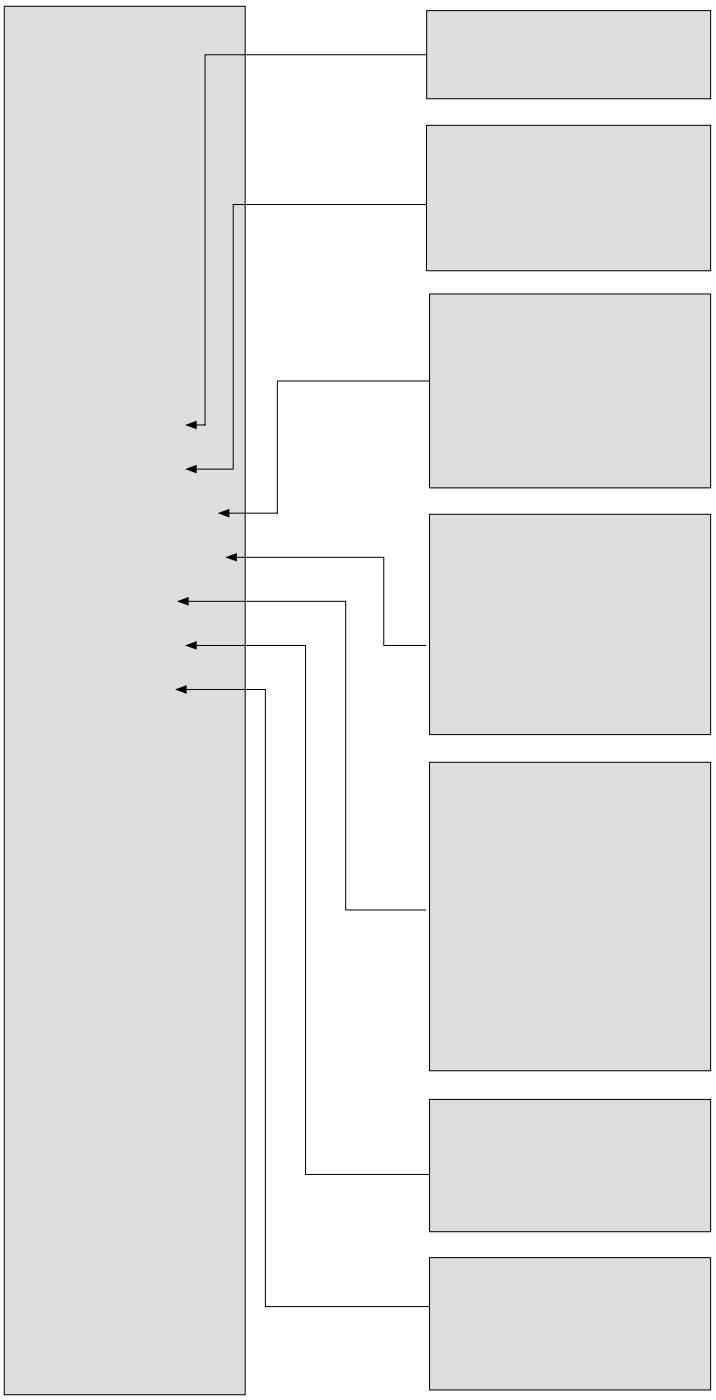
Start a SSH(Secure Shell) client session to login to the device

The SSH server daemon inside the device uses TCP port 22. User must use SSH client utility such as Putty to login to the device. The default password for user “root” is either “qwert” or “zplus12320400” depending on your firmware version. Once the user has logged in to the device, then the password can be changed by CLI command.

Execute CLI program

This program won’t execute automatically when user logs in to the device. The user must manually execute it by typing the case-sensitive command “cli”. Please note that modified settings won’t save permanently until the user executes “Apply Changes to Flash” and reboots the device. The new settings modified by CLI will take effect after rebooting the device.

Menu Tree List



Password

The SSH Configuration interface has password protection. Please note that this password is separate from the web configuration password.

A. Operation Mode

B. Wireless Setting

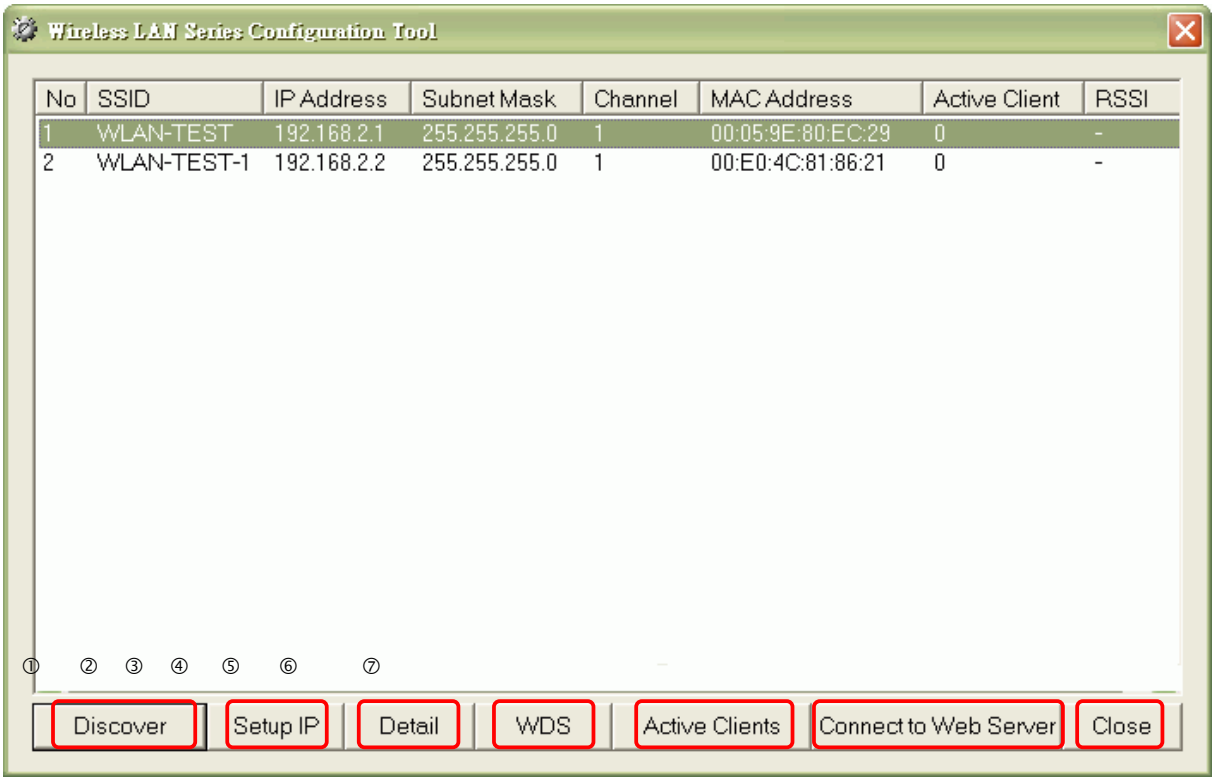
C. TCP/IP-LAN Setting

192.168.2.3 - PuTTY
System Settings===
A. Root Password
0. Exit
==
Please choice one selection:
Please key-in the Password:qwertyuiop
Changing password for root
Password changed.
Press any key to continue...

Auto Discovery Tool

Auto Discovery can be used to find out how many devices are in your local area network

The name of the tool is WirelessConf.exe.



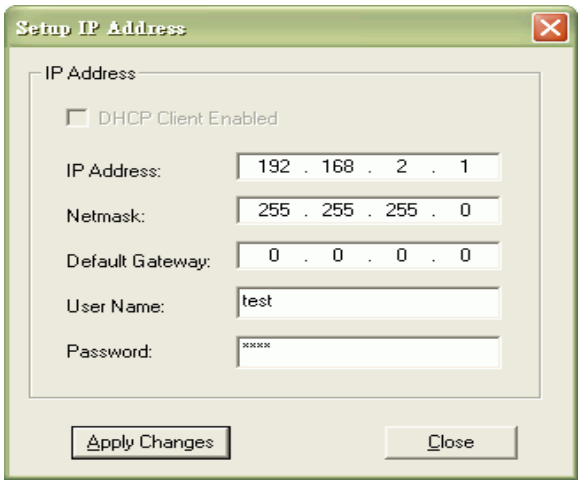
Discover

After pressing this button, you will see how many devices are in your network and you would see the basic information about these devices, such as:

- SSID
- IP Address
- Subnet Mask
- Channel number
- MAC Address

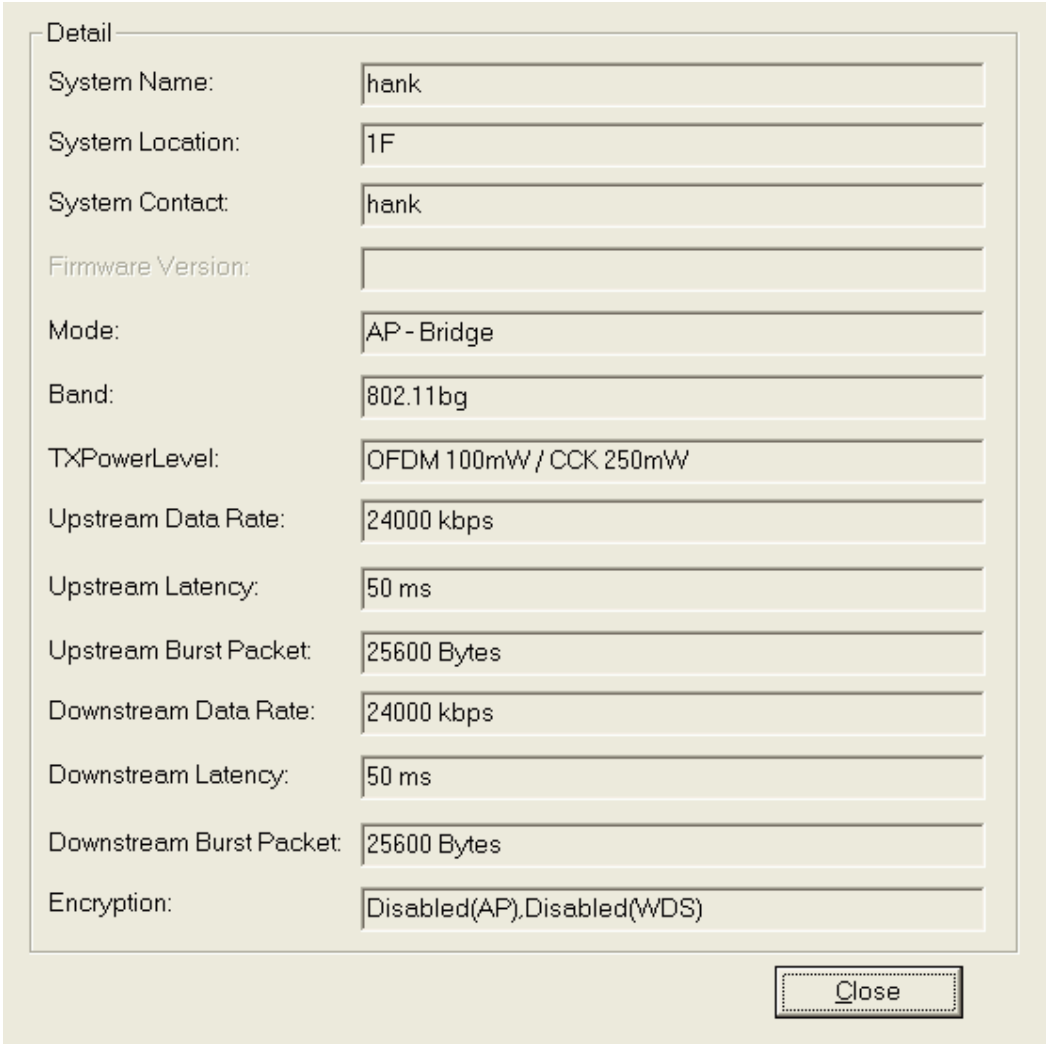
Setup IP

After you press the Setup IP button, you will see Setup IP Address window. You can change the device's IP Address, Netmask, and Default Gateway in this window. But if the device's web server needs User Name and Password to login, you should fill in these two fields and then apply changes.



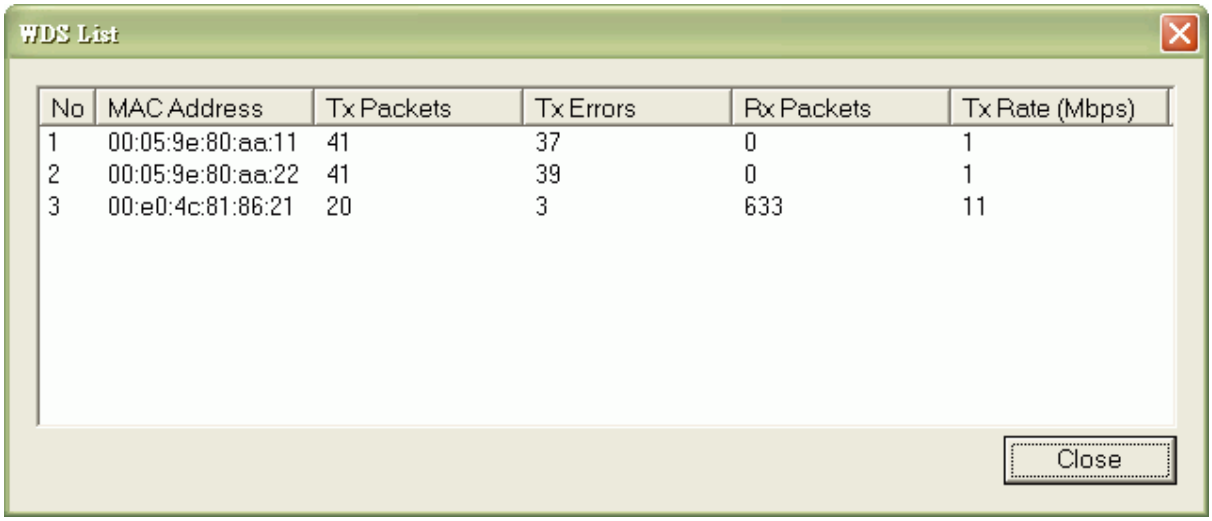
Detail

If you want to see more detailed information, you could press the Detail button, and then you will see the Detail Information window.



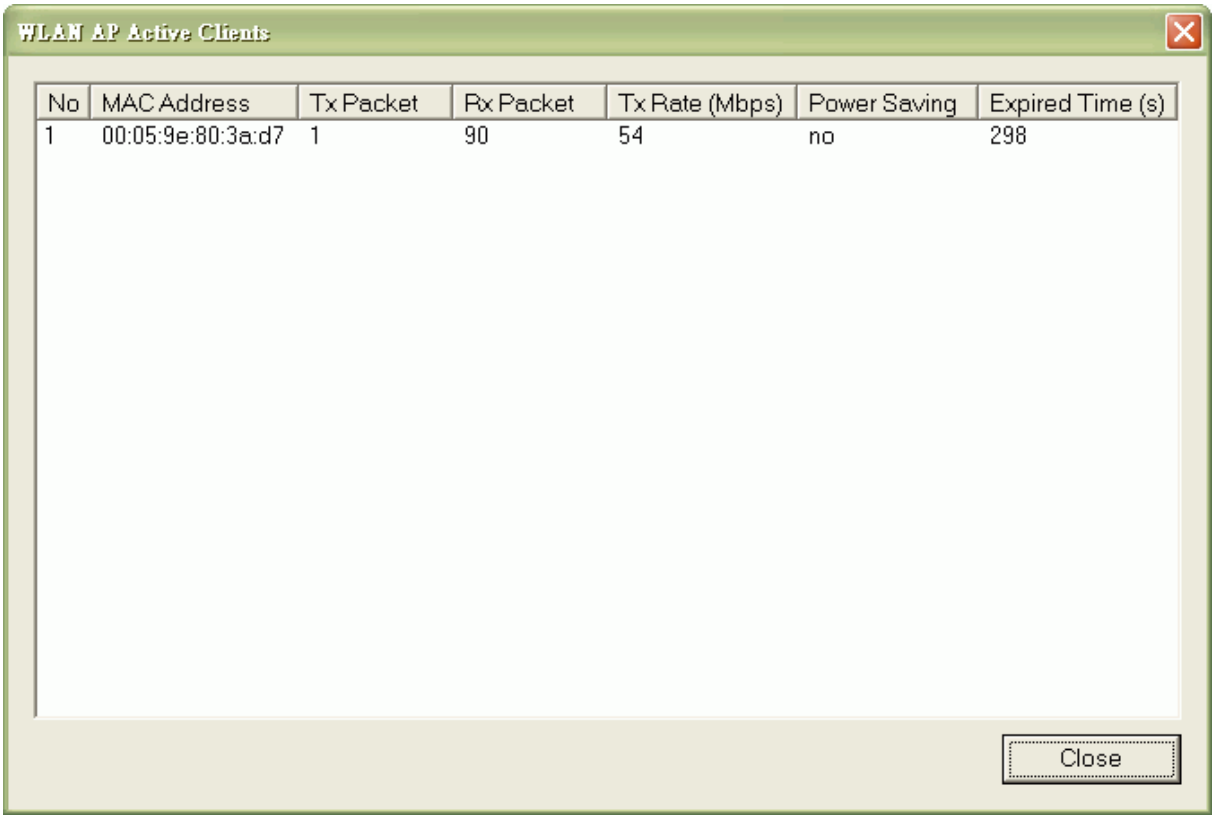
WDS

If the device you selected is in WDS mode or AP+WDS mode, you can press the WDS button and then you will see the WDS List window.



Active Clients

After pressing the Active Clients button, you will see the WLAN AP Active Clients window. with information, such as:



Connect to Web Server

If you want connect to device's web server you can press the Connect to Web Server button, or double-click on the device.