

User's Manual

WLAN Travel AP/Router

Version: 1.0

Trademarks

Copyright @2012

Contents are subject to change without notice.

All trademarks belong to their respective proprietors.

Copyright Statement

THIS DOCUMENT CONTAINS OF PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THIS COMPANY. AND NO PART OF THIS DOCUMENTATION MAY BE REPRODUCED, STORED IN A RETRIEVAL SYSTEM OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRICAL OR MECHANICAL, BY PHOTOCOPYING, RECORDING, OR OTHERWISE, WITHOUT THE PRIOR WRITTEN CONSENT OF THIS COMPANY.

Federal Communication Commission Interference Statement

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

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

Table of Contents

REVISION HISTORY I

TERMINOLOGY II

1 INTRODUCTION..... 1

 1.1 PACKAGE CONTENTS1

 1.2 PRODUCT FEATURES1

 1.3 PANEL DESCRIPTION3

2 INSTALLATION 4

 2.1 HARDWARE INSTALLATION4

 2.2 SOFTWARE INSTALLATION5

3 APP SOFTWARE CONFIGURATION..... 6

4 SOFTWARE CONFIGURATION 7

 4.1 PREPARE YOUR PC TO CONFIGURE THE WLAN TRAVEL AP/ROUTER7

 4.2 CONNECT TO THE WLAN TRAVEL AP/ROUTER9

 4.3 MANAGEMENT AND CONFIGURATION ON THE WLAN TRAVEL AP/ROUTER - AP MODE9

 4.3.1 Operation Mode 9

 4.3.2 Wireless - Basic Settings..... 10

 4.3.3 Wireless - Advanced Settings 12

 4.3.4 Wireless - Security Setup 14

 4.3.5 Site Survey 17

 4.3.6 WPS 18

 4.3.7 Schedule 19

 4.3.8 LAN Interface Setup 20

 I Static DHCP Setup22

 4.3.9 Status 23

 4.3.10 Management - Statistics 25

 4.3.11 Management - Time Zone Setting..... 25

 4.3.12 Management - Log 26

 4.3.13 Management - Upgrade Firmware 27

 4.3.14 Management Save/ Reload Settings..... 28

 4.3.15 Management - Password Setup 29

4.4	MANAGEMENT AND CONFIGURATION ON THE WLAN TRAVEL AP/ROUTER - ROUTER MODE	30
4.4.1	ULinker Operation Mode.....	30
4.4.2	Wireless - Basic Settings.....	30
4.4.3	Wireless - Advanced Settings	32
4.4.4	Wireless - Security Setup.....	34
4.4.5	Site Survey.....	37
4.4.6	WPS	38
4.4.7	Schedule.....	39
4.4.8	LAN Interface Setup.....	40
I	Static DHCP Setup.....	42
4.4.9	WAN Interface Setup.....	43
I	Static IP.....	43
II	DHCP Client	45
III	PPPoE	47
IV	PPTP	50
V	L2TP	54
4.4.10	Firewall - Port Filtering	57
4.4.11	Firewall - IP Filtering.....	58
4.4.12	Firewall - MAC Filtering.....	59
4.4.13	Firewall - Port Forwarding.....	60
4.4.14	Firewall – URL Filtering.....	61
4.4.15	Firewall - DMZ.....	62
4.4.16	Firewall – VLAN	63
4.4.17	QoS	64
4.4.18	Route Setup.....	66
4.4.19	Status.....	68
4.4.20	Management - Statistics	70
4.4.21	Management - Time Zone Setting.....	71
4.4.22	Management - Log.....	72
4.4.23	Management - Upgrade Firmware	72
4.4.24	Management Save/ Reload Settings.....	73
4.4.25	Management - Password Setup.....	74
5	FREQUENTLY ASKED QUESTIONS (FAQ).....	75
5.1	WHAT AND HOW TO FIND MY PC’S IP AND MAC ADDRESS?.....	75
5.2	WHAT IS WIRELESS LAN?	75
5.3	WHAT ARE ISM BANDS?	75

5.4	HOW DOES WIRELESS NETWORKING WORK?.....	75
5.5	WHAT IS BSSID?	76
5.6	WHAT IS ESSID?	76
5.7	WHAT ARE POTENTIAL FACTORS THAT MAY CAUSES INTERFERENCE?	77
5.8	WHAT ARE THE OPEN SYSTEM AND SHARED KEY AUTHENTICATIONS?	77
5.9	WHAT IS WEP?	77
5.10	WHAT IS FRAGMENT THRESHOLD?.....	77
5.11	WHAT IS RTS (REQUEST TO SEND) THRESHOLD?	78
5.12	WHAT IS BEACON INTERVAL?.....	78
5.13	WHAT IS PREAMBLE TYPE?	79
5.14	WHAT IS SSID BROADCAST?	79
5.15	WHAT IS WI-FI PROTECTED ACCESS (WPA)?	79
5.16	WHAT IS WPA2?	80
5.17	WHAT IS 802.1X AUTHENTICATION?	80
5.18	WHAT IS TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)?	80
5.19	WHAT IS ADVANCED ENCRYPTION STANDARD (AES)?	80
5.20	WHAT IS INTER-ACCESS POINT PROTOCOL (IAPP)?.....	80
5.21	WHAT IS WIRELESS DISTRIBUTION SYSTEM (WDS)?.....	81
5.22	WHAT IS UNIVERSAL PLUG AND PLAY (UPNP)?.....	81
5.23	WHAT IS MAXIMUM TRANSMISSION UNIT (MTU) SIZE?.....	81
5.24	WHAT IS CLONE MAC ADDRESS?.....	81
5.25	WHAT IS DDNS?.....	81
5.26	WHAT IS NTP CLIENT?	81
5.27	WHAT IS VPN?.....	81
5.28	WHAT IS IPSEC?.....	82
5.29	WHAT IS WLAN BLOCK RELAY BETWEEN CLIENTS?	82
5.30	WHAT IS WMM?.....	82
5.31	WHAT IS WLAN ACK TIMEOUT?	82
5.32	WHAT IS MODULATION CODING SCHEME (MCS)?	82
5.33	WHAT IS FRAME AGGREGATION?	82
5.34	WHAT IS GUARD INTERVALS (GI)?.....	83
6	CONFIGURATION EXAMPLES.....	83

Revision History

DATE	REVISION OF USER'S MANUAL	FIRMWARE
2012/12/25	Version 1.0	DAR1x1-3221.3

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 Travel AP/Router is an affordable IEEE 802.11b/g/n of wireless LAN Travel AP/Router solution; setting SOHO for high performance, secure, manageable and reliable WLAN.

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

1.1 Package contents

The package of the WLAN Travel AP/Router includes the following items,

- ✓ The WLAN Travel AP/Router
- ✓ The Documentation CD
- ✓ RJ-45 Cable Line (Optional)

1.2 Product Features

Generic AP

- Compatible with IEEE 802.11n Specifications provides wireless speed up to 150Mbps 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, 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption and WPA with Radius function to protect the wireless data transmission.
- Supports IEEE 802.1x Authentication.
- Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- Supports DHCP server to provide clients auto IP addresses assignment.
- Supports WEB based management and configuration.
- Supports NTP client service.
- Supports Log table and remote Log service.

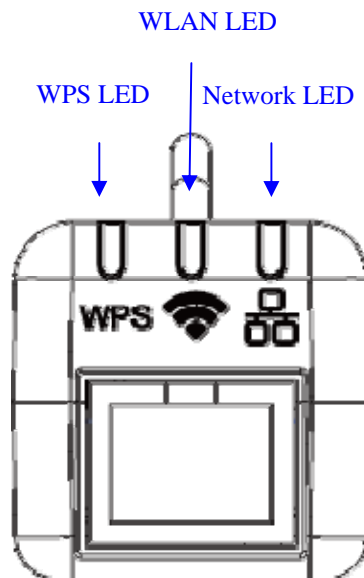
Generic Router

- 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, 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption and

-
- WPA with Radius function to protect the wireless data transmission.
 - Supports IEEE 802.1x Authentication.
 - Supports IEEE 802.3x 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, PPTP L2TP of WAN Interface.
 - Supports firewall security with Port filtering, IP filtering, MAC filtering, Port forwarding, DMZ hosting, URL filtering and Virtual Server functions.
 - Supports WEB based management and configuration.
 - Supports UPnP for automatic Internet access.
 - Supports Dynamic DNS service.
 - Supports NTP client service.
 - Supports Log table and remote Log service.
-

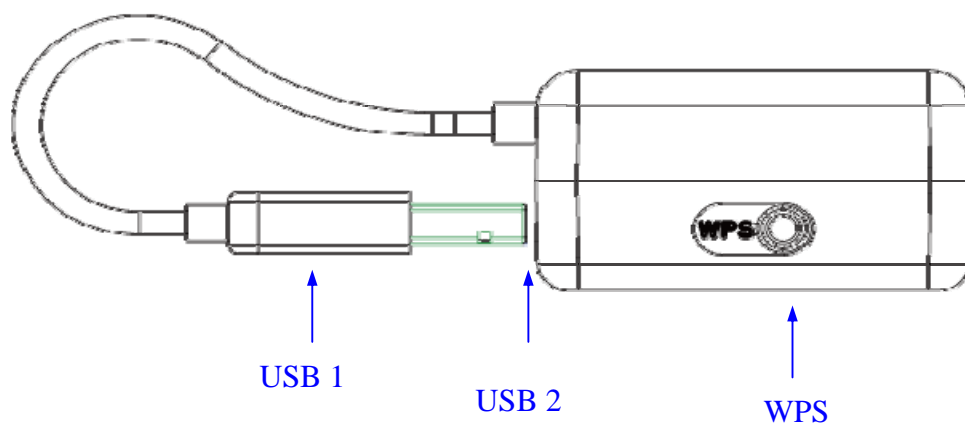
1.3 Panel Description

Front Description



LED Indicator	State	Description
1. WPS LED	Flashing	The WPS feature is Enabled.
	Off	The WPS feature is Disabled.
2. WLAN LED	Flashing	WLAN is transmitting data
	On	WLAN is on
	Off	WLAN is off
3. Network LED ACT	Flashing	Data is transmitting or receiving on the network interface.
	On	Port linked.
	Off	No link.

Side Description



Interfaces	Description
WPS	Push continually the reset button 5 ~ 10 seconds to enable the WPS feature.
USB 1	The USB port is for power adapter
USB 2	Charge mobile device

2 Installation

2.1 Hardware Installation

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

Step 2: Connect the WLAN Travel AP/Router to your wired network. Connect the Ethernet WAN interface of WLAN Travel AP/Router by category 5 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 Travel AP/Router. Use only the USB+AC/DC power adapter supplied with the WLAN Travel AP/Router; it may occur

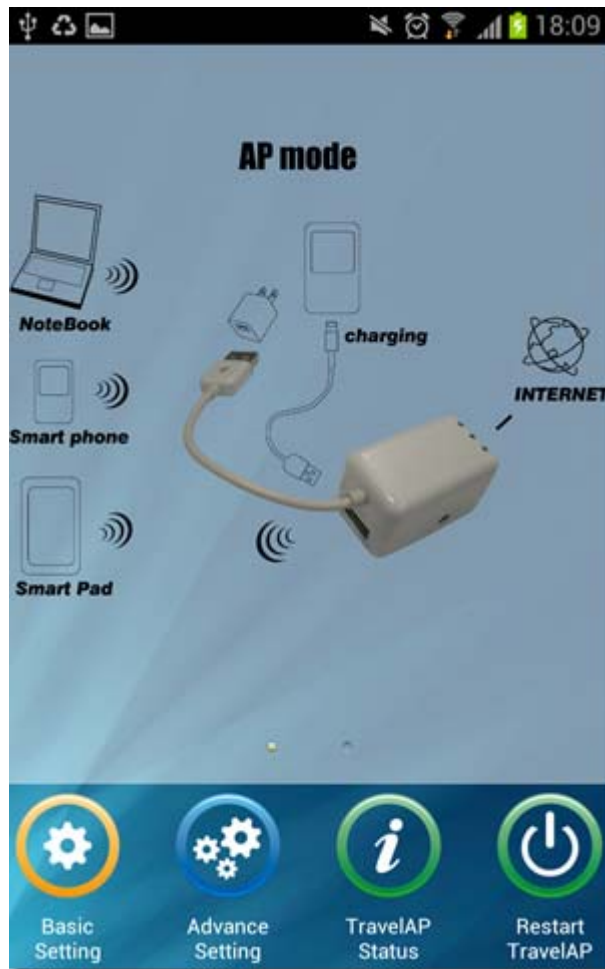
damage by using a different type of power adapter.
The hardware installation finished.

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 50 seconds to complete the boot up sequence after powered on the WLAN Travel AP/Router; After WPS LED flashing stop, the WLAN Travel AP/Router is ready now.

3 App Software Configuration



Screen snapshot – Homepage

Item	Description
Basic Setting	Set up hotspot name, hotspot security
Advance Setting	Set up operation mode, wan settings... etc
Travel AP Status	Show LAN & WAN status
Restart Travel AP	Restart Travel AP

4 Software Configuration

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

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

Default IP Address: **192.168.1.254**

Default IP subnet mask: **255.255.255.0**

WEB login User Name: *<empty>*

WEB login Password: *<empty>*

4.1 Prepare your PC to configure the WLAN Travel AP/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: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 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, XP:

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: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 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: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 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:

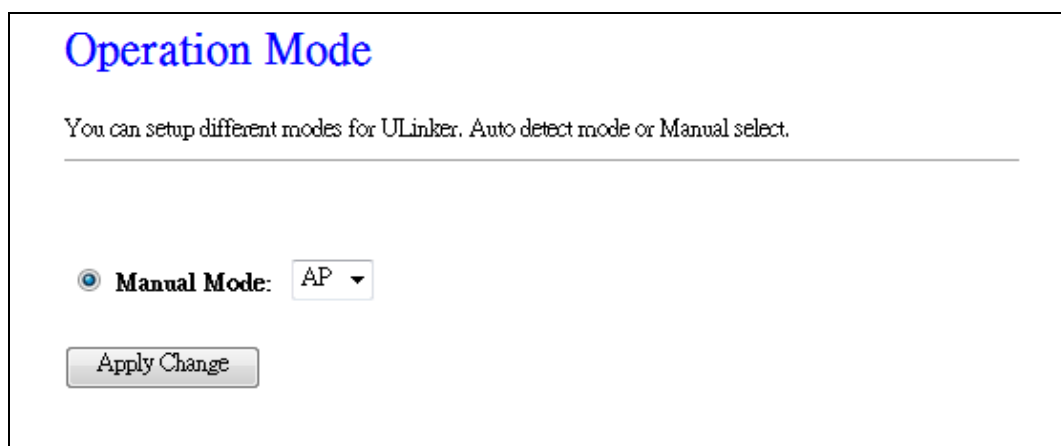
1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Move mouse and double-click the right button on *Network Connections* item. The *Network Connections* window will appear. Double click *Local Area Connection* icon, then *User Account 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: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 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.

4.2 Connect to the WLAN Travel AP/Router

Open a WEB browser, i.e. Microsoft Internet Explore 6.1 SP1 or above, then enter 192.168.1.254 on the URL to connect the WLAN Travel AP/Router.

4.3 Management and configuration on the WLAN Travel AP/Router - AP Mode**4.3.1 Operation Mode**

This page is used to configure which mode WLAN Travel AP/Router acts



Operation Mode

You can setup different modes for ULinker. Auto detect mode or Manual select.

Manual Mode: AP ▼

Apply Change

Screen snapshot – Operation Mode

Item	Description
AP	Each interface (LAN and Wireless) regards as bridge. NAT, Firewall and all router's functions are not supported
Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.

4.3.2 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Travel AP/Router. Here you may change wireless encryption settings as well as wireless network parameters.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band:

Mode:

Network Type:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Broadcast SSID:

WMM:

Data Rate:

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended

Interface:

Screen snapshot – Wireless Basic Settings

Item	Description
Band	Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(N) / 2.4GHz(B+G)/ 2.4GHz(G+N) / 2.4GHz(B+G+N)
Mode	Click to select the WLAN AP wireless mode.
Network Type	While Mode is selected to be Client . Click to select the network type infrastructure or Ad hoc.

SSID	It is the wireless network name. The SSID can be 32 bytes long.
Channel Width	Select the operating channel width 20 MHz or 40 MHz. [N band only]
Control Sideband	Select the Sideband with Upper or Lower for channel width 40MHz. [N band only]
Channel Number	Select the wireless communication channel from pull-down menu.
Broadcast SSID	Click to enable or disable the SSID broadcast function. Refer to 4.14 What is SSID Broadcast?
WMM	Click <i>Enabled/Disabled</i> to init WMM feature. [B/G/B+G Mode only]
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS. Refer to 4.32 What is Modulation Coding Schemes (MCS)?
Associated Clients	Click the <i>Show Active Clients</i> button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.
Enable Mac Clone (Single Ethernet Client)	Take Laptop NIC MAC address as wireless client MAC address. [Client Mode only]
Enable Universal Repeater Mode	Click to enable Universal Repeater Mode
SSID of Extended Interface	Assign SSID when enables Universal Repeater Mode.
Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.

4.3.3 Wireless - Advanced Settings

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

Wireless Advanced Settings

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

Fragment Threshold: (256-2346)
RTS Threshold: (0-2347)
Beacon Interval: (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
STBC: Enabled Disabled
20/40MHz Coexist: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%

Screen snapshot – Wireless Advanced Settings

Item	Description
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes. Refer to 4.10 What is Fragment Threshold?
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes. Refer to 4.11 What is RTS(Request To Send) Threshold?
Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms. Refer to 4.12 What is Beacon Interval?
Preamble Type	Click to select the <i>Long Preamble</i> or <i>Short Preamble</i> support on the wireless data packet transmission.

	Refer to 4.13 What is Preamble Type?
IAPP	Click to enable or disable the IAPP function. Refer to 4.20 What is Inter-Access Point Protocol(IAPP)?
Protection	Protect 802.11n user priority.
Aggregation	Click to enable or disable the Aggregation function. Refer to 4.33 What is Aggregation?
Short GI	Click to enable or disable the short Guard Intervals function. Refer to 4.34 What is Guard Intervals (GI)?
WLAN Partition	Click to enable or disable that prevents associated wireless clients from communication with each other.
STBC	Click to enable or disable the STBC function.
20/40MHz Coexist	Click to enable or disable the 20/40MHz Coexist function.
RF Output Power	To adjust transmission power level.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.3.4 Wireless - Security Setup

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

Wireless Security Setup

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

Select SSID:

Encryption:

802.1x Authentication:

Authentication: Open System Shared Key Auto

Key Length:

Key Format:

Encryption Key:

Wireless Security Setup

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

Select SSID:

Encryption:

Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key Format:

Pre-Shared Key:

Screen snapshot – Wireless Security Setup

Item	Description
Select SSID	Select the SSID from multiple APs.
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA, WPA2 or

	WPA-Mixed Refer to 4.9 What is WEP? 4.15 What is Wi-Fi Protected Access (WPA)? 4.16 What is WPA2?
Use 802.1x Authentication	While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function. Refer to 4.17 What is 802.1x Authentication?
Authentication Type	Click to select the authentication type in <i>Open System</i> , <i>Shared Key</i> or <i>Auto</i> selection.
Key Length	Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.
Encryption Key	Secret key of WEP security encryption function.
WPA Authentication Mode	While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key). Refer to 4.15 What is Wi-Fi Protected Access (WPA)?
WPA Cipher Suite	Select the Cipher Suite for WPA encryption. 4.18 What is Temporal Key Integrity Protocol (TKIP)? 4.19 What is Advanced Encryption Standard (AES)?
WPA2 Cipher Suite	Select the Cipher Suite for WPA2 encryption.
Pre-Shared Key Format	While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). [WPA, Personal(Pre-Shared Key) only]
Pre-Shared Key	Fill in the key value. [WPA, Personal(Pre-Shared Key) only]
Enable Pre-Authentication	Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only]
Authentication	Set the IP address, port and login password information

RADIUS Server	of authentication RADIUS sever.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

WEP encryption key (secret key) length:

Length \ Format	64-bit	128-bit
ASCII	5 characters	13 characters
HEX	10 hexadecimal codes	26 hexadecimal codes

4.3.5 Site Survey

This page is used to view or configure other APs near yours.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Site Survey

SSID	BSSID	Channel	Type	Encrypt	Signal
Belkin_N_Wireless	00:17:3f:c2:9d:2b	3 (B+G+N)	AP	no	46
TEST01	00:02:72:9d:5d:9f	11 (B+G+N)	AP	no	40
Kevin-WLAN	00:02:72:70:e6:11	11 (B+G)	AP	no	38
MyWLAN-mark	12:34:56:00:03:ab	6 (B+G+N)	AP	no	36
TOTOLINK N300RT	78:44:76:d6:82:80	2 (B+G+N)	AP	WPA2-PSK	26
gigabyte	00:18:e7:ed:27:ed	2 (B+G+N)	AP	no	26
Wayne2	00:0a:d8:02:19:02	5 (B+G+N)	AP	no	24
Y-36967	c8:6c:87:24:51:16	6 (B+G)	AP	WPA-PSK	24
Welead	90:94:e4:b1:59:6e	1 (B+G+N)	AP	WPA-PSK/WPA2-PSK	24
ianchen	20:10:7a:80:19:1d	9 (B+G)	AP	WPA-PSK/WPA2-PSK	24
Wayne	00:0a:d8:02:90:28	5 (B+G+N)	AP	WPA-PSK	24
Sky-Vault	00:0a:d8:02:6b:f4	11 (B+G+N)	AP	no	24
nexgen-ap2	48:5b:39:e8:76:ca	7 (B+G+N)	AP	WEP	24
SW-TEST1	00:1f:1f:38:65:6c	4 (B+G)	AP	WEP	22

Screen snapshot – Wireless Site Survey

Item	Description
Site Survey	Click the <i>SiteSurvey</i> button to re-scan site survey on the screen.
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Type	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.
Select	Click to select AP or client you'd like to connect.
Connect	Click the <i>Connect</i> button to establish connection.

4.3.6 WPS

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

Wi-Fi Protected Setup

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

Disable WPS

WPS Status:
 Configured
 UnConfigured

Auto-lock-down state: unlocked

Self-PIN Number: 21595684

Push Button Configuration:

STOP WSC

Client PIN Number:

Screen snapshot – Wi-Fi Protected Setup

Item	Description
Disable WPS	Click on to disable the Wi-Fi Protected Setup function.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
WPS Status	Show WPS status is <i>Configured</i> or <i>UnConfigured</i> .
Auto-lock-down state	Show Auto-lock-down state is <i>locked</i> or <i>Unlocked</i> .
Self-PIN Number	Fill in the PIN Number of AP to register the wireless distribution system access capability.
Push Button Configuration	The <i>Start PBC</i> button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could connect it automatically when client join PBC mode.
STOP WSC	Click on to stop the WSC function.
Client PIN Number	Fill in the <i>Client PIN Number</i> from your Client sites.

4.3.7 Schedule

This page is to configure the wireless activation timestamp by users.

Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

Enable Wireless Schedule

Enable	Day	From		To	
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)
<input type="checkbox"/>	Sun ▼	00 ▼ (hour)	00 ▼ (min)	00 ▼ (hour)	00 ▼ (min)

Screen snapshot – Wireless Schedule

Item	Description
Enable Wireless Schedule	Click on to enable the wireless schedule function.
Day	Click the one or more of days to set the rules.
From	Click 24 hrs or set the starting time.
To	Click 24 hrs or set the ending time.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.3.8 LAN Interface Setup

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

LAN Interface Setup

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

IP Address:

Subnet Mask:

DHCP: ▾

DHCP Client Range: -

DHCP Lease Time: (1 ~ 10080 minutes)

Static DHCP:

Domain Name:

802.1d Spanning Tree: ▾

Clone MAC Address:

Screen snapshot – LAN Interface Setup

Item	Description
IP Address	Fill in the IP address of LAN interfaces of this WLAN Access Point.
Subnet Mask	Fill in the subnet mask of LAN interfaces of this WLAN Access Point.
DHCP	Click to select <i>Disabled</i> , <i>Client</i> or <i>Server</i> in different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
Show Client	Click to open the <i>Active DHCP Client Table</i> window that shows the active clients with their assigned IP address, MAC address and time expired information. [Server mode only]
DHCP Lease Time	Fill in the DHCP Lease Time from the range.
Static DHCP	Select enable or disable the Static DHCP function from pull-down menu. [Server mode only]
Set Static DHCP	Manual setup Static DHCP IP address for specific MAC address. [Server mode only]
Domain Name	Assign Domain Name and dispatch to DHCP clients. It is optional field.
802.1d Spanning Tree	Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.

I Static DHCP Setup

Static DHCP Setup

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

Enable Static DHCP

IP Address:

MAC Address:

Comment:

Static DHCP List:

IP Address	MAC Address	Comment	Select

Screen snapshot – Static DHCP Setup

Item	Description
Enable Static DHCP	Click on to enable the Static DHCP function.
IP Address	If you select the Set Static DHCP on LAN interface, fill in the IP address for it.
MAC Address	If you select the Set Static DHCP on LAN interface, fill in the MAC address for it.
Comment	Fill in the comment tag for the registered Static DHCP.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Static DHCP List	It shows IP Address 、MAC Address from the Static DHCP.
Delete Selected	Click to delete the selected clients that will be removed from the Static DHCP list.
Delete All	Click to delete all the registered clients from the Static DHCP list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.3.9 Status

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

System	
Uptime	Oday:0h:4m:25s
Firmware Version	WS2x2-3.2.2.1
Build Time	Mon Nov 26 01:08:08 PST 2012
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	MyWLAN
Channel Number	11
Encryption	Disabled
BSSID	00:02:72:81:96:d1
Associated Clients	1
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:02:72:81:96:d1
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:02:72:81:96:d2

Screen snapshot – Status

Item	Description
System	
Uptime	It shows the duration since WLAN Travel AP/Router is powered on.
Firmware version	It shows the firmware version of WLAN Travel AP/Router.
Build time	It shows the Build-up time of firmware
Wireless configuration	
Mode	It shows wireless operation mode

Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this WLAN Travel AP/Router. The SSID is the unique name of WLAN Travel AP/Router and shared among its service area, so all devices attempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of the WLAN Travel AP/Router. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
TCP/IP configuration	
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of WLAN Travel AP/Router.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of WLAN Travel AP/Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of WLAN Travel AP/Router.
WAN configuration	
Attain IP Protocol	It shows how the WLAN Travel AP/Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP /GSM 3.5G connection.
IP Address	It shows the IP address of WAN interface of WLAN Travel AP/Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of WLAN Travel AP/Router.
Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
MAC Address	It shows the MAC address of WAN interface of WLAN Travel AP/Router.

WAN Link Status It shows WAN connection status.

4.3.10 Management - Statistics

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

Statistics

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

Wireless LAN	<i>Sent Packets</i>	1361
	<i>Received Packets</i>	25883
Ethernet LAN	<i>Sent Packets</i>	1529
	<i>Received Packets</i>	1269
Ethernet WAN	<i>Sent Packets</i>	597
	<i>Received Packets</i>	30386

Screen snapshot – Management - Statistics

Item	Description
Wireless LAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN <i>Received Packets</i>	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the Ethernet LAN interface.
Ethernet LAN <i>Received Packets</i>	It shows the statistic count of received packets on the Ethernet LAN interface.
Ethernet WAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the Ethernet WAN interface.
Ethernet WAN <i>Received Packets</i>	It shows the statistic count of received packets on the Ethernet WAN interface.
Refresh	Click the refresh the statistic counters on the screen.

4.3.11 Management - Time Zone Setting

This page is used to configure NTP client to get current time.

Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server :

(Manual IP Setting)

Screen snapshot – Management – Time Zone Settings

Item	Description
Current Time	It shows the current time.
Copy Computer Time	Click the <i>Copy Computer Time</i> button.
Time Zone Select	Click the time zone in your country.
Enable NTP client update	Click the checkbox to enable NTP client update. Refer to 4.26 What is NTP Client?
Automatically Adjust Daylight Saving	Click to enable Daylight Saving adjustment automatically.
NTP Server	Click select default or input NTP server IP address.
Apply Change	Click the <i>Apply Changes</i> button to save and enable NTP client service.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.
Refresh	Click the refresh the current time shown on the screen.

4.3.12 Management - Log

This page is used to configure the remote log server and shown the current log.

System Log

This page can be used to set remote log server and show the system log.

Enable Log
 system all **wireless** **DoS**
 Enable Remote Log **Log Server IP Address:**

```

Nov 26 05:54:56 klogd started: BusyBox v1.13.4 (2012-11-14 00:23:41 PST)
Nov 26 05:54:56 RTL8192C/RTL8188C driver version 1.5 (2012-05-04)
Nov 26 05:54:56 Probing RTL8186 10/100 NIC-kernel stack size order[3]...
Nov 26 05:54:56 chip name: 8196C, chip revid: 0
Nov 26 05:54:56 NOT YET
Nov 26 05:54:56 eth0 added. vid=9 Member port 0x1...
Nov 26 05:54:56 eth1 added. vid=8 Member port 0x10...
Nov 26 05:54:56 eth2 added. vid=9 Member port 0x2...
Nov 26 05:54:56 eth3 added. vid=9 Member port 0x4...
Nov 26 05:54:56 eth4 added. vid=9 Member port 0x8...
Nov 26 05:54:56 eth5 added. vid=9 Member port 0x0...
Nov 26 05:54:56 wlan0: A expired STA is resumed - 02:0A:D8:02:19:02
    
```

Screen snapshot – Management – Log

Item	Description
Enable Log	Click the checkbox to enable log.
<i>System all</i>	Show all log of WLAN Travel AP/Router
<i>Wirelessy</i>	Only show wireless log
<i>DoS</i>	Only show Denial-of-Service log
<i>Enable Remote Log</i>	Click the checkbox to enable remote log service.
<i>Log Server IP Address</i>	Input the remote log IP address
Apply Changes	Click the Apply Changes button to save above settings.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen

4.3.13 Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Firmware Version: WS2x2-3.2.2.1

Select File:

Screen snapshot – Management - Upgrade Firmware

Item	Description
Select File	Click the Browse button to select the new version of web firmware image file.
Firmware Version	It shows the current firmware version.
Upload	Click the Upload button to update the selected web firmware image to the WLAN Travel AP/Router.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.3.14 Management Save/ Reload Settings

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

Save/Reload Settings

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

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Screen snapshot – Management - Save/Reload Settings

Item	Description
Save Settings to File	Click the Save button to download the configuration parameters to your personal computer.
Load Settings from File	Click the Browse button to select the configuration files then click the Upload button to update the selected configuration to the WLAN Travel AP/Router.
Reset Settings to Default	Click the Reset button to reset the configuration parameter to factory defaults.

4.3.15 Management - Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Screen snapshot – Management - Password Setup

Item	Description
User Name	Fill in the user name for web management login control.
New Password	Fill in the password for web management login control.
Confirmed Password	Because the password input is invisible, so please fill in the password again for confirmation purpose.
Apply Changes	Clear the User Name and Password fields to empty, means to apply no web management login control. Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4 Management and configuration on the WLAN Travel AP/Router - Router Mode

4.4.1 ULinker Operation Mode

This page is used to configure which mode WLAN Travel AP/Router acts

Operation Mode

You can setup different modes for ULinker. Auto detect mode or Manual select.

Manual Mode:
Router ▼

Screen snapshot – ULinker Operation Mode

Item	Description
Router	Each interface (LAN and Wireless) regards as bridge. NAT, Firewall and all router's functions.
Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.

4.4.2 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Travel AP/Router. Here you may change wireless encryption settings as well as wireless network parameters.

Band: 2.4 GHz (B+G+N) ▼
Mode: AP ▼ Multiple AP
Network Type: Infrastructure ▼
SSID: Travel6cl Add to Profile
Channel Width: 40MHz ▼
Control Sideband: Upper ▼
Channel Number: 11 ▼
Broadcast SSID: Enabled ▼
WMM: Enabled ▼
Data Rate: Auto ▼
Associated Clients: Show Active Clients
 Enable Mac Clone (Single Ethernet Client)
 Enable Universal Repeater Mode (Acting as AP and client simultaneously)
SSID of Extended Add to Profile
Interface: Travel RPT0
Apply Changes Reset

Screen snapshot – Wireless Basic Settings

Item	Description
Band	Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(N) 2.4GHz(B+G)/ 2.4GHz(G+N) / 2.4GHz(B+G+N)
Mode	Click to select the WLAN AP wireless mode.
Network Type	While Mode is selected to be Client . Click to select the network type infrastructure or Ad hoc.
SSID	It is the wireless network name. The SSID can be 32 bytes long.
Channel Width	Select the operating channel width 20 MHz or 40 MHz. [N band only]
Control Sideband	Select the Sideband with Upper or Lower for channel

	width 40MHz. [N band only]
Channel Number	Select the wireless communication channel from pull-down menu.
Broadcast SSID	Click to enable or disable the SSID broadcast function. Refer to 4.14 What is SSID Broadcast?
WMM	Click <i>Enabled/Disabled</i> to init WMM feature. [B/G/B+G Mode only]
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS. Refer to 4.32 What is Modulation Coding Schemes (MCS)?
Associated Clients	Click the <i>Show Active Clients</i> button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.
Enable Mac Clone	Take Laptop NIC MAC address as wireless client MAC (Single Ethernet Client) address. [Client Mode only]
Enable Universal Repeater Mode	Click to enable Universal Repeater Mode
SSID of Extended Interface	Assign SSID when enables Universal Repeater Mode.
Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.

4.4.3 Wireless - Advanced Settings

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

Wireless Advanced Settings

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

Fragment Threshold: (256-2346)
RTS Threshold: (0-2347)
Beacon Interval: (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
20/40MHz Coexist: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%

Screen snapshot – Wireless Advanced Settings

Item	Description
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes. Refer to 4.10 What is Fragment Threshold?
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes. Refer to 4.11 What is RTS(Request To Send) Threshold?
Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms. Refer to 4.12 What is Beacon Interval?
Preamble Type	Click to select the <i>Long Preamble</i> or <i>Short Preamble</i> support on the wireless data packet transmission. Refer to 4.13 What is Preamble Type?
IAPP	Click to enable or disable the IAPP function.

	Refer to 4.20 What is Inter-Access Point Protocol(IAPP)?
Protection	Protect 802.11n user priority.
Aggregation	Click to enable or disable the Aggregation function. Refer to 4.33 What is Aggregation?
Short GI	Click to enable or disable the short Guard Intervals function. Refer to 4.34 What is Guard Intervals (GI)?
WLAN Partition	Click to enable or disable that prevents associated wireless clients from communication with each other.
20/40MHz Coexist	Click to enable or disable the 20/40MHz Coexist function.
RF Output Power	To adjust transmission power level.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.4 Wireless - Security Setup

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

Wireless Security Setup

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

Select SSID: Root AP - Travel6cl Apply Changes Reset

Encryption: WEP

802.1x Authentication:

Authentication: Open System Shared Key Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

Encryption Key: *****

Wireless Security Setup

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

Select SSID: Root AP - Travel6cl Apply Changes Reset

Encryption: WPA2

Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Screen snapshot – Wireless Security Setup

Item	Description
Select SSID	Select the SSID from multiple APs.
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA, WPA2 or WPA-Mixed Refer to 4.9 What is WEP? 4.15 What is Wi-Fi Protected Access (WPA)? 4.16 What is WPA2?
Use 802.1x Authentication	While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function. Refer to 4.17 What is 802.1x Authentication?
Authentication Type	Click to select the authentication type in Open System , Shared Key or Auto selection.
Key Length	Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys. The WEP key is composed of initialization vector (24

	bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.
Encryption Key	Secret key of WEP security encryption function.
WPA Authentication Mode	While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key). Refer to 4.15 What is Wi-Fi Protected Access (WPA)?
WPA Cipher Suite	Select the Cipher Suite for WPA encryption. 4.18 What is Temporal Key Integrity Protocol (TKIP)? 4.19 What is Advanced Encryption Standard (AES)?
WPA2 Cipher Suite	Select the Cipher Suite for WPA2 encryption.
Pre-Shared Key Format	While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). [WPA, Personal(Pre-Shared Key) only]
Pre-Shared Key	Fill in the key value. [WPA, Personal(Pre-Shared Key) only]
Authentication RADIUS Server	Set the IP address, port and login password information of authentication RADIUS sever.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

WEP encryption key (secret key) length:

		Length	
		64-bit	128-bit
Format	ASCII	5 characters	13 characters
	HEX	10 hexadecimal codes	26 hexadecimal codes

4.4.5 Site Survey

This page is used to view or configure other APs near yours.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Site Survey

SSID	BSSID	Channel	Type	Encrypt	Signal
TOTOLINK_N300RT	78:44:76:d6:82:80	2 (B+G+N)	AP	WPA2-PSK	40
Sky-Vault_08	00:0a:d8:02:6c:08	11 (B+G+N)	AP	no	40
328_test2	00:02:72:34:53:45	11 (B+G+N)	AP	WPA2-PSK	38
Belkin_N_Wireless	00:17:3f:c2:9d:2b	3 (B+G+N)	AP	no	38
SW-TEST1	00:1f:1f:38:65:6c	9 (B+G)	AP	WEP	36
ANDY_317	00:02:72:f1:23:a1	7 (B+G+N)	AP	WPA2-PSK	36

Screen snapshot – Wireless Site Survey

Item	Description
Site Survey	Click the <i>SiteSurvey</i> button to re-scan site survey on the screen.
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Type	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.

4.4.6 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.

Wi-Fi Protected Setup

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.

Disable WPS

WPS Status: Configured UnConfigured

Auto-lock-down state: unlocked

Self-PIN Number: 99956042

Push Button Configuration:

STOP WSC

Client PIN Number:

Screen snapshot – Wi-Fi Protected Setup

Item	Description
Disable WPS	Click on to disable the Wi-Fi Protected Setup function.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
WPS Status	Show WPS status is <i>Configured</i> or <i>UnConfigured</i> .
Auto-lock-down state	Show Auto-lock-down state is <i>locked</i> or <i>Unlocked</i> .
Self-PIN Number	Fill in the PIN Number of AP to register the wireless distribution system access capability.
Push Button	The <i>Start PBC</i> button provides tool to scan the wireless

Configuration	network. If any Access Point or IBSS is found, you could connect it automatically when client join PBC mode.
STOP WSC	Click on to stop the WSC function.
Client PIN Number	Fill in the <i>Client PIN Number</i> from your Client sites.

4.4.7 Schedule

This page is to configure the wireless activation timestamp by users.

Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

Enable Wireless Schedule

Enable	Day	From		To					
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
<input type="checkbox"/>	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)

Screen snapshot – Wireless Schedule

Item	Description
Enable Wireless Schedule	Click on to enable the wireless schedule function.
Day	Click the one or more of days to set the rules.
From	Click 24 hrs or set the starting time.
To	Click 24 hrs or set the ending time.

Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.8 LAN Interface Setup

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

LAN Interface Setup

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

IP Address:

Subnet Mask:

DHCP:

DHCP Client Range: -

DHCP Lease Time: (1 ~ 10080 minutes)

Static DHCP:

802.1d Spanning Tree:

Clone MAC Address:

Screen snapshot – LAN Interface Setup

Item	Description
IP Address	Fill in the IP address of LAN interfaces of this WLAN Access Point.
Subnet Mask	Fill in the subnet mask of LAN interfaces of this WLAN Access Point.

DHCP	Click to select <i>Disabled</i> , <i>Client</i> or <i>Server</i> in different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
Show Client	Click to open the <i>Active DHCP Client Table</i> window that shows the active clients with their assigned IP address, MAC address and time expired information. [Server mode only]
DHCP Lease Time	Fill in the DHCP Lease Time from the range.
Static DHCP	Select enable or disable the Static DHCP function from pull-down menu. [Server mode only]
Set Static DHCP	Manual setup Static DHCP IP address for specific MAC address. [Server mode only]
802.1d Spanning Tree	Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.

I Static DHCP Setup

Static DHCP Setup

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

Enable Static DHCP

IP Address:

MAC Address:

Comment:

Static DHCP List:

IP Address	MAC Address	Comment	Select

Screen snapshot – Static DHCP Setup

Item	Description
Enable Static DHCP	Click on to enable the Static DHCP function.
IP Address	If you select the Set Static DHCP on LAN interface, fill in the IP address for it.
MAC Address	If you select the Set Static DHCP on LAN interface, fill in the MAC address for it.
Comment	Fill in the comment tag for the registered Static DHCP.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Static DHCP List	It shows IP Address 、MAC Address from the Static DHCP.
Delete Selected	Click to delete the selected clients that will be removed from the Static DHCP list.
Delete All	Click to delete all the registered clients from the Static DHCP list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.9 WAN Interface Setup

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 IP, DHCP, PPPoE , PPTP L2TP or GSM 3.5G by click the item value of WAN Access Type.

I Static IP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: Static IP ▼

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

MTU Size: 1500 (1400-1500 bytes)

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

- Enable uPNP
- Enable IGMP Proxy
- Enable Ping Access on WAN
- Enable Web Server Access on WAN
- Enable IPsec pass through on VPN connection
- Enable PPTP pass through on VPN connection
- Enable L2TP pass through on VPN connection
- Enable IPv6 pass through on VPN connection

Screen snapshot – WAN Interface Setup – Static IP

Item	Description
Static IP	Click to select Static IP support on WAN interface. There

	are IP address, subnet mask and default gateway settings need to be done.
IP Address	If you select the Static IP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the Static IP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the Static IP support on WAN interface, fill in the default gateway for it.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1500.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy on WAN.
Enable Ping Access on WAN	Click the checkbox to enable Ping Access on WAN.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPsec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Enable IPv6 pass through VPN connection	Click the checkbox to enable IPv6 packet pass through.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.

Reset Click the *Reset* button to abort change and recover the previous configuration setting.

II DHCP Client

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client ▾

Host Name:

MTU Size: 1492 (1400-1492 bytes)

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

Enable uPNP

Enable IGMP Proxy

Enable Ping Access on WAN

Enable Web Server Access on WAN

Enable IPsec pass through on VPN connection

Enable PPTP pass through on VPN connection

Enable L2TP pass through on VPN connection

Enable IPv6 pass through on VPN connection

Apply Changes
Reset

Screen snapshot – WAN Interface Setup – DHCP Client

Item	Description
DHCP Client	Click to select DHCP support on WAN interface for IP address assigned automatically from a DHCP server.

Host Name	Fill in the host name of Host Name. The default value is empty
MTU Size	Fill in the mtu size of MTU Size. The default value is 1492
Attain DNS Automatically	Click to select getting DNS address for DHCP support. Please select Set DNS Manually if the DHCP support is selected.
Set DNS Manually	Click to select getting DNS address for DHCP support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPsec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Enable IPv6 pass through on VPN connection	Click the checkbox to enable IPv6 packet pass through
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

III PPPoE

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type:	<input type="text" value="PPPoE"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Service Name(AC):	<input type="text"/>
Connection Type:	<input type="text" value="Continuous"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Idle Time:	<input type="text" value="5"/> (1-1000 minutes)
MTU Size:	<input type="text" value="1452"/> (1360-1492 bytes)
<input type="radio"/> Attain DNS Automatically	
<input checked="" type="radio"/> Set DNS Manually	
DNS 1:	<input type="text"/>
DNS 2:	<input type="text"/>
DNS 3:	<input type="text"/>
Clone MAC Address:	<input type="text" value="000000000000"/>
<input type="checkbox"/> Enable uPNP	
<input checked="" type="checkbox"/> Enable IGMP Proxy	
<input type="checkbox"/> Enable Ping Access on WAN	
<input type="checkbox"/> Enable Web Server Access on WAN	
<input checked="" type="checkbox"/> Enable IPsec pass through on VPN connection	
<input checked="" type="checkbox"/> Enable PPTP pass through on VPN connection	
<input checked="" type="checkbox"/> Enable L2TP pass through on VPN connection	
<input type="checkbox"/> Enable IPv6 pass through on VPN connection	
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

Screen snapshot – WAN Interface Setup – PPPoE

Item	Description
PPPoE	Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.
User Name	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.
Service Name(AC)	Fill in the service name of Service Name. The default value is empty.
Connection Type	<p>Select the connection type from pull-down menu. There are <i>Continuous</i>, <i>Connect on Demand</i> and <i>Manual</i> three types to select.</p> <p><i>Continuous</i> connection type means to setup the connection through PPPoE protocol whenever this WLAN Broadband Router is powered on.</p> <p><i>Connect on Demand</i> connection type means to setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set.</p> <p><i>Manual</i> connection type means to setup the connection through the PPPoE protocol by clicking the <i>Connect</i> button manually, and clicking the <i>Disconnect</i> button manually.</p>
Idle Time	If you select the PPPoE and Connect on Demand connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1452. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Attain DNS Automatically	Click to select getting DNS address for <i>PPPoE</i> support. Please select <i>Set DNS Manually</i> if the <i>PPPoE</i> support is selected.

Set DNS Manually	Click to select getting DNS address for <i>Static IP</i> support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPsec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Enable IPv6 pass through on VPN connection	Click the checkbox to enable IPv6 packet pass through
Apply Changes	Click the <i>Apply Changes</i> button to complete the new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.

IV PPTP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type:

Dynamic IP (DHCP)
 Static IP

IP Address:
Subnet Mask:
Default Gateway:
Server IP Address(Or Domain Name):
User Name:
Password:

Connection Type:

Idle Time: (1-1000 minutes)
MTU Size: (1400-1460 bytes)

Request MPPE Encryption **Request MPPC Compression**

Attain DNS Automatically
 Set DNS Manually

DNS 1:
DNS 2:
DNS 3:

Clone MAC Address:

Enable uPNP
 Enable IGMP Proxy
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection
 Enable IPv6 pass through on VPN connection

Screen snapshot – WAN Interface Setup – PPTP

Item	Description
PPTP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection.
Dynamic IP (DHCP)	Click the checkbox to enable Dynamic IP (DHCP).
Static IP	Click the checkbox to enable Static IP.
IP Address	If you select the PPTP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the PPTP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the PPTP support on WAN interface, fill in the default gateway for it.
Server IP Address	Enter the IP address of the PPTP Server.
User Name	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Password	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Connection Type	Select the connection type from pull-down menu. There are Continuous , Connect on Demand and Manual three types to select. Continuous connection type means to setup the connection through PPTP protocol whenever this WLAN Broadband Router is powered on. Connect on Demand connection type means to setup the connection through PPTP protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPTP connection while there are no data sent out longer than the idle time set. Manual connection type means to setup the connection through the PPTP protocol by clicking the Connect button manually, and clicking the Disconnect button manually.
Idle Time	If you select the PPTP and Connect on Demand

	connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1460. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Request MPPE Encryption	Click the checkbox to enable request MPPE encryption.
Request MPPC Compression	Click the checkbox to enable request MPPC compression.
Attain DNS Automatically	Click to select getting DNS address for <i>PPTP</i> support. Please select <i>Set DNS Manually</i> if the <i>PPTP</i> support is selected.
Set DNS Manually	Click to select getting DNS address for <i>PPTP</i> support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPsec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Enable IPv6 pass through on VPN	Click the checkbox to enable IPv6 packet pass through

connection

Apply Changes

Click the *Apply Changes* button to complete the new configuration setting.

Reset

Click the *Reset* button to abort change and recover the previous configuration setting.

V L2TP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type:

Dynamic IP (DHCP)
 Static IP

IP Address:

Subnet Mask:

Default Gateway:

Server IP Address(Or Domain Name):

User Name:

Password:

Connection Type:

Idle Time: (1-1000 minutes)

MTU Size: (1400-1460 bytes)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable uPNP
 Enable IGMP Proxy
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection
 Enable IPv6 pass through on VPN connection

Screen snapshot – WAN Interface Setup – PPTP

Item	Description
L2TP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded L2TP client supported by this router to make a VPN connection.
Dynamic IP (DHCP)	Click the checkbox to enable Dynamic IP (DHCP).
Static IP	Click the checkbox to enable Static IP.
IP Address	If you select the L2TP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the L2TP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the PPTP support on WAN interface, fill in the default gateway for it.
Server IP Address	Enter the IP address of the L2TP Server.
User Name	If you select the L2TP support on WAN interface, fill in the user name and password to login the L2TP server.
Password	If you select the L2TP support on WAN interface, fill in the user name and password to login the L2TP server.
Connection Type	Select the connection type from pull-down menu. There are Continuous , Connect on Demand and Manual three types to select. Continuous connection type means to setup the connection through L2TP protocol whenever this WLAN Broadband Router is powered on. Connect on Demand connection type means to setup the connection through L2TP protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the L2TP connection while there are no data sent out longer than the idle time set. Manual connection type means to setup the connection through the L2TP protocol by clicking the Connect button manually, and clicking the Disconnect button manually.
Idle Time	If you select the L2TP and Connect on Demand connection type, fill in the idle time for auto-disconnect

	function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1460. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Attain DNS Automatically	Click to select getting DNS address for L2TP support. Please select Set DNS Manually if the L2TP support is selected.
Set DNS Manually	Click to select getting DNS address for L2TP support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPsec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Enable IPv6 pass through on VPN connection	Click the checkbox to enable IPv6 packet pass through
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.10 Firewall - Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering

Port Range: - Protocol: Both Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
20-21	TCP+UDP	FTP	<input type="checkbox"/>

Screen snapshot – Firewall - Port Filtering

Item	Description
Enable Port Filtering	Click to enable the port filtering security function.
Port Range	To restrict data transmission from the local network on certain ports, fill in the range of start-port and end-port, and the protocol, also put your comments on it. The Protocol can be TCP, UDP or Both. Comments let you know about whys to restrict data from the ports.
Protocol	
Comments	
Apply Changes	Click the Apply Changes button to register the ports to port filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.

Reset Click the *Reset* button to abort change and recover the previous configuration setting.

4.4.11 Firewall - IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering
 Local IP Address: Protocol: Both Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
192.168.1.201	TCP+UDP	ST-1	<input type="checkbox"/>
192.168.1.202	TCP	ST-2	<input type="checkbox"/>

Screen snapshot – Firewall - IP Filtering

Item	Description
Enable IP Filtering	Click to enable the IP filtering security function.
Local IP Address	To restrict data transmission from local network on certain IP addresses, fill in the IP address and the
Protocol	protocol, also put your comments on it.
Comments	The <i>Protocol</i> can be TCP, UDP or Both. <i>Comments</i> let you know about whys to restrict data from the IP address.
Apply Changes	Click the <i>Apply Changes</i> button to register the IP address to IP filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address that will be removed from the IP-filtering list.

Delete All	Click to delete all the registered entries from the IP-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.12 Firewall - MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable MAC Filtering

MAC Address: Comment:

Current Filter Table:

MAC Address	Comment	Select
00:02:72:00:81:90	ST-1	<input type="checkbox"/>
00:02:72:00:81:91	ST-2	<input type="checkbox"/>

Screen snapshot – Firewall - MAC Filtering

Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address	To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it.
Comments	Comments let you know about why to restrict data from the MAC address.
Apply Changes	Click the Apply Changes button to register the MAC address to MAC filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected MAC address that will be

	removed from the MAC-filtering list.
Delete All	Click to delete all the registered entries from the MAC-filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.13 Firewall - Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding

IP Address: Protocol: Both Port Range: - Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.1.201	TCP+UDP	20-21	FTP	<input type="checkbox"/>

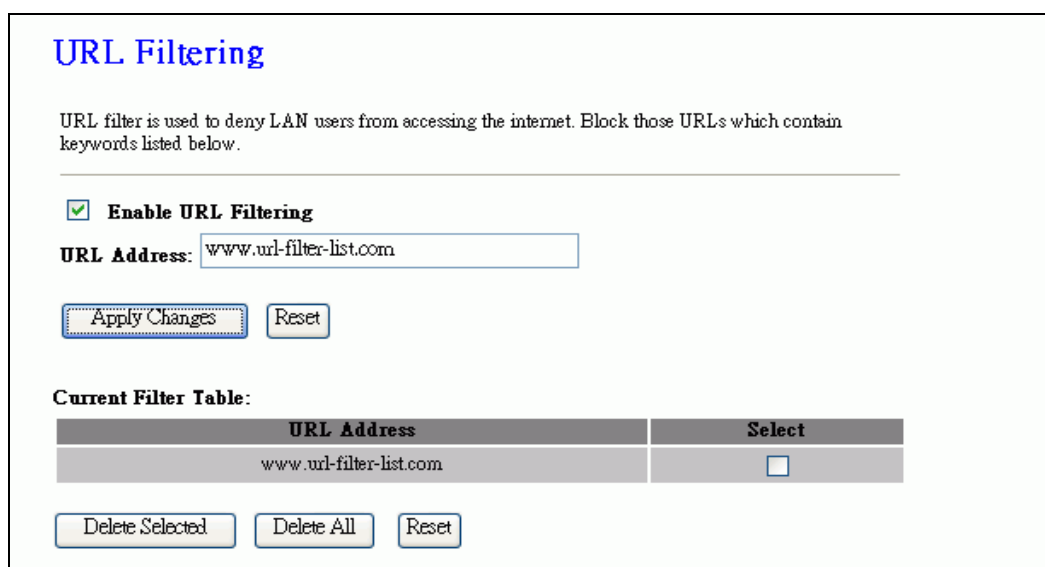
Screen snapshot – Firewall - Port Forwarding

Item	Description
Enable Port Forwarding	Click to enable the Port Forwarding security function.
IP Address	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address, protocol, port range and your comments.
Protocol	The Protocol can be TCP, UDP or Both.
Port Range	The Port Range for data transmission.
Comment	Comments let you know about whys to allow data

	packets forward to the IP address and port number.
Apply Changes	Click the Apply Changes button to register the IP address and port number to Port forwarding list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address and port number that will be removed from the port-forwarding list.
Delete All	Click to delete all the registered entries from the port-forwarding list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.14 Firewall – URL Filtering

URL Filtering is used to restrict users to access specific websites in internet.



Screen snapshot – Firewall – URL Filtering

Item	Description
Enable URL Filtering	Click to enable the URL Filtering function.
URL Address	Add one URL address.
Apply Changes	Click the Apply Changes button to save settings.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected URL address that will be

	removed from the URL Filtering list.
Delete All	Click to delete all the registered entries from the URL Filtering list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.15 Firewall - 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.



Screen snapshot – Firewall - DMZ

Item	Description
Enable DMZ	Click to enable the DMZ function.
DMZ Host IP Address	To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface.
Apply Changes	Click the Apply Changes button to register the IP address of DMZ host.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.16 Firewall – VLAN

Entries in this table could configure wired or wireless VLAN settings for scalability, security and network management.

VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

Enable VLAN

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1-4090)	Priority	CFI
<input type="checkbox"/>	Ethernet Port1	LAN	<input type="checkbox"/>	<input type="text" value="3022"/>	7 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port2	LAN	<input type="checkbox"/>	<input type="text" value="3030"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port3	LAN	<input type="checkbox"/>	<input type="text" value="500"/>	3 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port4	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wireless Primary AP	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP1	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP2	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP3	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP4	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port5	WAN	<input type="checkbox"/>	<input type="text" value="1"/>	0 <input type="button" value="v"/>	<input checked="" type="checkbox"/>

Screen snapshot – Firewall – VLAN

Item	Description
Enable VLAN	Click to enable the LAN function.
Enable	Click Enable Ethernet LAN port, Wireless, AP or WAN port.
Tag	When ‘Tag’ is enabled, Router will add a 802.1Q tagging (4 bytes long w/ VID, Priority, and CFI) in the header of each outgoing packet.
VID	The VID on WAN and LAN port need not be the same. When the packet is forwarded from LAN to WAN, the VID of LAN

port will be carried to WAN port. Also, when packet is come from WAN to LAN, router will forward this packet to the LAN port, with matched VID.

Priority	Select port priority.
CFI	Click to Enable CFI.

4.4.17 QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

Enable QoS

Automatic Uplink Speed

Manual Uplink Speed (Kbps):

Automatic Downlink Speed

Manual Downlink Speed (Kbps):

QoS Rule Setting:

Address Type: IP MAC

Local IP Address: -

MAC Address:

Mode:

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Comment:

Current QoS Rules Table:

Local IP Address	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select

Screen snapshot – QoS

Item	Description

Enable QoS	Click to enable the QoS function.
Automatic Uplink Speed	Click checkbox to enable Uplink speed by system.
Manual Uplink Speed(Kbps)	Input number to set Uplink speed.
Manual Downlink Speed(Kbps)	Click checkbox to enable Downlink speed by system.
Manual Downlink Speed(Kbps)	Input number to set Downlink speed.
QoS Rule Setting	
Address Type	Click the set type either IP or MAC address.
Local IP Address	Input the range IP address of LAN.
MAC Address	Input MAC address.
Mode	There are 2 options to control the bandwidth. One is <i>Guaranteed minimum bandwidth</i> . The other is <i>Restricted maximum bandwidth</i> .
Uplink bandwidth (Kbps)	Set Uplink bandwidth for range of IP addresses or specific MAC address
Downlink bandwidth (Kbps)	Set Downlink bandwidth for range of IP addresses or specific MAC address
Comment	Comment let you know about whys the restrict data from the QoS
Apply Change	Click <i>Apply Change</i> button to register the QoS list
Reset	Click <i>Reset</i> button to abort change and recover the previous configuration setting.

4.4.18 Route Setup

This page is used to setup dynamic routing protocol or edit static route entry.

Routing Setup

This page is used to setup dynamic routing protocol or edit static route entry.

Enable Dynamic Route

NAT: Enabled Disabled

Transmit: Disabled RIP 1 RIP 2

Receive: Disabled RIP 1 RIP 2

Enable Static Route

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface: ▾

Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select

Screen snapshot – Routing Setup

Item	Description
Enable Dynamic Route	Click to enable the Dynamic Router function.
NAT	Click to enable or disable the NAT function
Transmit	Click to disable or RIP1, RIP2 the Transmit function.
Receive	Click to disable or RIP1, RIP2 the Transmit function.
Enable Static Route	Click to Enable the Static Router function

IP Address	Manually Specify the packets arrive at the destination.
Subnet Mask	The internal network can be avoided through the Internet
Default Gateway	of the packet exchange.
Metric	Fill in the Metric value. The default value is empty.
Interface	Click to select LAN or WAN interface.
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Show Route Table	Click button to show route table
Reset	Click the Reset button to abort change and recover the previous configuration setting.

Enable Virtual Server

IP Address	Comments let you know about whys to allow data packets forward to the IP address and port number.
Protocol	
Public Port Range	
Comment	
Apply Changes	Click the Apply Changes button to register the IP address and port number to Port forwarding list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.
Delete Selected	
Delete All	Click to delete all the registered entries from the port-forwarding list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.19 Status

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

Access Point Status

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

System	
Uptime	0day:2h:16m:42s
Firmware Version	DAR1x1-3221.3
Build Time	Tue Jan 8 19:20:01 PST 2013
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	Travel6c1
Channel Number	11
Encryption	Disabled
BSSID	00:e0:4c:81:96:c1
Associated Clients	1
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:c1
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:96:c9

Screen snapshot – Status

Item	Description
System	
Uptime	It shows the duration since WLAN Travel AP/Router is powered on.
Firmware version	It shows the firmware version of WLAN Travel

	AP/Router.
Build time	It shows the Build-up time of firmware
Wireless configuration	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this WLAN Travel AP/Router. The SSID is the unique name of WLAN Travel AP/Router and shared among its service area, so all devices attempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of the WLAN Travel AP/Router. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
TCP/IP configuration	
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of WLAN Travel AP/Router.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of WLAN Travel AP/Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of WLAN Travel AP/Router.
WAN configuration	
Attain IP Protocol	It shows how the WLAN Travel AP gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP /GSM 3.5G connection.
IP Address	It shows the IP address of WAN interface of WLAN Travel AP/Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of WLAN Travel AP/Router.

Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
MAC Address	It shows the MAC address of WAN interface of WLAN Travel AP/Router.
WAN Link Status	It shows WAN connection status.

4.4.20 Management - Statistics

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

Statistics

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

Wireless LAN	<i>Sent Packets</i>	296
	<i>Received Packets</i>	3092
Ethernet LAN	<i>Sent Packets</i>	7940
	<i>Received Packets</i>	0

Screen snapshot – Management - Statistics

Item	Description
Wireless LAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN <i>Received Packets</i>	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the Ethernet LAN interface.
Ethernet LAN <i>Received Packets</i>	It shows the statistic count of received packets on the Ethernet LAN interface.

4.4.21 Management - Time Zone Setting

This page is used to configure NTP client to get current time.

Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server :

(Manual IP Setting)

Screen snapshot – Management – Time Zone Settings

Item	Description
Current Time	It shows the current time.
Copy Computer Time	Click the <i>Copy Computer Time</i> button.
Time Zone Select	Click the time zone in your country.
Enable NTP client update	Click the checkbox to enable NTP client update. Refer to 4.26 What is NTP Client?
Automatically Adjust Daylight Saving	Click to enable Daylight Saving adjustment automatically.
NTP Server	Click select default or input NTP server IP address.
Apply Change	Click the <i>Apply Changes</i> button to save and enable NTP client service.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.
Refresh	Click the refresh the current time shown on the screen.

4.4.22 Management - Log

This page is used to configure the remote log server and shown the current log.

System Log

This page can be used to set remote log server and show the system log.

Enable Log

system all
 wireless
 DoS

Enable Remote Log

Log Server IP Address:

```

Nov 26 05:54:56 klogd started: BusyBox v1.13.4 (2012-11-14 00:23:41 PST)
Nov 26 05:54:56 RTL8192C/RTL8188C driver version 1.5 (2012-05-04)
Nov 26 05:54:56 Probing RTL8186 10/100 NIC-kernel stack size order[3]...
Nov 26 05:54:56 chip name: 8196C, chip revid: 0
Nov 26 05:54:56 NOT YET
Nov 26 05:54:56 eth0 added. vid=9 Member port 0x1...
Nov 26 05:54:56 eth1 added. vid=8 Member port 0x10...
Nov 26 05:54:56 eth2 added. vid=9 Member port 0x2...
Nov 26 05:54:56 eth3 added. vid=9 Member port 0x4...
Nov 26 05:54:56 eth4 added. vid=9 Member port 0x8...
Nov 26 05:54:56 eth5 added. vid=9 Member port 0x0...
Nov 26 05:54:56 wlan0: A expired STA is resumed - 02:0A:D8:02:19:02
                    
```

Screen snapshot – Management – Log

Item	Description
Enable Log	Click the checkbox to enable log.
<i>System all</i>	Show all log of WLAN Travel AP/Router
<i>Wirelessy</i>	Only show wireless log
<i>DoS</i>	Only show Denial-of-Service log
<i>Enable Remote Log</i>	Click the checkbox to enable remote log service.
<i>Log Server IP Address</i>	Input the remote log IP address
Apply Changes	Click the Apply Changes button to save above settings.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen

4.4.23 Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Firmware Version: DAR1x1-3221.3

Select File:

Screen snapshot – Management - Upgrade Firmware

Item	Description
Select File	Click the Browse button to select the new version of web firmware image file.
Firmware Version	It shows the current firmware version.
Upload	Click the Upload button to update the selected web firmware image to the WLAN Travel AP/Router.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

4.4.24 Management Save/ Reload Settings

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

Save/Reload Settings

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

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Screen snapshot – Management - Save/Reload Settings

Item	Description
Save Settings to File	Click the Save button to download the configuration parameters to your personal computer.
Load Settings from File	Click the Browse button to select the configuration files then click the Upload button to update the selected configuration to the WLAN Travel AP/Router.
Reset Settings to Default	Click the Reset button to reset the configuration parameter to factory defaults.

4.4.25 Management - Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Screen snapshot – Management - Password Setup

Item	Description
User Name	Fill in the user name for web management login control.
New Password	Fill in the password for web management login control.
Confirmed Password	Because the password input is invisible, so please fill in the password again for confirmation purpose.
Apply Changes	Clear the User Name and Password fields to empty, means to apply no web management login control. Click the Apply Changes button to complete the new configuration setting.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

5 Frequently Asked Questions (FAQ)

5.1 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.

5.2 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.

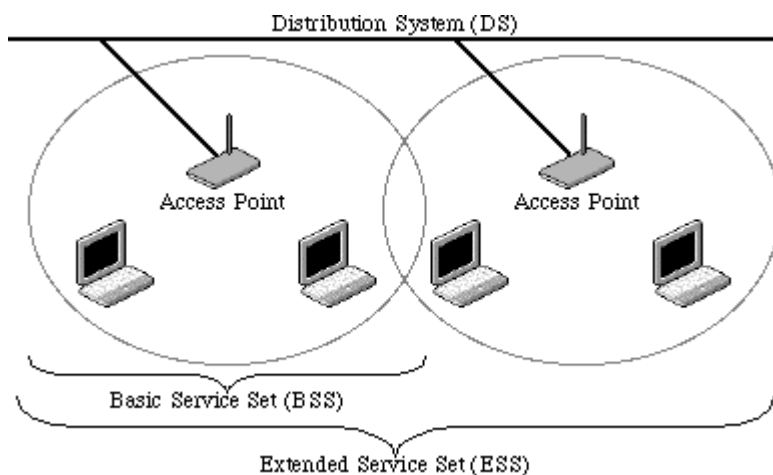
5.3 What are ISM bands?

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.

5.4 How does wireless networking work?

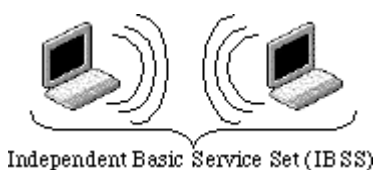
The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended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

5.5 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.

5.6 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.

5.7 What are potential factors that may cause 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, eg: microwaves, monitors, electric motors, ... etc.
- ✓ Add additional WLAN Access Points if necessary.

5.8 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.

5.9 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 encrypt 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.

5.10 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.

5.11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

5.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

5.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

5.14 What is SSID Broadcast?

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.

5.15 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.

5.16 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.

5.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

5.18 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.

5.19 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.

5.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

5.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

5.22 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.

5.23 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.

5.24 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 Travel AP/Router, so have the cloned MAC address set on the WLAN Travel AP/Router will solve the issue.

5.25 What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user own the DNS server with dynamic WAN IP address.

5.26 What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

5.27 What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to-point private link via shared or public network.

5.28 What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

5.29 What is WLAN Block Relay 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

5.30 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.

5.31 What is WLAN ACK TIMEOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

5.32 What is Modulation Coding Scheme (MCS)?

MCS is Wireless link data rate for 802.11n. The throughput/range performance of a AP will depend on its implementation of coding schemes. MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream. Radios establishing and maintaining a link must automatically negotiate the optimum MCS based on channel conditions and then continuously adjust the selection of MCS as conditions change due to interference, motion, fading, and other events.

5.33 What is Frame Aggregation?

Every 802.11 packet, no matter how small, has a fixed amount of overhead associated with it. Frame Aggregation combines multiple smaller packets together to form one larger packet. The larger packet can be sent without the overhead of the individual packets. This technique helps improve the efficiency of the 802.11n radio allowing more

end user data to be sent in a given time.

5.34 What is Guard Intervals (GI)?

A GI is a period of time between symbol transmission that allows reflections (from multipath) from the previous data transmission to settle before transmitting a new symbol.

The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive.

6 Configuration Examples

