

Single Radio 802.11a/b/g/n Indoor Access Point

BW1253s

User's Guide v1.0

Copyright

© 2002-2013 BROWAN COMMUNICATIONS.

This USER GUIDE is copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of BROWAN.

Notice

BROWAN reserves the right to change specifications without prior notice.

While the information in this document has been compiled with great care, it may not be deemed an assurance of product characteristics. BROWAN shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from BROWAN.

Trademarks

The product described in this book is a licensed product of BROWAN.

Microsoft, Windows 95, Windows 98, Windows Millennium, Windows NT, Windows 2000, Windows XP, Windows 7, and MS-DOS are registered trademarks of the Microsoft Corporation.

Novell is a registered trademark of Novell, Inc.

MacOS is a registered trademark of Apple Computer, Inc.

Java is a trademark of Sun Microsystems, Inc.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

All other brand and product names are trademarks or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

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.

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.

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.

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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

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.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Contents

Copyright	1
Notice	1
Trademarks	1
Federal Communication Commission Interference Statement	2
CONTENTS	3
ABOUT THIS GUIDE	6
Purpose	6
Prerequisite Skills and Knowledge	6
Conventions Used in this Document	6
CHAPTER 1 – INTRODUCTION	7
Product Overview	7
Features Highlight	8
CHAPTER 2 - INSTALLATION	9
The Product Package	9
Hardware Introduction	9
General Overview	9
Bottom Cover	11
Connect to the Power Source and Local Network	11
Access to your access point	12
Configuration	12
CHAPTER 3 – REFERENCE MANUAL---AP MODE	14
Web Interface	14
Status	15
Status Device Status	15
Status Wireless Status	17
Status Interface Statistics	17
Network	19
Network Interface	19
Network Bridge	20
Network Attack Countermeasure	21
Network RADIUS Server	22
Network RADIUS Properties	26
Network DHCP	27
Network DHCP Lease	31
Network Link Integrity	31
Network Tr069 Settings	33
Wireless	35
Wireless Basic	35
Wireless Advanced	41
Wireless WEP	49
Wireless MAC ACL	52
Wireless Layer 2 Isolation(Inter-BSS)	54
User	57
User Users	57
User Station Supervision	59
Services	60
Services Telnet	60
Services SNMP	61

Services Time	62
Services NTP	62
Services Watchdog	65
System.....	66
System Administrator.....	66
System System Log.....	67
System System Mode.....	68
System System Info.....	69
System Configuration	70
System Reset and Reboot.....	71
System Local Upgrade	72
System TFTP Upgrade	73
System Location Settings	74
CHAPTER 4 – REFERENCE MANUAL---AP-ROUTER MODE.....	75
Web Interface	75
Status	77
Status Device Status	77
Status Wireless Status.....	78
Status Interface Statistics	78
Network	80
Network Interface.....	80
Network PPPoE	82
Network L2TP	83
Network RADIUS Server	85
Network RADIUS Properties.....	89
Network DNS	91
Network DHCP	92
Network DHCP Lease.....	95
Network Static Route	95
Network Attack Countermeasure.....	96
Network Link Integrity	96
Network Tr069 Settings	98
Wireless.....	101
Wireless Basic	101
Wireless Advanced	107
Wireless WEP	114
Wireless MAC ACL	116
User.....	119
User Users	119
User Station Supervision	121
User User ACL	122
User Walled Garden	124
User WISP	125
User Start Page	127
User Customized UAM	128
User Pages	132
User Upload	134
User HTTP Headers	134
User Remote Authentication.....	135
Services.....	136
Services Telnet	136
Services SNMP	136
Services NTP	137
Services Time	140
Services Watchdog	140
System.....	142
System Administrator.....	142

System System Log	143
System System Mode	144
System System Info	145
System Configuration	146
System Reset and Reboot	147
System Local Upgrade	148
System TFTP Upgrade	149
System Location Settings	150
CHAPTER 5 – USER PAGES (BASED ON XSL).....	151
User Pages Overview.....	151
Welcome Page.....	151
Login Page.....	151
Logout Page.....	152
Help Page	153
Unauthorized Page	154
Example for External Pages	154
Example for Internal Pages	157
Extended UAM	160
Parameters Sent to WAS.....	162
CHAPTER 6 – CUSTOMIZED USER PAGE (HTML).....	166
Set up your customized user page.....	166
FAQ	171
APPENDIX.....	172
A) Specification	172
B) Factory Defaults for the BW1253s.....	173
Network Interface Configuration Settings	173
User Settings	175
System Settings	175
C) Location ID and ISO Country Codes	176

About this Guide

Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the high performance Indoor Access Point BW1253s.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

	Very important information. Failure to observe this may result in damage.
	Important information that should be observed.
	Additional information that may be helpful but which is not required.
bold	Menu commands, buttons and input fields are displayed in bold
code	File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type
<value>	Placeholder for certain values, e.g. user inputs
[value]	Input field format, limitations, and/or restrictions.

Chapter 1 – Introduction

Thank you for choosing the Indoor Access Point BW1253s.

The BW1253s is fully compliant to 802.11a/b/g/n standard and provides the flexibility of different kinds of 802.11n, 802.11a, 802.11g or 802.11b clients access to the BW1253s. With the high speed data rate(Max. 300Mbps) and security, feature rich software functionality, it provides the high performance wireless connection for the SMB, enterprise, and hotspot of public area.

Product Overview

Flexibility and high performance

BW1253s is a high-performance and feature-rich indoor Access Point. It provides high quality connectivity for Wi-Fi networks designed to support large hotspots. The platform providing powerful hardware processing ability and maximize its service coverage for deploying enterprise-scale Wi-Fi networks including warehouses, universities, airports, hospitals, and large corporations.

- Support IEEE802.11a/b/g/n Wi-Fi standard.
- Wireless AP router mode: NAT, Different IP subnet per BSSID, Support DHCP server or client.
- FAT AP with AP or AP Router mode configuration.
- THIN AP with centralize configuration.(2013/Q4 first release)
- Point to point or smart point to multi-point bridge.

Secure and reliable wireless networking

BW1253s supports and meets industry security requirement of wide area networking professionals for secured wireless network:

- Supports VLAN, up to 16 VLAN ID
- IEEE 802.1x/EAP with password, certificates and SIM card
- 64bits/128bits static and dynamic WEP encryption
- Supports Wi-Fi Protected Access (WPA/WPA2) with AES and TKIP support
- Layer 2 Isolation for preventing snooping on the same BSS
- MAC address filtering (ACL) for preventing illegal attacking from Internet
- Hidden SSID broadcast to prevent illegal users connection
- Built-in Web login authentication (UAM, AP Router mode)

Strong Anti-interference

Dynamic Channel Allocation (DCA) solution automatically selects optimal operational frequency channel during power up and the periodically monitors the environment and adjusts for best operational channel. DCA enhances BW1253s performance and provide continuous coverage under high AP density wireless network environment.

Multiple BSSID “Virtual AP” Technology

Supports up to16 BSSID and each can be configured independently to support range of security policies, authentication model, RADIUS servers and VLAN IDs. Each BSSID also can be set different priority based on 802.1p tag or 802.11e EDCA which enables WLAN client device to access wireless link QoS capabilities.

Ease Installation and Deployment

Power option includes an integrated IEEE 802.3af Power-over-Ethernet port enables effortless deployment in various environments.

Easy and Secure Remote Management

BW1253s supports secure remote management through HTTPS, CLISH, SNMP and TR-069(DMS) management.

- Secure management via HTTPs, CLISH, SNMP
- Support TR-069 protocol
- Detail client survey and site survey
- Remote firmware update via WEB UI, BROWAN DMS server
- Backup/Restore configuration file
- Command Line Interface(CLI) with optional SSH
- Simple Network Management Protocol(V1,V2)

Features Highlight

- Support IEEE802.11a/b/g/n Wi-Fi standard.
- Superior Wireless Bridging Capability (PtP, PtMP)
- Support up to 16 BSSID – “Virtual AP”
- Wi-Fi Protected Access (WPA and WPA2) with TKIP or AES
- Wired Equivalent Privacy (WEP) using static or dynamic key of 64 or 128 bits
- Anti-Interference with Dynamic Channel Allocation (DCA)
- Hidden SSID for blocking illegal users accessing
- Supports 802.1x authentication using EAP-TLS, EAP-TTLS, PEAP, and SIM
- MAC Access Control List (ACL)
- Layer2 Isolation for Peer to Peer client access protection
- Built-in Web user login Authentication
- DHCP server, DHCP client
- Support up to 16 VLAN ID
- RADIUS authentication
- Wireless Quality of Service
- Backup/Restore configuration settings
- System Log, Save/Send System Log to remote log server with different log levels
- NTP for clock Synchronization
- Remote firmware upgrade via HTTP
- Remote secure management by HTTPS and SNMP
- Software watchdog supported

Chapter 2 - Installation

This chapter provides installation instructions for the hardware and software components of the Access Point BW1253s. It also includes the procedures for the following tasks:

- Hardware Introduction (LEDs, Connectors)
- Connecting the Access Point
- Software Installation

The Product Package

The product comes with the following:

- Indoor Access Point (model: BW1253s)
- Mount kit(Screw Bag)
- Antenna (Dual-band Dipole Antennas with RP-SMA connector, 2 units)
- Ethernet patch cable (Cat5 UTP, 1.5m length, 1 unit)
- External power supply (Input:100-240VAC, 50-60Hz, Output: 12VDC/1.5A, 1 unit)

Hardware Introduction

General Overview



Figure 1 – BW1253s General View

The front panel of BW1253s contains:

- There are several indicator lights (**LEDs**) that help to describe the state of various networking and connection operations.

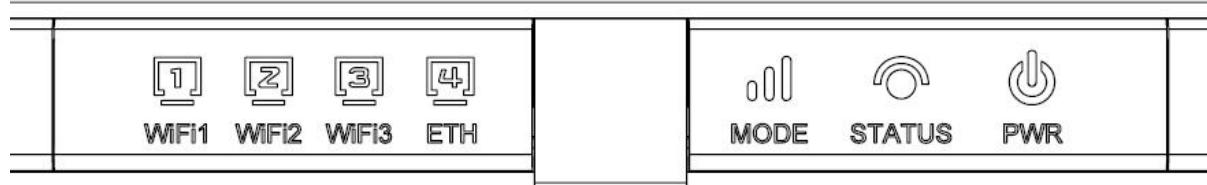


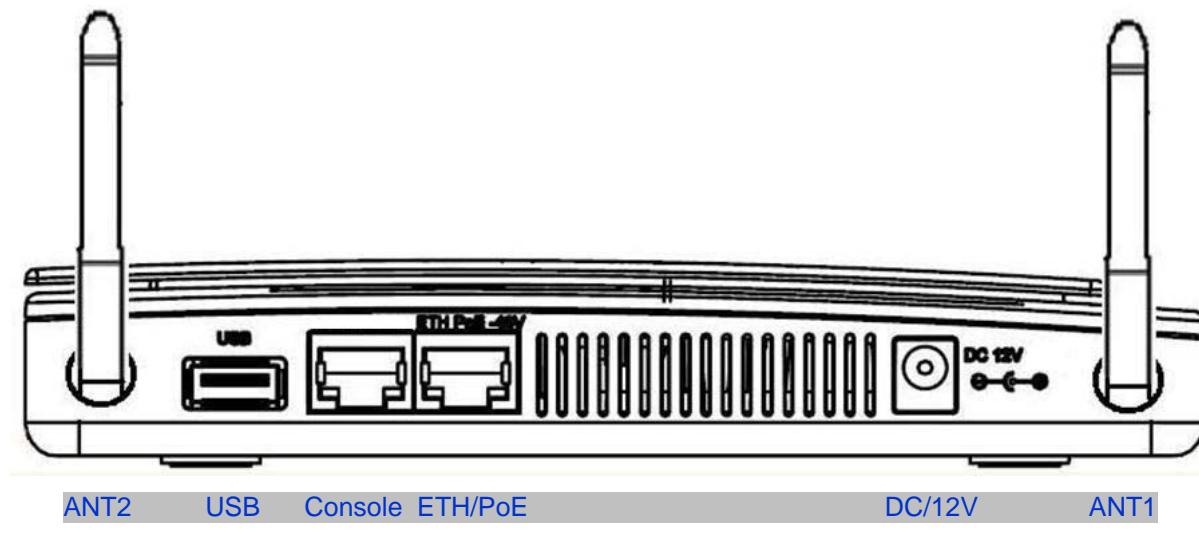
Figure 2 – BW1253s led indication

- LED Indicators

LED	Indication
Power(Green)	ON: the unit is power on and ready to work Blinking : the device is booting Off : the unit is power off
Mode	Green : FAT AP mode Amber: Thin AP mode Blinking(both green and amber) : the AP is firmware upgrading
Ethernet	Green : network speed of 1000Mbps Amber : network speed of 10/100Mbps Off : Ethernet link is unavailable
WiFi 1	Amber : the radio is operating Off : radio disable
STATUS/WIFI2	N/A

table 1 – BW1253s led definition

The rear panel of BW1253s:



- *Figure 3 – rear panel I/O port*
-
- Descriptions of the connectors are given in the following table:

Item	Connector	Description
1	ANT1/ANT2	RP-SMA Antenna connector
2	DC/12V	For power supply 12V DC jack
3	ETH/PoE	Connecting RJ-45 cable to ethernet network and for PoE power supply.
4	Console	For console use
5	USB	reserved

- *table 2 – BW1253s connectors*
-

Bottom Cover

The Bottom Cover of the BW1253s contains:

1. **Back Label** with MAC address and S/N, model name, certification...etc.
2. **MAC address**. The label shows the **WLAN** interface MAC address of the device.
The LAN MAC= WLAN MAC + 1(Hex, AP mode)
The WAN MAC=WLAN MAC + 2(Hex, AP router mode)
3. **Serial Number label** of the device.
4. **Reboot button** : press to reboot the device.

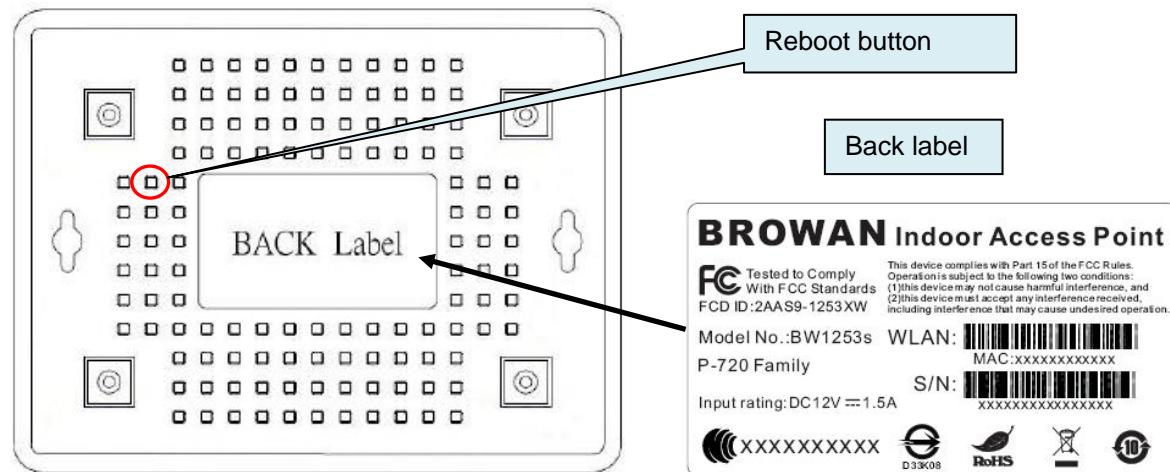


Figure 4 –Bottom Cover of the BW1253s

Connect to the Power Source and Local Network

There are two power supply methods can be used by BW1253s:

- ◆ Power-over-Ethernet equipment
- ◆ 12VDC Power adapter

Case 1 Use the BROWAN BE3013 PoE injector+DC 48V power adapter:



BE3013 PoE injector is optional which is non-compliant to 802.3af. BW1253s is compliant to 802.3af PoE standard.

Step 1 Place the Access Point on a flat work surface or hang on the wall.



Use the enclosed 2 screws mounting the Access Point to the wall.

Step 2 Connect DC 48V power supply to PoE injector DC jack.

Step 3 Connect the Ethernet cable from the BW1253s to PoE injector “P+data” out port.

- Step 4** Connect Ethernet cable from PoE injector “data in” port to the computer or through LAN switch connect to your local network. Please refer to the figure shown as below.

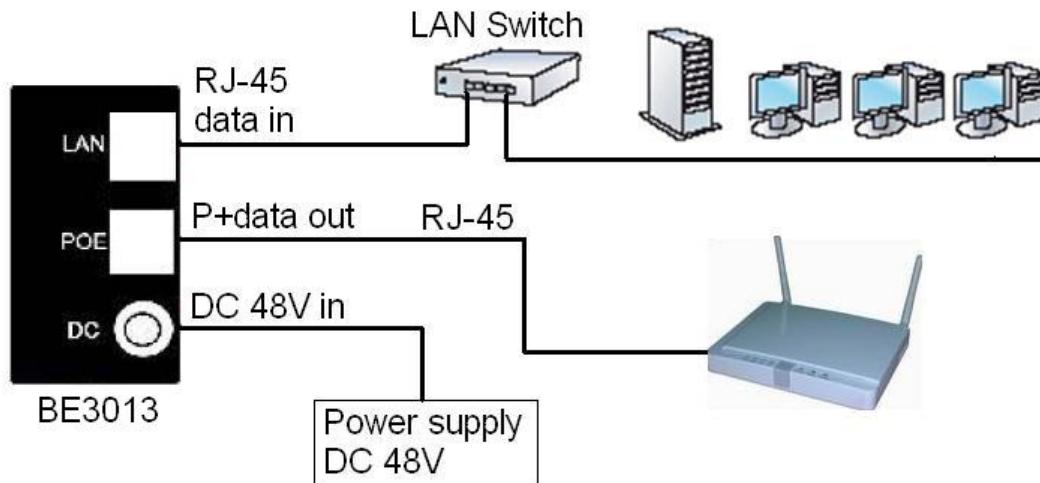


Figure 5 – Connecting BW1253s to Power source and network by PoE

Case 2 Use External Power Supply

- Step 1** Place the Access Point on a flat work surface or hang on the wall.
- Step 2** Use the enclosed Ethernet patch cable to connect the LAN port of the Access Point to the Switch or hub in the local network.
- Step 3** Connect the power supply to the Access Point.

Access to your access point

Configuration

Now it is ready to access and configure your access point. Open web browser and enter ip address. The default ip address for your new access point is:

IP 192.168.2.2 subnet 255.255.255.0

- Step 1** Configure your PC with a static IP address on the 192.168.2.x subnet with mask 255.255.255.0. Connect the BW1253s in to the same physical network as your PC. Open the Web browser and type the default IP address of the BW1253s:
<https://192.168.2.2/a.cgi>

- Step 2** Enter the BW1253s administrator login details to access the Web management.



The default administrator log on settings for all access point interfaces are:
User Name: **admin**
Password: **admin01**



Figure 6 – Security alert



Figure 7 – login page

Step 3 After successful administrator log on you will see the main page of the BW1253s **Web interface**:



Figure 8 – Web interface Management Menu

Now you are enabled to perform your configuration.

Chapter 3 – Reference Manual---AP Mode

This chapter describes the configuration of the BW1253s which works in AP mode using the Web Interface.



The BW1253s Web Interface in AP mode is different from that in AP-Router mode. To change your BW1253s to AP-Router mode, please refer to **System | System Mode**. For the detailed configuration of BW1253s working in AP-Router mode, please refer to the next chapter: **Chapter 4 – Reference Manual---AP-Router Mode**

The **web management** main menu consists of the following sub menus:

- **Status** – device status showing
- **Network** – device settings affecting networking
- **Wireless** – device settings related to the wireless part of the BW1253s
- **User** –device settings affecting the user interface
- **Services** – networking service settings of the BW1253s
- **System** – device system settings directly applicable to the BW1253s
- **Exit** – click exit and leave the web management then close your web-browser window.

Web Interface

The main **web management** menu is displayed at the top of the page after successfully logging into the system (see the figure below). From this menu all essential configuration pages are accessed.



Figure 9 – Main Configuration Management Menu

The **web management** menu has the following structure:

Status

- Device Status** – show the status related with the whole device
- Wireless Status** – show the status of the two radios
- Interface Statistics** – show the status of each network interface

Network

- Interface** – TCP/IP settings of BW1253s LAN (Bridge) port
- Bridge** – 802.1d settings of BW1253s bridge port
- Attack Countermeasure** – Anti-attack settings for protecting BW1253s
- RADIUS Server** – specify the accounting/authentication RADIUS server which is used by 802.1x or WPA
- RADIUS Properties** – specify the settings of the RADIUS properties, includes NAS server ID, RADIUS Retries and other settings
- DHCP** – specify the settings of DHCP server service
- DHCP lease** – display the DHCP lease information
- Link Integrity** – specify the status and settings of link integrity feature.

Tr069 settings – configure the remote management through TR069 ACS server(BROWAN DMS server)

Wireless

Basic – specify the basic settings related with wireless part

Advance – specify the settings of multiple BSSID or Bridge

WEP – specify the WEP settings related with static WEP encryption

MAC ACL – MAC ACL settings for BW1253s

Layer 2 Isolation – Inter-BSS layer2 Isolation settings of BW1253s

User

Users – show the connected users' statistics list and log-out user function

Station Supervision – monitor station availability with ARP-pings settings

Services

Telnet – Telnet/SSH service

SNMP – SNMP service

Time – manually set time

NTP – NTP settings of BW1253s

Watchdog – Enable the S/W or H/W watchdog of BW1253s

System

Administrator – set access permission to your BW1253s

System Log – check the system log locally or specify address where to send system log file

System Mode – specify whether the BW1253s works in AP mode or in AP router mode

System Info – specify some device related information for BW1253s

Configuration – system configuration utilities, including Backup/Upload configuration

Reset & Reboot – reboot device and restore systems to factory default

Local Upgrade – upgrade firmware from local PC

TFTP Upgrade –upgrade firmware from tftp server

Location settings – define AP location(Longitude/Latitude)

In the following sections, short references for all menu items are presented.

Status

Status | Device Status

The **Device Status** page shows important information of system status and network configuration for the BW1253s.

System	
System Mode	AP
System Version	BW1253s.BRO.1.0.14
Config Version	BW1253s.BRO.1.0.14
Up Time	0 day(s) 00:51
System Time	1970/01/01/ 00:51
WLAN1 MAC	00:16:16:28:80:A0
Free System Memory	21,740 K bytes
Total System Memory	61,784 K bytes

Network	
LAN Mode	static-IP
LAN MAC	00:16:16:28:80:A1
LAN IP	192.168.2.2
LAN Mask	255.255.255.0
Gateway	
VLAN	Disabled
VLAN ID	

Figure 10 – Device Status

System Mode – display whether the BW1253s works in AP mode or AP-Router mode

System Version display the current firmware version



This is important information for support requests and for preparing firmware upgrading

Config version – display current configure version

Up Time – indicate the time, expressed in days, hours and minutes since the system was last rebooted

System Time – show the current time of the BW1253s

Wlan1 MAC – show the MAC addresses of the wireless interfaces of the BW1253s

Free System Memory – indicate the memory currently available in the BW1253s

Total System Memory – indicate the total memory in the BW1253s

LAN Mode – indicate static IP or DHCP client is used for BW1253s LAN IP address

LAN MAC – display the Ethernet MAC address

LAN IP – show the LAN IP address of BW1253s

LAN Mask – show the LAN Network Mask of BW1253s

Gateway – show the default gateway of BW1253s

VLAN – show the status of LAN Interface VLAN of BW1253s

VLAN ID – display VLAN ID if configure the VLAN

Status | Wireless Status

The *wireless status* shows the information related with BW1253s wireless interfaces.

Radio1	
Channel	Current Frequency:2.462 GHz (Channel 11)
Domain	FCC
Mode	AP
Band	2.4GHz(11ng HT20)
Total Connected Clients	0
TxPower	14dBm
MAC ACL	disabled
SSID Number	1

Figure 11 – Wireless Status

Radio1 –wireless interfaces

Channel – indicate which channel is in use.

Domain – indicate regulatory domain set on the BW1253s.[The country code selection is for non US models only]

Mode – AP or Bridge mode is be used for this wireless interface

Band – specify which band is in use for wireless interface

Total Connected Clients – indicate number of the currently connected clients to your BW1253s

Tx Power – indicate radio transmit power of the BW1253s

MAC ACL – indicate the status of MAC ACL feature on BW1253s

SSID Number – indicate current number of enabled SSID on BW1253s

Status | Interface Statistics

The *Interface Statistics* shows each network interface status, including Input / Output bytes, packets or error.

Interface Statistics						
Interface Name	Input Bytes(KB)	Input Packets	Input Errors	Output Bytes(KB)	Output Packets	Output Errors
eth1	86	1077	0	70	166	0
Refresh						

Figure 12 – Interface Statistics

Interface Name – show the name of each network interface, where ixp0 is related to LAN interface, wlan1_x is related to wireless sub-interface.

Input Bytes (KB) – show the total number of bytes received on the network interface. The bytes number is displayed in KB.

Input Packets – show the packets number received on the network interface.

Input Errors – show the packets number which contain errors preventing them from being received correctly.

Output Bytes (KB) – show the total number of bytes transmitted out of the network interface. The bytes number is displayed in KB.

Output Packets – show the packets number transmitted out of the network interface.

Output Errors – show the packets number which contain errors preventing them from being transmitted out correctly.

Refresh – get the updated network interface information.

Network

Network | Interface

Interface						
IP Address	Netmask	Gateway Address	Protocol	VLAN	VLAN ID	Action
192.168.2.2	255.255.255.0	192.168.2.1	static	Disabled		Edit

Figure 13 – Interface Configuration Table

To change network interface configuration properties click the **Edit** button in the **Action** column. The **status** can be changed now:

Interface						
IP Address	Netmask	Gateway Address	Protocol	VLAN	VLAN ID	Action
192.168.2.2	255.255.255.0	0.0.0.0	static	Disabled	(1 - 4094)	Save Cancel

Figure 14 – Edit Interface Configuration Settings

IP Address – specify new interface IP address [in digits and dots notation, e.g. 192.168.2.2].

Netmask – specify the subnet mask [[0-255].[0-255].[0-255].[0-255]]. These numbers are a binary mask of the IP address, which defines IP address order and the number of IP addresses in the subnet

Gateway Address – interface gateway. For Bridge type interfaces, the gateway is always the gateway router

Protocol – specify **static** for setting IP address manually and **dhcp** for getting IP address dynamically acting as DHCP client

VLAN – Enable or disable VLAN on LAN (bridge) interface

VLAN ID – When enabled **VLAN**, specify the VLAN ID of it

Save – save the entered values.

Cancel – restore all previous values.

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Interface						
IP Address	Netmask	Gateway Address	Protocol	VLAN	VLAN ID	Action
192.168.2.2	255.255.255.0	192.168.2.1	static	Disabled		Edit

Apply Changes	Discard Changes
----------------------	------------------------

Figure 15 – Apply or Discard Interface Configuration Changes

Apply Changes – save all changes in the **interface** table at once.

Discard Changes – restore all previous values.

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Interface						
IP Address	Netmask	Gateway Address	Protocol	VLAN	VLAN ID	Action
192.168.2.2	255.255.255.0	192.168.2.1	static	Disabled		Edit

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 16 – Reboot Server

Reboot – click the button to restart the server and apply the changes.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

To reboot at once, click **Reboot** button and then it is necessary to wait a moment. And the message of reboot appears just like bellows:

System Reboot	
System is rebooting now. Please wait...	
4% [#=====>=====]	

Figure 17 – Reboot Information

Network | Bridge

The Spanning Tree Protocol is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation the results from them.

Specify STP(spanning tree protocol) status of 802.1d bridge here.

Bridge Settings	
STP Status	Disabled
Edit	

Figure 18– 802.1d bridge STP settings

STP Status – Enable or disable the 802.1d STP for BW1253s

Clicking **Edit**, the follow UI will be appear:

Bridge Settings	
STP Status	<input checked="" type="checkbox"/>
Save Cancel	

Figure 19 – Edit bridge settings

Save – save the entered values.

Cancel – restore all previous values.

Click **Save** button for applying the changes that modified.

Bridge Settings	
STP Status	Enabled
<input type="button" value="Edit"/> <input type="button" value="Apply Changes"/> <input type="button" value="Discard Changes"/>	

Figure 20 – Apply or Discard Bridge Settings Changes

Apply Changes – save all changes at once

Discard Changes – restore all previous values.

Click **Apply Changes** and then follow the instruction to reboot the device for all modified settings applied.

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
---	---

Network | Attack Countermeasure

To protect BW1253s from outside attack, anti-attack polices can be set here based on network needs.

Attack Countermeasure					
Item	Status	Max Load	Duration(seconds)	Expire(seconds)	Action
Anti-DOS	Disabled	400 TCP links/s		300	<input type="button" value="Edit"/>
Flow Control	Disabled	20480 Kbps	60	300	<input type="button" value="Edit"/>

Figure 21– Attack Countermeasure settings

Anti-DOS

Status – Enable or disable anti-dos policy for BW1253s. This policy is for TCP DOS attack.

Max Load – The attack threshold. BW1253s think there is TCP DOS attack and do the countermeasure if one client's TCP links exceed this threshold.

Expire(seconds) – If one client is considered as DOS attacker, BW1253s kicks it out and doesn't let it connect again during the time that **Expire** set.

Flow Control

Status – Enable or disable traffic flow control policy for BW1253s.

Max Load – The attack throughput threshold.

Duration(seconds) – if traffic exceeds the value of **Max Load** during the whole time that **Duration** set, BW1253s think there is traffic flow attack and implement the countermeasure.

Expire(seconds) – If one client is considered as traffic flow attacker, BW1253s kicks it out and doesn't let it connect again during the time that **Expire** set.

Network | RADIUS Server



Up to **32** different RADIUS servers can be configured in the **RADIUS servers** menu.

By default, one **RADIUS** server is specified for the system:

RADIUS Server					
Name	Type	IP Address	Port	Secret	Action
DEFAULT (default)	Authentication	0.0.0.0	1812	secret	Details Edit Delete
	Accounting	0.0.0.0	1813	secret	
Add					

Figure 22 – RADIUS Servers Settings

Details – show the detail information of this **RADIUS Server** profile

Edit – edit the selected **RADIUS Server** entry you want to configure

Delete – delete the selected **RADIUS Server** entry. The last entry can not be deleted

Add – add new RADIUS server.

Click **Details**, a similar page will be appeared as below:

RADIUS Server	
Description	Value
Name (default)	DEFAULT
Authentication IP	192.168.123.200
Authentication Port	1812
Authentication Secret	secret
Accounting IP	192.168.123.201
Accounting Port	1813
Accounting Secret	secret
User Password Md5sum Secret	disabled
Back Edit	

Figure 23 – Detail for Radius Server profile

Name – the new RADIUS server name which is used for selecting RADIUS server



If a “(default)” appears on the right side of the **Name** entry, it means this RADIUS server profile is the default profile.

Authentication IP – show the IP address of Authentication RADIUS server

Authentication Port – show the network port used to communicate with the Authentication RADIUS server

Authentication Secret – show the shared secret string that is used to make sure the integrity of data frames used for the Authentication RADIUS server

Accounting IP – show the IP address of Accounting RADIUS server



If the Accounting IP address is 0.0.0.0, it means that the Accounting service is disabled.

Accounting Port – show the network port used to communicate with the Accounting RADIUS server

Accounting Secret – show the shared secret string that is used to make sure the integrity of data frames used for the Accounting RADIUS server

User Password Md5sum Secret – show whether user input password is calculated md5-sum before pass to RADIUS server or not.

Back – back to the **RADIUS Server** main page

Edit – edit the selected **RADIUS Server** profile

Click **Edit** or click **Add / Edit** button in the main page to configure RADIUS server settings.

RADIUS Server	
Description	Value
Name	DEFAULT
Default	<input checked="" type="checkbox"/>
Authentication IP	192.168.123.100
Authentication Port	1812
Authentication Secret	secret
Accounting IP	192.168.123.200
Accounting Port	1813
Accounting Secret	secret
User Password Md5sum Secret	disabled <input type="button" value="▼"/>

Figure 24 – Edit the RADIUS Server's profile

RADIUS Server	
Description	Value
Name	<input type="text"/>
Default	<input checked="" type="checkbox"/>
Authentication IP	<input type="text"/>
Authentication Port	<input type="text"/>
Authentication Secret	<input type="text"/>
Accounting IP	<input type="text"/>
Accounting Port	<input type="text"/>
Accounting Secret	<input type="text"/>
User Password Md5sum Secret	disabled <input type="button" value="▼"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 25 – Add a new RADIUS Server's profile

Name – specify the new RADIUS server name which is used for selecting RADIUS server

Default – specify this RADIUS profile as default or not. When selected, the profile will be used as default

Authentication IP – specify the IP address of Authentication RADIUS server [dots and digits]

Authentication Port – specify the network port used to communicate with the Authentication RADIUS server [1-65535]

Authentication Secret – shared secret string that is used to make sure the integrity of data frames used for the Authentication RADIUS server

Accounting IP – specify the IP address of Accounting RADIUS server [dots and digits]

Accounting Port – specify the network port used to communicate with the Accounting RADIUS server [1-65535]

Accounting Secret – shared secret string that is used to make sure the integrity of data frames used for the Accounting RADIUS server



The default port value for authentication is 1812.
The default port value for accounting is 1813.
The port specified here must be the same with the one on the RADIUS server.

User Password Md5sum Secret – if enabled, user input password will be calculated md5-sum before pass to RADIUS server for more security [enabled/disabled]



This setting needs RADIUS server implement relevant configurations.

Save – save the entered values

Cancel – restore all previous values

After adding a new RADIUS server or editing an existing one, a page appears similar to the following:

RADIUS Server					
Name	Type	IP Address	Port	Secret	Action
DEFAULT (default)	Authentication	192.168.123.100	1812	secret	Details Edit Delete
	Accounting	192.168.123.200	1813	secret	Details Edit Delete
Add					

[Apply Changes](#) [Discard Changes](#)

Figure 26 – Apply or Discard RADIUS Server Changes

Details – show the detail information of this **RADIUS Server** profile

Edit – edit the selected **RADIUS Server** entry you want to configure

Delete – delete the selected **RADIUS Server** entry. The last entry can not be deleted

Add – add new RADIUS server.

Apply Changes – to save all changes at once.

Discard Changes – restore all previous values.

Click **Apply Changes** to apply all the changes. Then the follow similar page will appear:

RADIUS Server					
Name	Type	IP Address	Port	Secret	Action
DEFAULT (default)	Authentication	192.168.123.100	1812	secret	Details Edit Delete
	Accounting	192.168.123.200	1813	secret	Details Edit Delete
Add					

[Reboot](#)

System needs to be restarted to make the new configurations take effect.

Figure 27 – Reboot Server

Reboot – restart the access point to make applied changes work.

 If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.

Network | RADIUS Properties

General **RADIUS** settings are configured using the **RADIUS Properties** menu under the **network**:

RADIUS Properties		
Setting	Value	Action
RADIUS Retries	5	Edit
RADIUS Timeout (seconds)	2	Edit
NAS Server ID		Edit
User Session Timeout (seconds)	72000	Edit
User Accounting Update Interval (seconds)	600	Edit
User Accounting Update Retry (seconds)	60	Edit
User Idle Timeout (seconds)	900	Edit

Figure 28 – RADIUS Properties settings

RADIUS Retries – retry count of sending RADIUS packets before giving up [0-99]

RADIUS Timeout (seconds) – maximum amount of time before retrying RADIUS packets [1-999]

NAS Server ID – name of the RADIUS client

User Session Timeout (seconds) – amount of time from the user side (no network carrier) before closing the connect [1-999999999]

User Accounting Update Interval (Seconds) – period after which server should update accounting information [60-999999999]

User Accounting Update Retry (seconds) – retry time period in which server should try to update accounting information before giving up [60-999999999]

User Idle Timeout (seconds) – amount of user inactivity time, before automatically disconnecting user from the network [1-999999999]

Each setting in this table can be edited. Select **RADIUS** setting you need to update, click the **edit** next to the selected setting and change the value:

RADIUS Properties		
Setting	Value	Action
RADIUS Retries	5	Save Cancel
RADIUS Timeout (seconds)	2	
NAS Server ID		
User Session Timeout (seconds)	72000	
User Accounting Update Interval (seconds)	600	
User Accounting Update Retry (seconds)	60	
User Idle Timeout (seconds)	900	

Figure 29 – edit RADIUS properties

Use the **save** button to save an entered value. Now select another **RADIUS** property to edit, or **Apply Changes** and restart your AP if the configuration is finished:

RADIUS Properties		
Setting	Value	Action
RADIUS Retries	5	Edit
RADIUS Timeout (seconds)	2	Edit
NAS Server ID		Edit
User Session Timeout (seconds)	72000	Edit
User Accounting Update Interval (seconds)	600	Edit
User Accounting Update Retry (seconds)	60	Edit
User Idle Timeout (seconds)	900	Edit

Apply Changes – click if **RADIUS Properties** configuration is finished

Discard Changes – restore all previous values

Network | DHCP

In AP mode, BW1253s can act as DHCP server. The DHCP (Dynamic Host Configuration Protocol) service is supported on layer 2 interfaces.

DHCP server and DHCP relay are disabled by default.

DHCP	
Name	Value
Status	Disabled
Edit	

Figure 30 – DHCP Settings

Edit – edit the DHCP settings

To enable DHCP server click the **Edit** button.

DHCP	
Name	Value
Status	<input style="width: 100px; height: 20px; border: none; background-color: #f0f0f0; padding: 2px; margin-bottom: 5px;" type="button" value="Disabled"/> <div style="background-color: #f0f0f0; border: 1px solid #ccc; width: 100px; height: 20px; position: relative; z-index: 1;"> Disabled </div> <div style="background-color: #fff; border: 1px solid #ccc; width: 100px; height: 20px; position: relative; z-index: 2; opacity: 0;"> Enabled </div>

Figure 31 – DHCP Settings

Status – select status from the drop-down menu.

Disabled – disable the DHCP server service.

DHCP Server – enable the DHCP server service.

Choose DHCP Server to enable DHCP server service.

DHCP Server

This DHCP server service enables clients on the LAN to request configuration information, such as IP address, from a server. Settings of the DHCP service can be viewed just like the follow page.

DHCP	
Name	Value
Status	DHCP Server <input type="button" value="▼"/>
IP Address from	192.168.123.2
IP Address to	192.168.123.254
Netmask	255.255.255.0
Gateway	192.168.123.1
WINS Address	0.0.0.0
Lease Time (seconds)	864000
Domain	
DNS Address	0.0.0.0
DNS Secondary Address	0.0.0.0
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 32 – DHCP server Settings



By default, DHCP server is disabled.

IP Address from / IP Address to – specify the IP address range to be dynamically allocated by the DHCP server.

Netmask – enter the netmask for IP pool range.

Gateway – enter the gateway IP for wireless clients.

WINS Address (Windows Internet Naming Service) – specify server IP address if it is available on the network [dots and digits].

Lease Time – specify the IP address lease interval in seconds [1-1000000].

Domain – specify the DHCP domain name [optional, 1-128 sting].

DNS address – specify the DNS server's IP address [in digits and dots notation].

DNS secondary address – specify the secondary DNS server's IP address [in digits and dots notation].

Change status or leave in the default state if no editing is necessary and click the **Save** button.

DHCP	
Name	Value
Status	DHCP Server
IP Address from	192.168.123.2
IP Address to	192.168.123.254
Netmask	255.255.255.0
Gateway	192.168.123.1
WINS Address	0.0.0.0
Lease Time (seconds)	864000
Domain	
DNS Address	0.0.0.0
DNS Secondary Address	0.0.0.0
<input type="button" value="Edit"/>	

Figure 33 – Apply or Discard DHCP server Settings

 The DHCP server settings will be automatically adjusted to match the network interface settings.

 The Gateway of DHCP server settings must be same with the Gateway of BW1253s

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

DHCP	
Name	Value
Status	DHCP Server
IP Address from	192.168.123.2
IP Address to	192.168.123.254
Netmask	255.255.255.0
Gateway	192.168.123.1
WINS Address	0.0.0.0
Lease Time (seconds)	864000
Domain	
DNS Address	0.0.0.0
DNS Secondary Address	0.0.0.0
Edit	

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 34 – Reboot information

Reboot – click the button to restart the server and apply the changes.



If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.
And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.



When BW1253s network Interface uses DHCP to get IP address dynamically, DHCP server service cannot be enabled.

When BW1253s uses DHCP to get IP address, the similar WEB UI will be appeared:

Warning: DHCP server and DHCP relay cannot be set when AP as a DHCP client itself.

DHCP	
Name	Value
Status	Disabled

Figure 35 – Warning information

Network | DHCP Lease

This page display the DHCP lease information of wireless client which connect to the AP when DHCP server enable.

DHCP Lease			
Host Name	Mac Address	IP Address	Expires in
ggyy-40fbc8fbbae	00:13:02:01:14:5a	192.168.2.4	9 d 23 h 59 m 24 s
Refresh			

Figure 36 – DHCP lease information

Host Name – the host name of wireless client which associate to the access point.

Mac Address –the MAC address of wireless client which associate to the access point.

IP Address –the IP address of wireless client which associate to the access point.

Expires in – expire time of the wireless client which associate to the access point.

Network | Link Integrity

Specify Link Integrity feature's settings here. Enable Link Integrity, BW1253s will close wireless connections and kick out all the wireless clients when it detects that its Ethernet network cannot be accessed to the internet.

Link Integrity	
Name	Status
Status	Disabled
Edit	

Figure 37 – Link Integrity settings

Click **Edit** button to set the Link Integrity settings, the similar UI will be appeared as below:

Link Integrity	
Name	Status
Status	Enabled <input type="button" value="▼"/>
Target IP1	<input type="text" value="0.0.0.0"/>
Target IP2	<input type="text" value="0.0.0.0"/>
Target IP3	<input type="text" value="0.0.0.0"/>
Target IP4	<input type="text" value="0.0.0.0"/>
Target IP5	<input type="text" value="0.0.0.0"/>
Save Cancel	

Figure 38 – Edit Link Integrity settings

Status – Enable or disable the feature of Link Integrity

Target IP1 to Target IP5 – IP addresses for BW1253s detecting if its Ethernet interface can access network. The AP will ping every IP address 15 times in sequence. As long as one ping is successful it will consider the network is no problem. If ping fail for all IP address specified it will consider Ethernet link fail and all associated wireless client will be logged out. The AP will continue to ping from first IP address. If ping success the wireless client will access AP again.

Save – save the entered values.

Cancel – restore all previous values.

Click **Save**, the similar apply changes UI will be appeared:

Link Integrity	
Name	Status
Status	Enabled
Target IP1	192.168.123.69
Target IP2	192.168.123.1
Target IP3	0.0.0.0
Target IP4	0.0.0.0
Target IP5	0.0.0.0

Edit

Figure 39 –Apply or Discard Link Integrity Settings

Apply Changes – save all changes in the **interface** table at once.

Discard Changes – restore all previous values.

i	Maximum 5 target IP can be specified.
----------	---------------------------------------

The BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Link Integrity	
Name	Status
Status	Enabled
Target IP1	192.168.123.69
Target IP2	192.168.123.1
Target IP3	0.0.0.0
Target IP4	0.0.0.0
Target IP5	0.0.0.0

Edit

System needs to be restarted to make the new configurations take effect.

Figure 40 – Reboot Server

Reboot – click the button to restart the server and apply the changes.

i	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
----------	---

Network | Tr069 Settings

TR-069 is the Broadband Forum technical specification entitled CPE WAN Management Protocol(CWMP). It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment(CPE) and Auto Configuration Servers(ACS server). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. The protocol addressed the growing number of different internet access devices such as modems, routers, gateways, set-top-boxes, and VOIP-phones for the end users. The TR-069 standard was developed for automatic configuration of these devices with Auto Configuration Servers(ACS).

configure the remote management through TR069 ACS server(eg:BROWAN DMS server)

TR069 Settings	
Name	Status
Status	Disabled
<input type="button" value="Edit"/>	

Figure 41 – TR-069 settings

Click Edit button and the similar page will be appeared.

TR069 Settings	
Name	Status
Status	<input type="button" value="Enabled"/>
ACS URL	<input type="text" value="http://192.168.1.1:9090/dms/tr069"/>
ACS UserName	<input type="text" value="tr069"/>
ACS UserPassword	<input type="text" value="tr069passwd"/>
Enable Periodic Inform	<input type="button" value="Enabled"/>
Periodic Inform Interval	<input type="text" value="3600"/>
Connection Request UserName	<input type="text" value="server"/>
Connection Request Password	<input type="text" value="serverpasswd"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 42 – edit TR-069 settings

Status – enable or disable TR-069 setting.[enable/disable]

ACS URL – enter the ACS server URL.

ACS UserName – the user name for AP register to ACS server.

ACS UserPassword – the password for AP register to ACS server.

Enable Periodic Inform – when AP registered to the ACS server, it will automatically send inform message such as S/N,OUI,manufacturer and product name to the ACS server through TR-069 protocol in a periodic time.

Periodic Inform Interval – the inform interval.[in seconds, the value is 720~4294967295]

Connection Request UserName – when the ACS pulling a task to AP/CPE such as firmware upgrade/downgrade, AP need the user name to verify the task sending from ACS server.

Connection Request Password –when the ACS pulling a task to AP/CPE such as firmware upgrade/downgrade, AP need the password to verify the task sending from ACS server.

	Contact the ACS server administrator to get the user name and password for Connection Request UserName and Connection Request Password otherwise the AP will not accept the task pulling by ACS server.
---	---

After enter all field click **save** and **apply changes** button to take effect.

TR069 Settings	
Name	Status
Status	Enabled
ACS URL	http://192.168.1.1:9090/dms/tr069
ACS UserName	tr069
ACS Password	tr069passwd
Enable Periodic Inform	Enable
Periodic Inform Interval	3600
Connection Request UserName	server
Connection Request Password	serverpasswd

Figure 43 – save TR-069 settings

Reboot – click the button to restart the server and apply the changes.

TR069 Settings	
Name	Status
Status	Enabled
ACS URL	http://192.168.1.1:9090/dms/tr069
ACS UserName	tr069
ACS Password	tr069passwd
Enable Periodic Inform	Enable
Periodic Inform Interval	3600
Connection Request UserName	server
Connection Request Password	serverpasswd

System needs to be restarted to make the new configurations take effect.

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
---	---

Wireless

Wireless | Basic

Use the **Wireless | Basic** menu to configure wireless settings such as regulatory domain, channel, band, and power, layer 2 isolation. Click the edit button on the setting you need to change:

	The country code selection is for non US models only																														
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">Basic Wireless Setting</th> </tr> <tr> <th>Radio :</th> <td>wlan1</td> </tr> </thead> <tbody> <tr> <th>Name</th> <th>Value</th> </tr> <tr> <td>Mode</td> <td>AP</td> </tr> <tr> <td>Domain</td> <td>FCC</td> </tr> <tr> <td>Static Channel</td> <td>11</td> </tr> <tr> <td>Band</td> <td>2.4GHz(11ng HT20)</td> </tr> <tr> <td>TxPower</td> <td>14dBm</td> </tr> <tr> <td>RTS Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Fragment Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Beacon Interval</td> <td>100 ms</td> </tr> <tr> <td>DCA</td> <td>Disable</td> </tr> <tr> <td>Preamble</td> <td>auto</td> </tr> <tr> <td>Slot Time</td> <td>auto</td> </tr> <tr> <td>Action</td> <td style="text-align: center;">Edit Site Survey</td> </tr> </tbody> </table>		Basic Wireless Setting		Radio :	wlan1	Name	Value	Mode	AP	Domain	FCC	Static Channel	11	Band	2.4GHz(11ng HT20)	TxPower	14dBm	RTS Threshold	2347 bytes	Fragment Threshold	2347 bytes	Beacon Interval	100 ms	DCA	Disable	Preamble	auto	Slot Time	auto	Action	Edit Site Survey
Basic Wireless Setting																															
Radio :	wlan1																														
Name	Value																														
Mode	AP																														
Domain	FCC																														
Static Channel	11																														
Band	2.4GHz(11ng HT20)																														
TxPower	14dBm																														
RTS Threshold	2347 bytes																														
Fragment Threshold	2347 bytes																														
Beacon Interval	100 ms																														
DCA	Disable																														
Preamble	auto																														
Slot Time	auto																														
Action	Edit Site Survey																														

Figure 44 – Basic Wireless Settings with static channel selection

<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">Basic Wireless Setting</th> </tr> <tr> <th>Radio :</th> <td>wlan1</td> </tr> </thead> <tbody> <tr> <th>Name</th> <th>Value</th> </tr> <tr> <td>Mode</td> <td>AP</td> </tr> <tr> <td>Domain</td> <td>FCC</td> </tr> <tr> <td>Auto Channel</td> <td>1</td> </tr> <tr> <td>Band</td> <td>2.4GHz(11ng HT20)</td> </tr> <tr> <td>TxPower</td> <td>4dBm</td> </tr> <tr> <td>RTS Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Fragment Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Beacon Interval</td> <td>100 ms</td> </tr> <tr> <td>DCA</td> <td>Enable</td> </tr> <tr> <td>DCA Threshold</td> <td>10 mins</td> </tr> <tr> <td>DCA optional channel</td> <td>1,2,3,4,5,6,7,8,9,10,11 channel</td> </tr> <tr> <td>Preamble</td> <td>auto</td> </tr> <tr> <td>Slot Time</td> <td>auto</td> </tr> <tr> <td>Action</td> <td style="text-align: center;">Edit Site Survey</td> </tr> </tbody> </table>		Basic Wireless Setting		Radio :	wlan1	Name	Value	Mode	AP	Domain	FCC	Auto Channel	1	Band	2.4GHz(11ng HT20)	TxPower	4dBm	RTS Threshold	2347 bytes	Fragment Threshold	2347 bytes	Beacon Interval	100 ms	DCA	Enable	DCA Threshold	10 mins	DCA optional channel	1,2,3,4,5,6,7,8,9,10,11 channel	Preamble	auto	Slot Time	auto	Action	Edit Site Survey
Basic Wireless Setting																																			
Radio :	wlan1																																		
Name	Value																																		
Mode	AP																																		
Domain	FCC																																		
Auto Channel	1																																		
Band	2.4GHz(11ng HT20)																																		
TxPower	4dBm																																		
RTS Threshold	2347 bytes																																		
Fragment Threshold	2347 bytes																																		
Beacon Interval	100 ms																																		
DCA	Enable																																		
DCA Threshold	10 mins																																		
DCA optional channel	1,2,3,4,5,6,7,8,9,10,11 channel																																		
Preamble	auto																																		
Slot Time	auto																																		
Action	Edit Site Survey																																		

Figure 45 – Basic Wireless Settings with auto channel selection(DCA)

Radio – specify which wireless interface of BW1253s is shown.(There is only one WLAN1 interface in BW1253s)

Mode – show the radio operation mode. (AP mode or Bridge mode)

Domain – show the regulatory domain.[The country code selection is for non US models only]

Static Channel / Auto Channel – show the channel that the access point will use to transmit and receive information



If DCA (Dynamic Channel Allocation) is enabled, this will show Auto Channel and its channel number is chosen in auto channel selection.
If use static channel selection, this will show Static Channel and its channel number.



DCA (Dynamic Channel Allocation) is useful feature to help choose the best channel automatically and reduce interference among many Access Points.

Band – show the working bands on which the radio is working.

Seven bands listed: 2.4GHz(11ng HT20) , 2.4GHz(11ng HT40plus), 2.4GHz(11ng HT40minus) , 5GHz(11a), 5GHz(11na HT20) , 5GHz(11na HT40plus), 5GHz(11na HT40minus) .

Tx Power – show the BW1253s transmission output power (without antenna gain) in dBm.

RTS Threshold –the AP sends Request to Send(RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send(CTS) frame to acknowledge the right to begin transmission. The default value is 2347.[recommend].

Fragment Threshold –It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the fragmentation threshold. Setting the fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended. The default value is 2347.[recommend]

Beacon Interval –the Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network.

DCA – Enable or Disable DCA service. DCA can help to choose the best working channel automatically. And static channel selection will be forbidden if DCA is enabled.

DCA(Dynamic Channel Allocation) solution automatically select the optimal operational frequency channel when power up and periodically monitors the environment and adjusts for the best operational frequency channel.

DCA threshold – specify the value (in minutes) of DCA threshold. This threshold is been used to judge if there is no wireless users connected during this time. And if yes, BW1253s will monitor the environment and adjust channel for the best operational one.



If wireless network environment is stable which means auto channel selection needn't do frequently, set a big value for DCA threshold to gain a stable wireless users' connection.
If wireless network environment changes continually, frequent auto channel selection is needed. So set a relative small value for DCA threshold to let channel change based on wireless environment.

	Wireless users' will be kicked off when DCA is processing (new operational frequency channel takes effect).
--	---

DCA optional channel – show the channels only in which auto channel selection (DCA) will be processed to reduce interference.

	Only when DCA is enabled, DCA threshold and DCA optional channel will be shown.
--	---

Preamble – if your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble.

Auto: using long preamble when there are clients not supporting short preamble connected , otherwise using short preamble. The default is Auto.[recommend]

Short: always using short preamble.

Long: always using long preamble.

Slot Time – show the slot time policy when working in 2.4GHz band.

Auto: using long slot time when there are clients not supporting short slot time connected in, otherwise using short slot time. The Switching between long and short slot time is automatic.

Short: always using short slot time.

Long: always using long slot time.

	To Maximize the compatibility with some 11b clients, set both Preamble and Slot Time to long.
--	---

Edit – edit the wireless basic settings

To change basic wireless setting properties click the **Edit** button in the **Action** column. The **status** can be changed now:

Basic Wireless Setting	
Name	Value
Radio Name	wlan1
Mode	AP
Domain	FCC
Channel	1
Band	2.4GHz(11ng HT20)
TxPower	14 dBm
RTS Threshold	2347 bytes [0..2347]
Fragment Threshold	2347 bytes [0..2347]
Beacon Interval	100 ms [1..65536]
DCA	<input type="checkbox"/> Enable
DCA Threshold	10 mins
DCA optional channel	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> all
Preamble	auto
Slot Time	auto
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 46 – Edit Basic Wireless Settings with static channel selection

Basic Wireless Setting	
Name	Value
Radio Name	wlan1
Mode	AP
Domain	FCC
Channel	1
Band	2.4GHz(11ng HT20)
TxPower	14 dBm
RTS Threshold	2347 bytes [0..2347]
Fragment Threshold	2347 bytes [0..2347]
Beacon Interval	100 ms [1..65536]
DCA	<input checked="" type="checkbox"/> Enable
DCA Threshold	10 mins
DCA optional channel	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> all
Preamble	auto
Slot Time	auto
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 47 – Edit Basic Wireless Settings with DCA enabled

Radio Name – specify wireless interface of BW1253s is shown

Mode – configure the radio operation mode. [AP mode or Dynamic Bridge mode]. There will be different configuration for the two mode within **Wireless | Advanced** menu. Please refer to corresponding chapter.

Selecting the AP Mode:

Domain – show the regulatory domain. [The country code selection is for non US models only]

Channel – select the channel that the access point will use to transmit and receive information. Channels list will vary depending on selected band. [2.4GHz or 5GHz]

Band – working bands on which your radios are working.

Seven bands listed: 2.4GHz(11ng HT20) , 2.4GHz(11ng HT40plus), 2.4GHz(11ng HT40minus) , 5GHz(11a), 5GHz(11na HT20) , 5GHz(11na HT40plus), 5GHz(11na HT40minus) .

TxPower – the BW1253s transmission output power in dBm.

RTS Threshold – the AP sends Request to Send(CTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send(CTS) frame to acknowledge the right to begin transmission. The default value is 2347.[recommend]

Fragment Threshold – It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the fragmentation threshold. Setting the fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended. The default value is 2347.[recommend]

Beacon Interval – the Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network.

DCA – Enable or Disable DCA service. DCA can help to choose the best working channel automatically. And static channel selection will be forbidden if DCA is enabled.

DCA(Dynamic Channel Allocation) solution automatically select the optimal operational frequency channel when power up and periodically monitors the environment and adjusts for the best operational frequency channel.

DCA threshold – specify the value (in minutes) of DCA threshold. This threshold is been used to judge if there is no wireless users connected during this time. And if yes, BW1253s will monitor the environment and adjust channel for the best operational one.



If wireless network environment is stable which means auto channel selection needn't do frequently, set a big value for DCA threshold to gain a stable wireless users' connection.
If wireless network environment changes continually, frequent auto channel selection is needed. So set a relative small value for DCA threshold to let channel change based on wireless environment.



Wireless users' will be kicked off when DCA is processing (new operational frequency channel takes effect).

DCA optional channel – specify the channels only in which auto channel selection (DCA) will choose for reducing interference reference.



Only when DCA is enabled, **DCA threshold** and **DCA optional channel** will be shown.

Preamble – if your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble.

Auto: using long preamble when there are clients not supporting short preamble connected , otherwise using short preamble. The default is Auto.[recommend]

Short: always using short preamble.

Long: always using long preamble.

Slot Time – specify the slot time policy when working in 2.4GHz band.

Auto: using long slot time when there are clients not supporting short slot time connected in, otherwise using short slot time. The default is Auto.[recommend]

Short: always using short slot time.

Long: always using long slot time.



To Maximize the compatibility with some 11b clients, set both **Preamble** and **Slot Time** to long.

Configure the DynamicBridge Mode:

Basic Wireless Setting	
Name	Value
Radio Name	wlan1
Mode	DynamicBridge
Domain	FCC
Channel	1
Band	2.4GHz(11ng HT20)
TxPower	14 dBm
RTS Threshold	2347 bytes [0..2347]
Fragment Threshold	2347 bytes [0..2347]
Beacon Interval	100 ms [1..65536]
Preamble	auto
Slot Time	auto
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 48 – Edit Basic Wireless Settings with DynamicBridge mode

All the parameters same with AP mode. For more detail with DynamicBridge setting please refer to **Wireless | Advanced** page in DynamicBridge mode.

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Basic Wireless Setting	
Radio :	wlan1
Name	Value
Mode	DynamicBridge
Domain	FCC
Channel	1
Band	2.4GHz(11ng HT20)
TxPower	14dBm
RTS Threshold	2347 bytes
Fragment Threshold	2347 bytes
Beacon Interval	100 ms
DCA	Disable
Preamble	auto
Slot Time	auto
Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Discard Changes"/>	

Figure 49 – Apply or Discard dynamicbridge setting

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Basic Wireless Setting	
Radio :	wlan1
Name	Value
Mode	DynamicBridge
Domain	FCC
Channel	1
Band	2.4GHz(11ng HT20)
TxPower	14dBm
RTS Threshold	2347 bytes
Fragment Threshold	2347 bytes
Beacon Interval	100 ms
DCA	Disable
Preamble	auto
Slot Time	auto
Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>
<input type="button" value="Reboot"/>	

System needs to be restarted to make the new configurations take effect.

Figure 50 – Reboot Server

Reboot – click the button to restart the server and apply the changes.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Wireless | Advanced

BW1253s supports **Multiple BSSID (MBSSID)** function. You can configure up to 16 BSSIDs on BW1253s and assign different configuration settings to each BSSID. For wireless users, they can think BW1253s as single AP with multi service supporting, including different security policy, different VLAN ID, different authentication etc. All the BSSIDs are active at the same time that means client devices can associate to the access point for specific service. Use the **Wireless | Advanced** menu to configure properties related to Multiple BSSID, including configure SSID, Hidden SSID, VLAN, and Security for each SSID.



You can define different MBSSID if you configure **AP mode** in **Wireless | Basic** menu.

Each BSSID can have its own SSID. In this case, Multiple BSSID is the same with Multiple ESSID. Wireless users can think BW1253s as multiple virtual APs, each supporting different service, and connects one SSID for the special services.

There are different setting within **wireless | advanced** menu based on **AP mode** or **DynamicBridge mode** configured in **Wireless | Basic** menu.

AP Mode

If you configure AP mode, the page will be shown as below in **Wireless | Advanced** menu.

Advance Wireless Setting						
Radio: wlan1		AP Mode				
Interface	SSID	Hidden	Security	Current Connect #	Action	
wlan1_0	BW1253-11g-ggyy	Disabled	Disabled	0	Detail	Edit
					Delete	
					New	
Refresh						

Figure 51 – Advanced Wireless Setting (AP Mode)

Radio – specify wireless interface to be configured.[only one radio for BW1253s]

Mode – show the current operation mode of this radio (AP or Bridge)

Interface – display the interface which corresponding to the SSID. Each Interface maps to a BSSID

SSID – SSID name for wireless client searching and associating.

Hidden – show the status of Hidden SSID feature[disable/enable]

Security – show which security policy is used for this **MBSSID** entry

Current Connect # – show the number of current wireless clients associate to this MBSSID

New – create a new **MBSSID** entry

Detail – show the detail information of this **MBSSID** entry

Edit – edit the selected **MBSSID** entry you want to configure

Delete – delete the selected **MBSSID** entry. When in AP mode, you can not delete the last entry

Refresh – rescan the WEB page to get newer information

Clicking **New** or **Edit** button to configure the SSID parameters. Describe as below:

Advance Wireless Setting		
Radio	wlan1	
Interface	wlan1_0	
Mode	AP	
SSID	<input type="text" value="BW1253-11g"/> (Printable ASCII Characters)	
	<input type="checkbox"/> Need Hidden SSID	
	<input checked="" type="checkbox"/> SSID status	
	<input type="checkbox"/> Pureg	
	<input type="checkbox"/> Only 11n	
	<input type="checkbox"/> Disassociation low MCS	
Max Station Number	<input type="text" value="1~127"/> (1~127)	
Layer 2 Isolation	<input type="checkbox"/> Enable Intra-BSS Layer 2 Isolation (Inter-BSS Layer 2 Isolation can be configed in Wireless -> Layer 2 Isolation page.)	
Bandwidth		
	<input type="checkbox"/> Enable bandwidth	
	Download bandwidth	<input type="text"/> (Mbps)
	Upload bandwidth	<input type="text"/> (Mbps)

Figure 52 – BSSID Setting -1

Radio – show the wireless interface is being configured.

Interface – show the current sub-interface.

Mode – show the operation mode of current radio.

SSID – a unique ID for your wireless network. It is case sensitive and must not exceed 32 characters. The SSID is important for clients when connecting to the access point.

Need Hidden SSID – when enabled, the SSID of this Interface is invisible in the networks list while scanning the available networks for wireless client (SSID is not broadcasted with its Beacons). When disabled, the AP's SSID is visible in the available network list [enabled/disabled]. By default the Hidden SSID is disabled

SSID status – activated or deactivated the SSID. The default is activated SSID[check box].

Pureg – enable/disable 11b client connection. [check box] to enable the function.

Only 11n –only 802.11n client can connected to the SSID.

Max Station Number – define maximum number of associated wireless client to this SSID.Leave space means unlimited or fill in the value.[1~127 client]

Layer 2 Isolation – Specify the layer 2 isolation policy.

Enable Intra-BSS Layer 2 Isolation – when enabled, the clients that connect in this same BSS can't visit each other. By default the intra-BSS layer 2 isolation is disabled.

	Intra-BSS layer2 isolation – which enable or disable client isolation under same SSID. Inter-BSS layer2 isolation – which enable or disable client isolation between different SSID.
	Please go to Wireless Layer 2 Isolation(Inter-BSS) menu to configure inter-BSS layer 2 Isolation. Full layer 2 isolation need to set both intra-BSS and inter-BSS layer 2 isolation in the AP mode.

Bandwidth – enable/disable upstream/downstream bandwidth control per SSID.

Download bandwidth – specified the maximum downstream in Mbps controlled by the SSID.

Upload bandwidth – specify the maximum upstream in Mbps controlled by the SSID.

VLAN			
	<input type="checkbox"/> Enable VLAN		
		VLAN ID	<input type="text"/> (1~4094)
		802.1p Tag	<input type="text"/> Best Effort(0) (Class of Service)
Interface Priority			
		<input type="text"/> Best Effort(0) (Class of Service)	
WMM	<input checked="" type="checkbox"/> Enable WMM		
ESS in Tunnel	<input type="radio"/> Enabled		
		Remote Server IP	<input type="text"/>
	<input type="radio"/> Disabled		

Figure 53 – Multiple BSSID Setting -2

VLAN – specify VLAN policy

Enable VLAN – when enabled, the outgoing packets from this SSID device will be tagged with VLAN ID and 802.1p tag.

VLAN ID – configure VLAN ID for each Multiple SSID devices. Valid numbers are from 1 to 4094

802.1p Tag – configure 802.1p Tag for remote APC's or Router's QoS uses. Eight levels selective, Background(1), Spare(2), Best Effort(0), Excellent Effort(3), Controlled Load(4), Interactive Video(5), Interactive Voice(6), Network Control(7)

i	VLAN ID and 802.1p tag must cooperate with remote Router or APC.
----------	--

Interface priority – specify the traffic priority for this SSID interface, which is implemented according to 802.11e EDCA and makes sure the wireless downlink QoS. This priority is based on SSID, which means different BSSID can have different traffic priority and the traffic of the same SSID has the same priority

i	This traffic priority only makes sure the priority of downlink (from AP to wireless client). 8 levels priorities are supplied. 1, 2, 0, 3, 4, 5, 6, 7 is from lowest priority to highest priority. And if no special QoS is needed, leave priority to default (0). 0 means Best Effort priority.
----------	---

WMM – BW1253s support WMM wireless clients and implement WMM QoS with the WMM clients. [enable]

ESS in Tunnel – Settings for ESS in tunnel. When enabled, BW1253s setup tunnel with remote AC for passing through layer3 network.

Remote Server IP – IP address of remote AC product that setup tunnel with BW1253s

Security			
<input checked="" type="radio"/> WEP(Wired Equivalent Privacy)			
	WEP KeyIndex	1	<input type="button" value="▼"/>
<input checked="" type="radio"/> 802.1x	RADIUS Server Profile	DEFAULT	<input type="button" value="▼"/>
	Dynamic WEP Encryption	<input checked="" type="radio"/> Disabled <input type="radio"/> 64 bits <input type="radio"/> 128 bits	
		<input type="checkbox"/> Pass Through	
<input checked="" type="radio"/> WPA	RADIUS Server Profile	DEFAULT	<input type="button" value="▼"/>
	Algorithm	TKIP	<input type="button" value="▼"/>
	Group Key Rekey Interval	<input type="text"/> Minutes	
<input checked="" type="radio"/> WPA2	RADIUS Server Profile	DEFAULT	<input type="button" value="▼"/>
	Algorithm	TKIP	<input type="button" value="▼"/>
	Group Key Rekey Interval	<input type="text"/> Minutes	
<input checked="" type="radio"/> WPA2 MIXED	RADIUS Server Profile	DEFAULT	<input type="button" value="▼"/>
	Algorithm	TKIP/AES	
	Group Key Rekey Interval	<input type="text"/> Minutes	

Figure 54 – Multiple BSSID Setting – 3

Security – specify the security policy

WEP – Wired Equivalent Privacy(WEP) is a security algorithm for IEEE 802.11 wireless networks.

WEP Key Index – select the default key Index to make it the Default key and encrypt the data before being transmitted. All stations, including this SSID Entry, always transmit data encrypted using this Default Key. The key number (1, 2, 3, 4) is also transmitted. The receiving station will use the key number to determine which key to use for decryption. If the key value does not match with the transmitting station, the decryption will fail. The key value is set in **Wireless | WEP** web page

802.1x – when selected, the SSID entry will be configured as an 802.1x authenticator. It supports multiple authentication types based on EAP (Extensible Authentication Protocol) like EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM. The privacy will be configured as dynamic WEP

RADIUS Server Profile – select your RADIUS server profile



Please go to **Network | RADIUS Server** menu to configure your RADIUS server profile or add a new profile, and please refer to **Network | RADIUS Server** for its configuration.

Dynamic WEP Encryption – select whether using the dynamic 64-bits encryption, 128-bits encryption or without encryption

Pass Through – when enabled, client can access network whether it passed 802.1x authentication or not



Only when 802.1x enabled and dynamic key disabled this option can be enabled.

WPA – Wi-Fi Protected Access, When selected, the encrypt method will be WPA with RADIUS Server

WPA2 – when selected, the security policy will be WPA2 with RADIUS server. In this mode, WPA client is not permitted to connect

WPA2 MIXED – when selected, WPA2 client and WPA client are all permitted to connect

RADIUS Server Profile – select your RADIUS server profile



Please go to **Network | RADIUS Server** menu to configure your RADIUS server profile or add a new profile, and please refer to **Network | RADIUS Server** for its configuration.

Algorithm – choose WPA algorithm (TKIP, AES)

Group Key Rekey Interval – specify amount of minutes and WPA automatically will generate a new Group Key

<input type="radio"/> WPA-PSK	Use Pre-Shared Key	<input type="text"/>
	Algorithm	TKIP <input type="button" value="▼"/>
	Group Key Rekey Interval	<input type="text"/> Minutes
<input type="radio"/> WPA2-PSK	Use Pre-Shared Key	<input type="text"/>
	Algorithm	TKIP <input type="button" value="▼"/>
	Group Key Rekey Interval	<input type="text"/> Minutes
<input type="radio"/> WPA2-PSK MIXED	Use Pre-Shared Key	<input type="text"/>
	Algorithm	TKIP/AES
	Group Key Rekey Interval	<input type="text"/> Minutes
<input type="radio"/> MAC Auth	RADIUS Server Profile	DEFAULT <input type="button" value="▼"/>

Figure 55 – Multiple BSSID Setting – 4

WPA-PSK – when selected, the encrypt method will be WPA without RADIUS server

WPA2-PSK – when selected, the security policy will be WPA2 PSK without RADIUS server. In this mode, only WPA2 PSK client can connect with AP and WPA PSK client is not permitted to connect

WPA2-PSK MIXED – when selected, WPA2 PSK and WPA PSK clients are all permitted to connect with AP

Use Pre-Shared Key – specify more than 8 characters and less than 64 characters for WPA with pre-shared key encryption

Algorithm – choose WPA algorithm (TKIP, AES)

Group Key Rekey Interval – specify amount of minutes and WPA automatically will generate a new Group Key

MAC Auth – when selected, the MAC address of wireless client will be passed to RADIUS server for PAP authentication when it connects with BW1253s. The MAC address of wireless client acts as username and password

RADIUS Server Profile – select the default radius server name

<input type="radio"/> WAPI	AAA Server Profile:	DEFAULT <input type="button" value="▼"/>
	WAPI certificate has not been Uploaded. Click here to upload certificate.	
<input type="radio"/> WAPI-PSK	Encode:	HEX <input type="button" value="▼"/>
	Use Pre-Shared Key:	<input type="text"/>
<input type="radio"/> Disabled		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Figure 56 – Multiple BSSID Setting – 5

WAPI – WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese National Standard for wireless LAN(GB15629.11-2003).(Only for China)

It needs to upload WAPI certificate.

AAA Server Profile – select your RADIUS server profile

WAPI-PSK – the encrypt method will be WAPI without RADIUS server

Encode – Pre-shared key encode.[HEX/ASCII]

Use Pre-Shared key – specify more than 8 characters and less than 64 characters for WPA with pre-shared key encryption

Disabled – when selected, you don't select any security policy

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Advance Wireless Setting	
Radio	wlan1
Interface	wlan1_0
Mode	AP
SSID	SSID
Hidden SSID	Disabled
Intra-BSS Layer 2 Isolation	Disabled
Use VLAN	Disabled
Interface Priority	Best Effort(0) (Class of Service)
WMM	Enabled
ESS in Tunnel	Disabled
Security	Disabled
Current Connected Number	0

[Refresh](#) [Return](#)

[Apply Changes](#) [Discard Changes](#)

Figure 57 –Apply or Discard the advanced Settings in AP mode

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Advance Wireless Setting	
Radio	wlan1
Interface	wlan1_0
Mode	AP
SSID	SSID
Hidden SSID	Disabled
Intra-BSS Layer 2 Isolation	Disabled
Use VLAN	Disabled
Interface Priority	Best Effort(0) (Class of Service)
WMM	Enabled
ESS in Tunnel	Disabled
Security	Disabled
Current Connected Number	0

[Refresh](#) [Return](#)

[Reboot](#)

System needs to be restarted to make the new configurations take effect.

Figure 58 – Reboot information

Reboot – click the button to restart the server and apply the changes.

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
---	---

DynamicBridge Mode

DynamicBridge is smart, high efficiency, high performance, easy deployment and easy configuration for point to multi-point bridge link. It enables BW1253s to automatically seek and associate nearby root AP and dynamically self-configure for wireless bridge connection. Whenever a bridge link is broken, the network will auto re-configure route to minimize the lost of WLAN operation. It also minimized the technician intervention and reduce cost of going on-site to re-establish transmission paths.

NodeType	NetID	Security	Action
Root	default	Disabled	Edit

Figure 59 – Advanced Wireless Setting (Bridge Mode)

Radio – specify the wireless interface

NodeType – show the node type (root or normal)

NetID – Net ID for the association between root and normal(client) bridge link. It must be the same between root and normal(client) association.

Security – specify which security policy is used

Edit – edit the selected **Bridge link** entry you want to configure

Clicking **Edit** to configure the bridge parameters.

NodeType	NetID	Security	Action
Root	default	<input checked="" type="radio"/> WPAPSK-AES <input type="radio"/> Disabled	Save Cancel

Figure 60 – Bridge Link Setting

NodeType – determine the AP as Root or Normal(client) rule. As a root AP, the nearby bridge client will automatically associate to the root AP based on the signal quality. In case a bridge link is broken, the client AP will automatically seek the nearby root AP based on the best signal quality and same NetID to re-build a bridge link. For the normal(client) AP the NetID must same with root AP to distinguish which root AP is in the link table. And the frequency channel is determined by the root AP despite the client AP configured.

NetID – NetID is a very important element for the dynamicbridge link. The link between root and client AP will based on the same NetID to make the bridge link.

Security – specify the security policy of the bridge link. [WPA-PSK (AES)/disable]

WPAPSK-AES –specify more than 8 characters and less than 64 characters for WPA with pre-shared key encryption

Disable – no data encryption for the bridge link.

Click **Save** button to save the change of settings or **Cancel** button to discard the change

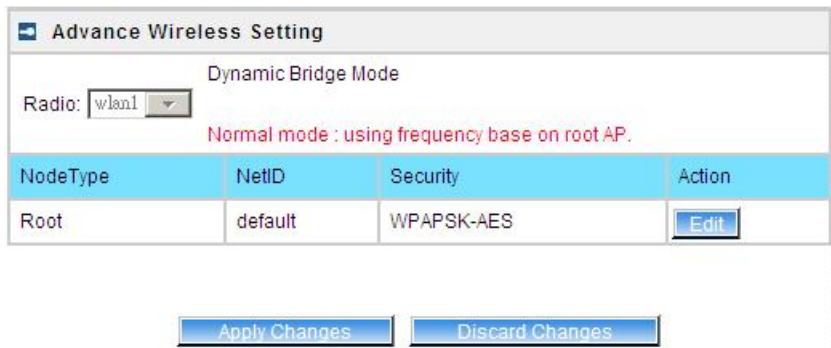


Figure 61 –Apply or Discard the advanced Settings in Bridge mode

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

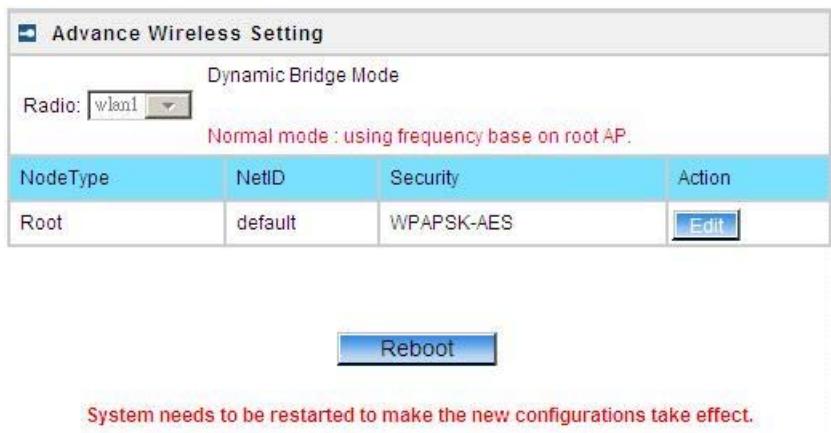


Figure 62 – Reboot information

Reboot – click the button to restart the server and apply the changes.



If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.
And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.

Wireless | WEP

Use the **Wireless | WEP** menu to configure static WEP settings.



This menu only set static WEP key value related with 4 key indexes. Enable or Disable static WEP is in the **Wireless | Advance** menu.

WEP Configuration

Radio	wlan1	
Index	Key	Action
Key 1	*****	Edit
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Figure 63 – WEP Settings

Radio –show the wireless interface.

Click **Edit** to edit the existing **wepkey1** to **wepkey4**.



By default, four WEP keys are all set to “aaaaa” (ascii characters) or “6161616161” (hexadecimal characters). They can be modified according to requirement.

WEP Configuration

Radio	wlan1	
Index	Key	Action
Key 1	<input type="text"/>	Save Cancel
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Figure 64 – Edit WEP Key

Change status or leave in the default state if no editing is necessary and click the **Save** button.

WEP Configuration		
Radio	wlan1	
Index	Key	Action
Key 1	*****	Edit
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Apply Changes **Discard Changes**

Figure 65 –Apply or Discard WEP Configuration

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

WEP Configuration		
Radio	wlan1	
Index	Key	Action
Key 1	*****	Edit
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 66 – Reboot information

Reboot – click the button to restart the server and apply the changes

i	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
----------	---

Wireless | MAC ACL

Use the **MAC ACL** service to control the default access to the wireless interface of the BW1253s or define special access rules for mobile clients. Configure the ACL using the **Wireless | MAC ACL** menu:

MAC ACL Configuration		
Radio	wlan1	
Policy	Allow	Edit
MAC List		Action
00:90:4B:C9:42:55		Delete
Add		

Figure 67 – MAC ACL Service

Radio – show the wireless interface.

	The wireless interface which is Bridge mode hasn't MAC ACL settings.
--	--

Policy – click the **edit** button to choose Allow, Deny or disable the access control service on device. By default the ACL service is disabled and all wireless clients connecting to the BW1253s are allowed (no ACL rules are applied to the wireless clients)

Select **Allow** means only the wireless clients whose MAC are listed in the **MAC List** would be permitted to access this AP. Other wireless client cannot access this AP.

Select **Deny** means only the wireless clients whose MAC are listed in the **MAC List** would be prevented from accessing. Other wireless clients can access this AP.

Select **Disabled** means no ACL service.

MAC ACL Configuration		
Radio	wlan1	
Policy	Allow	Save Cancel
MAC List		Action
Allow		
Deny		
Disabled		
00:90:4B:C9:42:55		Delete
Add		

Figure 68 – MAC ACL settings

You must create **MAC List** to work with **Policy** setting. The access control list is based on the network device's MAC address. In the MAC ACL Configuration table, you only need to specify the MAC address of wireless client. Click the **Add** button to create a new MAC entry:

MAC ACL Configuration		
Radio	wlan1	<input type="button" value="Edit"/>
Policy	Allow	<input type="button" value="Edit"/>
MAC List		Action
00:90:4B:C9:42:55		<input type="button" value="Delete"/>
<input type="text"/> Example: 00:90:4B:00:11:22		<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Figure 69 – Add MAC entry

MAC Address – enter the physical address of the network device you need to (MAC address). The format is a list of colon separated hexadecimal numbers (for example: 00:90:4B:00:11:22)

Save – click the button to save the new MAC entry

MAC ACL Configuration		
Radio	wlan1	<input type="button" value="Edit"/>
Policy	Allow	<input type="button" value="Edit"/>
MAC List		Action
00:90:4B:C9:42:55		<input type="button" value="Delete"/>
<input type="button" value="Add"/>		<input type="button" value="Apply Changes"/> <input type="button" value="Discard Changes"/>

Figure 70 – Apply or Discard MAC ACL Configuration Changes

Apply Changes – to save all changes made in the **interface** table at once

Discard Changes – restore all previous values

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

MAC ACL Configuration		
Radio	wlan1	<input type="button" value="Edit"/>
Policy	Allow	<input type="button" value="Edit"/>
MAC List		Action
00:90:4B:C9:42:55		<input type="button" value="Delete"/>
<input type="button" value="Add"/>		<input type="button" value="Reboot"/>

System needs to be restarted to make the new configurations take effect.

Figure 71 – Reboot Server

Reboot – click the button to restart the server and apply the changes

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
---	---

Wireless | Layer 2 Isolation(Inter-BSS)

Use the **Layer 2 Isolation** service to block inter-BSS communication of all users. Users can only access the AP connected, the gateway and devices in the allow MAC List.

	Please go to Wireless Advanced page to configure intra-BSS communication of users in the same BSS. Full layer 2 isolation need to set both intra-BSS and inter-BSS layer 2 isolation.
	The Wireless layer 2 isolation setting page is only exist in AP mode as it is only for inter-BSS layer 2 isolation. There is no Wireless layer 2 isolation setting page in AP-Router mode.

Layer 2 Isolation Setting (Inter-BSS)		
Status	disable	Edit
Intra-BSS Layer 2 Isolation can be configed for each BSS in Wireless -> Advanced page.		

Figure 72 – layer 2 Isolation Service

Edit – edit the layer 2 isolation settings.

To change layer 2 isolation setting properties click the **Edit** button.

Layer 2 Isolation Setting (Inter-BSS)		
Status	disable	Save Cancel
Intra-BSS Layer 2 Isolation can be configed for each BSS in Wireless -> Advanced page.		

Figure 73 – layer 2 Isolation Setting

Status –select status from the drop-down menu.

disable – disable the layer 2 isolation (Inter-BSS) service.

enable – enable the layer 2 isolation (Inter-BSS) service.

Only when Inter-BSS Isolation is enabled, the entry of the allowed MAC list can be added.

Layer 2 Isolation Setting (Inter-BSS)		
Status	enable	Save Cancel
Allowed MAC List		
Name	Allowed MAC	Action
No entry in list		
Add		
Intra-BSS Layer 2 Isolation can be configed for each BSS in Wireless -> Advanced page.		
The MAC addresses of AP and Gateway are always automatically added to Allowed MAC List without manual configuration.		

Figure 74 –Allowed MAC List

	The MAC addresses of AP and Gateway are always automatically added to allowed MAC list without manual configuration.
---	--

Click the **Add** button to create a new MAC entry or click **Edit** button to edit the MAC entry:

Layer 2 Isolation Setting (Inter-BSS)	
Allowed MAC List	
Name	Allowed MAC
default	00:00:00:00:00:00
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
Intra-BSS Layer 2 Isolation can be configed for each BSS in Wireless -> Advanced page.	
The MAC addresses of AP and Gateway are always automatically added to Allowed MAC List without manual configuration.	

Figure 75 –Add MAC entry

Name – the new Allowed MAC name, which length range is 1 to 32.

MAC Address – enter the physical address of the network device (MAC address). The format is a list of colon separated hexadecimal numbers (for example: 00:90:4B:00:11:22)

Save – click the button to save the new Allowed MAC List entry

Cancel – discard change and restore all previous values

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Layer 2 Isolation Setting (Inter-BSS)		
Status	<input type="button" value="enable"/> <input type="button" value=""/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		
Allowed MAC List		
Name	Allowed MAC	Action
PC1	00:90:4B:D5:11:22	<input type="button" value="Delete"/> <input type="button" value="Edit"/>
<input type="button" value="Add"/>		
Intra-BSS Layer 2 Isolation can be configed for each BSS in Wireless -> Advanced page.		
The MAC addresses of AP and Gateway are always automatically added to Allowed MAC List without manual configuration.		

Figure 76 –Save Allowed MAC List Changes

Apply Changes –Apply Changes – to save all changes at once.

Discard Changes –restore all previous values

Edit – edit layer 2 isolation settings

Delete – delete the selected **Allowed MAC** entry.

■ Layer 2 Isolation Setting (Inter-BSS)		
Status	enable	Edit
■ Allowed MAC List		
Name	Allowed MAC	Action
PC1	00:90:4B:D5:11:22	Delete Edit
Add		
Intra-BSS Layer 2 Isolation can be configed for each BSS in Wireless -> Advanced page.		
The MAC addresses of AP and Gateway are always automatically added to Allowed MAC List without manual configuration.		

Reboot**System needs to be restarted to make the new configurations take effect.***Figure 77 –apply changes***Reboot** – click the button to restart the server and apply the changes

If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

User

User | Users

The **User | Users** menu shows the statistics of connected users. The user can be monitored and managed such as drop from the network.

Users								
Index	User	Interface	User IP	Authed	Wireless Auth	Time Length	Idle Time	Action
01.	00:0c:41:16:97:aa	wlan1_0	192.168.120.62	No	NONE	00:26:53	00:00:25	<button>Details</button> <button>Kickoff</button>

Figure 78 – User's statistics

User – show the connected client's MAC address

Interface – show which BSS the client connected to

User IP – IP address, from which the user's connection is established [digits and dots]

Authed – indicate this client is authenticated or not

Wireless Auth – show the authentication method which user used to connect

Time Length – session duration since the user login [hh:mm:ss]

Idle Time – amount of user inactivity time [hh:mm:ss]

Action – view the statistics or kickoff the user.

Detail – click on user details to get more information about the client:

Kickoff – disconnect the user.

Users		
Description	Value	Action
user	00:0c:41:16:97:aa	
interface	wlan1_0	
user IP	192.168.120.62	
MAC address	00:0c:41:16:97:aa	
L2 Auth	NONE	
WISP	-	
session id	-	
time length	01:26:01	
remaining time length	-	
idle time	00:00:21	
idle timeout	-	
input bytes	183 KB	
output bytes	88 KB	
remaining input bytes	-	
remaining output bytes	-	
remaining total bytes	-	
bandwidth downstream	-	
bandwidth upstream	-	
		<input type="button" value="Back"/> <input type="button" value="Kickoff"/>
<input type="button" value="Refresh"/>		

Figure 79 – User's Details

MAC address – hardware address of the network device from which the user is connected

L2 Auth – show layer2 authentication status, including all supported EAP type of 802.1x auth and MAC auth

WISP – WISP domain name where the user belongs

Session ID – the unique user's session ID number. This can be used for troubleshooting purposes

Remaining Time Length – remaining user's session time [hh:mm:ss]. Session time for user is defined in the RADIUS Server

Idle time – specify current idle time.

Idle Timeout – specify the time of user idle timeout [hh:mm:ss]. When reach the time, the user will be logged out automatically.

Input Bytes – amount of data in bytes which the user network device has received [Bytes]

Output Bytes – amount of data in bytes, transmitted by the user network device [Bytes]

Remaining Input/Output Bytes – user session remaining input/output bytes. WISPr Operator can define the user session in bytes. Remaining bytes is received from RADIUS [Bytes/unlimited]

Remaining Total Bytes – user session remaining total bytes. WISPr Operator can define the user session in bytes. Remaining bytes is received from RADIUS [Bytes/unlimited]

Bandwidth Downstream/Upstream – user upstream and downstream bandwidth [in bps]

Back – returns to connect client's statistics list

Kickoff – click this button to disconnect the user from access point.

Refresh – click the button to refresh users' statistics

User | Station Supervision

The **Station Supervision** function is used to monitor the connected host station availability. This monitoring is performed with ping. If the specified number of ping failures is reached (**failure count**), the user is logged out from the BW1253s.

Station Supervision		
Interval	Failure Count	Action
20	3	Edit

Figure 80 – Station Supervision

To adjust the ping interval/failure count, click the **Edit** button.

Station Supervision		
Interval	Failure Count	Action
20	3	Save Cancel

Figure 81 – Edit Station Supervision

Interval – define interval of sending ping to host [in seconds]

Failure Count – failure count value after which the user is logged out from the system

Save – save station supervision settings

Cancel – cancel changes

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Station Supervision		
Interval	Failure Count	Action
20	3	Edit

Apply Changes

Discard Changes

Figure 82 –Apply or Discard Station Supervision Changes

Apply Changes – to save all changes made in the **interface** table at once

Discard Changes – restore all previous values

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Station Supervision		
Interval	Failure Count	Action
20	3	Edit

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 83 – Reboot Server

Reboot – click the button to restart the server and apply the changes

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
---	---

Services

Services | Telnet

Use **Services | Telnet** menu to manage the telnet/SSH service of your BW1253s.

Telnet		
Name	Status	Action
Telnet Service	Enabled	Edit
SSH Service	Enabled	Edit

Figure 84 – System Configuration settings

Telnet Service – Enable or disable telnet service of BW1253s

SSH Service – Enable or disable SSH service of BW1253s

The default of these two services are all **Enabled**. The current IETF SSH (SSHv2) is supported for security of accessing BW1253s via telnet/CLISH.

Services | SNMP

SNMP is the standard protocol that regulates network management over the Internet. To communicate with SNMP manager you must set up the same **SNMP** communities and identifiers on both ends: manager and agent.

Use the **Services | SNMP** menu to change current SNMP configuration.

The screenshot shows two tables under the 'Services | SNMP' menu:

- General Configuration:**

Name	Value	Action
Readonly community	public	Edit
Readwrite community	private	Edit
DefaultTrap community	public	Edit
HeartBeat Trap Interval	10 seconds	Edit
- Trap Configuration:**

Index	Host Ip	Host Port	Trap Type	Community	Action
1	192.168.120.62	162	trapsink	test	Delete

Buttons at the bottom: **Add** (highlighted), **Cancel**, **Save**.

Figure 85 – SNMP settings

Readonly community – community name is used in SNMP version 1 and version 2c. Read-only (public) community allows reading values, but denies any attempt to change values [1-32 all ASCII printable characters, no spaces]

Readwrite community – community name is used in SNMP version 1 and version 2c. Read-write (private) community allows to read and (where possible) change values [1-32 all ASCII printable characters, no spaces]

Default Trap community – the default SNMP community name used for traps without specified communities. The default community by most systems is "public". The community string must match the community string used by the SNMP network management system (NMS) [1-32 all ASCII printable characters, no spaces]

HeartBeat Trap Interval – defined the AP sending the trap interval to the SNMP server.[second]

Trap Configuration Table:

You can configure your SNMP agent to send **SNMP Traps** (and/or inform notifications) under the defined host (SNMP manager) and community name (optional).

Click **Add** to add a new SNMP manager or **Delete** to delete a specific SNMP manager. Clicking **Add**:

The screenshot shows the 'Trap Configuration' dialog box with the following fields:

Index	Host Ip	Host Port	Trap Type	Community	Action
No entry in list					
	192.168.123.66	162	trapsink	test	Save Cancel

A dropdown menu for 'Trap Type' is open, showing options: trapsink, trap2sink, trapinform, and informsink. The 'trapsink' option is currently selected.

Figure 86 – Add SNMP Trap

Host IP – enter SNMP manager IP address [dots and digits]

Host Port – enter the port number the trap messages should be send through [number]

Trap Type – select trap message type [v1/v2/inform]

Community – specify the community name at a SNMP trap message. This community will be used in trap messages to authenticate the SNMP manager. If not defined, the default trap community name will be used (specified in the SNMP table) [1-32 all ASCII printable characters, no spaces]

Save – save all current settings

Cancel – restore the last settings

Services | Time

Configure the system time manually under **Services | Time Settings** menu.

Date and Time	
Date	2013/08/30
Time	15:20
<input type="button" value="Edit"/> <input type="button" value="Refresh"/>	

Figure 87 – Time Settings

Click **Edit** to change current system time.

Date and Time	
Date	2013 / 08 / 30
Time	15 : 20
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 88 – Edit Date and Time Settings

Date – [yy/mm/dd]

Time – [hour/minute]

Change the Date and Time or leave in the default value if no editing is necessary and click the **Apply** button. Thus the modified time will be taken effect at once. No reboot is needed.



If NTP is enabled, the local time cannot be modified.



Since BW1253s hasn't RTC (real-time clock), the system time will back to 1970/01/01 00:00 when reboot.

Services | NTP

NTP (Network Time Protocol) is used to synchronize the system time with the selected network NTP server. Use the **Services | NTP** menu to configure the NTP service:

Name	ServerIP	Action
No entry in list		
Add		

Figure 89 – NTP Settings

NTP Status – specify enable or disable this NTP service

Time Zone – specify the time zone for NTP service

Delete – delete the existed NTP server

Edit – edit the settings of the existed NTP server

Add – add a new NTP server setting for synchronizing time

Clicking **Add** button to add a new NTP server:

Name	ServerIP
Ntpserver	207.46.103.100
Save Cancel	

Figure 90 – Add new NTP server setting



Two NTP servers can be configured under **Services | NTP** menu. And only IP address is accepted for NTP server.

Adding at least one NTP server before enable NTP service.



The **Name** of NTP server should be unique.

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Name	ServerIP	Action
time.nist.gov	192.43.244.18	Delete Edit
Add		
Apply Changes Discard Changes		

Figure 91 – Save the NTP server Changes

Change the Time Zone for your own local time and change the NTP status to enable or disable.

Name	ServerIP	Action
time.nist.gov	192.43.244.18	<input type="button" value="Delete"/> <input type="button" value="Edit"/>

Figure 92 – Edit Time Zone setting/NTP status

Click **Save** button to save new Time Zone setting.

Name	ServerIP	Action
time.nist.gov	192.43.244.18	<input type="button" value="Delete"/> <input type="button" value="Edit"/>

Figure 93 – Apply or Discard Time Zone/NTP status Changes

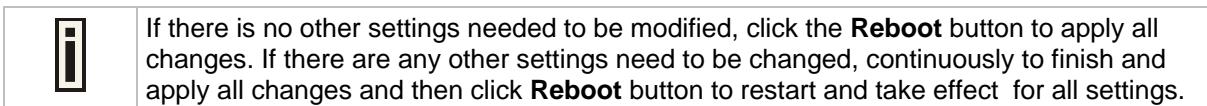
For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Name	ServerIP	Action
time.nist.gov	192.43.244.18	<input type="button" value="Delete"/> <input type="button" value="Edit"/>

System needs to be restarted to make the new configurations take effect.

Figure 94 – Reboot information

Reboot – click the button to restart the server and apply the changes



Services | Watchdog

BW1253s supports watchdog function for the reliability. Use **Services | Watchdog** to enable/disable watchdog service.

Watchdog			
Name	Status	Check Interval	Action
Software Watchdog	Enabled	10 Seconds	Edit
Hardware Watchdog	Enabled		Edit

Figure 95 – Watchdog settings

Click Edit button to edit software watchdog settings. The UI will appear as below:

Watchdog			
Name	Status	Check Interval	Action
Software Watchdog	Enabled ▼	10 Seconds	Save Cancel
Hardware Watchdog	Enabled		Edit

Figure 96 – edit Software Watchdog settings

Status – Enable or Disable software watchdog

Check Interval – the periodical time that software watchdog checks the whole file system of BW1253s.

The hardware watchdog function will protect device even the operation system crash.

Watchdog			
Name	Status	Check Interval	Action
Software Watchdog	Enabled	10 Seconds	Edit
Hardware Watchdog	Enabled ▼		Save Cancel

Figure 97 – edit hardware watchdog settings

Status – Enable or Disable hardware watchdog



The default value is enabled for both Software Watchdog and Hardware Watchdog. It is strongly recommended to enable the watchdog function.

Click **Save** and follow the UI instruction to apply changes and reboot the device for apply all the modified settings.

System

System | Administrator

The **System | Administrator** menu is for changing the administrator's settings: username and password:

Administrator	
User Name	<input type="text" value="admin"/>
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 98 – system security settings

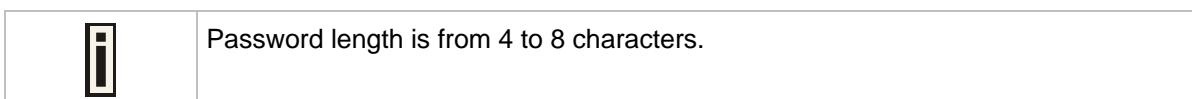
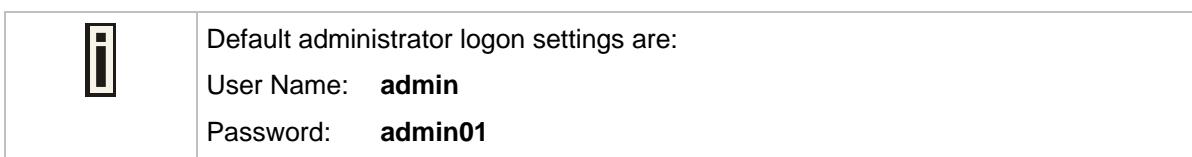
User Name – administrator username for access to BW1253s (e.g. web interface, CLI mode) [1-32 symbols, spaces not allowed]

Old Password – old password

New Password – new password value used for user authentication in the system [4-8 characters, spaces not allowed]

Confirm Password – re-enter the new password to verify its accuracy

Save – click to save new administrator settings.



After filling in the right Old password and the New Password, clicking the **Save** button for taking effect immediately.

After clicking **Save** button, the below UI will be shown to notify that the new password setting has been taken place:

Set password successfully.

Administrator	
User Name	<input type="text" value="admin"/>
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Set password successfully.

Figure 99 – system security settings save and take effect successfully

System | System Log

Use the **System | System Log** menu to trace your AP system processes and get the system log locally or on the remote log server.

Remote System Log			
Remote Log Status	Host IP	Log Level	Action
Disabled	192.168.2.1	info	Edit

Local System Log			
Local Log Status	Log Limit (bytes)	Log Level	Action
Enabled	102400	debug	Edit
View Log Messages			View

Figure 100 – System Log settings

To enable the **System Log** remote sending function, click the **Edit** button on the Remote System Log table and choose the **enabled** option:

Remote System Log			
Remote Log Status	Host IP	Log Level	Action
Enabled	192.168.2.1	Info	Save Cancel

Figure 101 – Configure Remote System Log Utility

Remote Log Status – choose disable/enable remote log function.[enabled/disabled]

Host IP – specify the host IP address where to send the **System Log** messages [dots and digits]

Log Level – specify the remote log message level you want to trace [critical, error, warning, info and debug]

	Do not output “debug” log unless there are important issue needs to be clarified. Debug log will output all of the information so that it will severely drop down the network performance.
	BW1253s support standard sys. log server.

Save – save changes

Cancel – restore the previous values

To view the **System Log** locally, click the **Edit** button on the Local System Log table and choose the **enabled** option:

Local System Log			
Local Log Status	Log Limit (bytes)	Log Level	Action
Enabled	102400	Debug	Save Cancel
View Log Messages			View

Figure 102 –Configure Local System Log

Local Log Status – choose disable/enable local log [enabled/disabled]

Log Limit – specify the maximum length of local log message in byte [20000-512000]

Log Level – specify the local log message level you want to trace [critical, error, warning, info and debug]

Save – save changes

Cancel – restore the previous values

View – view the log messages locally

Click **View** button, a similar screen will appear as below:

Local Log Messages	
Messages	Action
Clear All Log Messages:	<input type="button" value="Clear"/>
Jan 1 03:17:59 P720 [G8000]: messages is null, so continue	
Jan 1 03:18:05 P720 last message repeated 3 times	
Jan 1 03:18:08 P720 [G8000]: cmd is equal to refreshlog button	
Jan 1 03:18:08 P720 [G8000]: messages is null, so continue	
<input type="button" value="Refresh"/> <input type="button" value="Return"/>	

Figure 103 – View Local Log Messages

Clear – clear current log message

Refresh – get the updated log messages

Return – back to System Log page

System | System Mode

In this page, you can select the system mode of your BW1253s.

System Mode					
Mode	Interface	IP	Netmask	Gateway	Protocol
<input checked="" type="radio"/> AP					
	LAN	192.168.123.159	255.255.255.0	192.168.123.1	static <input type="button" value="▼"/>
<input type="radio"/> AP Router					
	WAN	192.168.123.159	255.255.255.0	192.168.123.1	static <input type="button" value="▼"/>
<input type="button" value="Apply and Reboot"/>					

Figure 104 – System Mode Settings

Mode – select whether the system mode of BW1253s is AP mode or AP Router mode

AP – The Ethernet interface and wireless interface will bridge into the same interface working as transparent access point.

AP Router – A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point. Under this mode the Ethernet will act as WAN interface and wireless interface will act as LAN.

IP – specify the IP address of current interface [dots and digits]

Netmask – specify the subnet mask of current interface [dots and digits]

Gateway – specify the gateway to other networks

Protocol – specify **static** for setting IP address manually and **dhcp** for getting IP address dynamically acting as DHCP client

Apply and Reboot – click the button to restart the device and apply all setting changes



The BW1253s Web Interface in AP mode is different from that in AP-Router mode. For the detailed configuration of BW1253s working in AP-Router mode, please refer to the next chapter: **Chapter 4 – Reference Manual---AP-Router Mode**

System | System Info

Administrator can self-define the device information including the system name, system location and system contact information of his BW1253s.

System Info		
Name	Value	Action
System Name	BW1253	<input type="button" value="Edit"/>
System Location	location	<input type="button" value="Edit"/>
System Contact	contact information	<input type="button" value="Edit"/>

Figure 105 – System info Settings

System Name – edit the system name, the column length range is 1 to 255.

System Info		
Name	Value	Action
System Name	<input type="text" value="BW1253"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
System Location	location	
System Contact	contact information	

Figure 106 –edit the system name

System Location – edit the system location, the column length range is 1 to 255.

System Info		
Name	Value	Action
System Name	BW1253	
System Location	<input type="text" value="Taipei 101"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
System Contact	contact information	

Figure 107 –edit the system location

System Contact – edit the system contact, the column length range is 1 to 255.

System Info		
Name	Value	Action
System Name	BW1253	
System Location	location	
System Contact	Engineer	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Figure 108 –edit the system contact

Save – click the button to save the change.

Cancel – restore all previous values

System | Configuration

Use the **System | Configuration** menu to download current configuration or restore specified configuration.

Configuration Backup – download current working system configuration for backup

Configuration Upload – upload system configuration for restore

Configuration Backup	
Description	Action
Configuration file to download	<input type="button" value="Preparation"/>
Configuration Upload	
Description	Action
Configuration file to upload	<input type="button" value="Browse..."/> <input type="button" value="Upload"/> <input type="button" value="Cancel"/>

Figure 109 – System Configuration settings

Click the **Preparation** button to start saving the configuration file.

Click the **Download** button to download current working configuration locally.

Configuration Backup	
Description	Action
Download and store Configuration backup file in safe place.	<input type="button" value="Download"/>

Figure 110 – Backup settings

By default the device configuration name is cfgbackup.cfg.



A configuration file name will be required when you download/save the configuration file. And please remember or re-name the file if needed. The configuration file name should only include characters or numbers. Otherwise, this configuration file will not upload to BW1253s.

You can upload saved configuration file any time you want to restore this configuration to the device by using the **Browse** button. Select the configuration file and upload it on the device:

The screenshot shows a configuration upload interface. At the top, there's a header "Configuration Upload". Below it is a table with two columns: "Description" and "Action". In the "Description" column, there's a text input field containing "C:\BW1253_cfgbackup.cfg". To the right of this field is a "Browse..." button. At the bottom of the table are two buttons: "Upload" and "Cancel".

Figure 111 – Configuration Upload/Restore - 1

Click **Upload** for upload the specified configuration and then the similar UI appears

The screenshot shows a confirmation dialog box. At the top, it says "Check it and Press **OK**, then device will reboot and the new configuration will take effect.". Below this is a "OK" button and a "Cancel" button.

Figure 112 – Configuration Upload/Restore - 2

Click **OK** button to restore and AP will reboot immediately to take effect.

The screenshot shows a progress bar indicating the reboot process. The text "Device is rebooting now. Please wait..." is displayed above the progress bar. The progress bar is at 4% completion.

Figure 113 – Configuration Upload/Restore - 3

System | Reset and Reboot

Use this function to reboot device or restore to factory default.

The screenshot shows a "System Reset and Reboot" configuration page. It has two main sections: "Reboot device" and "Restore the original configuration from factory". Each section has a "Reboot" button. Above the "Reboot device" section, the text "Current firmware version: BW1253s.BR0.1.0.14" is displayed.

Figure 114 – System Reset setting

Reboot – reboot the device

Reset – reset System to Factory Defaults

To reboot the device, click **Reboot** and then the below appears to make sure:

The screenshot shows a confirmation dialog box. It asks "Are you sure you want to REBOOT the device? It will take some time to boot up." At the bottom are two buttons: "Reboot" and "Cancel".

Figure 115 – Reboot the device

To reset the device, click **Reset** and then the below appears to make sure:

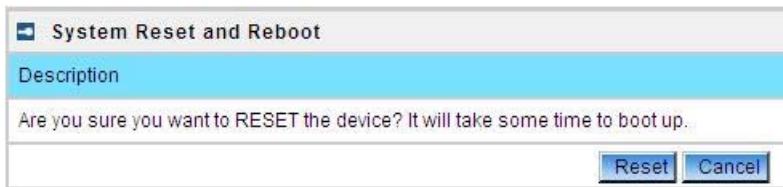


Figure 116 – Reset the device

Click reset button the device will reset and reboot immediately to take effect.



System | Local Upgrade

Upload – Update your device firmware locally.

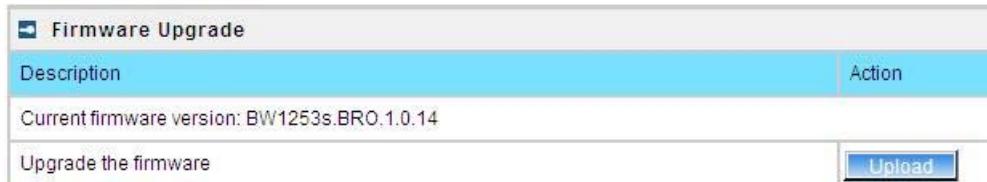


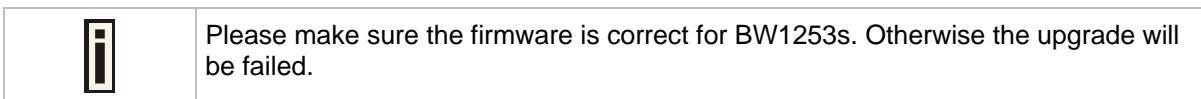
Figure 117 – Firmware Upgrade

Click the **Upload** and then click the browse button to specify the full path of the new firmware image and click the **Upload** button:



Figure 118 – Firmware Upgrade

Click the **Upgrade** button to flash and upgrade the firmware.



Firmware Upgrade	
Description	Action
Firmware image successfully uploaded. Press Upgrade button to Upgrade firmware now and reboot system.	Upgrade Cancel

Figure 119 – upgrade firmware

	Do not turn off the BW1253s during the firmware update process because the device could be damaged. It recommend to use the Ethernet connection (not wireless) for the firmware update process.
	Update firmware will take about 4 minutes.

System | TFTP Upgrade

BW1253s support firmware upgrade via TFTP server.

TFTP Firmware Upgrade		
Name	Value	Action
Current firmware version:	BW1253s.BRO.1.0.14	
TFTP server IP address		Edit
TFTP Time Out(Secs)		Edit
Firmware Filename		Edit
Download Firmware From TFTP server		Download

Figure 120 – TFTP Firmware Upgrade

Current firmware version – Show the current firmware version.

TFTP server IP address - Specify the IP address of TFTP server which firmware located.

TFTP Time Out(Secs) – Specify the TFTP server communication time out in second.

Firmware Filename – Specify the upgrade firmware name to be download.

TFTP Firmware Upgrade		
Name	Value	Action
Current firmware version:	BW1253s.BRO.1.0.14	
TFTP server IP address	61.17.23.100	
TFTP Time Out(Secs)	10	
Firmware Filename	<input type="text" value="BW1253s.BRO.1.0.15.bin"/>	Save Cancel
Download Firmware From TFTP server		Download

Figure 121 – TFTP Firmware Upgrade setting

Click “Edit” button to specify the TFTP server IP address, time out interval and firmware filename and save the configuration then press “Download” button to download the firmware.



Please make sure the firmware is correct for BW1253s. Otherwise the upgrade will be failed.



Do not turn off the BW1253s during the firmware update process because the device could be damaged. It recommend to use the Ethernet connection (not wireless) for the firmware update process.

System | Location Settings

You can define the longitude and latitude for the device information or for the NMS to locate the device location.

Location Settings	
Name	Value
Longitude	
Latitude	

[Edit](#)

Figure 122 – location setting

Click edit to enter the Longitude and Latitude in digit and dot format.

Location Settings	
Name	Value
Longitude	121.524611
Latitude	25.040917

[Save](#) [Cancel](#)

Figure 123 – edit location[longitude/latitude]

Click **save** button to save it.

Chapter 4 – Reference Manual---AP-Router Mode

This chapter describes the configuration of the BW1253s which works in AP-Router mode using the Web Interface.



The BW1253s Web Interface in AP-Router mode is different from that in AP mode. To change your BW1253s to AP mode, please refer to **System | System Mode**. For the detailed configuration of BW1253s working in AP mode, please refer to: **Chapter 3 – Reference Manual---AP Mode**

The **web management** main menu consists of the following sub menus:

- **Status** – device status showing
- **Network** – device settings affecting networking
- **Wireless** – device settings related to the wireless part of the BW1253s
- **User** – device settings affecting the user interface
- **Services** – networking service settings of the BW1253s
- **System** – device system settings directly applicable to the BW1253s
- **Exit** – click exit and leave the web management then close your web-browser window.

Web Interface

The main **web management** menu is displayed at the top of the page after successfully logging into the system (see the figure below). From this menu all essential configuration pages are accessed.



Figure 124 – Main Configuration Management Menu

The **web management** menu has the following structure:

Status

- Device Status** – show the status related with the whole device
- Wireless Status** – show the status of the wireless
- Interface Statistics** – show the status of each network interface

Network

- Interface** – TCP/IP settings of BW1253s
- PPPoE** – Configure the PPPoE tunnel
- L2TP** – Configure the L2TP tunnel
- RADIUS Server** – specify the accounting/authentication RADIUS server which is used by 802.1x or WPA
- RADIUS Properties** – specify the settings of the RADIUS properties, includes NAS server ID, RADIUS Retries and other settings
- DNS** – define DNS server settings
- DHCP** – specify the settings of DHCP server or DHCP relay service
- DHCP Lease** – display the DHCP lease information
- Static Route** – define new static route

Attack Countermeasure – Anti-attack settings for protecting BW1253s

Link Integrity – specify the status and settings of link integrity feature.

Tr069 settings – configure the remote management through TR069 ACS server(BROWAN DMS server)

Wireless

Basic – specify the basic settings related with wireless part

Advance – specify the settings of multiple BSSID or Bridge

WEP – specify the WEP settings related with static WEP encryption

MAC ACL – MAC ACL settings for BW1253s

Load Balance – specify the load balance settings of BW1253s

User

Users – show the connected users' statistics list and log-out user function

Station Supervision – monitor station availability with ARP-pings settings

User ACL – define packet filter rules

Walled Garden – free web site list

WISP – add new WISP on the system

Start Page – define start page URL

Customized UAM – customized user login and logout page based by HTML page

Pages – configure and upload user pages

Upload – upload new internal user pages

HTTP Headers – define http headers encoding and language

Remote Authentication – define external Web Application Server (WAS) to intercept/take part in the user authentication process

Services

Telnet – Telnet/SSH service

SNMP – SNMP service

NTP – NTP settings of BW1253s

Time – manually set time

Watchdog – Enable the S/W or H/W watchdog of BW1253s

System

Administrator – set access permission to your BW1253s

System Log – check the system log locally or specify address where to send system log file

System Mode – specify whether the BW1253s works in AP mode or in AP router mode

System Info – specify some device related information for BW1253s

Configuration – system configuration utilities, including Backup/Upload configuration

Reset & Reboot – reboot device and restore systems to factory default

Local Upgrade – upgrade firmware from local PC

TFTP Upgrade – upgrade firmware from tftp server

Location settings – define AP location(Longitude/Latitude)

In the following sections, short references for all menu items are presented.

Status

Status | Device Status

The **Device Status** page shows important information of system status and network configuration for the BW1253s.

System	
System Mode	AP-Router
System Version	BW1253s.BRO.1.0.14
Config Version	BW1253s.BRO.1.0.14
Up Time	0 day(s) 01:00
System Time	1970/01/01/ 01:00
WLAN1 MAC	00:16:16:28:80:A0
Free System Memory	22,516 K bytes
Total System Memory	61,784 K bytes

Network	
WAN Mode	static-IP
WAN MAC	00:16:16:28:80:A2
WAN IP	192.168.21.162
WAN Mask	255.255.255.0
Gateway	192.168.21.1

Figure 125 – Device Status

System Mode – display the BW1253s works in AP mode or AP-Router mode

System Version – display the current version of the firmware loaded to the AP



This is important information for support requests and for preparing firmware upgrading

Config version – display current configure version

Up Time – indicate the time, expressed in days, hours and minutes since the system was last rebooted

System Time – show the current time of the BW1253s

WLAN1 MAC – show the MAC addresses of the wireless interfaces of the BW1253s

Free System Memory – indicate the memory currently available in the BW1253s

Total System Memory – indicate the total memory in the BW1253s

WAN Mode – indicate static IP or DHCP client is used for BW1253s WAN IP address

WAN IP – show the WAN IP address of BW1253s

WAN Mask – show the WAN Network Mask of BW1253s

Gateway – show the default gateway of BW1253s

Status | Wireless Status

The *wireless status* shows the information related with BW1253s wireless interfaces.

Radio1	
Channel	Current Frequency:2.462 GHz (Channel 11)
Domain	FCC
Mode	AP
Band	2.4GHz(11ng HT20)
Total Connected Clients	0
TxPower	14dBm
MAC ACL	disabled
SSID Number	1

Figure 126 – Wireless Status

Radio1 – show the wireless interface.

Channel – indicate which channel is in use.

Domain – indicate regulatory domain set on the BW1253s.[The country code selection is for non US models only]

Mode – AP or Bridge mode is be used for this wireless interface

Band – specify which band is in use for wireless interface

Total Connected Clients – indicate number of the currently connected clients to your BW1253s

Tx Power – indicate radio transmit power of the BW1253s

MAC ACL – indicate the status of MAC ACL feature on BW1253s

SSID Number – indicate current number of enabled SSID on BW1253s

Status | Interface Statistics

The *Interface Statistics* shows each network interface status, including Input / Output bytes, packets or error.

Interface Statistics						
Interface Name	Input Bytes(KB)	Input Packets	Input Errors	Output Bytes(KB)	Output Packets	Output Errors
eth1	913	12399	0	323	595	0
Refresh						

Figure 127 – Interface Statistics

Interface Name – show the name of each network interface, where ixp0 is related to LAN interface, wlan1_x is related to wireless sub-interface.

Input Bytes (KB) – show the total number of bytes received on the network interface. The bytes number is displayed in KB.

Input Packets – show the packets number received on the network interface.

Input Errors – show the packets number which contain errors preventing them from being received correctly.

Output Bytes (KB) – show the total number of bytes transmitted out of the network interface. The bytes number is displayed in KB.

Output Packets – show the packets number transmitted out of the network interface.

Output Errors – show the packets number which contain errors preventing them from being transmitted out correctly.

Refresh – get the updated network interface information.

Network

Network | Interface

The AP-Router contains two kinds of network interfaces: eth1 is worked as wide area network (WAN) interface for Access Points; each BSS interface is worked as local area network (LAN) interface which bridge into the br0 interface. The WAN port connects to the Internet or the service provider's backbone network. Each BSS can be looked as a virtual AP, wlan1_0 is the virtual AP for wireless network.

All these interfaces are listed in the **Network Interfaces** page. All network interfaces available in the AP-Router are shown in the following table:

Network Interfaces									
Interface	Status	Type	IP Address	Netmask	Gateway	NAT	Web Auth	Action	
br0	enabled	LAN	192.168.3.1	255.255.255.0	eth1	enabled	enabled	Edit	
eth1	enabled	WAN	192.168.21.162	255.255.255.0	*192.168.21.1	---	---	Edit	
You may check the 'Static Route' settings, when modify interface settings!!! Or some route settings will be invalid.									

Figure 128 – Network Interface Table

To change network interface configuration properties click the **Edit** button in the **Action** column. The **status** can be changed now:

Network Interfaces									
Interface	Status	Type	IP Address	Netmask	Gateway	NAT	Web Auth	Action	
br0	<input type="button" value="enabled"/>	LAN	192.168.3.1	255.255.255.0	eth1	<input type="button" value="enabled"/>	<input type="button" value="enabled"/>	Continue	Cancel
eth1	enabled	WAN	192.168.21.162	255.255.255.0	*192.168.21.1	---	---		
You may check the 'Static Route' settings, when modify interface settings!!! Or some route settings will be invalid.									

Figure 129 – Edit Network Interfaces Settings - 1

Interface – standard interface name. This name cannot be edited

Status – select the status of interface [enabled/disabled]



Do not disable the interface through which you are connected to the AP Router. Disabling such interface will lose your connection to the device.



The interface eth1 can not be disabled.

Type – network type cannot be changed. There are two possible networking types:

LAN – interface is used as local area network (LAN) gateway, and is connected to a LAN

WAN – interface is used to access the ISP network

NAT – select enable/disable the NAT service of current interface. If enabled, users can access the Internet under its network gateway address [enabled/disabled]

Web Auth – select enable/disable the Web Login Authentication of current interface. With disabled authentication, the user from his LAN gets access to the Internet without any authentication. If enabled, authentication for Internet access is required for all users [enabled/disabled]

Change **status** or leave in the default state if no editing is necessary and click the **Continue** button. Then the following parameters can be changed:

Network Interfaces									
Interface	Status	Type	IP Address	Netmask	Gateway	NAT	Web Auth	Action	
eth1	enabled	WAN	192.168.2.2	255.255.255.0	*192.168.2.1	---	---	<input type="button" value="Save"/>	<input type="button" value="Cancel"/>
br0	enabled	LAN	<input type="text" value="192.168.3.1"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="eth1"/>	enabled	enabled	<input type="button" value="Save"/>	<input type="button" value="Cancel"/>
You may check the 'Static Route' settings, when modify interface settings!!! Or some route settings will be invalid.									

Figure 130 –Edit Interface Configuration Settings - 2

IP Address – specify new interface IP address [dots and digits]



Under ap-router mode, IP address of each interface should be configured different subnet; otherwise, you will receive an error message.

Netmask – specify the subnet mask [[0-255].[0-255].[0-255].[0-255]]. These numbers are a binary mask of the IP address, which defines IP address order and the number of IP addresses in the subnet

Gateway – interface gateway. For LAN type interfaces, the gateway is WAN interface. The gateway of the WAN interface is usually the gateway router of the ISP or other WAN network [Default gateway is marked with '*']

Save – save the entered values.

Cancel – restore all previous values.

Network Interfaces									
Interface	Status	Type	IP Address	Netmask	Gateway	NAT	Web Auth	Action	
eth1	enabled	WAN	192.168.2.2	255.255.255.0	*192.168.2.1	---	---	<input type="button" value="Edit"/>	
br0	enabled	LAN	192.168.3.1	255.255.255.0	eth1	enabled	enabled	<input type="button" value="Edit"/>	
You may check the 'Static Route' settings, when modify interface settings!!! Or some route settings will be invalid.									

Figure 131 – Apply or Discard Interface Configuration Changes

Apply Changes – save all changes in the **interface** table at once.

Discard Changes – restore all previous values.

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Network Interfaces									
Interface	Status	Type	IP Address	Netmask	Gateway	NAT	Web Auth	Action	
eth1	enabled	WAN	192.168.2.2	255.255.255.0	*192.168.2.1	---	---	Edit	
br0	enabled	LAN	192.168.3.1	255.255.255.0	eth1	enabled	enabled	Edit	
You may check the 'Static Route' settings, when modify interface settings!!! Or some route settings will be invalid.									

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 132 – Reboot Server

Reboot – click the button to restart the server and apply the changes.

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
---	---

Network | PPPoE

The Point-to-Point Protocol over Ethernet(PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. It is use mainly for DSL service.

Click Edit button to enable or disable the service.

PPPoE	
Name	Status
Status	Disabled
Edit	

Figure 133 – PPPoE service

Name – service name

Status – change status for this service.[disable/enable]

PPPoE	
Name	Status
Status	Disabled
Save Cancel	

Figure 134 – change PPPoE service

Enable the PPPoE service.

Username – enter the authorized user to connect to the server [text string, can not be empty].

	The same username should be configured on the PPPoE server.
---	---

Password – the password of the user. [text string, can not be empty]

PPPoE	
Name	Status
Status	Enabled
Username	pppoe_user
Password	pppoe_passwd

Save **Cancel**

Figure 135 – edit PPPoE service



Default WAN gateway specified in **Network | Interface** page will not be used, because all Internet traffic will be sent/received via the specified PPPoE server (tunnel).

Click **Save** and **Apply Changes** button to take effect the changes.

PPPoE	
Name	Status
Status	Enabled
Username	pppoe_user
Password	pppoe_passwd

Edit

Apply Changes **Discard Changes**

Figure 136 – apply changes

Reboot – click the button to restart the AP and apply all the changes.

PPPoE	
Name	Status
Status	Enabled
Username	pppoe_user
Password	pppoe_passwd

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 137 – reboot and take effect all changes



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Network | L2TP

Layer 2 Tunneling Protocol(L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

Click Edit button to enable or disable the service.

L2TP	
Name	Status
Status	Disabled
Edit	

Figure 138 – L2TP services

Name – service name

Status – change status for this service.[disable/enable]

Server IP – enter the server IP address. [in digits and dots notation, e.g. 192.168.2.2]

Username – enter the user name.

Password – password for the authorized user.

Timeout – in case of connection fail, the interval to re-connect to the server.

L2TP	
Name	Status
Status	Enabled <input type="button" value="▼"/>
Server IP	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Timeout	Redial Period <input type="text"/> 15 Second
Save Cancel	

Figure 139 – edit L2TP services

Click **Save** button and **Apply Changes** button to save the change or **discard changes** button to discard the change

L2TP	
Name	Status
Status	Enabled
Server IP	192.168.21.165
Username	test
Password	test
Timeout	Redial Period 15 Second
Edit	
Apply Changes Discard Changes	

Figure 140 – save the changes

Reboot – click the button to restart the AP and apply all the changes.

L2TP	
Name	Status
Status	Enabled
Server IP	192.168.21.165
Username	test
Password	test
Timeout	Redial Period 15 Second

Edit**Reboot**

System needs to be restarted to make the new configurations take effect.

Figure 141 – reboot and take effect the changes



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Network | RADIUS Server



Up to **32** different RADIUS servers can be configured in the **RADIUS servers** menu.

By default, one **RADIUS** server is specified for the system:

RADIUS Server					
Name	Type	IP Address	Port	Secret	Action
DEFAULT (default)	Authentication	0.0.0.0	1812	secret	Details Edit Delete
	Accounting	0.0.0.0	1813	secret	
Add					

Figure 142 – RADIUS Servers Settings

Details – show the detail information of this **RADIUS Server** profile

Edit – edit the selected **RADIUS Server** entry you want to configure

Delete – delete the selected **RADIUS Server** entry. The last entry can not be deleted

Add – add new RADIUS server.

Click **Details**, a similar page will be appeared as below:

RADIUS Server	
Description	Value
Name (default)	DEFAULT
Authentication IP	192.168.123.200
Authentication Port	1812
Authentication Secret	secret
Accounting IP	192.168.123.201
Accounting Port	1813
Accounting Secret	secret
User Password Md5sum Secret	disabled

[Back](#) [Edit](#)

Figure 143 – Detail for Radius Server profile

Name – the new RADIUS server name which is used for selecting RADIUS server



If a “(default)” appears on the right side of the **Name** entry, it means this RADIUS server profile is the default profile.

Authentication IP – show the IP address of Authentication RADIUS server

Authentication Port – show the network port used to communicate with the Authentication RADIUS server

Authentication Secret – show the shared secret string that is used to make sure the integrity of data frames used for the Authentication RADIUS server

Accounting IP – show the IP address of Accounting RADIUS server



If the Accounting IP address is 0.0.0.0, it means that the Accounting service is disabled.

Accounting Port – show the network port used to communicate with the Accounting RADIUS server

Accounting Secret – show the shared secret string that is used to make sure the integrity of data frames used for the Accounting RADIUS server

User Password Md5sum Secret – show whether user input password is calculated md5-sum before pass to RADIUS server or not.

Back – back to the **RADIUS Server** main page

Edit – edit the selected **RADIUS Server** profile

Click **Edit** or click **Add / Edit** button in the main page to configure RADIUS server settings.

RADIUS Server	
Description	Value
Name	<input type="text" value="DEFAULT"/>
Default	<input checked="" type="checkbox"/>
Authentication IP	<input type="text" value="192.168.123.100"/>
Authentication Port	<input type="text" value="1812"/>
Authentication Secret	<input type="text" value="secret"/>
Accounting IP	<input type="text" value="192.168.123.200"/>
Accounting Port	<input type="text" value="1813"/>
Accounting Secret	<input type="text" value="secret"/>
User Password Md5sum Secret	<input type="text" value="disabled"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 144 – Edit the RADIUS Server's profile

RADIUS Server	
Description	Value
Name	<input type="text"/>
Default	<input type="checkbox"/>
Authentication IP	<input type="text"/>
Authentication Port	<input type="text"/>
Authentication Secret	<input type="text"/>
Accounting IP	<input type="text"/>
Accounting Port	<input type="text"/>
Accounting Secret	<input type="text"/>
User Password Md5sum Secret	<input type="text" value="disabled"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 145 – Add a new RADIUS Server's profile

Name – specify the new RADIUS server name which is used for selecting RADIUS server

Default – specify this RADIUS profile as default or not. When selected, the profile will be used as default

Authentication IP – specify the IP address of Authentication RADIUS server [dots and digits]

Authentication Port – specify the network port used to communicate with the Authentication RADIUS server [1-65535]

Authentication Secret – shared secret string that is used to make sure the integrity of data frames used for the Authentication RADIUS server

Accounting IP – specify the IP address of Accounting RADIUS server [dots and digits]

Accounting Port –specify the network port used to communicate with the Accounting RADIUS server [1-65535]

Accounting Secret – shared secret string that is used to make sure the integrity of data frames used for the Accounting RADIUS server



The default port value for authentication is 1812.
The default port value for accounting is 1813.
The port specified here must be the same with the one on the RADIUS server.

User Password Md5sum Secret – if enabled, user input password will be calculated md5-sum before pass to RADIUS server for more security [enabled/disabled]



This setting needs RADIUS server do relevant configurations.

Save –save the entered values

Cancel – restore all previous values

After adding a new RADIUS server or editing an existing one, a page appears similar to the following:

RADIUS Server					
Name	Type	IP Address	Port	Secret	Action
DEFAULT (default)	Authentication	192.168.123.100	1812	secret	Details Edit Delete
	Accounting	192.168.123.200	1813	secret	
Add					
Apply Changes			Discard Changes		

Figure 146 – Apply or Discard RADIUS Server Changes

Details – show the detail information of this **RADIUS Server** profile

Edit – edit the selected **RADIUS Server** entry you want to configure

Delete – delete the selected **RADIUS Server** entry. The last entry can not be deleted

Add – add new RADIUS server.

Apply Changes – to save all changes at once.

Discard Changes – restore all previous values.

Click **Apply Changes** to apply all the changes. Then the follow similar page will appear:

RADIUS Server					
Name	Type	IP Address	Port	Secret	Action
DEFAULT (default)	Authentication	192.168.123.100	1812	secret	Details Edit Delete
	Accounting	192.168.123.200	1813	secret	
Add					

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 147 – Reboot Server

Reboot – restart the access point to make applied changes work.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Network | RADIUS Properties

General **RADIUS** settings are configured using the **RADIUS Properties** menu under the **network**:

RADIUS Properties		
Setting	Value	Action
RADIUS Retries	5	Edit
RADIUS Timeout (seconds)	2	Edit
NAS Server ID		Edit
User Session Timeout (seconds)	72000	Edit
User Accounting Update Interval (seconds)	600	Edit
User Accounting Update Retry (seconds)	60	Edit
User Idle Timeout (seconds)	900	Edit
Bandwidth Up (ex. 100000, 10kbps, 10m)	512 Kbps	Edit
Bandwidth Down (ex. 100000, 10kbps, 10m)	512 Kbps	Edit

Figure 148 – RADIUS Properties settings

RADIUS Retries – retry count of sending RADIUS packets before giving up [0-99]

RADIUS Timeout (seconds) – maximum amount of time before retrying RADIUS packets [1-999]

NAS Server ID – name of the RADIUS client

User Session Timeout (seconds) – amount of time from the user side (no network carrier) before closing the connect [1-999999999]

User Accounting Update Interval (Seconds) – period after which server should update accounting information [60-999999999]

User Accounting Update Retry (seconds) – retry time period in which server should try to update accounting information before giving up [60-999999999]

User Idle Timeout (seconds) – amount of user inactivity time, before automatically disconnecting user from the network [1-999999999]

Bandwidth Up – maximum bandwidth up at which corresponding user is allowed to transmit [bps]

Bandwidth Down – maximum bandwidth down at which corresponding user is allowed to receive [bps]

Each setting in this table can be edited. Select **RADIUS** setting you need to update, click the **edit** next to the selected setting and change the value:

RADIUS Properties		
Setting	Value	Action
RADIUS Retries	5	
RADIUS Timeout (seconds)	2	
NAS Server ID		
User Session Timeout (seconds)	72000	
User Accounting Update Interval (seconds)	600	
User Accounting Update Retry (seconds)	60	
User Idle Timeout (seconds)	900	
Bandwidth Up (ex. 100000, 10kbps, 10m)	99 Mbps	Save Cancel
Bandwidth Down (ex. 100000, 10kbps, 10m)	512 Kbps	

Figure 149 – edit RADIUS properties

Use the **save** button to save an entered value. Now select another **RADIUS** property to edit, or **Apply Changes** and restart your AP if the configuration is finished:

RADIUS Properties		
Setting	Value	Action
RADIUS Retries	5	Edit
RADIUS Timeout (seconds)	2	Edit
NAS Server ID		Edit
User Session Timeout (seconds)	72000	Edit
User Accounting Update Interval (seconds)	600	Edit
User Accounting Update Retry (seconds)	60	Edit
User Idle Timeout (seconds)	900	Edit
Bandwidth Up (ex. 100000, 10kbps, 10m)	99 Mbps	Edit
Bandwidth Down (ex. 100000, 10kbps, 10m)	512 Kbps	Edit

[Apply Changes](#) [Discard Changes](#)

Figure 150 – apply change RADIUS properties

Apply Changes – click if **RADIUS Properties** configuration is finished

Discard Changes – restore all previous values

Network | DNS

DNS (Domain Name Service) service allows BW1253s subscribers to enter URLs instead of IP addresses into their browser to reach the desired web site. You can enter the **DNS** server settings under the **Network | DNS** menu. The DNS server setting s table is displayed:

DNS		
Type	IP Address	Action
primary	0.0.0.0	Edit
secondary	0.0.0.0	Edit

Figure 151 – DNS Settings

You can enter the **primary** and **secondary DNS** servers' settings by click the **edit** button in the **action** column and type in the **DNS** server's IP address:

DNS		
Type	IP Address	Action
primary	202.96.209.5	Save Cancel
secondary	0.0.0.0	

Figure 152 – Edit DNS Settings

IP Address – enter the primary or secondary DNS server's IP address [dots and digits]

Change status or leave in the default state if no editing is necessary and click the **Save** button.

DNS		
Type	IP Address	Action
primary	202.96.209.5	Edit
secondary	202.96.209.13	Edit

Apply Changes **Discard Changes**

Figure 153 – Apply or Discard DNS server Settings

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

DNS		
Type	IP Address	Action
primary	202.96.209.5	Edit
secondary	202.96.209.13	Edit

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 154 – Reboot information

Reboot – click the button to restart the server and apply the changes.

i	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
----------	---

Network | DHCP

In AP Router mode, the BW1253s can act as a **DHCP Server**. The **DHCP** (Dynamic Host Configuration Protocol) service is supported on the LAN interfaces. This service enables clients on the LAN to request configuration information, such as an IP address, from a server. This service can be viewed in the following table:

DHCP Settings	
Name	Value
Mode	Disabled
Interface Name :	bx0

Figure 155 – DHCP Configuration

Interface Name – select which LAN interface to be configured.[only br0 interface in BW1253s]

Select the interface, and then click **Edit** button, a similar screen will appear as below:

DHCP Settings	
Name	Value
Interface Name	br0
Mode	Disabled
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 156 – Set DHCP Mode

Mode – DHCP service mode [DHCP server/Disabled]

When **DHCP Server** is selected, a page appears similar to the following:

DHCP Settings	
Name	Value
Interface Name	br0
Mode	DHCP Server
IP Address from	192.168.3.2
IP Address to	192.168.3.254
Netmask	255.255.255.0
Gateway	192.168.3.1
WINS Address	0.0.0.0
Lease time(seconds)	300
Domain	
DNS Address	8.8.8.8
DNS Secondary Address	168.95.1.1
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 157 – DHCP Server Settings

IP Address from/IP Address to – specify the IP address range supported for the **DHCP** service [mandatory fields]

Netmask – show the subnet mask of current interface

Gateway – show the interface gateway

WINS (Windows Internet Naming Service) Address – specify service IP address if it is available on the network [dots and digits]

Lease Time – specify the IP address renewal in seconds [1-1000000]

Domain – specify DHCP domain name [optional, 1-128 sting]

DNS Address – specify the DNS server's IP address [digits and dots]

DNS Secondary Address – specify the secondary DNS server's IP address [digits and dots]

	The DNS address is same with the setting in the Network DNS menu.
---	--

Change status or leave in the default state if no editing is necessary and click the **Save** button.

DHCP Settings	
Name	Value
Mode	DHCP Server
Interface Name :	bx0
IP Address from	192.168.3.2
IP Address to	192.168.3.254
Netmask	255.255.255.0
Gateway	192.168.3.1
WINS Address	0.0.0.0
lease time(seconds)	300
Domain	
DNS Address	8.8.8.8
DNS Secondary Address	168.95.1.1
	Edit

Figure 158 – Apply or Discard DHCP server Settings



The DHCP server settings will be automatically adjusted to match the network interface settings.

If all of the DHCP settings are correct, click **Apply Changes**, request for reboot server appears:

DHCP Settings	
Name	Value
Mode	DHCP Server
Interface Name :	bx0
IP Address from	192.168.3.2
IP Address to	192.168.3.254
Netmask	255.255.255.0
Gateway	192.168.3.1
WINS Address	0.0.0.0
lease time(seconds)	300
Domain	
DNS Address	8.8.8.8
DNS Secondary Address	168.95.1.1
	Edit

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 159 – Reboot information

Reboot – click the button to restart the server and apply the changes.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Network | DHCP Lease

This page display the DHCP lease information of wireless client which connect to the AP when DHCP server enable.

DHCP Lease			
Host Name	Mac Address	IP Address	Expires in
ggyy-40fbc8fbab	00:13:02:01:14:5a	192.168.2.4	9 d 23 h 59 m 24 s
<input type="button" value="Refresh"/>			

Figure 160 – DHCP lease information

Host Name – the host name of wireless client which associate to the access point.

Mac Address –the MAC address of wireless client which associate to the access point.

IP Address –the IP address of wireless client which associate to the access point.

Expires in – expire time of the wireless client which associate to the access point.

Network | Static Route

Opening the **Static Route Settings** page you will find a list of all pre-configured routes, each consisting of the related interface, the destination IP address, the gateway and the subnet mask.

The **Routing Table** content shows how the router will handle data packets received on an interface with specific destination addresses. By default no static routes are defined on the system:

Static Route					
Interface	Status	Gateway	Target IP Address	Netmask	Action
No routes are defined on system.					
<input type="button" value="Add"/>					

Figure 161 – Static Route Page

A routing rule is defined by the **target** subnet (target IP address and subnet mask), **interface** and/or **gateway** where to route the target traffic. A data packet that is directed to the **target** network is routed to the specified AC interface or to another gateway router. To add a new static route for the system, click the **new** button under the **action** column and specify the following parameters:

Static Route					
Interface	Status	Gateway	Target IP Address	Netmask	Action
br0	enabled	192.168.123.8	192.168.234.0	255.255.255.0	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Figure 162 – Add New Route

Interface – choose device interface for the route

Status – set new static route status: [enabled/disabled]

Gateway – enter the gateway address for the route. 0.0.0.0 stands for the default gateway of the selected interface [IP address]. The gateway is in the same subnet with selected interface.

Target IP address – enter host IP or network address to be routed to [IP address]

	In this case the class C network(192.168.234.x) is reachable.
---	---

Netmask – enter the target network netmask [dots and digits]

Save – save the new route

Cancel – restore all previous values

Static Route					
Interface	Status	Gateway	Target IP Address	Netmask	Action
bx0	enabled	192.168.123.8	192.168.234.0	255.255.255.0	Edit Delete
Add					

Figure 163 – Save New Route

	Static route will take effect immediately after click save button.
---	--

Network | Attack Countermeasure

To protect BW1253s from outside attack, anti-attack polices can be set here based on network needs.

Attack Countermeasure					
Item	Status	Max Load	Duration(seconds)	Expire(seconds)	Action
Anti-DOS	Disabled	400 TCP links/s		300	Edit
Flow Control	Disabled	20480 Kbps	60	300	Edit

Figure 164– Attack Countermeasure settings

Anti-DOS

Status – Enable or disable anti-dos policy for BW1253s. This policy is for TCP DOS attack.

Max Load – The attack threshold. BW1253s think there is TCP DOS attack and do the countermeasure if one client's TCP links exceed this threshold.

Expire(seconds) – If one client is considered as DOS attacker, BW1253s kicks it out and doesn't let it connect again during the time that **Expire** set.

Flow Control

Status – Enable or disable traffic flow control policy for BW1253s.

Max Load – The attack throughput threshold.

Duration(seconds) – if traffic exceeds the value of **Max Load** during the whole time that **Duration** set, BW1253s think there is traffic flow attack and do the countermeasure.

Expire(seconds) – If one client is considered as traffic flow attacker, BW1253s kicks it out and doesn't let it connect again during the time that **Expire** set.

Network | Link Integrity

Specify Link Integrity feature's settings here. Enable Link Integrity, BW1253s will close wireless connections and kick out all the wireless clients when it detects that its Ethernet network cannot be accessed to the internet.

Link Integrity	
Name	Status
Status	Disabled
Edit	

Figure 165 – Link Integrity settings

Click **Edit** button to set the Link Integrity settings, the similar UI will be appeared as below:

Link Integrity	
Name	Status
Status	Enabled
Target IP1	0.0.0.0
Target IP2	0.0.0.0
Target IP3	0.0.0.0
Target IP4	0.0.0.0
Target IP5	0.0.0.0
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 166 – Edit Link Integrity settings

Status – Enable or disable the feature of Link Integrity

Target IP1 to Target IP5 – IP addresses for BW1253s detecting if its Ethernet interface can access network. The AP will ping every IP address 15 times in sequence. As long as one ping is success it will consider the network is reachable. If ping fail for all IP address specified it will consider Ethernet link fail and all associated wireless client will be logged out. The AP will continue to ping from first IP address. If ping success the wireless will be enable again and client can access the AP.

Save – save the entered values.

Cancel – restore all previous values.

Click **Save**, the similar apply changes UI will be appeared:

Link Integrity	
Name	Status
Status	Enabled
Target IP1	192.168.123.69
Target IP2	192.168.123.1
Target IP3	0.0.0.0
Target IP4	0.0.0.0
Target IP5	0.0.0.0
<input type="button" value="Edit"/>	
<input type="button" value="Apply Changes"/> <input type="button" value="Discard Changes"/>	

Figure 167 –Apply or Discard Link Integrity Settings

Apply Changes – save all changes in the **interface** table at once.

Discard Changes – restore all previous values.

	Maximum 5 target IP can be specified.
---	---------------------------------------

The BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Link Integrity	
Name	Status
Status	Enabled
Target IP1	192.168.123.69
Target IP2	192.168.123.1
Target IP3	0.0.0.0
Target IP4	0.0.0.0
Target IP5	0.0.0.0

Edit

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 168 – Reboot Server

Reboot – click the button to restart the server and apply the changes.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Network | Tr069 Settings

TR-069 is the Broadband Forum technical specification entitled CPE WAN Management Protocol(CWMP). It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment(CPE) and Auto Configuration Servers(ACS server). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. The protocol addressed the growing number of different internet access devices such as modems, routers, gateways, set-top-boxes, and VOIP-phones for the end users. The TR-069 standard was developed for automatic configuration of these devices with Auto Configuration Servers(ACS).

configure the remote management through TR069 ACS server(eg:BROWAN DMS server)

TR069 Settings	
Name	Status
Status	Disabled

Edit

Figure 169 – TR-069 settings

Click Edit button and the similar page will be appeared.

TR069 Settings

Name	Status
Status	Enabled
ACS URL	http://192.168.1.1:9090/dms/tr069
ACS UserName	tr069
ACS UserPassword	tr069passwd
Enable Periodic Inform	Enabled
Periodic Inform Interval	3600
Connection Request UserName	server
Connection Request Password	serverpasswd

Save **Cancel**

Figure 170 – edit TR-069 settings

Status – enable or disable TR-069 setting.[enable/disable]

ACS URL – enter the ACS server URL.

ACS UserName – the user name for AP register to ACS server.

ACS UserPassword – the password for AP register to ACS server.

Enable Periodic Inform – when AP registered to the ACS server, it will automatically send inform message such as S/N,OUI,manufacturer and product name to the ACS server through TR-069 protocol in a periodic time.

Periodic Inform Interval – the inform interval.[in seconds, the value is 720~4294967295]

Connection Request UserName – when the ACS pulling a task to AP/CPE such as firmware upgrade/downgrade, AP need the user name to verify the task sending from ACS server.

Connection Request Password –when the ACS pulling a task to AP/CPE such as firmware upgrade/downgrade, AP need the password to verify the task sending from ACS server.



Contact the ACS server administrator to get the user name and password for **Connection Request UserName** and **Connection Request Password** otherwise the AP will not accept the task pulling by ACS server.

After enter all field click **save** and **apply changes** button to take effect.

TR069 Settings

Name	Status
Status	Enabled
ACS URL	http://192.168.1.1:9090/dms/tr069
ACS UserName	tr069
ACS Password	tr069passwd
Enable Periodic Inform	Enable
Periodic Inform Interval	3600
Connection Request UserName	server
Connection Request Password	serverpasswd

Edit

Apply Changes **Discard Changes**

Figure 171 – save TR-069 settings

Reboot – click the button to restart the server and apply the changes.

TR069 Settings	
Name	Status
Status	Enabled
ACS URL	http://192.168.1.1:9090/dms/tr069
ACS UserName	tr069
ACS Password	tr069passwd
Enable Periodic Inform	Enable
Periodic Inform Interval	3600
Connection Request UserName	server
Connection Request Password	serverpasswd

System needs to be restarted to make the new configurations take effect.

Figure 172 – reboot device



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Wireless

Wireless | Basic

Use the **Wireless | Basic** menu to configure wireless settings such as regulatory domain, channel, band, and power, layer 2 isolation. Click the edit button on the setting you need to change:

	The country code selection is for non US models only																														
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">Basic Wireless Setting</th> </tr> <tr> <th>Radio :</th> <td>wlan1 <input type="button" value="▼"/></td> </tr> </thead> <tbody> <tr> <td>Name</td> <td>Value</td> </tr> <tr> <td>Mode</td> <td>AP</td> </tr> <tr> <td>Domain</td> <td>FCC</td> </tr> <tr> <td>Static Channel</td> <td>11</td> </tr> <tr> <td>Band</td> <td>2.4GHz(11ng HT20)</td> </tr> <tr> <td>TxPower</td> <td>14dBm</td> </tr> <tr> <td>RTS Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Fragment Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Beacon Interval</td> <td>100 ms</td> </tr> <tr> <td>DCA</td> <td>Disable</td> </tr> <tr> <td>Preamble</td> <td>auto</td> </tr> <tr> <td>Slot Time</td> <td>auto</td> </tr> <tr> <td>Action</td> <td><input type="button" value="Edit"/> <input type="button" value="Site Survey"/></td> </tr> </tbody> </table>		Basic Wireless Setting		Radio :	wlan1 <input type="button" value="▼"/>	Name	Value	Mode	AP	Domain	FCC	Static Channel	11	Band	2.4GHz(11ng HT20)	TxPower	14dBm	RTS Threshold	2347 bytes	Fragment Threshold	2347 bytes	Beacon Interval	100 ms	DCA	Disable	Preamble	auto	Slot Time	auto	Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>
Basic Wireless Setting																															
Radio :	wlan1 <input type="button" value="▼"/>																														
Name	Value																														
Mode	AP																														
Domain	FCC																														
Static Channel	11																														
Band	2.4GHz(11ng HT20)																														
TxPower	14dBm																														
RTS Threshold	2347 bytes																														
Fragment Threshold	2347 bytes																														
Beacon Interval	100 ms																														
DCA	Disable																														
Preamble	auto																														
Slot Time	auto																														
Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>																														

Figure 173 – Basic Wireless Settings with static channel selection

<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">Basic Wireless Setting</th> </tr> <tr> <th>Radio :</th> <td>wlan1 <input type="button" value="▼"/></td> </tr> </thead> <tbody> <tr> <td>Name</td> <td>Value</td> </tr> <tr> <td>Mode</td> <td>AP</td> </tr> <tr> <td>Domain</td> <td>FCC</td> </tr> <tr> <td>Auto Channel</td> <td>1</td> </tr> <tr> <td>Band</td> <td>2.4GHz(11ng HT20)</td> </tr> <tr> <td>TxPower</td> <td>4dBm</td> </tr> <tr> <td>RTS Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Fragment Threshold</td> <td>2347 bytes</td> </tr> <tr> <td>Beacon Interval</td> <td>100 ms</td> </tr> <tr> <td>DCA</td> <td>Enable</td> </tr> <tr> <td>DCA Threshold</td> <td>10 mins</td> </tr> <tr> <td>DCA optional channel</td> <td>1,2,3,4,5,6,7,8,9,10,11 channel</td> </tr> <tr> <td>Preamble</td> <td>auto</td> </tr> <tr> <td>Slot Time</td> <td>auto</td> </tr> <tr> <td>Action</td> <td><input type="button" value="Edit"/> <input type="button" value="Site Survey"/></td> </tr> </tbody> </table>		Basic Wireless Setting		Radio :	wlan1 <input type="button" value="▼"/>	Name	Value	Mode	AP	Domain	FCC	Auto Channel	1	Band	2.4GHz(11ng HT20)	TxPower	4dBm	RTS Threshold	2347 bytes	Fragment Threshold	2347 bytes	Beacon Interval	100 ms	DCA	Enable	DCA Threshold	10 mins	DCA optional channel	1,2,3,4,5,6,7,8,9,10,11 channel	Preamble	auto	Slot Time	auto	Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>
Basic Wireless Setting																																			
Radio :	wlan1 <input type="button" value="▼"/>																																		
Name	Value																																		
Mode	AP																																		
Domain	FCC																																		
Auto Channel	1																																		
Band	2.4GHz(11ng HT20)																																		
TxPower	4dBm																																		
RTS Threshold	2347 bytes																																		
Fragment Threshold	2347 bytes																																		
Beacon Interval	100 ms																																		
DCA	Enable																																		
DCA Threshold	10 mins																																		
DCA optional channel	1,2,3,4,5,6,7,8,9,10,11 channel																																		
Preamble	auto																																		
Slot Time	auto																																		
Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>																																		

Figure 174 – Basic Wireless Settings with auto channel selection(DCA)

Radio – specify which wireless interface of BW1253s is shown.(There is only one WLAN1 interface in BW1253s)

Mode – show the radio operation mode. (AP mode or Bridge mode)

Domain – show the regulatory domain.[The country code selection is for non US models only]

Static Channel / Auto Channel – show the channel that the access point will use to transmit and receive information



If DCA (Dynamic Channel Allocation) is enabled, this will show Auto Channel and its channel number is chosen in auto channel selection.
If use static channel selection, this will show Static Channel and its channel number.



DCA (Dynamic Channel Allocation) is useful feature to help choose the best channel automatically and reduce interference among many Access Points.

Band – show the working bands on which the radio is working.

Seven bands listed: 2.4GHz(11ng HT20) , 2.4GHz(11ng HT40plus), 2.4GHz(11ng HT40minus) , 5GHz(11a), 5GHz(11na HT20) , 5GHz(11na HT40plus), 5GHz(11na HT40minus) .

Tx Power – show the BW1253s transmission output power (without antenna gain) in dBm.

RTS Threshold –the AP sends Request to Send(RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send(CTS) frame to acknowledge the right to begin transmission. The default value is 2347.[recommend].

Fragment Threshold –It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the fragmentation threshold. Setting the fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended. The default value is 2347.[recommend]

Beacon Interval –the Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network.

DCA – Enable or Disable DCA service. DCA can help to choose the best working channel automatically. And static channel selection will be forbidden if DCA is enabled.

DCA(Dynamic Channel Allocation) solution automatically select the optimal operational frequency channel when power up and periodically monitors the environment and adjusts for the best operational frequency channel.

DCA threshold – specify the value (in minutes) of DCA threshold. This threshold is been used to judge if there is no wireless users connected during this time. And if yes, BW1253s will monitor the environment and adjust channel for the best operational one.



If wireless network environment is stable which means auto channel selection needn't do frequently, set a big value for DCA threshold to gain a stable wireless users' connection.
If wireless network environment changes continually, frequent auto channel selection is needed. So set a relative small value for DCA threshold to let channel change based on wireless environment.

	Wireless users' will be kicked off when DCA is processing (new operational frequency channel takes effect).
--	---

DCA optional channel – show the channels only in which auto channel selection (DCA) will be processed to reduce interference.

	Only when DCA is enabled, DCA threshold and DCA optional channel will be shown.
--	---

Preamble – if your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble.

Auto: using long preamble when there are clients not supporting short preamble connected , otherwise using short preamble. The default is Auto.[recommend]

Short: always using short preamble.

Long: always using long preamble.

Slot Time – show the slot time policy when working in 2.4GHz band.

Auto: using long slot time when there are clients not supporting short slot time connected in, otherwise using short slot time. The Switching between long and short slot time is automatic.

Short: always using short slot time.

Long: always using long slot time.

	To Maximize the compatibility with some 11b clients, set both Preamble and Slot Time to long.
--	---

Edit – edit the wireless basic settings

To change basic wireless setting properties click the **Edit** button in the **Action** column. The **status** can be changed now:

Basic Wireless Setting	
Name	Value
Radio Name	wlan1
Mode	AP
Domain	FCC
Channel	1
Band	2.4GHz(11ng HT20)
TxPower	14 dBm
RTS Threshold	2347 bytes [0..2347]
Fragment Threshold	2347 bytes [0..2347]
Beacon Interval	100 ms [1..65536]
DCA	<input type="checkbox"/> Enable
DCA Threshold	10 mins
DCA optional channel	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> all
Preamble	auto
Slot Time	auto
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 175 – Edit Basic Wireless Settings with static channel selection

Basic Wireless Setting	
Name	Value
Radio Name	wlan1
Mode	AP
Domain	FCC
Channel	1
Band	2.4GHz(11ng HT20)
TxPower	14 dBm
RTS Threshold	2347 bytes [0..2347]
Fragment Threshold	2347 bytes [0..2347]
Beacon Interval	100 ms [1..65536]
DCA	<input checked="" type="checkbox"/> Enable
DCA Threshold	10 mins
DCA optional channel	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> all
Preamble	auto
Slot Time	auto
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 176 – Edit Basic Wireless Settings with DCA enabled

Radio Name – specify wireless interface of BW1253s is shown

Mode – configure the radio operation mode.



In AP-Router mode, the radio only support AP mode for wireless client connection.

Domain – show the regulatory domain.[The country code selection is for non US models only]

Channel – select the channel that the access point will use to transmit and receive information. Channels list will vary depending on selected band. [2.4GHz or 5GHz]

Band – working bands on which your radios are working.

Seven bands listed: 2.4GHz(11ng HT20) , 2.4GHz(11ng HT40plus), 2.4GHz(11ng HT40minus) , 5GHz(11a), 5GHz(11na HT20) , 5GHz(11na HT40plus), 5GHz(11na HT40minus) .

TxPower – the BW1253s transmission output power in dBm.

RTS Threshold – the AP sends Request to Send(RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send(CTS) frame to acknowledge the right to begin transmission. The default value is 2347.[recommend]

Fragment Threshold – It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the fragmentation threshold. Setting the fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended. The default value is 2347.[recommend]

Beacon Interval – the Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network.

DCA – Enable or Disable DCA service. DCA can help to choose the best working channel automatically. And static channel selection will be forbidden if DCA is enabled.

DCA(Dynamic Channel Allocation) solution automatically select the optimal operational frequency channel when power up and periodically monitors the environment and adjusts for the best operational frequency channel.

DCA threshold – specify the value (in minutes) of DCA threshold. This threshold is been used to judge if there is no wireless users connected during this time. And if yes, BW1253s will monitor the environment and adjust channel for the best operational one.



If wireless network environment is stable which means auto channel selection needn't do frequently, set a big value for DCA threshold to gain a stable wireless users' connection.
If wireless network environment changes continually, frequent auto channel selection is needed. So set a relative small value for DCA threshold to let channel change based on wireless environment.



Wireless users' will be kicked off when DCA is processing (new operational frequency channel takes effect).

DCA optional channel – specify the channels only in which auto channel selection (DCA) will choose for reducing interference reference.



Only when DCA is enabled, **DCA threshold** and **DCA optional channel** will be shown.

Preamble – if your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble.

Auto: using long preamble when there are clients not supporting short preamble connected , otherwise using short preamble. The default is Auto.[recommend]

Short: always using short preamble.

Long: always using long preamble.

Slot Time – specify the slot time policy when working in 2.4GHz band.

Auto: using long slot time when there are clients not supporting short slot time connected in, otherwise using short slot time. The default is Auto.[recommend]

Short: always using short slot time.

Long: always using long slot time.



To Maximize the compatibility with some 11b clients, set both **Preamble** and **Slot Time** to long.

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Basic Wireless Setting	
Radio :	wlan1 <input type="button" value="▼"/>
Name	Value
Mode	AP
Domain	FCC
Static Channel	1
Band	2.4GHz(Mixed 11g)
Total Output Power (EIRP)	14dBm
Antenna Gain	2dBi
RTS Threshold	2347 bytes
Preamble	auto
Slot Time	auto
Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>

Figure 177 – Apply or Discard Basic Wireless Settings with Static Channel selection

Basic Wireless Setting	
Radio :	wlan1 <input type="button" value="▼"/>
Name	Value
Mode	AP
Domain	FCC
Auto Channel	auto
Band	2.4GHz(Mixed 11g)
Total Output Power (EIRP)	14dBm
Antenna Gain	2dBi
RTS Threshold	2347 bytes
DCA Threshold	10 mins
DCA optional channel	4,5,7 channel
Preamble	auto
Slot Time	auto
Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>

Figure 178 – Apply or Discard Basic Wireless Settings with DCA enabled

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Basic Wireless Setting	
Radio :	wlan1
Name	Value
Mode	AP
Domain	FCC
Auto Channel	1
Band	2.4GHz(Mixed 11g)
Total Output Power (EIRP)	14dBm
Antenna Gain	2dBi
RTS Threshold	2347 bytes
DCA Threshold	10 mins
DCA optional channel	4,5,7 channel
Preamble	auto
Slot Time	auto
Action	<input type="button" value="Edit"/> <input type="button" value="Site Survey"/>

System needs to be restarted to make the new configurations take effect.

Figure 179 – Reboot Server

Reboot – click the button to restart the server and apply the changes.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Wireless | Advanced

BW1253s supports **Multiple BSSID (MBSSID)** function. You can configure up to 16 BSSIDs on BW1253s and assign different configuration settings to each BSSID. For wireless users, they can think BW1253s as single AP with multi service supporting, including different security policy, different VLAN ID, different authentication etc. All the BSSIDs are active at the same time that means client devices can associate to the access point for specific service. Use the **Wireless | Advanced** menu to configure properties related to Multiple BSSID, including configure SSID, Hidden SSID, VLAN, and Security for each SSID.



Each BSSID can have its own SSID. In this case, Multiple BSSID is the same with Multiple ESSID. Wireless users can think BW1253s as multiple virtual APs, each supporting different service, and connects one SSID for the special services.

AP Mode

If you configure AP mode, the page will be shown as below in **Wireless | Advanced** menu.

Advance Wireless Setting						
Radio: wlan1		AP Mode				
Interface	SSID	Hidden	Security	Current Connect #	Action	
wlan1_0	BW1253-11g-gyy	Disabled	Disabled	0	Detail	Edit
						Delete
						New
Refresh						

Figure 180 – Advanced Wireless Setting (AP Mode)

Radio – specify wireless interface to be configured.[only one radio for BW1253s]

Mode – show the current operation mode of this radio (AP or Bridge)

Interface – display the interface which corresponding to the SSID. Each Interface maps to a BSSID

SSID – SSID name for wireless client searching and associating.

Hidden – show the status of Hidden SSID feature[disable/enable]

Security – show which security policy is used for this **MBSSID** entry

Current Connect # – show the number of current wireless clients associate to this MBSSID

New – create a new **MBSSID** entry

Detail – show the detail information of this **MBSSID** entry

Edit – edit the selected **MBSSID** entry you want to configure

Delete – delete the selected **MBSSID** entry. When in AP mode, you can not delete the last entry

Refresh – rescan the WEB page to get newer information

Clicking **New** or **Edit** button to configure the SSID parameters. Describe as below:

Advance Wireless Setting			
Radio	wlan1		
Interface	wlan1_0		
Mode	AP		
SSID	BW1253-11g (Printable ASCII Characters)		
	<input type="checkbox"/> Need Hidden SSID		
	<input checked="" type="checkbox"/> SSID status		
	<input type="checkbox"/> Pureg		
	<input type="checkbox"/> Only 11n		
	<input type="checkbox"/> Disassociation low MCS		
Max Station Number	(1~127)		
Layer 2 Isolation	<input type="checkbox"/> Enable Intra-BSS Layer 2 Isolation (Inter-BSS Layer 2 Isolation can be configed in Wireless -> Layer 2 Isolation page.)		
Bandwidth	<input type="checkbox"/> Enable bandwidth	Download bandwidth	(Mbps)
		Upload bandwidth	(Mbps)

Figure 181 – BSSID Setting -1

Radio – show the wireless interface is being configured.

Interface – show the current sub-interface.

Mode – show the operation mode of current radio.

SSID – a unique ID for your wireless network. It is case sensitive and must not exceed 32 characters. The SSID is important for clients when connecting to the access point.

Need Hidden SSID – when enabled, the SSID of this Interface is invisible in the networks list while scanning the available networks for wireless client (SSID is not broadcasted with its Beacons). When disabled, the AP's SSID is visible in the available network list [enabled/disabled]. By default the Hidden SSID is disabled

SSID status – activated or deactivated the SSID. The default is activated SSID[check box].

Pureg – enable/disable 11b client connection. [check box] to enable the function.

Only 11n –only 802.11n client can connected to the SSID.

Max Station Number – define maximum number of associated wireless client to this SSID.Leave space means unlimited or fill in the value.[1~127 client]

Layer 2 Isolation – Specify the layer 2 isolation policy.

Enable Intra-BSS Layer 2 Isolation – when enabled, the clients that connect in this same BSS can't visit each other. By default the intra-BSS layer 2 isolation is disabled.

	Intra-BSS layer2 isolation – which enable or disable client isolation under same SSID. Inter-BSS layer2 isolation – which enable or disable client isolation between different SSID.
	Please go to Wireless Layer 2 Isolation(Inter-BSS) menu to configure inter-BSS layer 2 Isolation. Full layer 2 isolation need to set both intra-BSS and inter-BSS layer 2 isolation in the AP mode.

Bandwidth – enable/disable upstream/downstream bandwidth control per SSID.

Download bandwidth – specified the maximum downstream in Mbps controlled by the SSID.

Upload bandwidth – specify the maximum upstream in Mbps controlled by the SSID.

VLAN	<input type="checkbox"/> Enable VLAN		
		VLAN ID	<input type="text" value="1~4094"/>
		802.1p Tag	<input type="text" value="Best Effort(0)"/> (Class of Service)
Interface Priority		<input type="text" value="Best Effort(0)"/> (Class of Service)	
WMM	<input checked="" type="checkbox"/> Enable WMM		
ESS in Tunnel	<input type="radio"/> Enabled		
	<input type="radio"/> Disabled	Remote Server IP	<input type="text"/>

Figure 182 – Multiple BSSID Setting -2

VLAN – specify VLAN policy

Enable VLAN – when enabled, the outgoing packets from this SSID device will be tagged with VLAN ID and 802.1p tag.

VLAN ID – configure VLAN ID for each Multiple SSID devices. Valid numbers are from 1 to 4094

802.1p Tag – configure 802.1p Tag for remote APC's or Router's QoS uses. Eight levels selective, Background(1), Spare(2), Best Effort(0), Excellent Effort(3), Controlled Load(4), Interactive Video(5), Interactive Voice(6), Network Control(7)



VLAN ID and 802.1p tag must cooperate with remote Router or APC.

Interface priority – specify the traffic priority for this SSID interface, which is implemented according to 802.11e EDCA and makes sure the wireless downlink QoS. This priority is based on SSID, which means different BSSID can have different traffic priority and the traffic of the same SSID has the same priority



This traffic priority only makes sure the priority of downlink (from AP to wireless client).
8 levels priorities are supplied. 1, 2, 0, 3, 4, 5, 6, 7 is from lowest priority to highest priority.
And if no special QoS is needed, leave **priority** to default (0). 0 means Best Effort priority.

WMM – BW1253s support WMM wireless clients and implement WMM QoS with the WMM clients. [enable]

ESS in Tunnel – Settings for ESS in tunnel. When enabled, BW1253s setup tunnel with remote AC for passing through layer3 network.

Remote Server IP – IP address of remote AC product that setup tunnel with BW1253s

Security			
<input type="radio"/> WEP(Wired Equivalent Privacy)			
	WEP KeyIndex	1	
<input type="radio"/> 802.1x	RADIUS Server Profile	DEFAULT	
	Dynamic WEP Encryption	<input checked="" type="radio"/> Disabled <input type="radio"/> 64 bits <input type="radio"/> 128 bits	
		<input type="checkbox"/> Pass Through	
<input type="radio"/> WPA	RADIUS Server Profile	DEFAULT	
	Algorithm	TKIP	
	Group Key Rekey Interval		Minutes
<input type="radio"/> WPA2	RADIUS Server Profile	DEFAULT	
	Algorithm	TKIP	
	Group Key Rekey Interval		Minutes
<input type="radio"/> WPA2 MIXED	RADIUS Server Profile	DEFAULT	
	Algorithm	TKIP/AES	
	Group Key Rekey Interval		Minutes

Figure 183 – Multiple BSSID Setting – 3

Security – specify the security policy

WEP – Wired Equivalent Privacy(WEP) is a security algorithm for IEEE 802.11 wireless networks.

WEP Key Index – select the default key Index to make it the Default key and encrypt the data before being transmitted. All stations, including this MSSID Entry, always transmit data encrypted using this Default Key. The key number (1, 2, 3, 4) is also transmitted. The receiving station will use the key number to determine which key to use for decryption. If the key value does not match with the transmitting station, the decryption will fail. The key value is set in **Wireless | WEP** web page

802.1x – when selected, the MSSID entry will be configured as an 802.1x authenticator. It supports multiple authentication types based on EAP (Extensible Authentication Protocol) like EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM. The privacy will be configured as dynamic WEP

RADIUS Server Profile – select your RADIUS server profile



Please go to **Network | RADIUS Server** menu to configure your RADIUS server profile or add a new profile, and please refer to **Network | RADIUS Server** for its configuration.

Dynamic WEP Encryption – select whether using the dynamic 64-bits encryption, 128-bits encryption or without encryption

Pass Through – when enabled, client can access network whether it passed 802.1x authentication or not



Only when 802.1x enabled and dynamic key disabled this option can be enabled.

WPA – Wi-Fi Protected Access, When selected, the encrypt method will be WPA with RADIUS Server

WPA2 – when selected, the security policy will be WPA2 with RADIUS server. In this mode, WPA client is not permitted to connect

WPA2 MIXED – when selected, WPA2 client and WPA client are all permitted to connect

RADIUS Server Profile – select your RADIUS server profile



Please go to **Network | RADIUS Server** menu to configure your RADIUS server profile or add a new profile, and please refer to **Network | RADIUS Server** for its configuration.

Algorithm – choose WPA algorithm (TKIP, AES)

Group Key Rekey Interval – specify amount of minutes and WPA automatically will generate a new Group Key

<input type="radio"/> WPA-PSK		
	Use Pre-Shared Key	<input type="text"/>
	Algorithm	TKIP <input type="button" value="▼"/>
	Group Key Rekey Interval	<input type="text"/> Minutes
<input type="radio"/> WPA2-PSK		
	Use Pre-Shared Key	<input type="text"/>
	Algorithm	TKIP <input type="button" value="▼"/>
	Group Key Rekey Interval	<input type="text"/> Minutes
<input type="radio"/> WPA2-PSK MIXED		
	Use Pre-Shared Key	<input type="text"/>
	Algorithm	TKIP/AES
	Group Key Rekey Interval	<input type="text"/> Minutes
<input type="radio"/> MAC Auth		
	RADIUS Server Profile	DEFAULT <input type="button" value="▼"/>

Figure 184 – Multiple BSSID Setting – 4

WPA-PSK – when selected, the encrypt method will be WPA without RADIUS server

WPA2-PSK – when selected, the security policy will be WPA2 PSK without RADIUS server. In this mode, only WPA2 PSK client can connect with AP and WPA PSK client is not permitted to connect

WPA2-PSK MIXED – when selected, WPA2 PSK and WPA PSK clients are all permitted to connect with AP

Use Pre-Shared Key –specify more than 8 characters and less than 64 characters for WPA with pre-shared key encryption

Algorithm – choose WPA algorithm (TKIP, AES)

Group Key Rekey Interval –specify amount of minutes and WPA automatically will generate a new Group Key

MAC Auth – when selected, the MAC address of wireless client will be passed to RADIUS server for PAP authentication when it connects with BW1253s. The MAC address of wireless client acts as username and password

RADIUS Server Profile – select the default radius server name

<input type="radio"/> WAPI	AAA Server Profile:	DEFAULT <input type="button" value="▼"/>
	WAPI certificate has not been Uploaded. Click here to upload certificate.	
<input type="radio"/> WAPI-PSK	Encode:	HEX <input type="button" value="▼"/>
	Use Pre-Shared Key:	<input type="text"/>
<input type="radio"/> Disabled		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Figure 185 – Multiple BSSID Setting – 5

WAPI – WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese National Standard for wireless LAN(GB15629.11-2003).(Only for China)

It needs to upload WAPI certificate.

AAA Server Profile – select your RADIUS server profile

WAPI-PSK – the encrypt method will be WAPI without RADIUS server

Encode – Pre-shared key encode.[HEX/ASCII]

Use Pre-Shared key – specify more than 8 characters and less than 64 characters for WPA with pre-shared key encryption

Disabled – when selected, you don't select any security policy

Change status or leave in the default state if no editing is necessary and click the **Save** button.

<input type="checkbox"/> Advance Wireless Setting	
Radio	wlan1
Interface	wlan1_0
Mode	AP
SSID	SSID
Hidden SSID	Disabled
Intra-BSS Layer 2 Isolation	Disabled
Use VLAN	Disabled
Interface Priority	Best Effort(0) (Class of Service)
WMM	Enabled
ESS in Tunnel	Disabled
Security	Disabled
Current Connected Number	0
<input type="button" value="Refresh"/> <input type="button" value="Return"/>	
<input type="button" value="Apply Changes"/> <input type="button" value="Discard Changes"/>	

Figure 186 –Apply or Discard the advanced Settings in AP mode

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Advance Wireless Setting	
Radio	wlan1
Interface	wlan1_0
Mode	AP
SSID	SSID
Hidden SSID	Disabled
Intra-BSS Layer 2 Isolation	Disabled
Use VLAN	Disabled
Interface Priority	Best Effort(0) (Class of Service)
WMM	Enabled
ESS in Tunnel	Disabled
Security	Disabled
Current Connected Number	0

[Refresh](#) [Return](#)

[Reboot](#)

System needs to be restarted to make the new configurations take effect.

Figure 187 – Reboot information

Reboot – click the button to restart the server and apply the changes.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Wireless | WEP

Use the **Wireless | WEP** menu to configure static WEP settings.



This menu only set static WEP key value related with 4 key indexes. Enable or Disable static WEP is in the **Wireless | Advance** menu.

WEP Configuration		
Radio	Wlan1	Action
Index	Key	Action
Key 1	*****	Edit
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Figure 188 – WEP Settings

Radio –show the wireless interface.

Click **Edit** to edit the existing **wepkey1** to **wepkey4**.

	By default, four WEP keys are all set to “aaaaa” (ascii characters) or “6161616161” (hexadecimal characters). They can be modified according to requirement.
---	--

WEP Configuration

Radio	wlan1	
Index	Key	Action
Key 1		Save Cancel
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Figure 189 – Edit WEP Key

Change status or leave in the default state if no editing is necessary and click the **Save** button.

WEP Configuration

Radio	wlan1	
Index	Key	Action
Key 1	*****	Edit
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Apply Changes **Discard Changes**

Figure 190 –Apply or Discard WEP Configuration

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

WEP Configuration

Radio	wlan1	
Index	Key	Action
Key 1	*****	Edit
Key 2	*****	Edit
Key 3	*****	Edit
Key 4	*****	Edit

The network password needs to be 64bits or 128bits depending on your network configuration. This can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 191 – Reboot information

Reboot – click the button to restart the server and apply the changes



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

Wireless | MAC ACL

Use the **MAC ACL** service to control the default access to the wireless interface of the BW1253s or define special access rules for mobile clients. Configure the ACL using the **Wireless | MAC ACL** menu:

MAC ACL Configuration

Radio	wlan1	
Policy	Allow	Edit
MAC List	Action	
00:90:4B:C9:42:55	Delete	
Add		

Figure 192 – MAC ACL Service

Radio – show the wireless interface.



The wireless interface which is Bridge mode hasn't MAC ACL settings.

Policy – click the **edit** button to choose Allow, Deny or disable the access control service on device. By default the ACL service is disabled and all wireless clients connecting to the BW1253s are allowed (no ACL rules are applied to the wireless clients)

Select **Allow** means only the wireless clients whose MAC are listed in the **MAC List** would be permitted to access this AP. Other wireless client cannot access this AP.

Select **Deny** means only the wireless clients whose MAC are listed in the **MAC List** would be prevented from accessing. Other wireless clients can access this AP.

Select **Disabled** means no ACL service.

The screenshot shows a configuration interface titled "MAC ACL Configuration". It has a "Radio" dropdown set to "wlan1". A "Policy" dropdown is open, showing three options: "Allow", "Deny", and "Disabled", with "Allow" selected. Below the policy dropdown is a table with one row. The first column contains the MAC address "00:90:4B:C9:42:55". The second column is labeled "Action" and contains a "Delete" button. At the bottom left is an "Add" button, and at the bottom right are "Save" and "Cancel" buttons.

Figure 193 – MAC ACL settings

You must create **MAC List** to work with **Policy** setting. The access control list is based on the network device's MAC address. In the MAC ACL Configuration table, you only need to specify the MAC address of wireless client. Click the **Add** button to create a new MAC entry:

The screenshot shows the same "MAC ACL Configuration" interface. The "Policy" dropdown is now set to "Allow". The table has one row with the MAC address "00:90:4B:C9:42:55" and a "Delete" button. At the bottom left is a text input field containing "Example: 00:90:4B:00:11:22". At the bottom right are "Save" and "Cancel" buttons.

Figure 194 – Add MAC entry

MAC Address – enter the physical address of the network device you need to (MAC address). The format is a list of colon separated hexadecimal numbers (for example: 00:90:4B:00:11:22)

Save – click the button to save the new MAC entry

The screenshot shows the "MAC ACL Configuration" interface again. The "Policy" dropdown is set to "Allow". The table has one row with the MAC address "00:90:4B:C9:42:55" and a "Delete" button. At the bottom left is an "Add" button. At the very bottom are two buttons: "Apply Changes" and "Discard Changes".

Figure 195 – Apply or Discard MAC ACL Configuration Changes

Apply Changes – to save all changes made in the **interface** table at once

Discard Changes – restore all previous values

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

MAC ACL Configuration		
Radio	wlan1	
Policy	Allow	Edit
MAC List	Action	
00:90:4B:C9:42:55		Delete
	Add	

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 196 – Reboot Server

Reboot – click the button to restart the server and apply the changes



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

User

User | Users

The **User | Users** menu shows the statistics of connected users. The user can be monitored and managed such as drop from the network.

Users									
Index	User	Interface	User IP	Authed	Wireless Auth	Time Length	Idle Time	Action	
01.	00:0c:41:16:97:aa	wlan1_0	192.168.120.62	No	NONE	00:26:53	00:00:25	Details	Kickoff
Refresh									

Figure 197 – User's statistics

User – show the connected client's MAC address

Interface – show which BSS the client connected to

User IP – IP address, from which the user's connection is established [digits and dots]

Authed – indicate this client is authenticated or not

WEB Auth/L2 Auth – show the authentication method which user uses to connect

Time Length – session duration since the user login [hh:mm:ss]

Idle Time – amount of user inactivity time [hh:mm:ss]

Action – view the statistics or kickoff the user.

Detail – click on user details to get more information about the client:

Kickoff – disconnect the user.

Users		
Description	Value	Action
user	rock	
interface	wlan1_0	
user IP	192.168.3.3	
MAC address	00904B238D42	
WEB Auth / L2 Auth	UAM / NONE	
WISP		
session id	00000828A9B1	
time length	02:12:21	
remaining time length	4 days 18:27:39	
idle time	00:00:21	
idle timeout	00:01:00	
input bytes	2 MB	
output bytes	961 KB	
remaining input bytes	-	
remaining output bytes	-	
remaining total bytes	-	
bandwidth downstream	512 Kbps	
bandwidth upstream	512 Kbps	
		<input type="button" value="Back"/> <input type="button" value="Kickoff"/>
		<input type="button" value="Refresh"/>

Figure 198 – User's Details

User – login user name

interface – the interface that wireless client associated.

User IP – the IP address of wireless client.

MAC address – hardware address of the network device from which the user is connected

WEB Auth/L2 Auth – show web authentication and layer2 authentication status, layer2 authentication include all supported EAP type of 802.1x auth and MAC auth

WISP – WISP domain name where the user belongs

Session ID – the unique user's session ID number. This can be used for troubleshooting purposes

Remaining Time Length – remaining user's session time [hh:mm:ss]. Session time for user is defined in the RADIUS Server

Idle time – specify current idle time.

Idle Timeout – specify the time of user idle timeout [hh:mm:ss]. When reach the time, the user will be logged out automatically.

Input Bytes – amount of data in bytes which the user network device has received [Bytes]

Output Bytes – amount of data in bytes, transmitted by the user network device [Bytes]

Remaining Input/Output Bytes – user session remaining input/output bytes. WISPr Operator can define the user session in bytes. Remaining bytes is received from RADIUS [Bytes/unlimited]

Remaining Total Bytes – user session remaining total bytes. WISPr Operator can define the user session in bytes. Remaining bytes is received from RADIUS [Bytes/unlimited]

Bandwidth Downstream/Upstream – user upstream and downstream bandwidth [in bps]

Back – returns to connect client's statistics list

Kickoff – click this button to disconnect the user from access point.

Refresh – click the button to refresh users' statistics

User | Station Supervision

The **Station Supervision** function is used to monitor the connected host station availability. This monitoring is performed with ping. If the specified number of ping failures is reached (**failure count**), the user is logged out from the BW1253s.

Station Supervision		
Interval	Failure Count	Action
20	3	Edit

Figure 199 – Station Supervision

To adjust the ping interval/failure count, click the **Edit** button.

Station Supervision		
Interval	Failure Count	Action
<input type="text" value="20"/>	<input type="text" value="3"/>	Save Cancel

Figure 200 – Edit Station Supervision

Interval – define interval of sending ping to host [in seconds]

Failure Count – failure count value after which the user is logged out from the system

Save – save station supervision settings

Cancel – cancel changes

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Station Supervision		
Interval	Failure Count	Action
20	3	Edit

Apply Changes **Discard Changes**

Figure 201 –Apply or Discard Station Supervision Changes

Apply Changes – to save all changes at once

Discard Changes – restore all previous values

For such change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Station Supervision		
Interval	Failure Count	Action
20	3	Edit

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 202 – Reboot Server

Reboot – click the button to restart the server and apply the changes



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

User | User ACL

User ACL provide high flexibility for administrator to define the rules for BW1253s to filter the packets which will forward or masquerade by it.

User ACL												
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	
No ACLs are defined on system.												
												Add

Figure 203 – User ACL

To add a new rule, just click the **Add** button.

User ACL												
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	
1	DROP	tcp	any	any	-	-	-	-	-	-	Conti	

Figure 204 – Create a new rule (first step)

First step select the rule policy [drop/accept/masquerade] to deal with packet and the packet type [all/TCP/UDP/ICMP] and which interface the rule will act on.

Policy – define the policy of client through the access point. It supports three types of rules: DROP, ACCEPT and MASQUERADE. The appropriate policy defines what to do if the data packet received matches the rule

Protocol – network protocol which the rule affects. Can be specified as one of “TCP/UDP/ICMP” or “any”

In Interface – the data packet to the current interface must obey the rule

Out Interface – the data packet from the current interface must obey the rule

User ACL													
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	Continue	Cancel
1	DROP	tcp	any	any	Special IP	-	-	Special IP	-	-	Continue	Cancel	

Figure 205 – Create a new rule (second step)

Second step select the type of source IP and destination IP [special IP/any IP].

User ACL													
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	Continue	Cancel
1	DROP	tcp	any	any	special	-	Special Port	special	-	Special Port	Continue	Cancel	

Figure 206 – Create a new rule (third step)

Third step choose the type of source port and destination port [any port/special port].

User ACL													
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	Save	Cancel
1	DROP	tcp	any	any		255.255.255.255			255.255.255.255			Save	Cancel

Figure 207 – Create a new rule (fourth step)

Fourth step, fill out the source IP address and destination IP address (including IP address and net mask, if you choose “any IP” in second step, you need not fill out the IP address); fill out the source port and destination port (if you select any port in third step or select protocol ICMP/all, you need not fill out the port).

User ACL													
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	Delete	Edit Sort
1	ACCEPT	tcp	wlan1_0	bridge2_0	192.168.3.0	255.255.255.0	12	192.168.6.0	255.255.255.0	45		Delete	Edit Sort

Figure 208 – Create a new rule (fifth step)

After complete the rule configuration, click the “apply changes” button to save your configuration.

You can also re-order your rules if you have many rules configured and arrange the priority of them. The rule with index 1 has the highest priority; with index 2 has the second high priority and so on.

User ACL													
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	Save	Cancel
1	ACCEPT	tcp	wlan1_0	bridge2_0	192.168.3.0	255.255.255.0	12	192.168.6.0	255.255.255.0	45			
2	DROP	icmp	any	any	any	-	any	192.168.2.0	255.255.255.255	any	Save	Cancel	

Figure 209 – re-order rules

Click **Edit Sort** button of one rule to re-order its priority and then select the index number, click **Save** button to save your changes.

User ACL												
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source IP	Source Netmask	Source Port	Dest IP	Dest Netmask	Dest Port	Action	
1	ACCEPT	tcp	wlan1_0	bridge2_0	192.168.3.0	255.255.255.0	12	192.168.6.0	255.255.255.0	45	Delete Edit Sort	
2	DROP	icmp	any	any	any	-	any	192.168.2.0	255.255.255.255	any	Delete Edit Sort	
Add												
Apply Changes Discard Changes												

Figure 210 –Apply or Discard User ACL Changes

Apply Changes – to save all changes of User ACL at once

Discard Changes – restore all previous values



Please be careful to use the DROP policy. For example, if DROP tcp for any source IP, BW1253s web UI will not be accessed.

User | Walled Garden

The **walled garden** is an environment that controls the user's access to Web content and services. It is to define a free, restricted service set for a user do not logged into the system. Use the **User | walled garden** menu to view or change the free URLs or hosts:

Walled Garden URLs				
URL for User	String to Display	Action		
no free site (or walled garden) URL is specified			new URL	
Walled Garden Hosts				
Type	Host	Netmask	Port	Action
no free site (or walled garden) host is specified			new host	

Figure 211 –Walled Garden

New URL – click the **new URL** button and enter the new URL and its description. Save entered information by clicking the **update** button:

Walled Garden URLs		
URL for User	String to Display	Action
<input type="text" value="http://www.test.com"/>	<input type="text" value="welcome"/>	Save Cancel

Figure 212 – Add New URL part 1

URL for User – define full URL address. Ex:[http://www.test.com]

String to Display – site description visible to user listed on the **welcome** and **login** page:

Figure 213 – Walled Garden link in the Welcome Page

New Host – If you need to define hosts (web servers) for walled garden, specify hosts by clicking the **new host** button and click the **update** button:

Walled Garden Hosts				
Type	Host	Netmask	Port	Action
TCP		255.255.255.255		Save Cancel

Figure 214 – Walled Garden Host

Type –select the data traffic protocol for host server [TCP/UDP].

Host – Web server address [IP address or host name].

Netmask – enter the network mask to specify the host servers network.

Port – network port, which is used to reach the host [1-65535]. For standard protocols use the default ports:

Protocol	Port
HTTP	80
HTTPS	443
FTP	21

User | WISP

Different **WISPs** (Wireless Internet Service Providers) can be associated with appropriate RADIUS servers and device interfaces using the **User | WISP** menu:

WISP		
Domain Policy	Username Prefix Length	Action
Username@Domain	N/A	edit_policy
Name	RADIUS Name	Action
No WISPs are defined on system.		
Add WISP		
Note: When select the policy "use username prefix", assure the length of the wisp name will be equal to the setting of "Username Prefix Length"		

Figure 215 – WISP Menu

Domain policy means BW1253s use which policy to fetch WISP name from user name then to judge user belong which domain.

	Up to 32 WISP entries can be defined using the User WISP menu.
---	--

The owner can use three policies to judge the WISP name from user name:

1. username follow the format: **username@WISPdomain**
2. username follow the format: **WISPdomain/username**
3. use prefix of username as wisp name, the range of prefix length is from 2 to 6

WISP		
Domain Policy	Username Prefix Length	Action
use username prefix	4	Save Cancel
Username@Domain	RADIUS Name	Action
Domain/UserName		
use username prefix		
No WISP's are defined on system.		
Add WISP		

Note: When select the policy "use username prefix", assure the length of the wisp name will be equal to the setting of "Username Prefix Length"

Figure 216 – Domain Policy

Add WISP – click to define WISP for RADIUS server

WISP		
Domain Policy	Username Prefix Length	Action
Username@Domain	N/A	edit policy
Name	RADIUS Name	Action
browan	DEFAULT	Save Cancel
Note: When select the policy "use username prefix", assure the length of the wisp name will be equal to the setting of "Username Prefix Length"		

Figure 217 – Define New WISP

Name – new WISP domain name [string, up to 256 symbols, no space, dot or dash allowed]

RADIUS Name – select RADIUS for new WISP from list box [non editable]

Save – click the button to save the new WISP

Cancel – restore all previous values

WISP		
Domain Policy	Username Prefix Length	Action
Username@Domain	N/A	edit policy
Name	RADIUS Name	Action
browan	DEFAULT	Edit Delete
Add WISP		

Note: When select the policy "use username prefix", assure the length of the wisp name will be equal to the setting of "Username Prefix Length"

Figure 218 – Apply or Discard Changes of WISP settings

BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

WISP		
Domain Policy	Username Prefix Length	Action
Username@Domain	N/A	edit_policy
Name	RADIUS Name	Action
browan	DEFAULT	Edit Delete
		Add WISP

Note: When select the policy "use username prefix", assure the length of the wisp name will be equal to the setting of "Username Prefix Length"

Reboot

System needs to be restarted to make the new configurations take effect.

Figure 219 – Reboot information

Reboot – click the button to restart the server and apply the changes.



If there is no other settings needed to be modified, click the **Reboot** button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click **Reboot** button to restart and take effect for all settings.

User | Start Page

The **start page** is the default web page where users will be redirected after log-on. This value will be overwritten by the WISP RADIUS attribute no.4 “Redirection-URL” if provided in the authentication response message. Use the **User | Start Page** menu to view or change the start page URL:

Start Page		
Name	Value	Action
Start Page URL	http://www.xooo.com	Edit

Figure 220 – Start Page

The administrator can change the **start page** by clicking the **Edit** button. The value entry field will change into an editable field:

Start Page		
Name	Value	Action
Start Page URL	http://www.xooo.com	Save Cancel

Figure 221 – Edit Start Page

Value – enter new redirection URL of start page in valid format [http://www.startpageurl.com]

Save –click the button to save new settings

Cancel – restores all previous values

Name	Value	Action
Start Page URL	http://www.xxxx.com	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Figure 222 – Apply or Discard Changes of Start Page

BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Name	Value	Action
Start Page URL	http://www.xxxx.com	<input type="button" value="Edit"/>

System needs to be restarted to make the new configurations take effect.

Figure 223 – reboot device

Reboot – click the button to restart the server and apply the changes.

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
--	---

User | Customized UAM

Customized UAM let owner upload their own login and logout page to BW1253s to apply with enterprise style or do advertisements.

User customized page is based on HTML.

BW1253s support internal and external customized UAM. Internal means user can upload their html login and logout page to BW1253s. External means BW1253s will go to an external web server to fetch login and logout page the local and push to web login client.

	Please contact with BROWAN if you need the internal customized UAM template sample.
--	---

Customized UAM in default is disabled. Click the **Edit** button on the setting you need to change:

Description	Status	Action
Use SSL	disabled	<input type="button" value="Edit"/>
Customize Page	disabled	<input type="button" value="Edit"/>

Figure 224 – Customized UAM page

Use SSL – select enable or disable to use SSL encryption for the HTTP session of the user login page

Customize Page – enable the configuration if you want to use customized UAM function

After successfully enabled customized UAM configuration, this configuration page will be extended to the follow page which includes three columns.

Customized UAM		
Description	Status	Action
Use SSL	enabled	Edit
Customize Page	enabled	Edit
Pop Logout Page	enabled	Edit
Logout Page width size: 350 Logout Page Height size: 390		Edit
Use External Page	disabled	Edit

Update HTML Files		
Description	Action	
Delete all uploaded HTML and images files!	Delete	
Upload HTML and image files!	Upload	
See example login html page here and See example logout html page here		

Uploaded File List		
---------------------------	--	--

Figure 225 – Customized UAM enabled

First is Customized UAM status configuration:

Pop Logout Page – after user successful web login, if this item is enabled, BW1253s will pop out a logout page for user. In default this setting is enabled if customized page is enabled

Logout Page's Dimension – for the difference of logout page's dimension which make by customer, BW1253s will use this data to pop out user's customized logout page

Use External Page – if this item is enabled, BW1253s will fetch login and logout page from an external web server

Second is update html files, for user delete or upload login and logout pages. There also has two URL point to example page in html format for login and logout page which user can reference to make their own pages.

The third is uploaded file list, where user can find which files have been uploaded.

Press upload button on second column will coming into upload files pages:

Customized UAM		
Description	Status	Action
Use SSL	enabled	<input type="button" value="Edit"/>
Customize Page	enabled	<input type="button" value="Edit"/>
Pop Logout Page	enabled	<input type="button" value="Edit"/>
Logout Page width size: 350 Logout Page Height size: 390		<input type="button" value="Edit"/>
Use External Page	disabled	<input type="button" value="Edit"/>

Update Custom UAM Files		
Login File	<input type="text" value="F:\uploads\aplogin.html"/>	<input type="button" value="Browse..."/>
Logout File	<input type="text" value="F:\uploads\aplogout.html"/>	<input type="button" value="Browse..."/>
Additional file 01	<input type="text" value="F:\uploads\back.gif"/>	<input type="button" value="Browse..."/>
Additional file 02	<input type="text" value="F:\uploads\by.jpg"/>	<input type="button" value="Browse..."/>
Additional file 03	<input type="text" value="F:\uploads\line1.gif"/>	<input type="button" value="Browse..."/>
Additional file 04	<input type="text" value="F:\uploads\line2.gif"/>	<input type="button" value="Browse..."/>
Additional file 05	<input type="text" value="F:\uploads\line.jpg"/>	<input type="button" value="Browse..."/>
Additional file 06	<input type="text" value="F:\uploads\logo.jpg"/>	<input type="button" value="Browse..."/>
Additional file 07	<input type="text"/>	<input type="button" value="Browse..."/>
Additional file 08	<input type="text"/>	<input type="button" value="Browse..."/>
Additional file 09	<input type="text"/>	<input type="button" value="Browse..."/>
Additional file 10	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Upload"/> <input type="button" value="Cancel"/>		

Figure 226 – Upload Pages

Login File is for customized login page; **Logout File** is for customized logout page.

Additional file 01~10 is for uploading picture and CSS files. Current support picture file format is JPG, GIF, PNG and CSS.



Picture and CSS files name need be consistent with your login or logout html pages. The login and logout html file can be what ever you want.



Don't forget fill out the **Logout page's dimension**, or logon user maybe can only see part of your logout page.

After select the file you want, press upload button and the files will upload to BW1253s. after successful upload files, you can see the page below:

Customized UAM		
Description	Status	Action
Use SSL	enabled	Edit
Customize Page	enabled	Edit
Pop Logout Page	enabled	Edit
Logout Page width size: 350 Logout Page Height size: 390		Edit
Use External Page	disabled	Edit

Update HTML Files		
Description	Action	
Delete all uploaded HTML and images files!	Delete	
Upload HTML and image files!	Upload	

See example login html page [here](#) and See example logout html page here

Uploaded File List		
aclogin.html		
aclogout.html		
back.gif		
by.jpg		
line.jpg		
line1.gif		
line2.gif		
logo.jpg		

Figure 227 – Flash upload files OK

After successful flash the files, uploaded files will appear in uploaded file list.

Next is an example for customized login and logout page.



Figure 228 – Example login and logout page

For external page, enabled the “Use External Page” as below.

Customized UAM		
Description	Status	Action
Use SSL	disabled	Edit
Customize Page	enabled	Edit
Pop Logout Page	enabled	Edit
Logout Page width size: 350 Logout Page Height size: 390		Edit
Use External Page	enabled	Edit
External Login page URL:	http://192.168.123.6/login.html	
External Logout page URL:	http://192.168.123.80/logout.html	Edit
Update external page interval(Sec.):	7200	Edit
Update extern login and logout URL page immediately		Done
See example external login html page here and See example external logout html page here		

Figure 229 – External Page Configuration

Fill out the external login page and external logout page [http://host IP address:port/path]. BW1253s would auto-update the external page every 7200 seconds or you change the interval update time. External page example will be found in the links under the last line.



In External page mode, BW1253s will only fetch the login and logout html page to local, the picture or the CSS file which link on the customized login/logout page will not be fetch. So the link to the picture and CSS file on user customized html file need to be an absolute address which point to the external web server.



BW1253s would use the default login or logout page if user did not upload the customized pages or BW1253s did not get the external page from the external login/logout page IP.

User | Pages



Detailed description about user page customization is given in the **Chapter 5 – User Pages**.

The **welcome/login/logout/help** pages can be easily changed to user defined pages by choosing the **edit** menu. The **pages** configuration menu is displayed by default:

Pages				
Page	Use	Status	Location	Action
welcome	internal	enabled	welcome.xsl	Edit
login	internal	-	login.xsl	Edit
logout	internal	-	logout.xsl	Edit
help	internal	-	/tmp/links/help.html	Edit
unauthorized	internal	-	/tmp/links/unauthorized.html	Edit

Caching	
Status	Action
enabled	Edit
clear cached templates	Clear

Figure 230 – Available User Pages for Configuration

Login/Logout/Help/Unauthorized pages settings detailed description is given in the **Chapter 5 – User Pages**. Only **Welcome** page settings reference is provided here.

Welcome – first page the user gets when he/she opens its browser and enters the URL.

Internal – choose this option when using the internal user pages templates.

External – choose this option when uploading your own user pages templates.

Redirect – choose this option when using the **Extended UAM** function (see **Chapter 5 – User Pages**).

Status – choose enable/disable welcome page status. Note that redirect option with status ‘disabled’ would work.

Location – enter location for external templates or redirect (e.g. WAS IP address).

Pages				
Page	Use	Status	Location	Action
welcome	redirect	enabled	http://192.168.123.81/portal/	Edit
login	internal	-	login.xsl	Edit
logout	internal	-	logout.xsl	Edit
help	internal	-	/usr/local/G8000/links/help.html	Edit
unauthorized	internal	-	/usr/local/G8000/links/unauthorized.html	Edit

Figure 231 – Redirect User Pages

Welcome page with **redirect** option selected redirects the user authentication process to the specified location. The user welcome/login/logout page can be implemented as simple HTML (not required to use the .XSL or default user pages templates) in such case.



The redirect location URL should be specified in Walled Garden URL, otherwise the redirect would NOT WORK.

Caching	
Status	Action
enabled	Edit
clear cached templates	Clear

Figure 232 – Caching Option

Caching option can be used for caching the external uploaded user pages (available choice: enabled/disabled)

Clear – click the button to clear cached user pages.

	Controller cache is also cleared after device reboot/reset.
---	---

User | Upload

	Please contact with BROWAN if you need the user pages template sample .
---	--

 Upload	
Description	Action
Before uploading new template files and images, please delete old files. There is limited space on server for templates and images.	
Upload new template files and images. Old files will be overwritten, if exist with the same name. If you need, you can repeat upload process few times, until upload all needed images (you do not need to upload template files twice). Please remember, that server space is limited! All files will be uploaded to "images" directory, please prepare your templates to use images and stylesheets from that directory.	

Figure 233 – Upload Page

Delete – click the button to delete earlier uploaded files from controller memory.

Upload – click the button to select and upload new user pages.

	How to upload user pages see in the Chapter 5 – User Pages .
---	---

User | HTTP Headers

System administrator can set **HTML headers encoding** and **language** settings for BW1253s web management interface and new uploaded user pages. Select **User | HTTP Headers** menu:

 HTTP Headers			
Description	Enabled	Value	Action
Content-Type	no	-	
Content-Language	no	-	

Figure 234 – HTTP Headers Settings

BW1253s device supports some http META tags. Syntax of such META tags:

```
<META HTTP-EQUIV="name" CONTENT="content">
```

Currently BW1253s supports **Content-Type** and **Content-Language** tags:

- **Content-Type** is used to define document char set (used, when text has non-Latin letters, like language letters).
- **Content-Language** may be used to declare the natural language of the document.

BW1253s automatically adds defined content-type and content-language to generated XML. Then user pages (.XSL) templates will use these parameters to generate the output HTML.

Click the change button to define new headers of the web management interface on user pages templates. The default HTML encoding is **ISO-8859-1**, language = **English**. Enable the HTTP header status and default values appear:

HTTP Headers			
Description	Enabled	Value	Action
Content-Type	<input type="button" value="no"/>	ISO-8859-1	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
Content-Language	no	-	

Figure 235 – Set HTTP Headers

The system administrator can set his own header encoding and language settings.



Use the HTML 4.01 specification to define the header encoding and language.

User | Remote Authentication



Read more about the extended UAM feature in **Chapter 5 – User Pages**, section: **Extended UAM**

The **Remote Authentication** feature under the **User** menu allows an external Web Application Server (WAS) to intercept/take part in the user authentication process, and to log on and log off users externally. It provides a means to query user session information as well. By default such remote authentication is disabled:

Remote Authentication			
Description	Value	Action	
remote authentication	disabled	<input type="button" value="Edit"/>	
shared secret	none	<input type="button" value="Edit"/>	

Figure 236 – Remote Authentication

Click the **edit** button next to appropriate settings to specify **remote authentication** parameters:

Remote Authentication			
Description	Value	Action	
remote authentication	disabled		
shared secret	none	<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 237 – Enable Remote Authentication

Remote Authentication – select status: [enabled/disabled].

Shared Secret – enter password for WAS to communicate with AC [string (4-32), no spaces allowed].



The shared secret must match that configured on the WAS. This shared secret allows the WAS to initiate a secure (SSL) command session with the BW1253s to pass login commands.

Services

Services | Telnet

Use **Services | Telnet** menu to manage the telnet/SSH service of your BW1253s.

Telnet		
Name	Status	Action
Telnet Service	Enabled	Edit
SSH Service	Enabled	Edit

Figure 238 – System Configuration settings

Telnet Service – Enable or disable telnet service of BW1253s

SSH Service – Enable or disable SSH service of BW1253s

The default of these two services are all **Enabled**. The current IETF SSH (SSHv2) is supported for security of accessing BW1253s via telnet/CLISH.

Services | SNMP

SNMP is the standard protocol that regulates network management over the Internet. To communicate with SNMP manager you must set up the same **SNMP** communities and identifiers on both ends: manager and agent.

Use the **Services | SNMP** menu to change current SNMP configuration.

General Configuration		
Name	Value	Action
Readonly community	public	Edit
Readwrite community	private	Edit
DefaultTrap community	public	Edit
HeartBeat Trap Interval	0 seconds	Edit

Trap Configuration					
Index	Host Ip	Host Port	Trap Type	Community	Action
1	192.168.120.62	162	trapsink	test	Delete
Add					

Figure 239 – SNMP settings

Readonly community – community name is used in SNMP version 1 and version 2c. Read-only (public) community allows reading values, but denies any attempt to change values [1-32 all ASCII printable characters, no spaces]

Readwrite community – community name is used in SNMP version 1 and version 2c. Read-write (private) community allows to read and (where possible) change values [1-32 all ASCII printable characters, no spaces]

Default Trap community – the default SNMP community name used for traps without specified communities. The default community by most systems is "public". The community string must match the community string used by the SNMP network management system (NMS) [1-32 all ASCII printable characters, no spaces]

HeartBeat Trap Interval – define the interval that AP send trap information to the server.[in seconds]

Trap Configuration Table:

You can configure your SNMP agent to send **SNMP Traps** (and/or inform notifications) under the defined host (SNMP manager) and community name (optional).

Trap Configuration					
Index	Host Ip	Host Port	Trap Type	Community	Action
1	192.168.120.62	162	trapsink	test	Delete
Add					

Figure 240 – SNMP Trap table settings

Click **Add** to add a new SNMP manager or **Delete** to delete a specific SNMP manager. Clicking **Add**:

Trap Configuration					
Index	Host Ip	Host Port	Trap Type	Community	Action
No entry in list					
	192.168.123.66	162	trapsink	test	Save Cancel
			<input type="button" value="trapsink"/> <input type="button" value="trap2sink"/> <input type="button" value="informsink"/>		

Figure 241 – Add SNMP Trap

Host IP – enter SNMP manager IP address [dots and digits]

Host Port – enter the port number the trap messages should be send through [number]

Trap Type – select trap message type [v1/v2/inform]

Community – specify the community name at a SNMP trap message. This community will be used in trap messages to authenticate the SNMP manager. If not defined, the default trap community name will be used (specified in the SNMP table) [1-32 all ASCII printable characters, no spaces]

Save – save all current settings

Cancel – restore the last settings

Services | NTP

NTP (Network Time Protocol) is used to synchronize the system time with the selected network NTP server. Use the **Services | NTP** menu to configure the NTP service:

NTP Server		
NTP Status	disable	<input type="button" value=""/>
Time Zone	GMT-12:00	<input type="button" value=""/>
Name	ServerIP	Action
No entry in list		
Add		

Figure 242 – NTP Settings

NTP Status – specify enable or disable this NTP service

Time Zone – specify the time zone for NTP service

Delete – delete the existed NTP server

Edit – edit the settings of the existed NTP server

Add – add a new NTP server setting for synchronizing time

Clicking **Add** button to add a new NTP server:

NTP Server	
Name	ServerIP
Ntpserver	207.46.103.100
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 243 – Add new NTP server setting



Two NTP servers can be configured under **Services | NTP** menu. And only IP address is accepted for NTP server.

Please enter at least one NTP server when enable NTP service.



The **Name** of NTP server should be unique.

Change status or leave in the default state if no editing is necessary and click the **Save** button.

NTP Server		
NTP Status <input type="button" value="enable"/>		
Time Zone <input type="button" value="GMT-12:00"/>		
Name	ServerIP	Action
time.nist.gov	192.43.244.18	<input type="button" value="Delete"/> <input type="button" value="Edit"/>
<input type="button" value="Add"/>		
<input type="button" value="Apply Changes"/> <input type="button" value="Discard Changes"/>		

Figure 244 – Save the NTP server Changes

Change the Time Zone for your own local time and change the NTP status to enable or disable.

NTP Server

NTP Status	enable	
Time Zone	GMT+08:00	
Name	ServerIP	Action
time.nist.gov	192.43.244.18	<input type="button" value="Delete"/> <input type="button" value="Edit"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Figure 245 – Edit Time Zone setting/NTP status

Click **Save** button to save new Time Zone setting.

NTP Server

NTP Status	enable	
Time Zone	GMT+08:00	
Name	ServerIP	Action
time.nist.gov	192.43.244.18	<input type="button" value="Delete"/> <input type="button" value="Edit"/>
<input type="button" value="Add"/>		

Figure 246 – Apply or Discard Time Zone/NTP status Changes

For each change of settings, the BW1253s needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

NTP Server

NTP Status	enable	
Time Zone	GMT+08:00	
Name	ServerIP	Action
time.nist.gov	192.43.244.18	<input type="button" value="Delete"/> <input type="button" value="Edit"/>
<input type="button" value="Add"/>		
<input type="button" value="Reboot"/>		

System needs to be restarted to make the new configurations take effect.

Figure 247 – Reboot information

Reboot – click the button to restart the server and apply the changes

	If there is no other settings needed to be modified, click the Reboot button to apply all changes. If there are any other settings need to be changed, continuously to finish and apply all changes and then click Reboot button to restart and take effect for all settings.
---	---

Services | Time

Configure the system time manually under **Services | Time** menu.

Date and Time	
Date	2006/07/07
Time	18:46
<input type="button" value="Edit"/> <input type="button" value="Refresh"/>	

Figure 248 – Time Settings

Click **Edit** to change current system time.

Date and Time	
Date	2006 / 07 / 7
Time	18 : 46
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 249 – Edit Date and Time Settings

Change the Date and Time or leave in the default value if no editing is necessary and click the **Apply** button. Thus the modified time will be taken effect at once. No reboot is needed.

	If NTP is enabled, the local time cannot be modified.
---	---

	Since BW1253s hasn't RTC (real-time clock), the system time will back to 1970/01/01 00:00 when reboot.
---	--

Services | Watchdog

BW1253s supply watchdog function for the reliability. Use **Services | Watchdog** to enable/disable watchdog service.

Watchdog			
Name	Status	Check Interval	Action
Software Watchdog	Enabled	10 Seconds	<input type="button" value="Edit"/>
Hardware Watchdog	Enabled		<input type="button" value="Edit"/>

Figure 250 – Watchdog settings

Click Edit button to edit watchdog settings. The similar UI will be appeared like below:

Watchdog			
Name	Status	Check Interval	Action
Software Watchdog	Enabled	10 Seconds	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
Hardware Watchdog	Enabled		<input type="button" value="Edit"/>

Figure 251 – edit Software Watchdog settings

Status – Enable or Disable software watchdog

Check Interval – the periodical time that software watchdog checks the whole file system of BW1253s.

The hardware watchdog function will protect device even the operation system crash.

Watchdog			
Name	Status	Check Interval	Action
Software Watchdog	Enabled	10 Seconds	<input type="button" value="Edit"/>
Hardware Watchdog	Enabled		<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Figure 252 – edit hardware watchdog settings

Status – Enable or Disable hardware watchdog



The default value is enabled for both Software Watchdog and Hardware Watchdog. It is strongly recommended to enable the watchdog function.

Click **Save** and follow the UI instruction to apply changes and reboot the device for apply all the modified settings.

System

System | Administrator

The **System | Administrator** menu is for changing the administrator's settings: username and password:

Administrator	
User Name	<input type="text" value="admin"/>
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 253 – system security settings

User Name – administrator username for access to BW1253s (e.g. web interface, CLI mode) [1-32 symbols, spaces not allowed]

Old Password – old password value

New Password – new password value used for user authentication in the system [4-8 characters, spaces not allowed]

Confirm Password – re-enter the new password to verify its accuracy

Save – click to save new administrator settings.

	Default administrator logon settings are: User Name: admin Password: admin01
	Password length is from 4 to 8 characters.

After filling in the right Old password and the New Password, clicking the **Save** button for taking effect immediately.

After clicking **Save** button, the below UI will be shown to notify that the new password setting has been taken place:

Set password successfully.

Administrator	
User Name	<input type="text" value="admin"/>
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 254 – system security settings save and take effect successfully

System | System Log

Use the **System | System Log** menu to trace your AP system processes and get the system log locally or on the remote log server.

The screenshot shows two tables side-by-side:

Remote System Log			
Remote Log Status	Host IP	Log Level	Action
Disabled	192.168.2.1	info	Edit

Local System Log			
Local Log Status	Log Limit (bytes)	Log Level	Action
Enabled	102400	debug	Edit
View Log Messages			View

Figure 255 – System Log settings

To enable the **System Log** remote sending function, click the **Edit** button on the Remote System Log table and choose the **enabled** option:

The configuration dialog box for the Remote System Log:

Remote System Log			
Remote Log Status	Host IP	Log Level	Action
Enabled <input type="button" value="▼"/>	192.168.2.1	Info <input type="button" value="▼"/>	Save Cancel

Figure 256 – Configure Remote System Log Utility

Remote Log Status – choose disable/enable remote log [enabled/disabled]

Host IP – specify the host IP address where to send the **System Log** messages [dots and digits]

Log Level – specify the remote log message level you want to trace [critical, error, warning, info and debug]

This table provides information about the configuration options:

	Do not output “debug” log unless there are important issue needs to be clarified. Debug log will output all of the information so that it will severely drop down the network performance.
	BW1253s support standard sys. log server.

Save – save changes

Cancel – restore the previous values

To view the **System Log** locally, click the **Edit** button on the Local System Log table and choose the **enabled** option:

The configuration dialog box for the Local System Log:

Local System Log			
Local Log Status	Log Limit (bytes)	Log Level	Action
Enabled <input type="button" value="▼"/>	102400	Debug <input type="button" value="▼"/>	Save Cancel
View Log Messages			View

Figure 257 – Configure Local System Log

Local Log Status – choose disable/enable local log [enabled/disabled]

Log Limit – specify the maximum length of local log message in byte [20000-512000]

Log Level – specify the local log message level you want to trace [critical, error, warning, info and debug]

Save – save changes

Cancel – restore the previous values

View – view the log messages locally

Click **View** button, a similar screen will appear as below:

Local Log Messages	
Messages	Action
Clear All Log Messages:	Clear
Jan 1 03:17:59 P720 [G8000]: messages is null, so continue	
Jan 1 03:18:05 P720 last message repeated 3 times	
Jan 1 03:18:08 P720 [G8000]: cmd is equal to refreshlog button	
Jan 1 03:18:08 P720 [G8000]: messages is null, so continue	
<input type="button" value="Refresh"/> <input type="button" value="Return"/>	

Figure 258 – View Local Log Messages

Clear – clear current log message

Refresh – get the updated log messages

Return – back to System Log page

System | System Mode

In this page, you can select the system mode of your BW1253s.

System Mode					
Mode	Interface	IP	Netmask	Gateway	Protocol
<input checked="" type="radio"/> AP					
	LAN	192.168.123.159	255.255.255.0	192.168.123.1	static <input type="button" value="▼"/>
<input checked="" type="radio"/> AP Router					
	WAN	192.168.123.159	255.255.255.0	192.168.123.1	static <input type="button" value="▼"/>
Apply and Reboot					

Figure 259 – System Mode Settings

Mode – select whether the system mode of BW1253s is AP mode or AP Router mode

IP – specify the IP address of current interface [dots and digits]

Netmask – specify the subnet mask of current interface [dots and digits]

Gateway – specify the gateway to other networks

Protocol – specify **static** for setting IP address manually and **dhcp** for getting IP address dynamically acting as DHCP client

Apply and Reboot – click the button to restart the device and apply all setting changes



The Web Interface in AP-Router mode is different from that in AP mode. For the detailed configuration of BW1253s working in AP mode, please refer to: **Chapter 3 – Reference Manual---AP Mode**

System | System Info

Administrator can self-define the device information including the system name, system location and system contact information of his BW1253s.

System Info		
Name	Value	Action
System Name	BW1253	Edit
System Location	location	Edit
System Contact	contact information	Edit

Figure 260 – System info Settings

System Name –edit the system name, the column length range is 1 to 255.

System Info		
Name	Value	Action
System Name	BW1253	Save Cancel
System Location	location	
System Contact	contact information	

Figure 261 –edit the system name

System Location – edit the system location, the column length range is 1 to 255.

System Info		
Name	Value	Action
System Name	BW1253	
System Location	Taipei 101	Save Cancel
System Contact	contact information	

Figure 262 –edit the system laocation

System Contact – edit the system contact, the column length range is 1 to 255.

System Info		
Name	Value	Action
System Name	BW1253	
System Location	location	
System Contact	Engineer	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Figure 263 –edit the system contact information

Save – click the button to save the change.

Cancel – restore all previous values

System | Configuration

Use the **System | Configuration** menu to download current configuration or restore specified configuration.

Configuration Backup – download current working system configuration for backup

Configuration Upload – upload system configuration for restore

Configuration Backup	
Description	Action
Configuration file to download	<input type="button" value="Preparation"/>
Configuration Upload	
Description	Action
Configuration file to upload	<input type="button" value="Browse..."/> <input type="button" value="Upload"/> <input type="button" value="Cancel"/>

Figure 264 – System Configuration settings

Click the **Preparation** button to start saving the configuration file.

Click the **Download** button to download current working configuration locally.

Configuration Backup	
Description	Action
Download and store Configuration backup file in safe place.	<input type="button" value="Download"/>

Figure 265 – Backup settings

By default the device configuration name is cfgbackup.cfg.



A configuration file name will be required when you download/save the configuration file. And please remember or re-name the file if needed. The configuration file name should only include characters or numbers. Otherwise, this configuration file will not upload to BW1253s.

You can upload saved configuration file any time you want to restore this configuration to the device by using the **Browse** button. Select the configuration file and upload it on the device:

The screenshot shows a configuration upload interface. At the top, there's a header "Configuration Upload". Below it is a table with two columns: "Description" and "Action". In the "Description" column, there's a text input field containing "C:\BW1253_cfgbackup.cfg". To the right of this field is a "Browse..." button. At the bottom of the table are two buttons: "Upload" and "Cancel".

Figure 266 – Configuration Upload/Restore - 1

Click **Upload** for upload the specified configuration and then the similar UI appears

The screenshot shows a confirmation dialog box. At the top, it says "Check it and Press **OK**, then device will reboot and the new configuration will take effect.". Below this is a "OK" button and a "Cancel" button.

Figure 267 – Configuration Upload/Restore - 2

Click OK button to restore and AP will reboot immediately to take effect.

The screenshot shows a progress bar with the text "Device is rebooting now. Please wait..." above it. Below the progress bar is a status bar showing "4% [##----]".

Figure 268 – Configuration Upload/Restore - 3

System | Reset and Reboot

Use this function to reboot device or restore to factory default.

The screenshot shows a "System Reset and Reboot" configuration screen. It has a table with two columns: "Description" and "Action". In the "Description" column, there's a text input field containing "Current firmware version: BW1253s.BR0.1.0.14". In the "Action" column, there are two buttons: "Reboot" and "Reset".

Figure 269 – System Reset setting

Reboot – reboot the device

Reset – reset System to Factory Defaults

To reboot the device, click **Reboot** and then the below appears to make sure:

The screenshot shows a confirmation dialog box. At the top, it asks "Are you sure you want to REBOOT the device? It will take some time to boot up.". Below this is a "Reboot" button and a "Cancel" button.

Figure 270 – Reboot the device

To reset the device, click **Reset** and then the below appears to make sure:

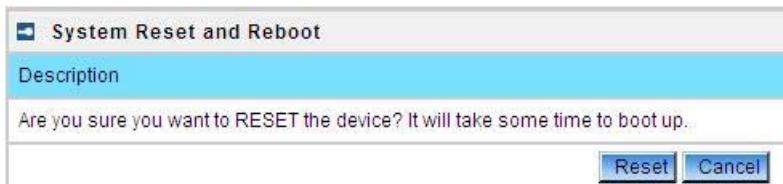


Figure 271 – Reset the device

Click reset button the device will reset and reboot immediately to take effect.



System | Local Upgrade

Upload – Update your device firmware locally.

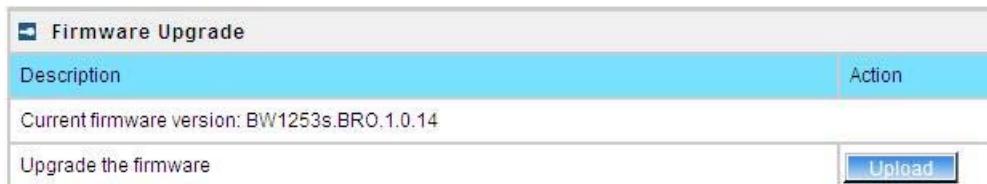


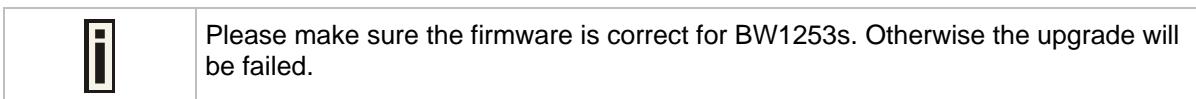
Figure 272 – Firmware Upgrade

Click the **Upload** and then click the browse button to specify the full path of the new firmware image and click the **Upload** button:



Figure 273 – Firmware Upgrade

Click the **Upgrade** button to flash and upgrade the firmware.



Firmware Upgrade	
Description	Action
Firmware image successfully uploaded. Press Upgrade button to Upgrade firmware now and reboot system.	Upgrade Cancel

Figure 274 – upgrade firmware

	Do not turn off the BW1253s during the firmware update process because the device could be damaged. It recommend to use the Ethernet connection (not wireless) for the firmware update process.
	Update firmware will take about 4 minutes.

System | TFTP Upgrade

BW1253s support firmware upgrade via TFTP server.

TFTP Firmware Upgrade		
Name	Value	Action
Current firmware version:	BW1253s.BRO.1.0.14	
TFTP server IP address		Edit
TFTP Time Out(Secs)		Edit
Firmware Filename		Edit
Download Firmware From TFTP server		Download

Figure 275 – TFTP Firmware Upgrade

Current firmware version – Show the current firmware version.

TFTP server IP address - Specify the IP address of TFTP server which firmware located.

TFTP Time Out(Secs) – Specify the TFTP server communication time out in second.

Firmware Filename – Specify the upgrade firmware name to be download.

TFTP Firmware Upgrade		
Name	Value	Action
Current firmware version:	BW1253s.BRO.1.0.14	
TFTP server IP address	61.17.23.100	
TFTP Time Out(Secs)	10	
Firmware Filename	<input type="text" value="BW1253s.BRO.1.0.15.bin"/>	Save Cancel
Download Firmware From TFTP server		Download

Figure 276 – TFTP Firmware Upgrade setting

Click “Edit” button to specify the TFTP server IP address, time out interval and firmware filename and save the configuration then press “Download” button to download the firmware.



Please make sure the firmware is correct for BW1253s. Otherwise the upgrade will be failed.



Do not turn off the BW1253s during the firmware update process because the device could be damaged. It recommend to use the Ethernet connection (not wireless) for the firmware update process.

System | Location Settings

You can define the longitude and latitude for the device information or for the NMS to locate the device location.

Location Settings	
Name	Value
Longitude	
Latitude	

[Edit](#)

Figure 277 – location setting

Click edit to enter the Longitude and Latitude in digit and dot format.

Location Settings	
Name	Value
Longitude	121.524611
Latitude	25.040917

[Save](#) [Cancel](#)

Figure 278 – edit location[longitude/latitude]

Click **save** button to save it.

Chapter 5 – User Pages (Based on XSL)

This chapter describes the user pages based on XSL format. Detailed instructions on how to change and upload new user pages are given below.

When launching his/her web browser the user's initial HTTP request will be redirected to an operator defined set of web pages, further called the "user pages". User pages are:

- **Welcome** page— the first page presented to the user.
- **Login** page— subscriber authentication page, allows the user to login to the network.
- **Logout** page— small pop-up window for logged-on user statistics and log-out function.
- **Help** page – get help with the login process.
- **Unauthorized** page – this page is displayed when web login or EAP login methods are disabled on the BW1253s for subscribers.
-

	The following mentioned user pages are factory default. The operator/owner can upload new templates for all user pages based on their designed.
	Contact with BROWAN if you need the User Pages templates samples.

User Pages Overview

Welcome Page

Welcome page is the first page a subscriber receives when he starts his web browser and enters any URL. By default it's a very simple page and provides only a link to the **login** page.



Figure 279 – Welcome Page



The operator/owner can change the **welcome** page according to their designed. See more details in section: **Changing User Pages**.

Login Page

The subscriber gets to the **login** page after clicking the link on the **welcome** page. The **login** page is loaded from the BW1253s. To get access to the network, the user should enter his authentication settings: **login name** and **password** and click the **login** button:

IP address 192.168.2.1
MAC address 00:13:D4:D8:DB:7E

login name	test
password	****
	<input type="button" value="login"/> <input type="button" value="reset"/>

Get help [here](#)

Figure 280 – Simple Login Page



The login name and password can be obtained from your Hotspot Operator.

The **login** page also displays subscriber's logical and physical network addresses (IP and MAC). Once authenticated, a **start** page appears. In addition, a smaller **logout** window (page) pops up.



The operator/owner can change the **login** page according to its needs. See more details in section: **Changing User Pages**.

Logout Page



Make sure the JavaScript is enabled on your Web browser; otherwise you will not receive the **logout** page.

The **Logout** page contains the detailed subscriber's session information and provides function for logging out of the network:

user	user1
user IP	192.168.3.2
MAC address	00904BBFC873
time length	00:00:02
download bytes	84 bytes
upload bytes	1.04 KB
download bytes left	unlimited
upload bytes left	unlimited
total bytes left	unlimited
time length left	19:59:58
bandwidth downstream	4.00 Mbps
bandwidth upstream	4.00 Mbps

Figure 281 – Logout Page

Detailed subscriber's session information includes:

Logout button – click the button to logout from the network. The log-out pop-up window closes.

Bill button – display subscriber's billing information (not include current session).

Passwd button – click the button to change subscriber's password.

User – subscriber's login name.

User IP – subscriber's logical network name (IP address).

MAC Address – subscriber's physical network address.

time length – subscriber's time length from client log on in format: [hours: minutes: seconds].

Download/upload bytes – subscriber's session download and upload statistics in bytes.

Download/upload bytes left – session download and upload bytes left for subscriber limited from RADIUS [in B, KB, MB, GB and unlimited].

Total bytes left – session total (download and upload) bytes left for subscriber limited form RADIUS [in B, KB, MB, GB and unlimited].

time length left – time length left in format: [hours: minutes: seconds].

Bandwidth downstream/upstream – available upstream and downstream bandwidth for subscriber limited from RADIUS [in bps].

Refresh button – click the button to refresh the subscriber session information.



The operator/owner can change the **logout** page interface according to its needs. See more details in section: **Changing User Pages**. All session details are further accessible via the operator XML interface.

Help Page

The screenshot shows a 'LOGIN TO' form with the following fields:

- IP address: 192.168.2.1
- MAC address: 00:13:D4:D8:DB:7E
- login name: test
- password: (redacted)
- Buttons: login, reset

Below the form is a link: Get help [here](#).

Figure 282 – Get help page

Click on the **get help** link in the **login** page for help tips related to network registration. A page appears similar to the following:

The screenshot shows a 'HELP PAGE for PAC' page with the following content:

You got to the login screen, because you are not registered to network. If you want to browse the internet, first you need to log-in. You are not required to log-in, to browse sites, which are listed on login screen bottom. This PAC also could be configured not to allow any free sites (otherwise known as walled garden).

To register to network, [go back to login screen](#), enter your login name and password and press login. If you do not have login name, ask at nearest information center where you can get/buy account information to register to network at this place.

Figure 283 – Get help page



The operator/owner can change the **help** page according to its needs. See more details in section: **Changing User Pages**.

Unauthorized Page

If web log-on method (UAM) or EAP-based authentication methods are disabled on the AC and the subscriber attempts to login to the network, he will receive the following page:

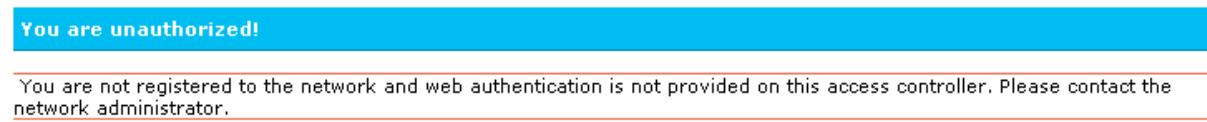


Figure 284 – Get help page



The operator/owner can change the **unauthorized** page according to its needs. See more details in section: **Changing User Pages**.

Changing User Pages

As the operator/owner you can modify the user pages freely according to your personal needs and preferences. User Page templates can be either stored locally on the AC or on an external web server.

Use the **user interface | configuration** menu to modify user pages. There are two ways to change and store new user page templates:

External – linking new user page templates from an external server.

Internal – upload new templates to local memory.

Supported user pages template formats:

XSL (Extensible Style sheet Language) for welcome/login/logout/one click pages.

HTML (Hypertext Markup Language for help/unauthorized pages.



The welcome, Login and logout pages must be in .XSL format.

The following image formats are supported for new templates. Other formats are not accepted:

- **PNG**
- **GIF**
- **JPG**

The following examples demonstrate the use of internal and external user pages.



Contact with BROWAN if you need the **User Pages templates samples**.

Example for External Pages

- Step 1** Prepare your new user pages template for each user page: welcome/login/logout/help/unauthorized.
- Step 2** Under the **user interface | configuration | pages** menu select the user page you want to change (e.g. login)

Pages				
Page	Use	Status	Location	Action
welcome	internal	enabled	welcome.xsl	
login	internal	-	login.xsl	Save Cancel
logout	internal	-	logout.xsl	
help	internal	-	/usr/local/G8000/links/help.html	
unauthorized	internal	-	/usr/local/G8000/links/unauthorized.html	

Figure 285 - configure external pages

Step 3 Choose the **external** option under the **use** column:

Pages				
Page	Use	Status	Location	Action
welcome	internal	enabled	welcome.xsl	
login	external	-	login.xsl	Save Cancel
logout	internal	-	logout.xsl	
help	internal	-	/usr/local/G8000/links/help.html	
unauthorized	internal	-	/usr/local/G8000/links/unauthorized.html	

Figure 286 - configure external pages

Step 4 Specify the new user page location in the **location** field (<http://servername/filelocation>):

Pages				
Page	Use	Status	Location	Action
welcome	internal	enabled	welcome.xsl	
login	external	-	http://192.168.2.100/login.xsl	Save Cancel
logout	internal	-	logout.xsl	
help	internal	-	/usr/local/G8000/links/help.html	
unauthorized	internal	-	/usr/local/G8000/links/unauthorized.html	

Figure 287 - configure external pages



Do not upload different type of formats. It will not be displayed properly.

Step 5 Save entered changes with the **apply changes** button:

Pages				
Page	Use	Status	Location	Action
welcome	internal	enabled	welcome.xsl	<input type="button" value="Edit"/>
login	external	-	http://192.168.2.100/login.xsl	<input type="button" value="Edit"/>
logout	internal	-	logout.xsl	<input type="button" value="Edit"/>
help	internal	-	/usr/local/G8000/links/help.html	<input type="button" value="Edit"/>
unauthorized	internal	-	/usr/local/G8000/links/unauthorized.html	<input type="button" value="Edit"/>

Caching	
Status	Action
enabled	<input type="button" value="Edit"/>
clear cached templates	<input type="button" value="Clear"/>

Figure 288 - configure external pages

Step 6 Check for new uploaded user page (e.g. login):

===== NEW LOGIN =====

login name

password

IP address 192.168.2.27

MAC address 000347C92B1C

[Get help here](#)

Figure 289 - login page



If at anytime you wish to restore factory default user pages, click the **reset** button under the **system | reset & reboot** menu.

Example for Internal Pages

We will use the **user pages** templates to show the example how to upload the internal pages. Follow the steps below:

	Contact with BROWAN if you need the User Pages templates samples .
---	---

- Step 1** Ensure that **internal** option is selected for **all** user pages you want to change. By default internal option is defined for all pages:

Pages				
Page	Use	Status	Location	Action
welcome	internal	enabled	welcome.xsl	Edit
login	internal	-	login.xsl	Edit
logout	internal	-	logout.xsl	Edit
help	internal	-	/usr/local/G8000/links/help.html	Edit
unauthorized	internal	-	/usr/local/G8000/links/unauthorized.html	Edit

Figure 290 - internal pages

- Step 2** Under the **user | upload** menu click the **upload** button to upload new prepared user pages:

Upload	
Description	Action
Before uploading new template files and images, please delete old files. There is limited space on server for templates and images.	Delete
Upload new template files and images. Old files will be overwritten, if exist with the same name. If you need, you can repeat upload process few times, until upload all needed images (you do not need to upload template files twice). Please remember, that server space is limited! All files will be uploaded to "images" directory, please prepare your templates to use images and stylesheets from that directory.	Upload

Figure 291 - upload page

	The memory space in the AP for internal user pages is limited to 1 MB .
---	--

- Step 3** Specify the location of new user page templates by clicking the **browse** button or enter the location manually.

Specify the location for the additional files of new user page templates: images and a cascading style sheet file (**css**) by clicking the **browse** button or enter the location manually:

Upload		
user template files		
welcome.xsl	D:\Data\P-720\cd content\Examples\welcome.xsl	<input type="button" value="Browse.."/>
login.xsl	D:\Data\P-720\cd content\Examples\login.xsl	<input type="button" value="Browse.."/>
logout.xsl	D:\Data\P-720\cd content\Examples\logout.xsl	<input type="button" value="Browse.."/>
help.html	D:\Data\P-720\cd content\Examples\help.html	<input type="button" value="Browse.."/>
unauthorized.html	D:\Data\P-720\cd content\Examples\unauthorized.html	<input type="button" value="Browse.."/>
oneclickuser.xsl		<input type="button" value="Browse.."/>
images and stylesheet (css) files for templates		
additional file 01	D:\Data\P-720\cd content\Examples\images\login.css	<input type="button" value="Browse.."/>
additional file 02	D:\Data\P-720\cd content\Examples\images\logout.css	<input type="button" value="Browse.."/>
additional file 03	D:\Data\P-720\cd content\Examples\images\background.gif	<input type="button" value="Browse.."/>
additional file 04	D:\Data\P-720\cd content\Examples\images\entr.gif	<input type="button" value="Browse.."/>
additional file 05	D:\Data\P-720\cd content\Examples\images\logo.gif	<input type="button" value="Browse.."/>
additional file 06	D:\Data\P-720\cd content\Examples\images\right.gif	<input type="button" value="Browse.."/>
additional file 07	D:\Data\P-720\cd content\Examples\images\top.gif	<input type="button" value="Browse.."/>
additional file 08		<input type="button" value="Browse.."/>
additional file 09		<input type="button" value="Browse.."/>
additional file 10		<input type="button" value="Browse.."/>
<input type="button" value="upload"/> <input type="button" value="Cancel"/>		

Figure 292 - upload template files

Step 4 Click the **upload** button to upload specified templates and files.



You do not need to upload all additional files at once. You can repeat the upload process a number of times until all necessary images are uploaded.

Step 5 Check for the newly uploaded user pages and images to ensure that everything is uploaded and displayed correctly. Go to the link:

<https://<device-IP-address>/> to get to the new user **welcome** page:



Figure 293 - customize welcome page

Click the **here** link or enter the link directly:

<https://<device-IP-address>/login.user> to get to the new user **login** page:



Figure 294 - customize login page



If at anytime you wish to restore the factory default user pages, click the **reset** button under the **system | reset & reboot** menu.

Extended UAM

The **Extensions** feature (**User** menu) allows an external Web Application Server (WAS) to intercept/take part in the user authentication process externally log on and log off the user as necessary. It provides means to query user session information as well.

See the following schemes to understand how the remote client authentication works.

Scheme 1:

The remote authentication method when client's authentication request is re-directed to the external server (WAS):

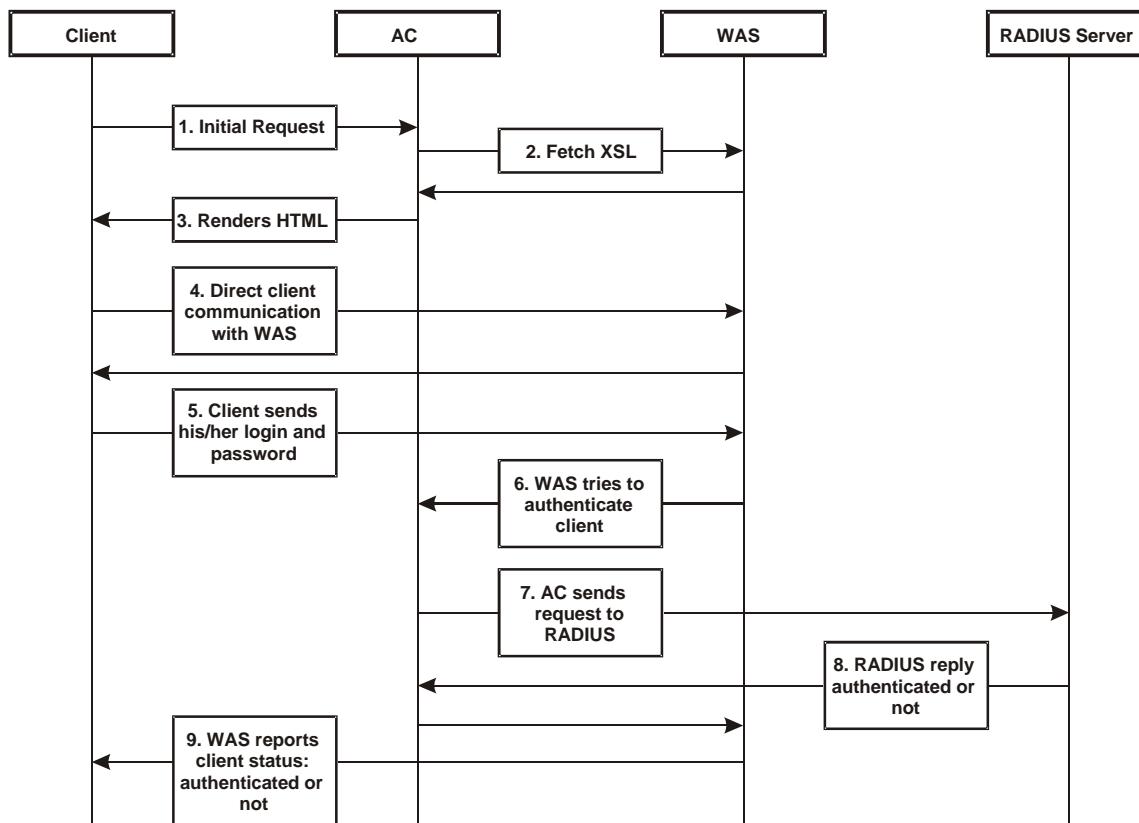


Figure 295 – Client Remote Authentication Scheme (1)

The Client initiates (1) authentication process. AC intercepts any access to the Internet via HTTP and redirects the client to the **welcome**, or **login** URL on AC. In order to render the custom login screen HTML page, the AC must be configured to (2) fetch .XSL script from a remote server, which in this case is a Web Application Server (WAS), or have custom .XSL uploaded on the AC. There is the ability to enable caching of .XSL scripts (see: **User | Pages**), thus avoiding fetching of the same document every time a client requests authentication.

The AC (3) uses .XSL script to render HTML output, which is done by feeding a XML document to a parsed and prepared for rendering .XSL script. The latter XML document contains all needed information for Web Application Server like user name, password (if one was entered), user IP address, MAC address and NAS-Id. Custom .XSL script must generate initial welcome/login screen so that it embeds all the needed information in a HTML FORM element as hidden elements and POST data not back to the AC, but to the Web Application Server (5). Thereafter the client communicates directly with the Web Application Server.

When the Web Application server has all needed data from the client, it must try to authenticate (6) the client. Authentication is done by the RADIUS server but through the AC. At this step the **shared secret** is used to make the connection between the WAS and the AC. The AC re-sends the authentication request to the RADIUS server (7). Depending on the status, appropriate authentication status must be returned back to the WAS but through the AC (8). In step (9), the Web Application Server knows the client authentication status and reports success or failure back to the client.



The Web Application Server (WAS) must be configured as a free site in the Walled Garden area.

There is an ability to skip the rendering initial user pages from the .XSL. See the following scheme when the user initial request is redirected to the specified location.

Scheme 2:

The remote authentication method when client with proxy authentication request is re-directed to the external server (WAS):

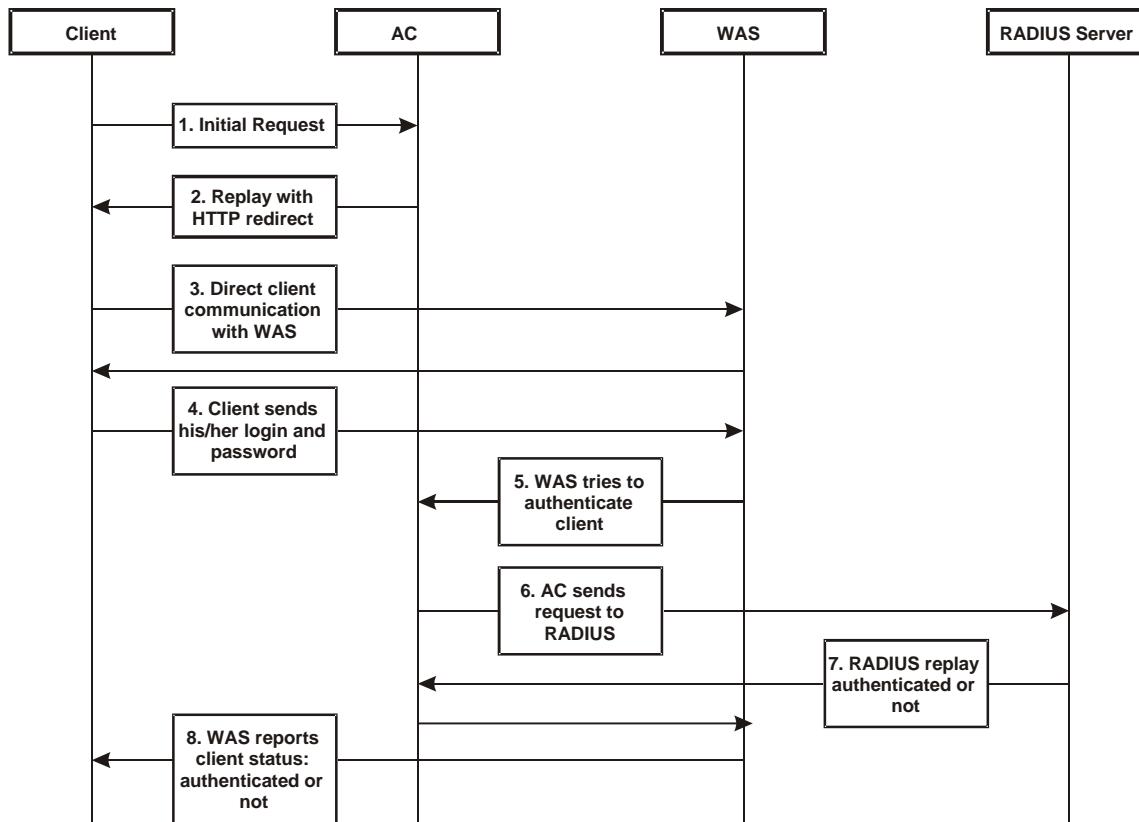


Figure 296 – Client Remote Authentication Scheme (2)

The initial client request (1) can be redirected to the specified location, as **redirection URL** on the Web Application server. In such case the client who wants to authenticate gets the redirection from AC (2). In other words the AC intercepts any access to the Internet via HTTP and redirects the client to the defined **welcome**, or **login** URL on WAS (also see: **User | Pages**). The further actions are the same as described in the **Scheme 1** (Figure 295 – Client Remote Authentication Scheme (1)).



The WAS location URL under welcome page redirect must be configured as a free site in the Walled Garden area.

To define such redirection URL use the **user | pages** menu. Enable **welcome** page, set the **redirect** setting and specify the redirect location for such authentication process (also see: **User | Pages**).

Parameters Sent to WAS

Parameters that are send to the external server (WAS) using the remote user authentication method (UAM).

Parameter	Description	Comments
nasid	NAS server ID value	Can be specified under the Network RADIUS Properties menu
nasip	WAN IP address for WAS	Can be changed or specified under the Network Interface menu.
clientip	Client IP address	Cannot be defined manually.
mac	Client MAC address	Cannot be defined manually.
ourl	Initial URL where not authorized client enter to his/her browser and tries to browse. After authentication the client is redirected in this URL	Optional.
sslport	HTTPS port number of AC (by default: 443).	Not configurable.
lang	Parameter "accept-language" from client browser request	Optional.
Lanip	The IP address of the LAN interface the user is connected to.	Can be changed or specified under the Network Interface menu.

In order to logon, log-off or get user status WAS submits POST request to the following URLs:

1. Remote user logon

Script name: pplogon.user

Parameters:

secret	shared secret, to protect page from accidental use
ip	IP address of user to be logged on.
Username	Username of the user to be logged on.
password	Password of the user to be logged on.

All parameters are required.

Script call example:

```
https://P720/pplogon.user?secret=sharedSecret&ip=<user_IP_address>&username=<userName>&password=<UserPassword>
```

Script produces XML output:

```
<logon>
<status>Ok</status>
<error>0</error>
<description>User logged on.</description>
<replymessage>Hello user!</replymessage>
</logon>
```

Response status and error codes:

status	error	description
OK	0	User is logged on.
Not checked	100	Logon information not checked.
No IP	101	No user IP address supplied.
No username	102	No username supplied.

Disabled	103	Remote authentication is disabled.
Bad secret	104	Incorrect shared secret supplied.
No password	105	No user password.
OK	110	User already logged on.
Failed to authorize	111	Failed to authorize user.
Bad password	112	Incorrect username or/and password.
Network failed	113	Network connection failed.
Accounting error	114	Accounting error.
Too many users	115	Too many users connected.
Unknown authorization error	120	Unknown authorization error.

<replymessage> is RADIUS Reply-Message attribute value. If RADIUS responds with Reply-Message(s), they are added to logon response. If RADIUS does not respond with Reply-Message, <replymessage> attribute is not added to output XML.

2. Remote user log-off

Script name: pplogoff.user

Parameters:

secret	shared secret, to protect page from accidental use
ip	IP address of user to be logged off.
username	Username of the user to be logged off.
mac	AC address of the user to be logged off.

All parameters are required, except the IP and MAC. At least one of IP and MAC addresses should be supplied. If supplied only IP, user is checked and logged off by username and IP. If IP and MAC addresses are supplied, then user is checked and logged off by username, IP and MAC addresses.

Script call example:

```
https://P720/pplogoff.user?secret=sharedSecret&username=UserName&ip=<user_IP_address>
```

Script produces XML output:

```
<logoff>
<status>Ok</status>
<error>0</error>
<description>User logged off.</description>
</logoff>
```

Response statuses and error codes:

status	error	Description
OK	0	User is logged off.
Not checked	100	Logoff information not checked.
No username	102	No username supplied.
Disabled	103	Remote authentication is disabled.
Bad secret	104	Incorrect shared secret supplied.
No IP/MAC	106	No user IP and/or MAC address supplied.
No user by MAC	121	User with supplied MAC address not

		found.
No user by IP	122	User with supplied IP address and username not found.
No user by IP and MAC	123	User with supplied IP, MAC addresses and username not found.
Failed to logoff	131	Failed to logoff user.
Cannot resolve IP	132	Cannot resolve user IP.
Unknown logoff error	140	Unknown logoff error.

3. Remote user status

- Script name: ppstatus.user
- Parameters:
 - secret shared secret, to protect page from accidental use
 - ip IP address of user to get status.
 - username Username of the user to get status.

All parameters are required.

Script call example:

```
https://P720/ppstatus.user?secret=sharedSecret&username=UserName&ip=<user_IP_address>
```

Script produces XML output:

- XML output, when some error occurs:

```
<ppstatus>
  <status>No user by IP</status>
  <error>122</error>
  <description>User with supplied IP address not found.</description>
</ppstatus>
```

Response statuses and error codes:

status	error	description
OK	0	User status is ok.
Not checked	100	Status information not checked.
No IP	101	No user IP address supplied.
No username	102	No username supplied.
Disabled	103	Remote authentication is disabled.
Bad secret	104	Incorrect shared secret supplied
No user by IP	122	User with supplied IP address not found.
No user by IP and username	141	User with supplied IP address and username not found.

- XML output when no errors and user statistics got successfully:

```
<ppstatus>
  <status>Ok</status>
  <error>0</error>
  <description>Got user status.</description>
```

```

<entry id="1">g17</entry>
<entry id="2">192.168.2.117</entry>
<entry id="3">200347C92B63</entry>
<entry id="4">00:00:05</entry>
<entry id="5">3E64C7967A36</entry>
<entry id="6">00:01:10</entry>
<entry id="7">0 bytes</entry>
<entry id="8">0 bytes</entry>
<entry id="9">testlab</entry>
<entry id="10">unlimited</entry>
<entry id="11">unlimited</entry>
<entry id="12">unlimited</entry>
<entry id="13">32 Mbps</entry>
<entry id="14">32 Mbps</entry>
<entry id="15">04:59:55</entry>
<entry id="16">EAP</entry>
</ppstatus>

```

Status detailed information by ID:

id	description
1	User name
2	User IP address
3	User MAC address
4	Session time
5	Session ID
6	User idle time
7	Output bytes
8	Input bytes
9	User WISP name
10	Remaining bytes
11	Remaining output bytes
12	Remaining input bytes
13	Bandwidth upstream
14	Bandwidth downstream
15	Remaining session time
16	Authentication method

Chapter 6 – Customized User page (HTML)

This chapter assist you on configuring BW1253s customized login/logout pages using the BROWAN sample templates. There are coffee bar and general samples. User can also create a personalized login/logout pages based on the provided sample templates.



Contact with BROWAN if you need the templates samples.

Set up your customized user page

Step1. Configure and Upload Customized Login/Logout Page files

Login BW1253s as super administrator and go to **User | Customized UAM**.

In order to configure BW1253s using the customized login/logout page, Customize Page status must be set to enable.

To enable Customized Page, edit the Customize page status(**User | Customized UAM**) and set to **Enabled**. See the diagram below:

Customized UAM		
Description	Status	Action
Use SSL	disabled	Edit
Customize Page	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Save Cancel

Figure 297 – enable customize page status

Customized UAM		
Description	Status	Action
Use SSL	disabled	Edit
Customize Page	enabled	Edit
Pop Logout Page	enabled	Edit
Logout Page width size: 350 Logout Page Height size: 390		Edit
Use External Page	disabled	Edit
Update HTML Files		
Description		Action
Delete all uploaded HTML and images files!		Delete
Upload HTML and image files!		Upload
See example login html page here and See example logout html page here		
Uploaded File List		

Figure 298 – customize page status is enabled

To start to upload the customized template files, click the upload button. (We will use the coffee bar style template files that BROWAN provided for this demonstration).

After clicking the upload button, an **Update Custom UAM Files** screen will appear. (See diagram below).

Customized UAM		
Description	Status	Action
Use SSL	disabled	<input type="button" value="Edit"/>
Customize Page	enabled	<input type="button" value="Edit"/>
Pop Logout Page	enabled	<input type="button" value="Edit"/>
Logout Page width size: 350 Logout Page Height size: 390		
Use External Page	disabled	<input type="button" value="Edit"/>
Update Custom UAM Files		
Login File	<input type="text"/>	<input type="button" value="Browse.."/>
Logout File	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 01	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 02	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 03	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 04	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 05	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 06	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 07	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 08	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 09	<input type="text"/>	<input type="button" value="Browse.."/>
Additional file 10	<input type="text"/>	<input type="button" value="Browse.."/>
<input type="button" value="Upload"/> <input type="button" value="Cancel"/>		

Figure 299 – upload files

Enter the physical path and filename of the coffee template files, or click the “**browse**” button to search the coffee template files are located.



The first two items are for login.html and logout.html files only. Additional files are for CSS and image files, such as jpg, gif, png and etc.

Update Custom UAM Files

Login File	D:\Data\P720\cd content\Examples(HTML)\coffee\login.htm	<input type="button" value="Browse.."/>
Logout File		<input type="button" value="Browse.."/>
Additional file 01		<input type="button" value="Browse.."/>
Additional file 02		<input type="button" value="Browse.."/>
Additional file 03		<input type="button" value="Browse.."/>
Additional file 04		<input type="button" value="Browse.."/>
Additional file 05		<input type="button" value="Browse.."/>
Additional file 06		<input type="button" value="Browse.."/>
Additional file 07		<input type="button" value="Browse.."/>
Additional file 08		<input type="button" value="Browse.."/>
Additional file 09		<input type="button" value="Browse.."/>
Additional file 10		<input type="button" value="Browse.."/>

Figure 300 – upload login.html

After entering all the template files, press upload button to start the uploading files to BW1253s.



Only ten Additional files can be uploaded at one time. To upload more additional file, repeat the same upload process in step 2-4, but please be aware of the first two items are only for login.html and logout.html files. Image files can only be uploaded to Additional file fields

Update Custom UAM Files

Login File	D:\Data\P720\cd content\Examples(HTML)\coffee\login.htm	<input type="button" value="Browse.."/>
Logout File	D:\Data\P720\cd content\Examples(HTML)\coffee\logout.htm	<input type="button" value="Browse.."/>
Additional file 01	D:\Data\P720\cd content\Examples(HTML)\coffee\images\but.gif	<input type="button" value="Browse.."/>
Additional file 02	D:\Data\P720\cd content\Examples(HTML)\coffee\images\but_ove	<input type="button" value="Browse.."/>
Additional file 03	D:\Data\P720\cd content\Examples(HTML)\coffee\images\icon2.jp	<input type="button" value="Browse.."/>
Additional file 04	D:\Data\P720\cd content\Examples(HTML)\coffee\images\icon.gif	<input type="button" value="Browse.."/>
Additional file 05	D:\Data\P720\cd content\Examples(HTML)\coffee\images\line.gif	<input type="button" value="Browse.."/>
Additional file 06	D:\Data\P720\cd content\Examples(HTML)\coffee\images\login_0	<input type="button" value="Browse.."/>
Additional file 07	D:\Data\P720\cd content\Examples(HTML)\coffee\images\login_0	<input type="button" value="Browse.."/>
Additional file 08	D:\Data\P720\cd content\Examples(HTML)\coffee\images\login_0	<input type="button" value="Browse.."/>
Additional file 09	D:\Data\P720\cd content\Examples(HTML)\coffee\images\login_0	<input type="button" value="Browse.."/>
Additional file 10	D:\Data\P720\cd content\Examples(HTML)\coffee\images\login_0	<input type="button" value="Browse.."/>

Figure 301 – upload other files

Once all files are uploaded successfully, a list of Uploaded File List will show.

Update HTML Files	
Description	Action
Delete all uploaded HTML and images files!	Delete
Upload HTML and image files!	Upload
See example login html page here and See example logout html page here	
Uploaded File List	
aclogin.html	
aclogout.html	
but.gif	
but_over.gif	
icon.gif	
icon2.jpg	
line.gif	
login_01.jpg	

Figure 302 – files have been uploaded

Verify if all files are uploaded successfully

Step2. Configure the pixels of logout window.

The README file in each template directory contains the information of the pixels settings for the logout page. Enter the width size and height size setting of logout page and press the **Save** button. E.g. the coffee bar template, the suggested size of logout page is 760 x 601.

Customized UAM		
Description	Status	Action
Use SSL	disabled	Edit
Customize Page	enabled	Edit
Pop Logout Page	enabled	Edit
Logout Page width size: <input type="text" value="760"/>	Logout Page Height size: <input type="text" value="601"/>	Save Cancel
Use External Page	disabled	Edit

Figure 303 – set the pixels of logout window

Step3. Everything is ready

Now, any users that access the internet via the BW1253s will see the new personalized login and logout pages.

Let's look at the new appearance of login and logout page based on the coffee bar template.

	Make sure your computer is in the same network with BW1253s and enter https://device IP address for the customized page test.
---	--



Figure 304 – example of coffee bar login page

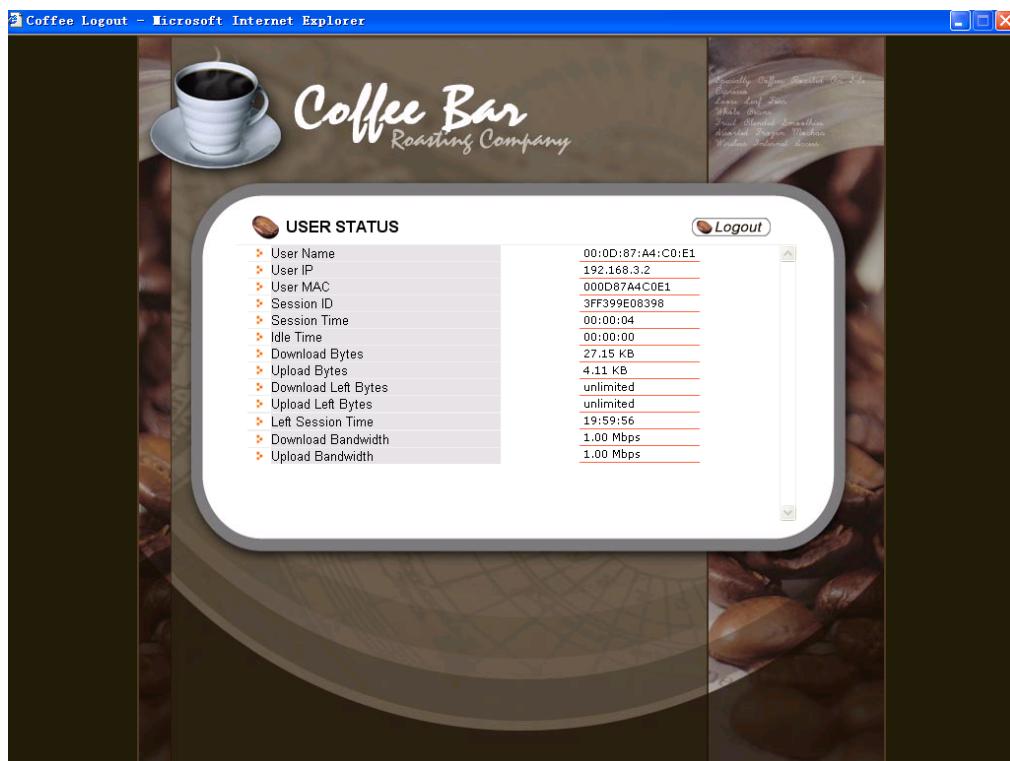


Figure 305 – example of coffee bar logout page

FAQ

1. **Question:** How to add some links that could be accessed without authentication?

Answer: These authentication-free sites for users are so called “walled garden” area. Please refer to the user's guide to do the relating settings.

2. **Question:** How to hide the user login session information from my customers?

Answer: You can find these set of html code in logout.html we provided:

```
<td width="265" valign="top"><iframe src="logout.user?cmd=status" width="250" height="240" marginwidth="0" marginheight="0" scrolling="yes" frameborder="0"></iframe></td>
```

These set of code uses an embedded window to show the session data in logout window. Comment them with HTML comments language “<!--” and “//-->” will hide the session data in logout window.

3. **Question:** If I don't want the logout window to pop-up to users, how could I do?

Answer: Please login BW1253s and go to **User | Customized UAM** to disable “pop logout page.”

4. **Question:** If I close the logout window, how can I logout?

Answer: 1. just un-plug your wireless card, or un-plug your network cable if you use a wired card.
2. Open a browser window, and input the URL: “logout.usr”, then you will be redirect to logout window.

Appendix

A) Specification

Wireless

Standard	IEEE 802.11b(DSSS), IEEE 802.11g(OFDM) and IEEE 802.11a(OFDM)
	802.11n : 300,270,240,200,180,150,120,100,54,48,36,24,18,12,11,9,6,5.5,2,1Mbps
Data Rate	802.11a : 54,48,36,24,18,12,9,6Mbps 802.11g : 54,48,36,24,18,12,9,6Mbps 802.11b : 11,5.5,2,1Mbps (auto fallback)
Transmit Power (adjustable RF power)	Max. 20 dBm ± 2dBm @6~24Mbps Max. 13 dBm ± 2dBm @54Mbps

Antennas

Antennas	2 Dual-band Dipole Antennas with RP-SMA plug connector
----------	--

Encryption

Encryption	WPA/WPA2 (TKIP and CCMP-AES) , Dynamic/static 64bits and 128bits WEP
------------	--

DynamicBridge

DynamicBridge	Up to 31 bridge links
---------------	-----------------------

Interface

LAN	10/100/100Mb Ethernet, auto sensing, RJ-45
-----	--

Console

Console	1 for RJ-45 interface
---------	-----------------------

Management

Interfaces	HTTPs, Secure Telnet(SSHv2), SNMP
------------	-----------------------------------

Software Update

Software Update	Remote software update via HTTPs
-----------------	----------------------------------

Reset

Reset	H/W and S/W restore factory default
-------	-------------------------------------

Physical Specification

Dimension	175 mm x 135 mm x 27 mm
-----------	-------------------------

Weight

Weight	520g
--------	------

Environment Specification

	Temperature	Humidity
Operating	0 to +50°C	20% to 90%, non-condensing

Power Supply

POE	48V, IEEE802.3af-2003 compliance
-----	----------------------------------

Power adaptor

Power adaptor	External power supply, input: 100-240 VAC, 50-60Hz and output: 12VDC
---------------	--

LEDs

4 LEDs	Power,MODE, LAN, WLAN
--------	-----------------------

Warranty

1 years	
---------	--

Package Contents

▪ BW1253s Indoor Access Point	▪ Ethernet patch cable
▪ Screw Bag	▪ 2xAntennas
▪ power supply	▪

Related Products

Controllers:	BG-6020G/G-4200 Public Access Controller	
Access Points:	BW1254 dual radio 802.11a/b/g/n hotspot indoor access point	BW2251 dual radio 802.11a/b/g/n hotspot outdoor access point

B) Factory Defaults for the BW1253s

Network Interface Configuration Settings

Operation Mode

Mode AP

Network | Interface

AP Mode (Default)

Interface	Br0
Type	LAN
IP Address	192.168.2.2
Netmask	255.255.255.0
Gateway	0.0.0.0

AP Router Mode

Interface	eth1
Type	WAN
IP Address	192.168.2.2
Netmask	255.255.255.0
Gateway	192.168.2.1
Interface	Wlan1
Type	LAN
IP Address	192.168.3.1
Netmask	255.255.255.0
Gateway	eth1

Network | RADIUS Properties

RADIUS Retries	5
RADIUS Timeout	2
NAS Server ID	-
User Session Timeout	72000
User Accounting Update Interval	600
User Accounting Update Retry	60
User Idle Timeout	900
Bandwidth Up	512 Kbits
Bandwidth Down	512 Kbits

Network | RADIUS Servers

Name	DEFAULT (default)
Type	Authentication

IP Address	0.0.0.0
Port	1812
Secret	password (case sensitive)
Type	Accounting
IP Address	0.0.0.0
Port	1813
Secret	secret (case sensitive)
User Password Md5sum Secret	disabled

Network | DHCP Server**DHCP Server**

Status	Disabled
IP Address from	192.168.3.3
IP Address to	192.168.3.254
Netmask	255.255.255.0
Gateway	192.168.3.1
WINS Address	0.0.0.0
Lease Time (seconds)	86400
DNS address	0.0.0.0
DNS Secondary address	0.0.0.0

Network | DNS (only for AP router mode)

Type	Primary
IP Address	0.0.0.0
Type	Secondary
IP Address	0.0.0.0

Network | Static Route (only for AP router mode)

No routes are defined on system.

WISP

No WISP defined on system.

Wireless | Basic

Regulatory Domain	FCC
Channels	11(static)
Wireless Band	2.4GHz(Mixed 11g)
Total Output Power(EIRP)	14dBm
RTS Threshold	2347bytes
Layer2 Isolation	disabled
Operation Mode	AP

Wireless | Advanced

SSID	BW1253-11g
Hidden SSID	Disabled
Security	Disabled

Wireless | MSSID

No multiple BSSID entry

Wireless | WEP

Status	Disabled
Key1 to Key4	aaaaa

Wireless |MAC ACL

ACL Policy	Disabled
------------	----------

User Settings

User | Customized UAM (Only for AP router mode)

Use SSL	Disabled
Customize Page	Disabled

User | Station Supervision

Interval	20
Failure count	3

User | WISP(Only for AP router mode)

Domain Policy	Username@domain
No WISP defined on system	

System Settings

System | Administrator

Super administrator:	Username: admin (case sensitive) Password: admin01 (case sensitive)
----------------------	--

System | SNMP

SNMP Service	Enabled
Readonly Community	public
Readwrite Community	private
Default Trap Community	public

There are no SNMP traps on system.

System | Telnet

Telnet Service	Enabled
SSH Service	Enabled

System | NTP

NTP Service	Disabled
Time Zone	GMT-12:00

There are no NTP Server settings on system.

System | Time

Date	1970/01/01
------	------------

System | System Log

Remote Log Status	Disabled
-------------------	----------

Host IP	192.168.2.1
Log Level	info
Local Log Status	Enabled
Log Limit(bytes)	102400
Log Level	info

C) Location ID and ISO Country Codes

This list states the **country names** (official short names in English) in alphabetical order as given in ISO 3166-1 and the corresponding **ISO 3166-1-alpha-2 code elements**.

It lists 239 official short names and code elements.

Location ID	Country	Location ID	Country
AF	Afghanistan	LI	Liechtenstein
AL	Albania	LT	Lithuania
DZ	Algeria	LU	Luxembourg
AS	American Samoa	MO	Macao
AD	Andorra	MK	Macedonia, the former Yugoslav republic of
AO	Angola	MG	Madagascar
AI	Anguilla	MW	Malawi
AQ	Antarctica	MY	Malaysia
AG	Antigua and Barbuda	MV	Maldives
AR	Argentina	ML	Mali
AM	Armenia	MT	Malta
AW	Aruba	MH	Marshall islands
AU	Australia	MQ	Martinique
AT	Austria	MR	Mauritania
AZ	Azerbaijan	MU	Mauritius
BS	Bahamas	YT	Mayotte
BH	Bahrain	MX	Mexico
BD	Bangladesh	FM	Micronesia, federated states of
BB	Barbados	MD	Moldova, republic of
BY	Belarus	MC	Monaco
BE	Belgium	MN	Mongolia
BZ	Belize	MS	Montserrat
BJ	Benin	MA	Morocco
BM	Bermuda	MZ	Mozambique
BT	Bhutan	MM	Myanmar

BO	Bolivia	NA	Namibia
BA	Bosnia and Herzegovina	NR	Nauru
BW	Botswana	NP	Nepal
BV	Bouvet island	NL	Netherlands
BR	Brazil	AN	Netherlands Antilles
IO	British Indian ocean territory	NC	New Caledonia
BN	Brunei Darussalam	NZ	New Zealand
BG	Bulgaria	NI	Nicaragua
BF	Burkina Faso	NE	Niger
BI	Burundi	NG	Nigeria
KH	Cambodia	NU	Niue
CM	Cameroon	NF	Norfolk island
CA	Canada	MP	Northern Mariana islands
CV	Cape Verde	NO	Norway
KY	Cayman islands	OM	Oman
CF	Central African republic	PK	Pakistan
TD	Chad	PW	Palau
CL	Chile	PS	Palestinian territory, occupied
CN	China	PA	Panama
CX	Christmas island	PG	Papua new guinea
CC	Cocos (keeling) islands	PY	Paraguay
CO	Colombia	PE	Peru
KM	Comoros	PH	Philippines
CG	Congo	PN	Pitcairn
CD	Congo, the democratic republic of the	PL	Poland
CK	Cook islands	PT	Portugal
CR	Costa Rica	PR	Puerto Rico
CI	Côte d'ivoire	QA	Qatar
HR	Croatia	RE	Réunion
CU	Cuba	RO	Romania
CY	Cyprus	RU	Russian federation
CZ	Czech republic	RW	Rwanda
DK	Denmark	SH	Saint Helena
DJ	Djibouti	KN	Saint Kitts and Nevis
DM	Dominica	LC	Saint Lucia
DO	Dominican republic	PM	Saint Pierre and Miquelon
EC	Ecuador	VC	Saint Vincent and the grenadines
EG	Egypt	WS	Samoa
SV	El Salvador	SM	San Marino
GQ	Equatorial guinea	ST	Sao tome and Principe
ER	Eritrea	SA	Saudi Arabia

EE	Estonia	SN	Senegal
ET	Ethiopia	SC	Seychelles
FK	Falkland islands (malvinas)	SL	Sierra Leone
FO	Faroe islands	SG	Singapore
FJ	Fiji	SK	Slovakia
FI	Finland	SI	Slovenia
FR	France	SB	Solomon islands
GF	French Guiana	SO	Somalia
PF	French Polynesia	ZA	South Africa
TF	French southern territories	GS	South Georgia and the south sandwich islands
GA	Gabon	ES	Spain
GM	Gambia	LK	Sri Lanka
GE	Georgia	SD	Sudan
DE	Germany	SR	Suriname
GH	Ghana	SJ	Svalbard and Jan Mayan
GI	Gibraltar	SZ	Swaziland
GR	Greece	SE	Sweden
GL	Greenland	CH	Switzerland
GD	Grenada	SY	Syrian Arab republic
GP	Guadeloupe	TW	Taiwan, province of china
GU	Guam	TJ	Tajikistan
GT	Guatemala	TZ	Tanzania, united republic of
GN	Guinea	TH	Thailand
GW	Guinea-Bissau	TL	Timor-leste
GY	Guyana	TG	Togo
HT	Haiti	TK	Tokelau
HM	Heard island and McDonald islands	TO	Tonga
VA	Holy see (Vatican city state)	TT	Trinidad and Tobago
HN	Honduras	TN	Tunisia
HK	Hong Kong	TR	Turkey
HU	Hungary	TM	Turkmenistan
IS	Iceland	TC	Turks and Caicos islands
IN	India	TV	Tuvalu
ID	Indonesia	UG	Uganda
IR	Iran, Islamic republic of	UA	Ukraine
IQ	Iraq	AE	United Arab emirates
IE	Ireland	GB	United kingdom
IL	Israel	US	United states
IT	Italy	UM	United states minor outlying islands
JM	Jamaica	UY	Uruguay
JP	Japan	UZ	Uzbekistan

JO	Jordan	VU	Vanuatu
KZ	Kazakhstan		Vatican city state see holy see
KE	Kenya	VE	Venezuela
KI	Kiribati	VN	Viet nam
KP	Korea, democratic people's republic of	VG	Virgin islands, British
KR	Korea, republic of	VI	Virgin islands, u.s.
KW	Kuwait	WF	Wallis and Futuna
KG	Kyrgyzstan	EH	Western Sahara
LA	Lao people's democratic republic	YE	Yemen
LV	Latvia	YU	Yugoslavia
LB	Lebanon		Zaire see Congo, the democratic republic of the
LS	Lesotho	ZM	Zambia
LR	Liberia	ZW	Zimbabwe
LY	Libyan Arab Jamahiriya		