

BROWAN

BW1330 High Performance Hotspot Access Point

User Guide
Version 1.0
September, 2006

www.browan.com

Copyright©2006 BROWAN Communications, Inc.

Copyright

© 2002-2006 Browan Communications.

This user's guide and the software described in it are 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 Communications.



Notice

Browan Communications reserves the right to change specifications without prior notice.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Browan Communications 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 Communications.

Trademarks

The product described in this book is a licensed product of Browan Communications.

Microsoft, Windows 95, Windows 98, Windows Millennium, Windows NT, Windows 2000, Windows XP, 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.



National Radio Regulations

The usage of wireless network components is subject to national and or regional regulations and laws. Administrator must ensure that they select the correct radio settings according to their regulatory domain. Refer to the **B) Regulatory Domain/Channels** chapter in the appendix to get more information on regulatory domains. Please check the regulations valid for your country and set the parameters concerning frequency, channel, and output power to the permitted values!



FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

FCC Caution

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.



CE Mark Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.



R&TTE Compliance Statement

This equipment complies with all the requirements of the Directive 1999/5/EC of the European Parliament and the Council of 9 March 1999 on Radio Equipment and Telecommunication Terminal Equipment and the Mutual Recognition of their Conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not Intended for Use

None..

Contents

Copyright	1
Notice	1
Trademarks	1
National Radio Regulations.....	1
FCC Warning.....	2
CE Mark Warning	2
R&TTE Compliance Statement	2
CONTENTS	3
ABOUT THIS GUIDE.....	7
Purpose	7
Prerequisite Skills and Knowledge.....	7
Conventions Used in this Document	7
Help Us to Improve this Document!	7
Browan Communications Technical Support	7
CHAPTER 1 – INTRODUCTION	8
Product Overview	8
Management Options.....	8
The BW1330 Features	9
CHAPTER 2 – INSTALLATION	10
The Product Package.....	10
Hardware Introduction.....	11
General Overview	11
Back Panel.....	12
LEDs	12
Connectors.....	13
Stand.....	14
Wall Mount.....	14
Connecting the Access Controller.....	15
Initialization.....	16
Access Your BW1330.....	16
Software Introduction: KickStart	17
Step by Step Setup	20
CHAPTER 3 – UNIVERSAL ADDRESS TRANSLATION	23
What is UAT	23
UAT Principle	23
UAT Limitation.....	23
CHAPTER 4 – USER PAGES (BASED ON XSL).....	25
User Pages Overview.....	25
Welcome Page.....	25
Login Page.....	25
Logout Page.....	26
Help Page	27
Unauthorized Page	27
Example for External Pages	28
Example for Internal Pages	30
Extended UAM	33
Parameters Sent to WAS.....	35

CHAPTER 5 – CUSTOMIZED USER PAGE (HTML)	39
Determine Your Access Policy	39
Configure Authentication-Free Access Policy	39
FAQ	45
CHAPTER 6 – COMMAND LINE INTERFACE	46
Introduction.....	46
Get Connection to CLI.....	46
Telnet Connection.....	46
SSH Connection	47
Terminal Connection.....	47
Login.....	47
Connection	48
Network	48
User	51
Status	52
System.....	53
Telnet.....	53
Reboot.....	53
Reset	53
Exit.....	53
CHAPTER 7 – SNMP MANAGEMENT	54
Introduction.....	54
SNMP Versions	54
SNMP Agent.....	55
SNMP Community Strings.....	55
Use SNMP to Access MIB.....	55
BROAN Private MIB	56
CHAPTER 8 – REFERENCE MANUAL	57
Web Interface	57
Network Interface	59
Network Interface Configuration Interface Configuration.....	59
Network Interface Configuration Bridge.....	60
Network Interface Configuration VLAN.....	62
Network Interface Configuration Route.....	63
Network Interface Configuration Port Forwarding	64
Network Interface Configuration DHCP Relay.....	65
Network Interface Configuration User ACL.....	65
Network Interface Configuration Management Subnet.....	66
Network Interface DNS	67
Network Interface DHCP	68
Network Interface POP3	70
Network Interface RADIUS	70
Network Interface RADIUS Settings.....	70
Network Interface RADIUS Servers.....	72
Network Interface RADIUS WISP.....	74
Network Interface RADIUS Proxy.....	75
Network Interface RADIUS Accounting Backup	76
Network Interface Tunnels.....	77
Network Interface Tunnels PPPoE/GRE	77
Network Interface Tunnels GRE Client for VPN	78
Network interface wireless Basic	80
Network interface wireless Advance.....	82
Network Interface Wireless WDS	85
Network interface wireless Sec WEP	86

User Interface.....	87
User Interface Configuration Pages.....	87
User Interface Configuration Upload	88
User Interface Configuration Headers	88
User Interface Configuration Remote Authentication	89
User Interface Configuration Custom Uam.....	89
User Interface Administrator	94
User Interface Start Page	95
User Interface Walled Garden	95
User Interface Web Proxy.....	96
System	97
System Configuration Syslog.....	97
System Configuration Clock	98
System Configuration NTP	98
System Configuration Certificate	99
System Configuration Save and Restore.....	100
System Configuration Domain Name	101
System Configuration Share Username	102
System Access Access Control	102
System Access Telnet	104
System Access AAA	104
System Access UAT	105
System Access Isolation.....	106
System Access NAV	106
System Access SNMP	106
System Access Web Auth.....	109
System Access Mac List.....	110
System Access HTTPC	110
System Status.....	110
System Reset.....	112
System Update	113
Connection	115
Connection Users	115
Connection E-mail Redirection	117
Connection Station Supervision.....	117
Built-In AAA	118
Built-in AAA E-Billing	118
Built-in AAA E-Billing User Control	118
Built-in AAA E-Billing Band Class	121
Built-in AAA E-Billing Bill setting	121
Built-in AAA E-Billing Power cut protection.....	122
Built-in AAA pre-paid	123
Built-in AAA pre-paid user account.....	123
Built-in AAA pre-paid price/unit.....	124
Built-in AAA pre-paid account life	124
Built-in AAA pre-paid receipts.....	124
Built-in AAA pre-paid timeunit.....	125
Built-in AAA pre-paid account reminder.....	125
Built-in AAA pre-paid manage net print	125
Built-in AAA Configuration	126
Built-in AAA Configuration Language	126
Built-in AAA Configuration Backup and restore.....	126
Built-in AAA pre-paid WEP key and SSID	126
Built-in AAA Configuration title.....	126
APPENDIX.....	128
A) Access Controller Specification	128
Technical Data	128

- B) Regulatory Domain/Channels..... 130
- C) CLI Commands and Parameters..... 131
 - Network Commands 131
 - User Commands 135
 - System Commands 137
 - Status Commands 140
 - Connection Commands 140
- D) Location ID and ISO Country Codes 141
- E) User Pages Templates Syntax 145
- GLOSSARY 150**

About this Guide

Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the Browan Communications high performance hotspot access point model BW1330. The BW1330 is a highly integrated Access Controller with built-in AAA systems for public access hotspot. We will call it AC later in the manual.




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.

Help Us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the manual please send e-mail directly to:

manuals@browan.com

Browan Communications Technical Support

If you encounter problems when installing or using this product, please consult the Browan Communications website at <http://www.browan.com/> for:

- Direct contact to the Browan Communications support centers.
- Frequently Asked Questions (FAQ).
- Download area for the latest software, user documentation and product updates.

Chapter 1 – Introduction

Thank you for choosing the Browan Communications High Performance Hotspot Access Point.

The BW1330 is a high performance and highly integrated Access Controller for public access networks. It combines a high-speed wireless LAN Access Point, an IP Router, one LAN port and a complete Access Controller for Wi-Fi Hotspot. One single BW1330 can serve up to 30 simultaneous connected wireless client stations, takes control over authentication, accounting and routing to the Internet as well as to the operator's central network.

Product Overview

Authentication, Authorization & Accounting

The BW1330 supports multiple secure authentication methods from standard web browser login (Universal Access Method), MAC authentication, to 802.1x/EAP with passwords, certificates or SIM cards. The integrated real-time accounting system is based on standard RADIUS/EAP and supports various billing plans from prepaid, pay-per-time, per-volume, per-use or flat rate. Integration into existing OSS/BSS systems can be done with ease.

Service Differentiation

The integrated Web server of the BW1330 allows flexible interaction with common web application servers, facilitating the provisioning of differentiated services with bandwidth management, location based and personalized services. Inter-Provider roaming and multi-OSS support is guaranteed by the persistent usage of standardized protocols and interfaces like RADIUS, HTTPS and XML. As all BW1330 are compliant with the recommendations of the Wi-Fi Alliance WISP roaming group.

Remote Control

The BW1330 is placed at the edge of a broadband access network and allows operators to provide cost effective public Wi-Fi services, by managing per user access control, device configuration, and radio performance centrally from the operations centre. HTTPs, telnet, SSH or SNMP over VPN can be used for secure remote management.

Privacy

BW1330 supports different levels of security and data encryption. Client stations can be separated on link layer (Layer2 User Isolation), preventing intruders from accessing the hard discs of other users. User credentials (passwords) are protected by SSL or EAP-based authentication methods. User traffic can be encrypted by VPNs (pass-through). Operators and service providers can make use of the integrated VPN/tunneling protocols to protect AAA and management traffic.

Management Options

You can use the Access Controller management systems through the following interfaces:

- Web-browser interface
- Command Line interface (CLI)
- Simple Network Management Protocol (SNMP v1, v2, v3)

The AC management system pages are organized the same way for the web-browser interface and the CLI. This user manual provides detailed description of each management option.

The BW1330 Features

WLAN

- 802.11b+g compliant, 1-54Mbps with auto-fallback
- Wi-Fi compliant
- Support Multiple BSSID up to 16 "Virtual AP"
- Concurrent 802.11b and 802.11g access
- WDS support (concurrent bridge and AP mode)
- WPA/WPA2 (Wi-Fi Protected Access) support
- R-TNC connectors for external antennas
- RF output power
- High receiver sensitivity (up to -91 dBm@1Mbps, 8%PER)

AAA

- Multiple authentication methods: UAM, 802.1x/EAP, RADIUS, MAC, Smart Client (e.g. iPass)
- Per LAN/VLAN AAA, IP policies
- WISPr compliant
- Internal and external accounting backups
- Internal or external web server
- Remote user login, logout, session status control via https/XML
- AAA proxy server (for simultaneous EAP and UAM)
- Per user bandwidth management
- Web proxy support

IP Router and IP address management

- Static IP routing table
- NAT/NAPT (IP masquerading)
- Port-forwarding
- 802.1q VLAN support
- Transparent VPN client pass-through (PPTP, IPsec ESP)
- Selective source routing
- PPPoE client
- GRE Tunnel
- DHCP server, relay gateway (suboptions), DHCP client
- Multiple IP pools per user group
- UAT (Universal Address Translation)
- SMTP redirection (e-mail)

VPN

- GRE VPN client

Ethernet port

- One WAN port, One LAN port 10/100Mb, auto-sensing

Management

- Secure management via https, SSH, SNMP
- SNMP proxy
- SNMPv3 (incl. authentication and encryption)
- Management subnet for remote AP and switch management
- Remote firmware update

Chapter 2 – Installation

This chapter provides installation instructions for the hardware and software components of the Access Controller BW1330. It also includes the procedures for the following tasks:

- Hardware Introduction (LEDs, Connectors)
- Connecting the Access Controller
- First Configuration
- Step-by-Step Setup
-
-

The Product Package

The Access Controller comes with the following:

- High Performance Hopspot Access Point (model: BW1330)
- Detachable Antennas (Dipole Antenna with R-TNC plug connector, 2 units)
- External power supply (Input:100-240VAC, 50-60Hz, Output: 12VDC, 1 unit)
- Ethernet Patch Cable (STP, 1.5 m length, 1 unit)
- Installation CD containing:
 - BW1330 User Guide in PDF format
 - KickStart Utility
 - Product Firmware
 - Release Notes
 - Adobe Acrobat Readers
- Printed Warranty Note(3 year)
- Console cable
- Screw bag



If any of these items are missing or damaged, please contact your reseller or Browan Communications sales representative.

Hardware Introduction

General Overview

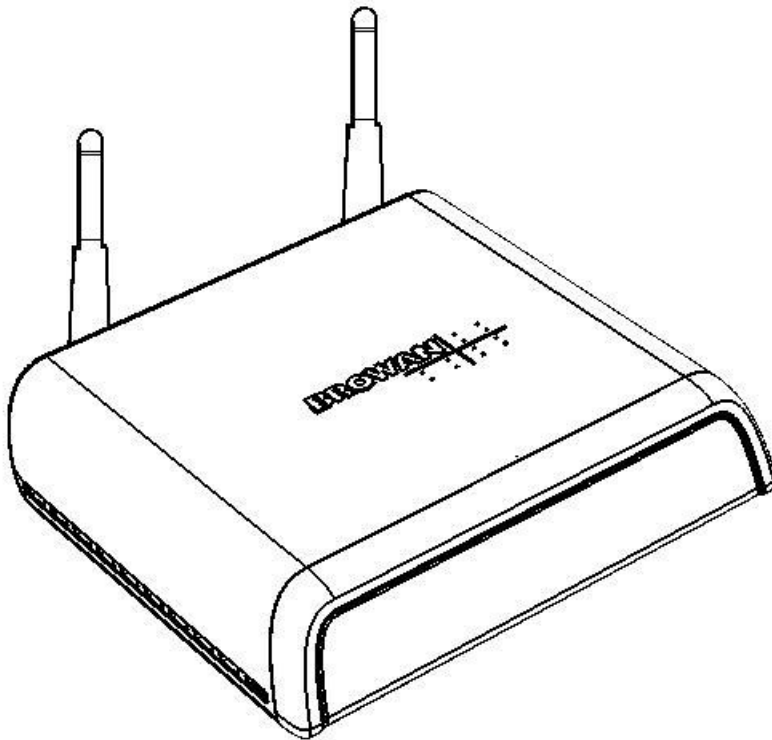


Figure 1 –BW1330 Access Controller General View

The front panel of the Access Controller contains:

- A series of indicator lights (**LEDs**) that help describe the state of various networking and connection operations.

The reverse panel of the Access Controller contains:

- **Connectors** which enable you to make different network connections for the controller
- **Reset** button enables you to reboot or reset the device configuration to the factory defaults



Press the **Reset** button for less than **3** seconds to **reboot** the controller.

Press the **Reset** button for more than **10** seconds to **set the controller to factory defaults**.

Back Panel

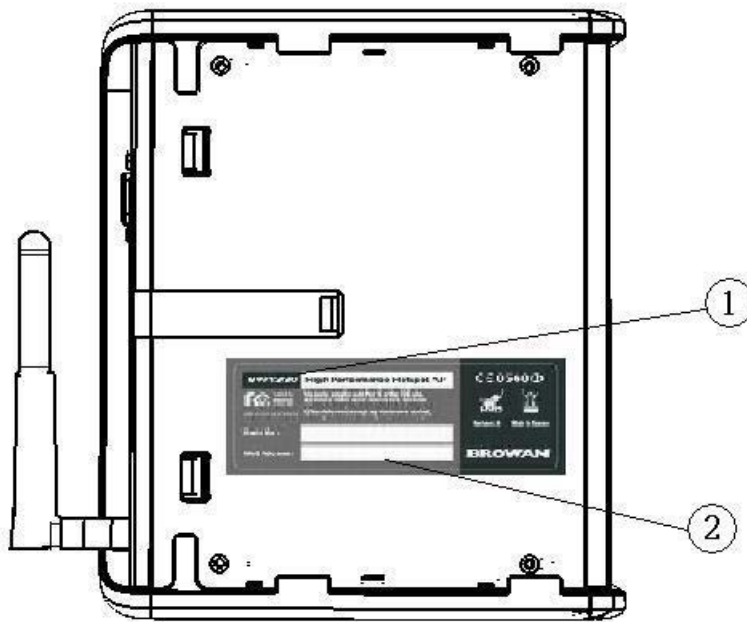


Figure 2 – Back Panel of the BW1330

The back panel of the Access Controller contains:

- **Model and device name** (see item 1 in figure above). The official device name is **High Performance Hopspot Access Point, model BW1330**.
- **MAC address** of the device. The label (item 2 in figure above) shows the **LAN interface MAC** address of the device. You can determine the **WAN** and **WLAN(Up to 16 MBSSID)** interfaces' MAC addresses by a simple calculation:
 - **WAN interface MAC = LAN MAC + 1 (Hex)**
 - **WLAN(MBSSID) interface MAC = LAN MAC + 1 (Hex) by sequence up to 16 MAC**

LEDs

The Access Controller has several LEDs located on the front panel:

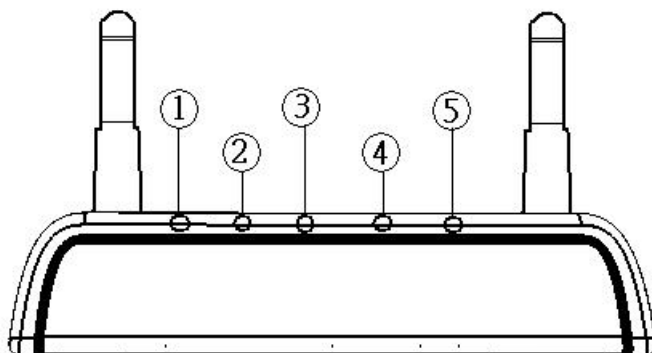


Figure 3 – LEDs of the BW1330

The various states of the LEDs indicate different networking and connection operations as follows:

Item	LED	Color	Status	Indication
1	Power	Green	On	system is active/working
			Blinking	system is booting
		Orange	On	Writing to FLASH memory
2	Online	Green	On	PPPoE/PPTP/GRE tunnel for DSL is activated.
			Off	PPPoE/PPTP/GRE tunnel for DSL is deactivated.
3	WAN	Green	On	WAN active/working
			Blinking	Data transmitting
4	LAN	Green	On	100 Mbps network connection exists
			Blinking	Data transmitting
		Orange	On	10 Mbps network connection exists
			Blinking	Data transmitting
5	WLAN	Green	On	WLAN active/working
			Blinking	Data transmitting

Connectors

The Access Controller has several connectors on the rear panel:

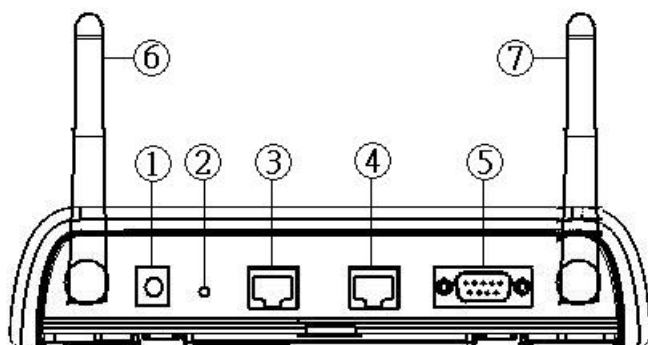


Figure 4 – Connectors

Descriptions of the connectors are given in the following table:

Item	Connector	Description
1	Power	For power supply
2	Reset	Reboot or reset to factory defaults. Press the reset button for less than 3 seconds to reboot the controller. Press the reset button for more than 10 seconds to set the controller to factory defaults
3	WAN	For Internet connection and PoE input
4	LAN	For enterprise applications use this port to connect your company LAN, Intranet or to hotspot access points
5	RS232	Console port
6	Antenna	The MAIN antenna
7	Antenna	The AUX antenna

Stand

The BW1330 is designed standing on the desk or wall mount. Refer to the direction of red arrow to release and insert the stand at the back of BW1330.

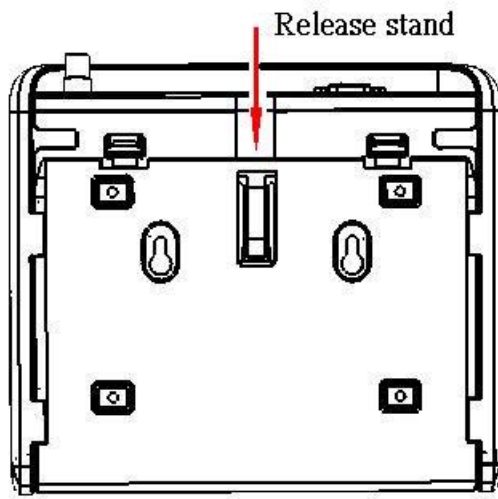


figure 5 – release stand

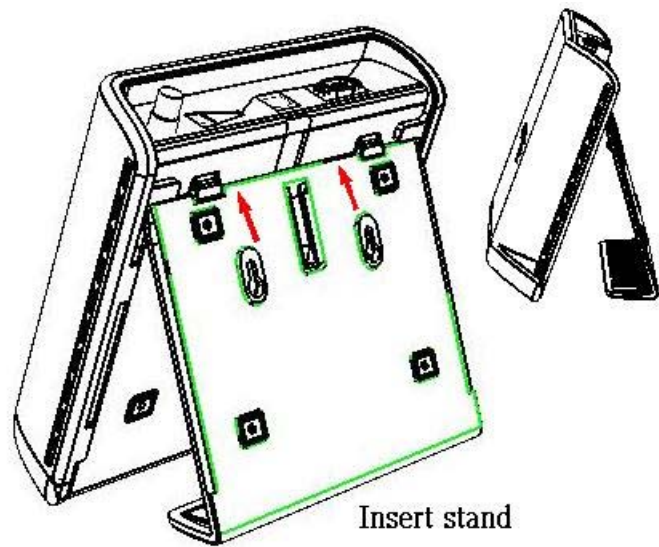


figure 6 – insert stand

Wall Mount

BW1330 is also designed for wall mounting. Refer to the step 1 and step 2 to fix the stand on the wall and lock the BW1330 on it.

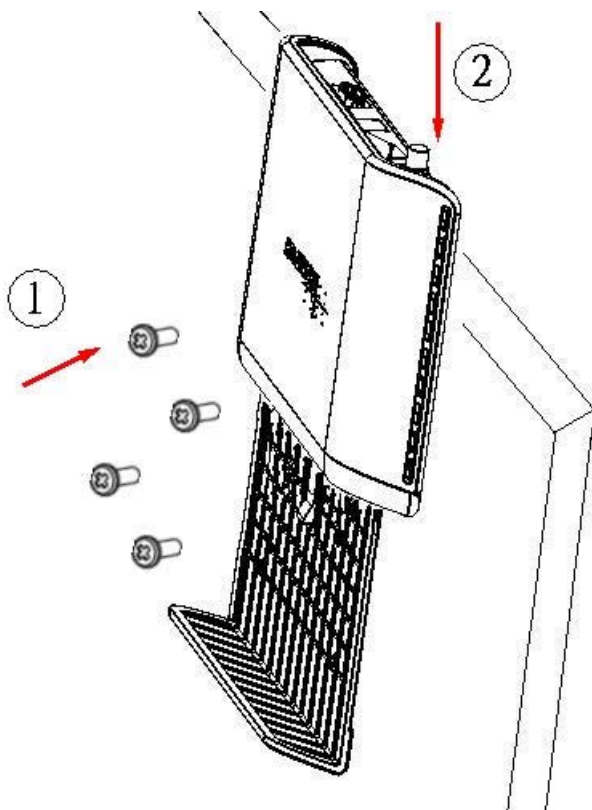


figure 7 – wall mount

Connecting the Access Controller

Use the following procedure to prepare your network connection to your BW1330.



Use the enclosed power adapter for power supply of your BW1330.

- Step 1** Place the Access Controller on a flat work surface.
- Step 2** Connect one Ethernet patch cable to the LAN port of the Access Controller and to a free hub port on your local network.
- Step 3** Connect the WAN port of the Access Controller to an Ethernet port of a broadband Internet modem or router.
- Step 4** Connect the power adapter to the Access Controller.
- Step 5** Wait 30 seconds until the boot process is finished and check to ensure that at least the following LEDs are ON:
- Power LED (steady On)
 - WAN LED
 - LAN LED
 - WLAN link LED

Initialization

This paragraph describes how to access the Web configuration interface of the BW1330. After unpacking and connecting the product for the first time it responds to a dynamic IP address given by the DHCP server on LAN or WLAN interface.

The default network settings for your new access controller are:

```

Ixp1(WAN) port:           IP 192.168.2.66           subnet 255.255.255.0
Br1                       IP 192.168.3.1           subnet 255.255.255.0
Ixp0 (LAN) port:         In Bridge
WLAN1_0(first virtual AP): In Bridge
    
```



For other management methods: SNMP and command line interface (CLI) please refer to their respective chapters.

Access Your BW1330

After connecting the BW1330 device to network, try to access the BW1330 via one of the method: Follow these instructions to access your BW1330 using the Web browser:

Step 1

- Access your device via LAN connected by RJ-45 cat.5 cable or wirelessly connect to BW1330 by default SSID "BW1330" without any encryption. Waiting for DHCP server to give an IP address 192.168.3.x to your client PC. Open the Web browser and type the IP address of the BW1330:

`https://192.168.3.1/a.rg`

- Configure your PC with a static IP address on the 192.168.2.x subnet with mask 255.255.255.0. Connect the BW1330 WAN interface into the same physical network as your PC. Open the web browser and type the default IP address of the BW1330:

`https://192.168.2.66/a.rg`

Step 2 Enter the BW1330 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**

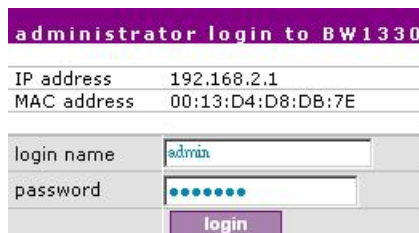


figure 8 login page

Step 3 After successful administrator log on you will see the main page of the access controller's **Web interface**:

BW1330						
Network Interface	User Interface	System	Connection	Built-in AAA		
		Configuration	Access	Status	Reset	Update
device statistics						
description	value					
device name:	BROWAN Inc. , SMB PAC, model: BW1330					
firmware version:	BW1330.BRO.2.22.0009					
device status:	running					
currently connected administrators:	admin @ 192.168.2.1 Idling: 00:00:00					
uptime:	00:33:35					
software runtime:	00:33:11					
total memory:	63220 kB					
free memory:	31764 kB					
average load:	1min: 0.99					
	5min: 0.97					
	15min: 0.84					
<u>connected clients number:</u>	0					
connected clients input bytes:	0 bytes					
connected clients output bytes:	0 bytes					
WAN (ixp1)						
description	value					
<u>IP address:</u>	192.168.2.66					
netmask:	255.255.255.0					
gateway:	192.168.2.1					
MAC:	00:16:16:02:07:A1					

figure 9 administrator page

Software Introduction: KickStart

- Another way is launch the **KickStart** utility that is provided with your product CD. The **KickStart** is a software utility that is included on the Installation CD. The utility automatically detects access points and access controllers installed on your network, regardless of its host IP address and lets you configure each unit's IP settings. The feature list for the **KickStart** utility is listed below:
 - Scanning your subnet for all connected APs, ACs
 - Quick access to your AC via HTTPS, telnet, SSH
 - Setting new IP address of your AC
 - Reset to factory default settings
 - Default access (in case of lost administrator password)
 - Firmware updates

To install the **KickStart** utility insert the Installation CD into your CD-ROM drive. Find and install the utility from the product CD into the computer.



If the Installation CD does not start automatically, please run "**autorun.exe**" manually from the root directory of the installation CD.

Step 1

Install the **KickStart** utility from the **Installation CD**. Click **Start > Programs > BROWAN > KickStart** to launch the application. If the BW1330 device is connected to your network, the utility will automatically find your AC:

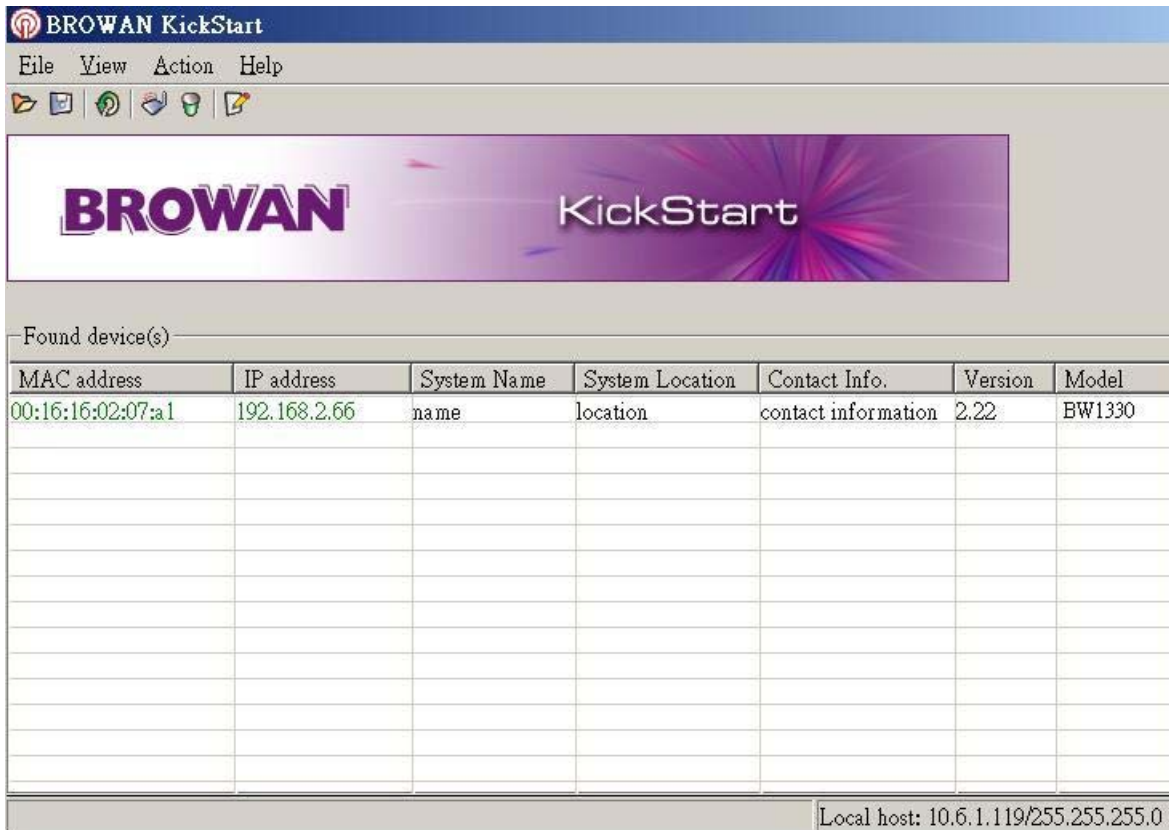


figure 10 kick start utility

Step 2 Select your controller and right click. Select **Open WEB** item to launch the web management interface through the secure https connection:

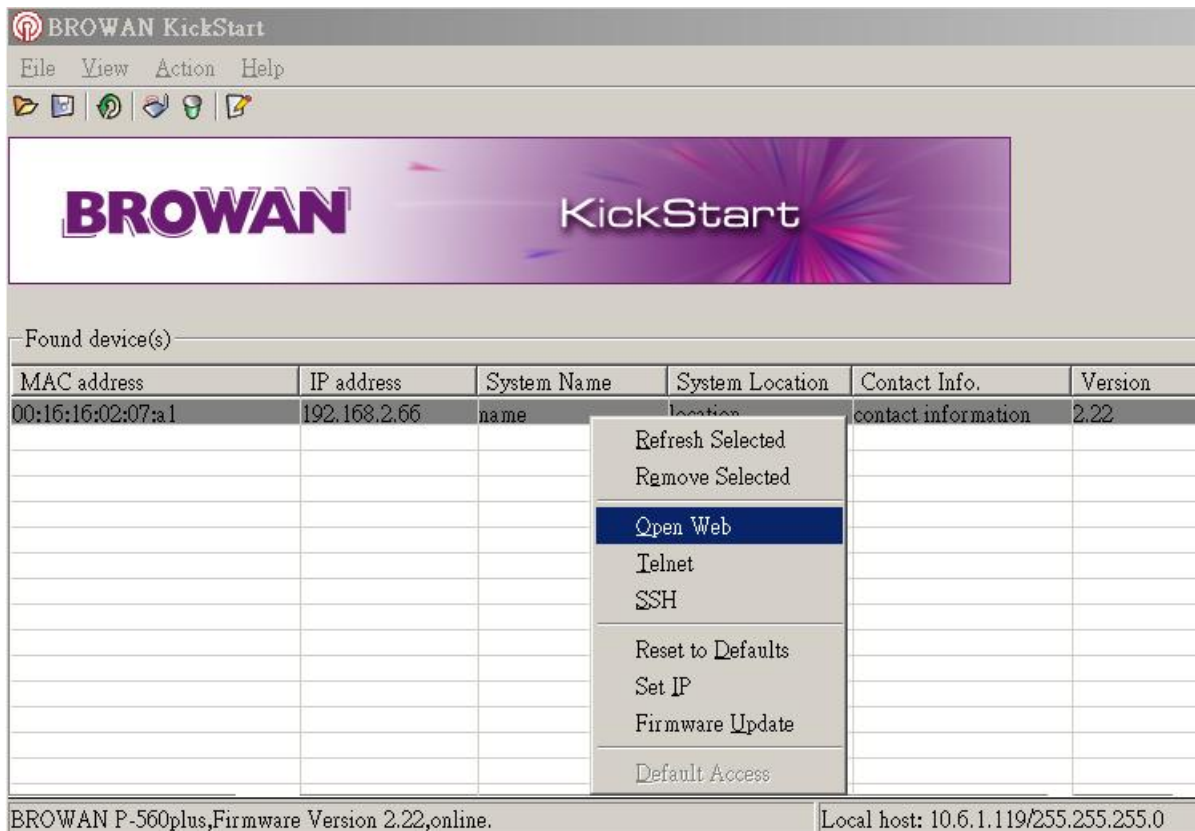


figure 11 kick start utility

Step 3 Enter the Access Controller administrator log on settings to access the **web management** interface.



The default administrator log on settings for all controller interfaces are:

User name: **admin**

Password: **admin01**

Step 4 After successful administrator log on you will see the controller **web interface**. The controller system statistics page is displayed by default:



figure 12 administrator page



If you cannot connect to the device via your web browser because of TCP/IP mis-configuration, you can reset the product to the factory default. Press the reset button for more than 10 seconds.

Now you are enabled to perform the initial controller configuration. Follow the next section for step-by-step setup instruction to configure the device according to your needs.

Step by Step Setup

Step 1. Interface Set-Up

In the **network interface | configuration | interface configuration** menu you can set the TCP/IP settings. br1 is pre-configured as the WLAN port of your Access Controller, ixp1 is the WAN port. By default the bridge interface br1 initially contains two interfaces: wlan1_0 and ixp0. Wlan1_0 is the first virtual AP which you can configure up to 16 virtual AP(16 MBSSID) and ixp0 is the LAN port. Both ixp0 and wlan1_0 are DHCP server enabled by default.

You can modify these settings according to your local network requirements. Make sure that IP subnets do not overlap.

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled	LAN	192.168.3.1	255.255.255.0	ixp1	edit
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	edit

Figure 13 – Interface Configuration Settings



If DHCP client, or PPPoE, is selected as a dial-up protocol for the WAN interface the WAN settings of this table will be overwritten by the values retrieved from the Internet Provider.

Step 2. DNS Set-Up

In the **network interface | DNS** menu you can specify your local domain name server or enter the DNS server provided by your ISP (Internet Service Provider).

DNS			
type	IP address		action
primary	202.96.209.5		edit
secondary	0.0.0.0		edit

Figure 14 – DNS Redirection



DNS is set automatically if provided by the ISP dynamically via DHCP, PPPoE.

Step 3. IP Address Management

For automatic IP assignments to client stations, set the **DHCP settings** in the **network interface | DHCP** menu according to your TCP/IP configuration from **step 1**. Only use address ranges within the corresponding IP subnet of the LAN interface. In addition you can switch on the Universal Address Translation function in the **system | access | UAT** menu. With **UAT** users do not need to change their local TCP/IP settings to log on to the Access Controller. The Access Controller will translate fixed IP numbers used in private networks transparently for the user.



Please refer to **Chapter 3 – Universal Address Translation** for further details to avoid IP conflicts.

Step 4. RADIUS Set-Up

In the **network interface | RADIUS settings** menu you can first define the local settings of the integrated **RADIUS** client of the Access Controller. For example you can modify timeouts and the **NAS server ID** (name of the RADIUS client):

RADIUS settings		
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
location ISO country code	us	edit
location E.164 country code	1	edit
location E.164 area code	408	edit
location network	GEMTEK_SYSTEMS	edit
hotspot operator name	GEMTEK_SYSTEMS	edit
location	Terminal_Worldwide	edit
bandwidth up	1.00 Mbps	edit
bandwidth down	1.00 Mbps	edit

Figure 15 – RADIUS Settings

On the second page: **network interface | RADIUS | servers** you can specify up to 32 different **RADIUS** servers for authentication and accounting (see Figure 16 – RADIUS Servers). One of the RADIUS server entries can be specified as the default server. Thus, if a user cannot be associated to any specific service provider by his login name, the Access Controller will send authentication and accounting messages to the default **RADIUS** server.

RADIUS servers					
name	type	IP address	port	secret	action
DEFAULT	authentication	0.0.0.0	1812	secret	details edit delete
(default)	accounting	0.0.0.0	1813	secret	new

Figure 16 – RADIUS Servers

Make sure that the **RADIUS** server is up and running and is able to receive authentication requests from the Access Controller.

Step 5. Welcome/Login/Start pages

The most popular authentication method for public users is the **UAM** (Universal Access Method). **UAM** can be enabled using the **system | access | AAA** menu. With UAM users can log-on to the Access Controller using their web browser. As an operator of a wireless access service you can provide a custom set of web pages to your subscribers.

- **welcome** page (default = Internal , Enabled) - the first page that is presented when users start their web browser.
- **login** page (default = Internal) – the page containing the log-on fields for user name and password. This page is presented as default when the welcome page is disabled.
- **logout** page (default = Internal) - the page that pops up after successful authentication. It includes information about the online session such as online time and transferred data.
- **help** page (default = Internal) - the page with online help information for log-on.
- **unauthorized** page (default = Internal) - the page which appears if web login method is disabled.

The default user login page looks like the picture below:

LOGIN TO BW1330

IP address 192.168.3.7
MAC address 00:90:4B:D2:A2:C2

login name gary
password ●●●●

login reset

Get help [here](#)

Figure 17 – Example of a Simple Login Page

You have full flexibility to modify and adapt all these pages to your needs and personal designs. For initial set up and testing we recommend you use the default configuration, which will present a simple login window with input fields for user name and password.

Enter any **start** page you like in the **user interface | start page** menu. In addition you can define a number of free web sites in the **walled garden** table on the **user interface** menu.



For more information on how to build your own user pages please refer to **Chapter 4 – User Pages**.

Step 6. Change Administrator Password

Before saving your initial configuration don't forget to change the administrator password in the **user interface | administrator** menu.

Step 7. E-mail Redirection

If you have a SMTP mail server available for your subscribers enter its IP address and SMTP port number in the **connection** menu under the item **e-mail redirection**. All outgoing e-mail passing through the Access Controller will be redirected to this server.

Step 8. Save Configuration and Restart

Make sure you have saved your changes from each of the first seven steps and then press the **save and reboot** button on the lower side of the **web management** screen. After 10-15 seconds you can re-load the admin pages or start to log on to the Access Controller as a user.

Users connected to the LAN port of the Access Controller can type in any URL in their browser and they will be redirected to your defined **welcome** (if enabled) and **login** pages. Administrators can monitor connected users via the **connection | users** menu.

Chapter 3 – Universal Address Translation

What is UAT

Universal Address Translation (UAT) allows Hotspot operators to offer true IP Plug&Play access for their subscribers.

With **UAT** enabled, the Access Controller will automatically and transparently translate fixed IP settings (IP address, gateway, DNS, proxy server) on a user's PC enabling him to connect to the broadband Internet service, even if the client's IP overlaps the IP subnet of the WAN port.

Without **UAT** public access, subscribers are forced to switch their TCP/IP settings to **DHCP** (automatic IP address assignment), potentially losing any fixed IP address settings they previously entered.

UAT Principle

BW1330 acts as an ARP proxy to each client who has a fixed IP which not belong to the subnet of LAN interface. As below figure descript, BW1330 will automatic reply a client's ARP Request if its IP doesn't belong to its LAN subnet to pretend as if BW1330 is its Gateway; then inside BW1330, a unicast router will be added for UAT client.

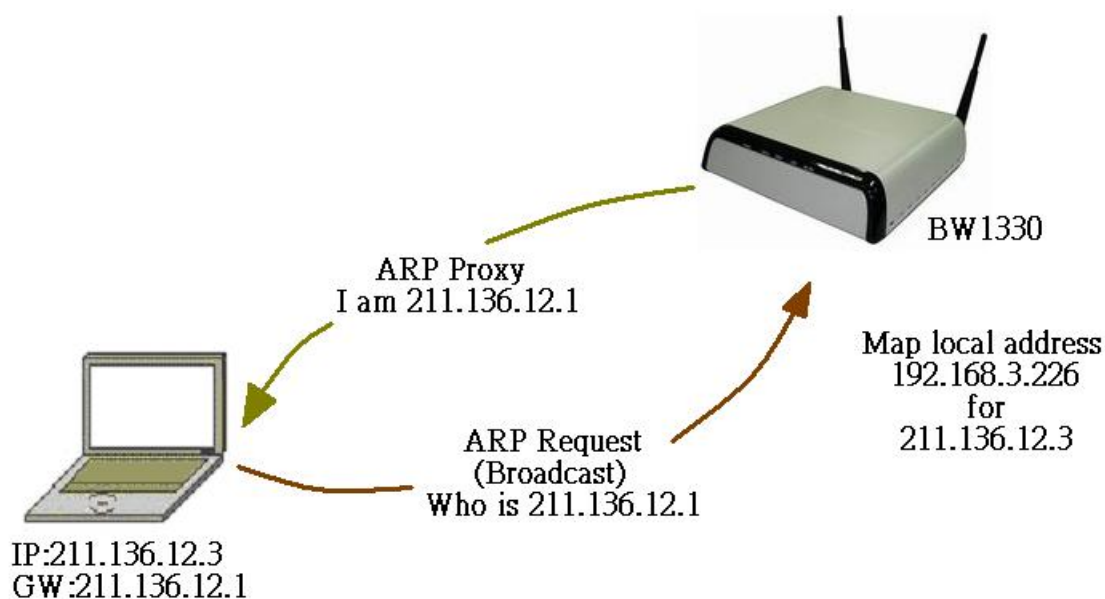


Figure 18 – UAT Principle

UAT Limitation

When using **UAT** operators have to be aware of some principal limitations:

If UAT mode is enabled on BW1330, BW1330 will act as an ARP Proxy under its LAN interface. If there has a sub-net behind a router which under the LAN of BW1330 and there has a PC whose IP belong to the sub-net as the figure show, the communication between PC2 and PC1 will be failed for the reason of BW1330's ARP proxy packet.

But if the router is working under NAT mode, the communication from PC2 to PC1 will be OK.

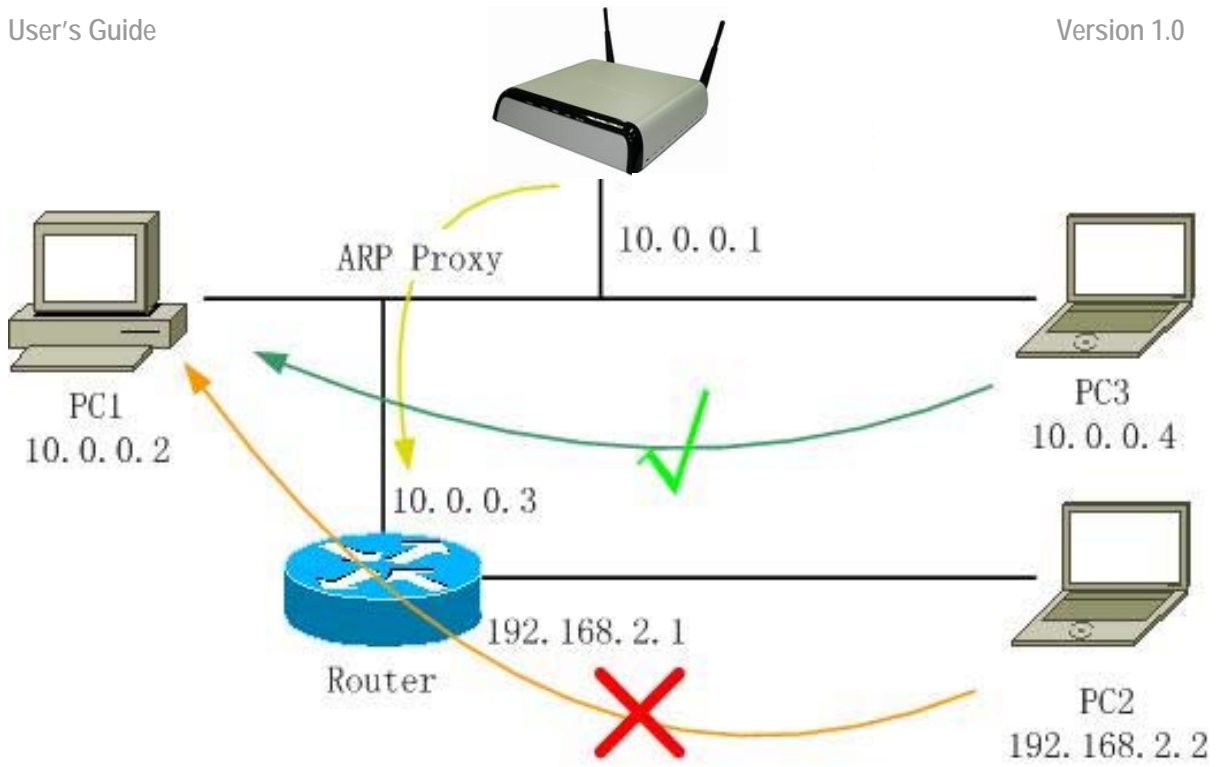


figure 19 UAT Limitation

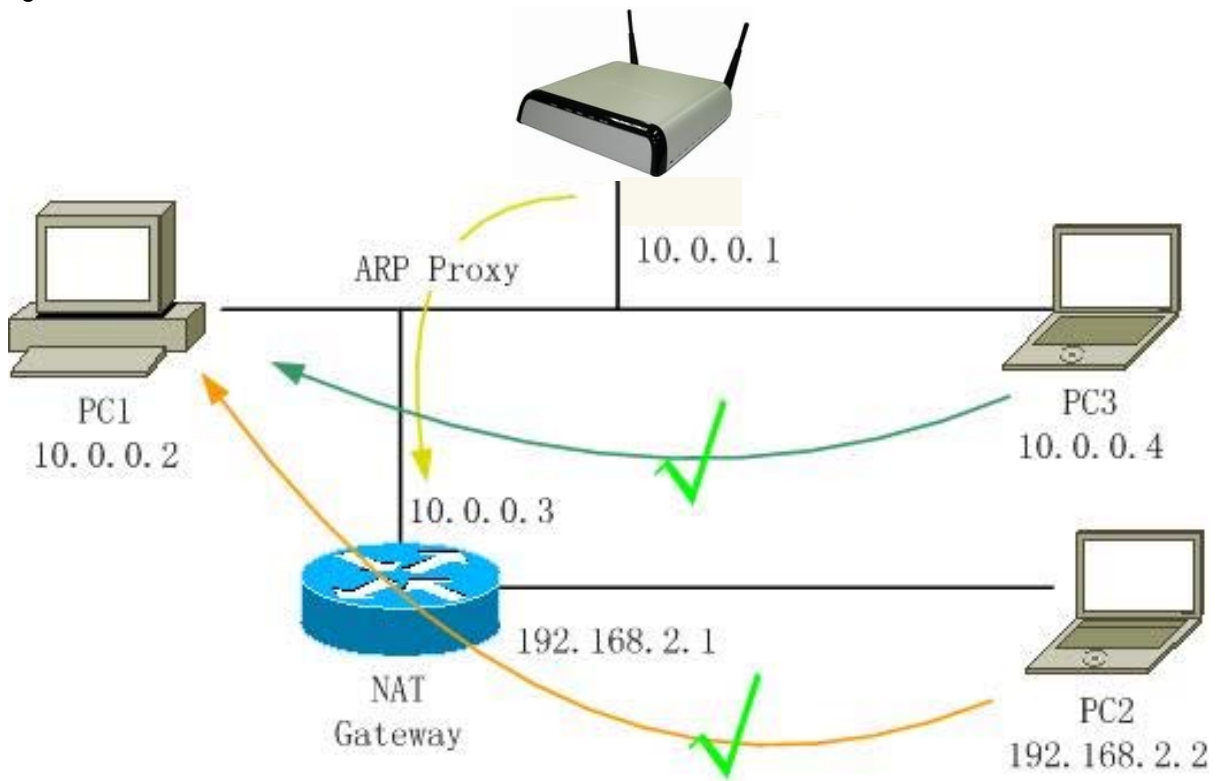


Figure 20 – another subnet under BW1330

Chapter 4 – User Pages (Based on XSL)

This chapter describes what the user pages are and how to manage them. 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 Access Controller for subscribers.



All further presented user pages are factory default. The Hotspot operator can upload new templates for all user pages.

User Pages Overview

Welcome Page

Welcome page is the first page a Hotspot 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 21 – Welcome Page



The Hotspot operator can change the **welcome** page according its needs. 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 Access Controller. To get access to the network, the user should enter his authentication settings: **login name** and **password** and click the **login** button:

Figure 22 – Simple Login Page



The login name and password can be obtained from your Hotspot Operator. Login format available for BW1330:

- username@WISPdomain
- WISPdomain/username

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 Hotspot operator 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:

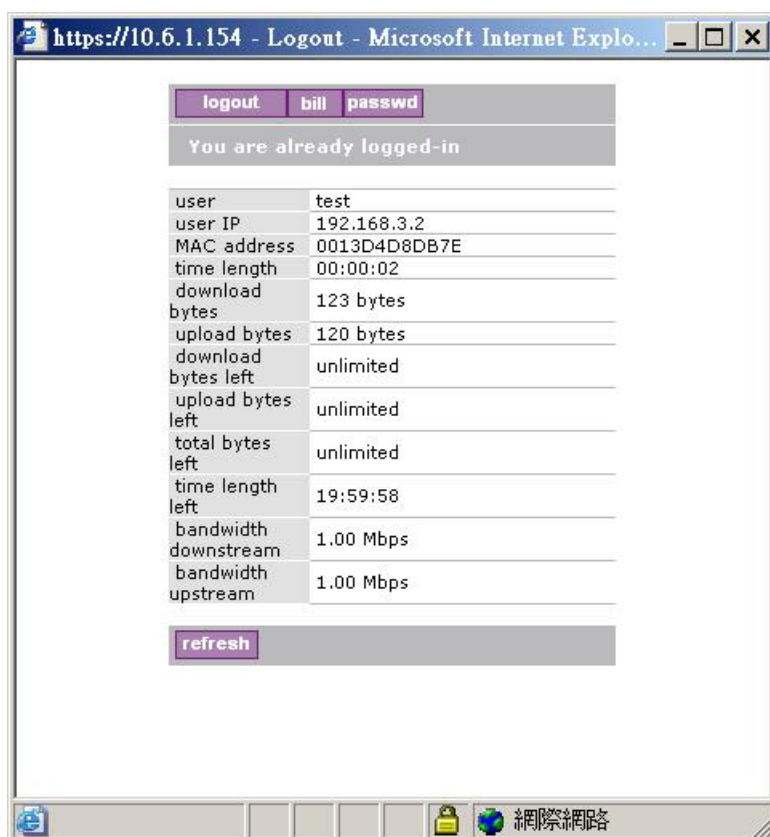


Figure 23 – Logout Page

Detailed AC 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 Hotspot operator 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

Click on the **get help** link in the **login** page for help tips related to network registration. A page appears similar to the following:



Figure 24 – Help Page



The Hotspot operator 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:

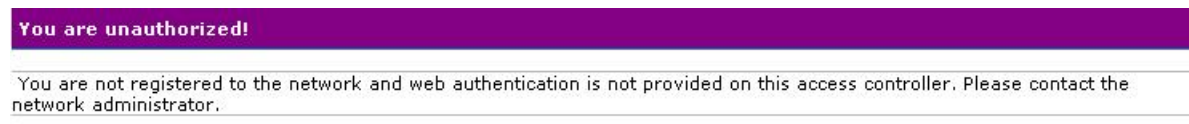


Figure 25 – Unauthorized Page



The Hotspot operator can change the **unauthorized** page according to its needs. See more details in section: **Changing User Pages**.

Changing User Pages

As the Hotspot operator 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 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.



User Pages templates samples can be found in the **Installation CD** delivered to you with the product.

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	<input type="text" value="internal"/>	-	<input type="text" value="login.xsl"/>	<input type="button" value="update"/> <input type="button" value="cancel"/>
logout	internal	-	logout.xsl	
help	internal	-	images/help.html	
unauthorized	internal	-	images/unauthorized.html	

figure 26 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	<input type="text" value="external"/>	-	<input type="text" value="login.xsl"/>	<input type="button" value="update"/> <input type="button" value="cancel"/>
logout	internal	-	logout.xsl	
help	internal	-	images/help.html	
unauthorized	internal	-	images/unauthorized.html	

figure 27 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.xml	
login	external	-	<input type="text" value="http://192.168.2.27/login.xml"/>	<input type="button" value="update"/> <input type="button" value="cancel"/>
logout	internal	-	logout.xml	
help	internal	-	images/help.html	
unauthorized	internal	-	images/unauthorized.html	

figure 28 configure external pages



Do not try to upload other than supported formats. Such uploaded pages 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.xml	<input type="button" value="change"/>
login	external	-	http://192.168.2.27/login.xml	<input type="button" value="change"/>
logout	internal	-	logout.xml	<input type="button" value="change"/>
help	internal	-	images/help.html	<input type="button" value="change"/>
unauthorized	internal	-	images/unauthorized.html	<input type="button" value="change"/>

figure 29 configure external pages

Step 6 Check for new uploaded user page (e.g. login):

----- NEW LOGIN -----

login name	<input style="width: 100%;" type="text"/>
password	<input style="width: 100%;" type="password"/>
IP address	192.168.2.27
MAC address	000347C92B1C
<input type="button" value="login"/> <input type="button" value="reset"/>	
Get help here	

figure 30 new login page



If at anytime you wish to restore factory default user pages, click the **reset** button under the **system | reset** menu.

Example for Internal Pages

We will use the **user pages** templates from the **Installation CD** to show the example how to upload the internal pages. Follow the steps below:

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.xml	change
login	internal	-	login.xml	change
logout	internal	-	logout.xml	change
help	internal	-	images/help.html	change
unauthorized	internal	-	images/unauthorized.html	change

figure 31 internal pages

Step 2 Under the **user interface | configuration | 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 32 upload page



The memory space in the AC for internal user pages is limited to **1 MB**.

Step 3 Specify the location (**Examples** directory if you use the **Installation CD**) 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.xml	C:\woding\projects\BW1330\samples\welcome.xml	浏览...
login.xml	C:\woding\projects\BW1330\samples\login.xml	浏览...
logout.xml	C:\woding\projects\BW1330\samples\logout.xml	浏览...
help.html	C:\woding\projects\BW1330\samples\help.html	浏览...
unauthorized.html	C:\woding\projects\BW1330\samples\unauthorized.html	浏览...
onclickuser.xml		浏览...
images and stylesheet (css) files for templates		
additional file 01	C:\woding\projects\BW1330\samples\welcome\welcome.gif	浏览...
additional file 02	C:\woding\projects\BW1330\samples\login\login.gif	浏览...
additional file 03	C:\woding\projects\BW1330\samples\login\reset.gif	浏览...
additional file 04	C:\woding\projects\BW1330\samples\login\login.css	浏览...
additional file 05		浏览...
additional file 06		浏览...
additional file 07		浏览...
additional file 08		浏览...
additional file 09		浏览...
additional file 10		浏览...
upload cancel		

figure 33 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 34 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 35 customize login page



If at anytime you wish to restore the factory default user pages, click the **reset** button under the **system | reset** menu.

Extended UAM

The **Extensions** feature (**user interface | configuration** 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):

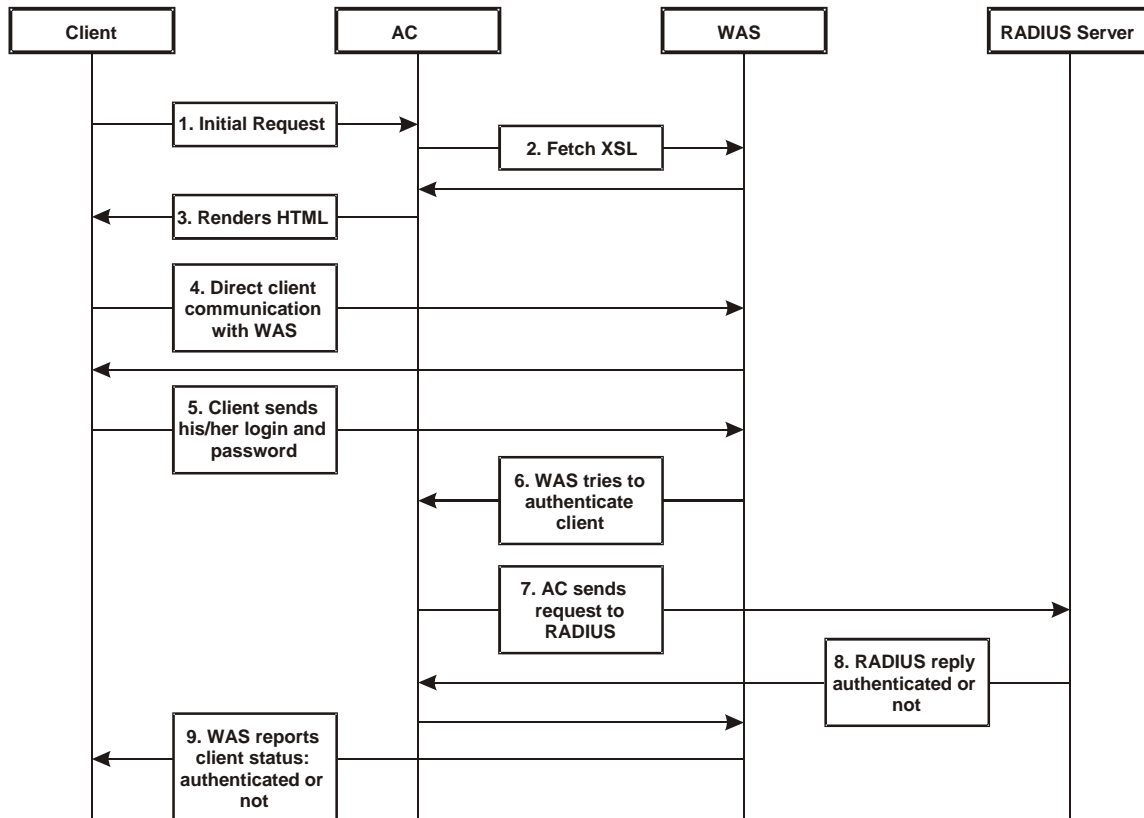


Figure 36 – Client Remote Authentication Scheme (1)

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 Interface | Configuration | 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.



Find more details on how to prepare the .XSL templates to render the HTML in Appendix: **E) User Pages Templates Syntax**.

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):

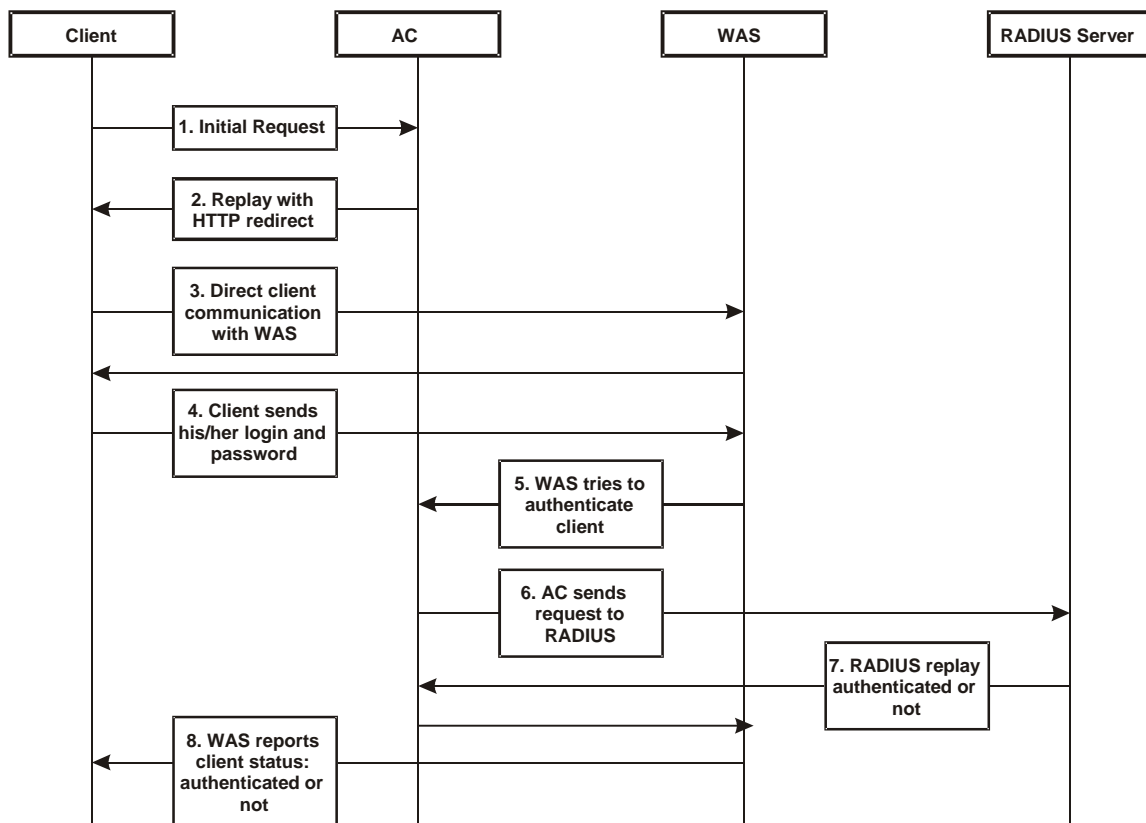


Figure 37 – Client Remote Authentication Scheme (2)

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 Interface | Configuration | Pages**). The further actions are the same as described in the **Scheme 1** (Figure 36 – 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 interface | configuration | pages** menu. Enable **welcome** page, set the **redirect** setting and specify the redirect location for such authentication process (also see: **User Interface | Configuration | Pages**).

Parameters Sent to WAS

Parameters that are sent 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 interface RADIUS RADIUS settings menu
nasip	WAN IP address for WAS	Can be changed or specified under the network interface configuration interface configuration 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 configuration interface configuration 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: pologon.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://BW1330/ppologon.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://BW1330/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://BW1330/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 5 – Customized User page (HTML)

This chapter will assist you on configuring BW13330 customized login/logout pages using the sample templates in BW13330 CD. BW13330 CD includes four different styles of templates (based on HTML). There are three authentication-enabled styles (coffee bar, general and hotel), and one authentication-free hotel style. User can also create a personalized login/logout pages based on the provided sample templates.

Determine Your Access Policy

Determine if the BW13330 access policy requires user authentication: Choose either the authentication-enabled policy (user authentication require) style template or authentication-free policy (no user authentication require) style template as the base template. Step 2 will show how to configure authentication-free access policy on BW13330. User may use any HTML editing tools to modify the template contents to create a new personalized login/logout page.

Configure Authentication-Free Access Policy

Login BW13330 as super administrator and go to **system | access | Web auth** menu. From the diagram below, edit the **ip web auth method** status and set to **enabled**.

web_auth_methods		
method	status	action
ip	disabled	edit
pre-paid	enabled	edit
e-billing	enabled	edit
radius	enabled	edit
pop3	disabled	edit

Figure 38 – configure IP authentication.



Once the status of the ip web auth method is set to enabled, any end-user trying to access to Internet from BW1330 will not require user authentication. More detail please refer to the system | access | Web auth in chapter 8.

Step1. Configure and Upload Customized Login/Logout Page files

Login BW1330 as super administrator and go to user interface | configuration | Custom UAM.

In order to configure BW1330 using the customized login/logout page, Customize Page status must be set to enable.

To enable Customized Page, edit the Customize page status(**user interface |configuration |custom uam**) and set to **Enabled**. See the diagram below:

Customize Page Status		
Description	Status	Action
Customize Page	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	save cancel

Figure 39 – enable customize page status

Customize Page Status		
Description	Status	Action
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 40 – 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 in the BW1330 CD for this demonstration).

After clicking the upload button, an **Update Custom UAM Files** screen will appear. (See diagram below).

Customize Page Status		
Description	Status	Action
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 Custom UAM Files		
Login File	<input type="text"/>	瀏覽...
Logout File	<input type="text"/>	瀏覽...
Additional file 01	<input type="text"/>	瀏覽...
Additional file 02	<input type="text"/>	瀏覽...
Additional file 03	<input type="text"/>	瀏覽...
Additional file 04	<input type="text"/>	瀏覽...
Additional file 05	<input type="text"/>	瀏覽...
Additional file 06	<input type="text"/>	瀏覽...
Additional file 07	<input type="text"/>	瀏覽...
Additional file 08	<input type="text"/>	瀏覽...
Additional file 09	<input type="text"/>	瀏覽...
Additional file 10	<input type="text"/>	瀏覽...

[upload](#) [cancel](#)

Figure 41 – upload files

Enter the physical path and filename of the coffee template files, or click the “browse” button to search the BW1330 CD where coffee template files are located.



The first two items are for login.html and logout.html files. Additional files are for CSS and image files, such as jpg, gif, png and etc.

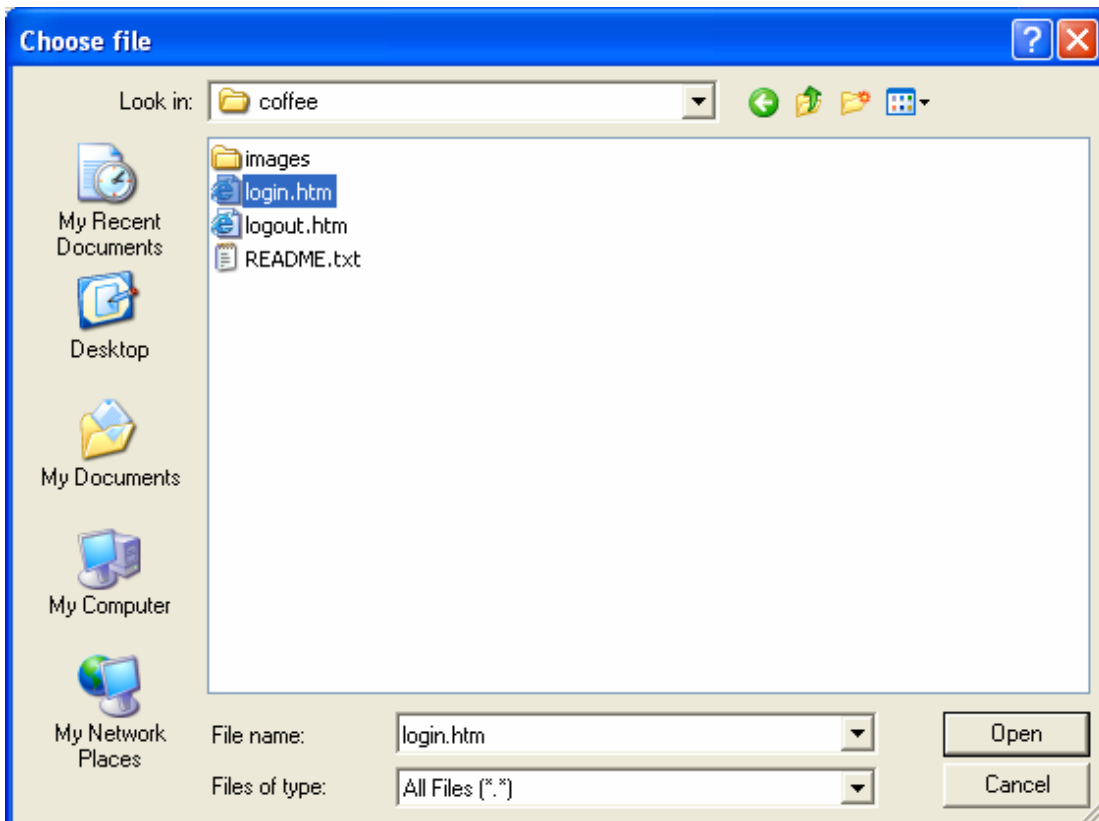


Figure 42 – select example files

Customize Page Status		
Description	Status	Action
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 Custom UAM Files		
Login File	D:\Data\BW1330\CD\coffee\login.htm	瀏覽...
Logout File		瀏覽...
Additional file 01		瀏覽...
Additional file 02		瀏覽...
Additional file 03		瀏覽...
Additional file 04		瀏覽...
Additional file 05		瀏覽...
Additional file 06		瀏覽...
Additional file 07		瀏覽...
Additional file 08		瀏覽...
Additional file 09		瀏覽...
Additional file 10		瀏覽...
		upload cancel

Figure 43 – upload login.html

After entering all the template files, press upload button to start the uploading files to BW1330.



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

Customize Page Status		
Description	Status	Action
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 Custom UAM Files		
Login File	<input type="text" value="D:\Data\BW1330\CD\coffee\login.htm"/>	瀏覽...
Logout File	<input type="text" value="D:\Data\BW1330\CD\coffee\logout.htm"/>	瀏覽...
Additional file 01	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_01.jpg"/>	瀏覽...
Additional file 02	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_02.jpg"/>	瀏覽...
Additional file 03	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_03.jpg"/>	瀏覽...
Additional file 04	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_04.jpg"/>	瀏覽...
Additional file 05	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_05.jpg"/>	瀏覽...
Additional file 06	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_06.jpg"/>	瀏覽...
Additional file 07	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_07.jpg"/>	瀏覽...
Additional file 08	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_08.jpg"/>	瀏覽...
Additional file 09	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_09.jpg"/>	瀏覽...
Additional file 10	<input type="text" value="D:\Data\BW1330\CD\coffee\images\login_10.jpg"/>	瀏覽...
<input type="button" value="upload"/> <input type="button" value="cancel"/>		

Figure 44 – upload other files

Once all files are uploaded successfully, a list of Uploaded File List will show.

Customize Page Status		
Description	Status	Action
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		
login_01.jpg		
login_02.jpg		
login_03.jpg		
login_04.jpg		
login_05.jpg		
login_06.jpg		
login_07.jpg		
login_08.jpg		
login_09.jpg		
login_10.jpg		

Figure 45 – files have been uploaded

Verify if all files are uploaded successfully

Uploaded File List
aclogin.html
aclogout.html
but.gif
but_over.gif
icon.gif
line.gif
login_01.jpg
login_02.jpg
login_03.jpg
login_04.jpg
login_05.jpg
login_06.jpg
login_07.jpg
login_08.jpg
login_09.jpg
login_10.jpg
logout_01.jpg
logout_02.jpg
logout_03.jpg
logout_04.jpg
logout_05.jpg
logout_06.jpg

Figure 46 – verify all files

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 1024 x 768.

Customize Page Status		
Description	Status	Action
Customize Page	enabled	edit
Pop Logout Page	enabled	edit
Logout Page width size: <input type="text" value="1024"/> Logout Page Height size: <input type="text" value="768"/>		save cancel
Use External Page	disabled	edit

Figure 47 – set the pixels of logout window

Step3. Everything is ready

Now, any users that access the internet via the BW1330 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.



Figure 48 – example of coffee bar login page

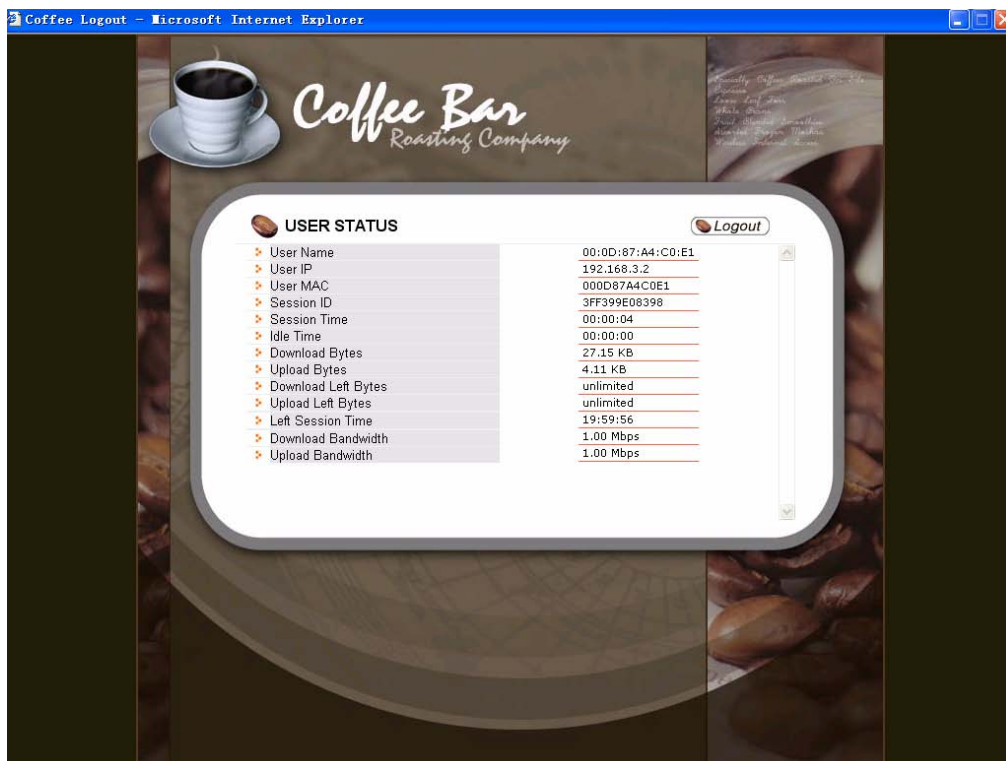


Figure 49 – example of coffee bar logout page

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 BW1330 and go to **user interface | configuration | Custom UAM** to disable "pop logout page."

4. Question: If I happen close the logout window, how can I logout?

Answer: 1. just un-plug you wireless card, or un-plug you network wire 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.

If you still have any question and any comments, please email to sse@browan.com

Chapter 6 – Command Line Interface

Introduction

The CLI (Command Line Interface) software is a configuration shell for the Access Controller. Using the CLI system operator can configure:

- User interface
- Network interface
- System

Using the CLI system operator can check:

- Status (device, network, service)
- Connection

All available key combinations in CLI mode are listed in the table below:

Key and/or Combination	Function
?	Get context-sensitive help
<TAB>	Complete the current keyword or list all the options
<CTRL> <D>	Break out the sub-shell
<CTRL> <A>	Jump to the beginning of the line
<CTRL> <E>	Jump to the end of the line
<CursUP>/<CursDOWN>	Scroll through the history of commands

Get Connection to CLI

There are three different ways to get a connection to the CLI of the Access Controller, via the:

- **Telnet**
- **SSH client**
- **Terminal**

Telnet Connection



Make sure that **default access status** is allowed and **telnet** function is enabled on the AC before trying to connect via **telnet**. Otherwise, no **telnet** connection will be available.

Connect the Access Controller via LAN or WAN ports using the enclosed UTP cable and start a telnet session (using a telnet application). For example, connect your device via the WAN port, and then make a telnet connection as the following:

```
telnet 192.168.2.66
```

where 192.168.2.66 is the default WAN interface IP. Login to CLI mode and the prompt will be displayed automatically. Enter the administrator login settings (refer to the **Login** section for details).

SSH Connection



Make sure that **default access status** is set to allow on the AC before attempting to connect via **SSH**. Otherwise no **SSH** connection will be available.

Connect the Access Controller via LAN or WAN ports using the enclosed UTP cable and start a SSH session (using an application as PuTTY). For example connect your device via the WAN port and then make a SSH connection to host IP: 192.168.2.66 (default WAN interface IP).

Login to CLI mode prompt will be displayed automatically. Enter the administrator login settings (refer to the next section for details).

Terminal Connection

A serial console port RS-232 on the BW1330 enables a connection to PC or terminal directly.

1. Connect one of the connectors of the RS-232 cable directly to the console port on the BW1330.
2. Connect the other end of the cable to the COM port of the PC or the terminal running the communication software.



The connection operates at 9600 baud, 8 data bits, 1 stop bit and no parity.

Login

Enter the administrator login settings in the displayed CLI command prompt.



The default administrator login settings:

Login: **admin**

Password: **admin01**

```
BW1330 login: admin
Password:
Press '?' for more information on available commands.
>
```

Figure 50 – CLI Login

After a successful login command prompt is displayed, the CLI is ready for commands. Press '?' to get a list of main commands:

```
connection: Device settings related to user's connection with device.
exit       : Exit command line interface.
network   : Device configuration settings affecting networking.
reboot    : Reboots the device.
reset     : Resets configuration to defaults and reboots the device.
shell     : Starts the shell.
status    : Device status information commands.
system    : System configuration.
telnet    : Runs telnet client.
user      : Device configuration settings affecting user's interface.
```

Figure 51 – Main CLI Commands



'?' will not appear on the screen. While pressing this character, the display changes to the desired help page. To enter '?' as character type '\?'.

Connection

Connection is a category of command that is related to the user's connection with the device.



A full list of all available **connection** commands/subcommands and its parameters is available in the Appendix section: **C) CLI Commands and Parameters**.

In general, connection usage is as follows:

```
connection <command> <value>
```

To get a list of all available commands in the connection category type:

```
connection ?
>connection

Device settings related to user's connection with device.
email      : Outgoing Main (SMTP) Redirection settings.
supervision: Settings for station availability monitoring with ARP-Pings.
```

Figure 52 – Connection Commands

Network

Network is a category of commands that configures controller interface settings, DNS, DHCP, UAT and RADIUS settings.



A full list of all available **network** commands/subcommands and its parameters is available in the Appendix section **C) CLI Commands and Parameters**.

The **network** commands themselves contain several subcommands and the subcommands again contain several parameters. In general, **network** command usage is as follows:

```
network <command> <subcommand1> <subcommand2> [-parameter] <value>
```

To get a list of all available commands in the configure category, type:

```
network ?
>network

Device configuration settings affecting networking.
configuration: Device configuration.
dhcp         : Dynamic Host Configuration Protocol services configuration.
dns          : DNS Server settings.
radius       : Configuration set for changing RADIUS Server settings.
tunnels      : Tunnels configuration commands.
```

Figure 53 – Network Commands List

To get a list of all-available subcommands for a specific command, type:

```
network <command> ?, (e.g. network radius ?)
```

All available subcommands for radius are displayed:

```
>network radius

Configuration set for changing RADIUS Server settings.
accounting_log: For sending RADIUS accounting via syslog.
proxy          : RADIUS Proxy configuration.
servers        : Up to 32 different RADIUS servers' configuration.
settings       : General RADIUS settings configuration.
wisp           : WISP information and setup.
```

Figure 54 – Configure Network (1)

Specific command contains several subcommands:

```
network <command> <subcommand1> ?, (e.g. network radius servers ?)
```

All available subcommands are displayed:

```
>network radius servers

Up to 32 different RADIUS servers' configuration.
accounting      : Accounting RADIUS servers' configuration.
authentication  : Authentication RADIUS servers' configuration.
backup          : Accounting information backup servers configuration.
```

Figure 55 – Configure Network (2)

To get a list for available parameters on selected subcommand, type:

```
network <command> <subcommand1> <subcommand2> ?, (e.g. network radius
servers accounting ?)
```

All available parameters on entered subcommand are displayed:

```
>network radius servers accounting

Accounting RADIUS servers' configuration.
<id>          : RADIUS server id.
-a <ip_address> : RADIUS server IP address used for Radius accounting.
-p <port>       : RADIUS server port used for Radius accounting.
-s <secret>     : Shared secret key for accounting(must be the same on RADIUS
server and RADIUS client).
```

Figure 56 – Configure Network (3)

To configure the desired controller interface setting, type all required parameters with values and subcommands:

```
network <command> <subcommand1> <subcommand2> [-parameter] <value>
(e.g. network radius servers accounting 1 -a 127.0.0.2 -p 1814 -s
testing111), where parameters are as follows:
```

- a – RADIUS server IP address used for RADIUS accounting
- p – RADIUS server port number used for RADIUS accounting
- s – Shared secret key for accounting.

```
>network radius servers accounting 0 -a 127.0.0.2 -p 1814 -s testing111
Command completed successfully.
```

Figure 57 – Configure Network (4)



If successful, a message regarding the successful completion is displayed; otherwise, an error message is displayed.

In some cases, entered commands without parameters display current controller configuration or settings:

`network <command> <subcommad1> <subcommad2>`, (e.g. `radius servers accounting`), displays available RADIUS servers and its settings list (in this case, the RADIUS accounting server which is already updated):

```
>network radius servers accounting
Id Name      Address      Port  Shared Secret Key
0  DEFAULT  127.0.0.2    1814  testing111
```

Figure 58 – Configure Network (5)

User

User is a category of commands that configures controller interface settings, affecting the user's interface: redirection URL, free sites (walled garden), system management access, administrator login/password.



A full list of all available **user** commands/subcommands and their parameters is available in the Appendix section: **C) CLI Commands and Parameters**.

In general, the **user** command usage is as follows:

```
user <command> <subcommand1> <subcommand2> [-parameter] <value>
```

To get the full list of the **user** commands, type:

```
user ?
```

```
>user
Device configuration settings affecting user's interface.
administrator: Administrator login and password change.
connected      : Connected users list.
oneclick       : One click roaming configuration.
start_page     : Definition of first URL after user login.
walled_garden : Free Web sites list.
webproxy       : Web proxy configuration.
```

Figure 59 – User Commands List

To get a list of all-available subcommands for a specific command, type:

```
user <command> ?, (e.g. user walled_garden ?)
```

All available subcommands for walled garden (free sites) are displayed:

```
>user walled_garden
Free Web sites list.
host: Configures free web sites that are not displayed to users.
url : Configure free web sites that are displayed to users.
```

Figure 60 – Configure User Interface (1)

To configure selected user interface settings, type:

```
User <command> <subcommand1> <subcommand2> [-parameter] <value>,
(e.g. user walled_garden url A -u www.gemtek-systems.com -s gemtek site),
where parameters are as follows:
```

A – action: add URL

-u – define URL address

-s – define URL description, visible for user:

```
>user walled_garden url A -u www.browan.com -s browan site
Command completed successfully.
```

Figure 61 – Configure User Interface (2)



If successful, a message regarding the successful completion is displayed; otherwise, an error message is displayed.

Status

Status is a category of commands that's displays:

- General **devices** status (model, firmware version, uptime, memory)
- All interface **network** settings (IP address/netmask, MAC address, gateway, RX/TX statistics)
- Currently running **services** (DHCP, routes, port forward, telnet, SNMP, UAT, ..).



A full list of all available **status** commands/subcommands and their parameters is available in the Appendix section: **C) CLI Commands and Parameters**.

In general the **status** command usage is as follows:

```
Status <command>
```

To get the full list of the **status** commands, type:

```
status ?
```

```
>status
Device status information commands.
device : General system information.
network: Network information.
service: Services information.
```

Figure 62 – System Status Commands List

To get the general device status information, type:

```
status device :
```

```
>status device
Device name      : BROWAN Inc. , SMB PAC, model: BW1330
Firmware version: BW1330.BRO.2.22.0014
Uptime          : 07:13:41
Software runtime: 07:13:16
Total memory    : 63220 kB
Free memory     : 28196 kB
Average load    :
1min:          : 1.01
5min:          : 1.03
15min:         : 1.00
```

Figure 63 – Device Status



Here you can find the current firmware **version** of your AC. This is important information for support requests and for preparing firmware uploads.

System

System is a category of commands that configures access to controller (telnet, AAA methods, L2 isolation, SNMP, UAT) and configuration: clock, NTP, pronto, syslog, trace and firmware upgrade.



A list of all available **system** commands/subcommands and their parameters are available in the Appendix section: **C) CLI Commands and Parameters**.

In general, the **system** command usage is as follows:

```
system <command> <subcommand1> <subcommand2> [-parameter] <value>
```

To get the full list of the **system** commands, type:

```
system
```

```
>system
System configuration.
access      : System access configuration.
configuration: System configuration.
```

Figure 64 – System Commands List

Telnet

To make a telnet connection, type the **telnet** command in the command line:

```
telnet
```

The telnet client is activated and ready for a telnet session.

```
>telnet 192.168.2.151
Entering character mode
Escape character is '^]'.
```

Figure 65 – Telnet Session

Quit the telnet to return to CLI interface.

Reboot

To stop the controller and reboot the device, type the **reboot** command in the command line. No configuration changes are done. The last saved configuration is applied to the rebooted controller.

Reset

To reset the controller to factory defaults, type the **reset** command. The device is restarted and defaults values are set.



Please note that even the administrator password will be set back to the factory default.

Exit

To leave the **CLI** mode, type the **Exit** command in the command line.

Chapter 7 – SNMP Management

Introduction

Another way to configure and monitor the Access Controller (BW1330) via a TCP/IP network is **SNMP** (Simple Network Management Protocol).

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

The SNMP agent and management information base (MIB) reside on the Access Controller. To configure SNMP on the controller, you define the relationship between the Network Management System (NMS) and the SNMP agent (our AC). The SNMP agent contains **MIB** and Brown Communications **private MIB** variables whose values the SNMP manager can request or change. A NMS can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.



In order to manage the device you have to provide your Network Management System software with adequate MIB files. Please consult your management software manuals on how to do that.

SNMP Versions

The BW1330 supports the following versions of SNMP:

- **SNMPv1** – the Simple Network Management Protocol: A Full Internet Standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- **SNMPv2c** – the community-string based Administrative Framework for SNMPv2. SNMPv2c (the "C" stands for "community") is an Experimental Internet Protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic), and uses the community-based security model of SNMPv1.
- **SNMPv3** – SNMP v3 is based on version 2 with added security features. It addresses security requirements through encryption, authentication, and access control rules.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

The Access Controller implementation of SNMP supports all MIB II variables (as described in RFC 1213) and defines all traps using the guidelines described in RFC 1215. The traps described in this RFC are:

coldStart

A coldStart trap signifies that the SNMP entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.

WarmStart

A WarmStart trap signifies that the SNMP entity, acting in an agent role, is reinitializing itself and that its configuration is unaltered.

authenticationFailure

An authenticationFailure trap signifies that the SNMP entity, acting in an agent role, has received a protocol message that is not properly authenticated.

linkDown

A linkDown trap signifies that the SNMP entity, acting in an agent role, recognizes a failure in one of the communication links represented in the agent's configuration.

linkUp

A linkUp trap signifies that the SNMP entity, acting in an agent role, recognizes that one of the communication links represented in the agent's configuration has come up.

SNMP Agent

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable – the SNMP agent begins this function in response to a request from the SNMP manager. The agent retrieves the value of the requested MIB variable and responds to the manager with that value.
- Set a MIB variable – the SNMP agent begins this function in response to a message from the SNMP manager. The SNMP agent changes the value of the MIB variable to the value requested by the manager.

The SNMP agent also sends unsolicited trap messages to notify an SNMP manager that a significant event has occurred (e.g. authentication failures) on the agent.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the SNMP manager to access the controller, the community string must match one of the two community string definitions on the controller. A community string can be as follows:

- Read-only – gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access.
- Read-write – gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings.

Use SNMP to Access MIB

As shown in the picture *as below* SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.



figure 66 SNMP Management

BROAN Private MIB

In addition to standard SNMP MIBs, BW1330 supports the Browan Communications private MIB. The private MIBs are enterprise specific and serve to extend the functionality of the standard MIBs. The Private MIB identifies manageable objects and their properties that are specific to the managed device. MIBs let you manage device not only by using WEB or Command Line Interface but also using SNMP protocol. The descriptions and brief explanations of managed objects are available in the MIB file. The MIB file is a specially formatted text file. It is using the so-called ASN.1 standard syntax.

Chapter 8 – Reference Manual

This chapter contains BW1330 web management reference information.

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

- **Network Interface** – device configuration settings affecting networking.
- **User Interface** – device configuration settings affecting the user interface.
- **System** – device system configuration settings directly applicable to the controller.
- **Connection** – device settings related to user's connection with the BW1330.
- **Built-In AAA** – Built-in AAA system for web authentication and accounting.
- **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 67 – Main Configuration Management Menu

By default the **system | status** menu is activated and the current AC system status is displayed. The active menu is displayed in a different color.

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

Network Interface

- Configuration** – configuration page for all controller network interfaces
 - Interface configuration** – network interfaces configuration
 - Bridge** – bridge configuration
 - VLAN** – define VLAN on your controller
 - Route** – define new static route on the controller interface
 - Port forwarding** – port-forwarding rules
 - DHCP Relay** – DHCP relay server configuration
 - User ACL** – define packet filter rules
 - Management subnet** – access points (APs) management
- DNS** – define DNS server settings
- DHCP** – Dynamic Host Configuration Protocol services configuration
- POP3** – POP3 server address configuration for client authentication
- RADIUS** – configuration set for RADIUS servers, includes menu:
 - RADIUS settings** – NAS server ID, hotspot operator name and other settings
 - RADIUS servers** – accounting, authentication RADIUS servers IP, port and other settings
 - WISP** – add new WISP on the system.
 - Proxy** – configure the AC to act as RADIUS server proxy.
 - Accounting backup** – backup authentication logs in the remote or external server
- Tunnels** – set tunnels:
 - PPPoE/ GRE for DSL** – connect to ISP via the PPPoE or GRE tunnel
 - GRE Client for VPN** – set the GRE (Generic Routing Encapsulation) tunnels for the BW1330
- Wireless** – wireless interface configuration
 - Basic** – primary SSID, regulatory domain, network mode, channels selection
 - Advanced** – multiple SSID configuration
 - WDS** – access point and WDS modes
 - SecWep** – WEP and WPA

User Interface

- Configuration** – Welcome/Login/Logout/Help page customization
- Pages** – configure and upload user pages

- Upload** – upload new internal user pages
- Headers** – define http headers encoding and language
- Remote authentication** –
- Custom Uam** – customized user login and logout page based by HTML page.
- Administrator** – administrator login and password change
- Start page** – define start page URL
- Walled Garden** – free web site list
- Web Proxy** – web proxy settings for clients

System

- Configuration** – system configuration utilities:
 - Syslog** – specify address where to send system log file
 - Clock** – system clock settings
 - NTP** – get time from network time protocol service
 - Certificate**– upload new certificates into the local controller memory
 - Save and restore** – save current device configuration for backup
 - Domain Name** – Configure BW1330 domain for uniform digital certificate.
 - Share Username** - setting user account shared status
- Access** – configure access to your controller:
 - Access Control** – set default access to your AC
 - Telnet** – enable/disable telnet connections
 - AAA** – define different AAA methods
 - UAT** – enable/disable universal address translation
 - Isolation** – restricts clients from communicating along Level 2 separation
 - NAV** – NAT, authentication and visitor access control
 - SNMP** – SNMP service and proxies
 - Web Auth** – Settings for auth methods of Built-in AAA
 - MAC List** –MAC ACL table.
 - HTTTPC** – Configure if client use HTTPS or HTTP for web authentication.
- Status** – AC system status
- Reset** – reset configuration to factory defaults values and/or reboot
- Update** – find out current software version and update with new firmware

Connection

- Users** – connected users' statistics list and log-out user function
- E-Mail Redirection** – outgoing mail (SMTP) redirection settings
- Station Supervision** – monitor station availability with ARP-pings settings

Built-in AAA

- E-Billing** – Post paid built-in AAA system
 - User Control** – management E-Billing (Built-in AAA) user account.
 - Band Class** – band width management for E-Billing account.
 - Bill settings** – configure the billing policy and price for E-Billing account
 - Power cut protection** – setting for power off protection
- Pre-paid** – per-paid built-in AAA system
 - User account** – show current generated pre-paid account
 - Price/unit** –setting of price and unit
 - Account life** –setting of receipts available life
 - Web key and SSID** –setting Web key and SSID printed on receipts
 - Receipts** – history of printed receipts and profit
 - Timeunit** –define the charge time by hour or day for the pre-paid user
 - Account reminder** – remind hot spot owner checking the income of prepaid account.
 - Manage net print** –set up the network printer for BW1330.
- Configuration** – Billing Backup and restore; Receipt Language and title configuration.
 - Language** – setting language of printed receipts
 - Backup and Restore** – Backup and restore Built-in AAA account and billing records.
 - Title** – setting of venue name

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

Network Interface

Network Interface | Configuration | Interface Configuration

The SMB Public Access Controller contains two multi-purpose network interfaces: br1 and ixp1.

These interfaces can be configured to work as either local area network (LAN) or wide area network (WAN) interfaces or wireless area network(WLAN) for Access Points. LAN is used to connect hubs, switches, Access Points and subscribers. The WAN port connects to the Internet or the service provider's backbone network. The wlan1_0 is the first virtual AP for wireless network.

All these interfaces are listed in the **interface configuration** page. By default a bridge exists (labeled br1) which contains two interfaces: wlan1 and ixp0. All network interfaces available in the SMB Public Access Controller are shown in the following table:

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled	LAN	192.168.3.1	255.255.255.0	ixp1	edit
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	edit

Figure 68 – Interface Configuration Table

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

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled <input type="button" value="v"/>	LAN	192.168.3.1	255.255.255.0	ixp1	continue cancel
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	

Figure 69 – Edit Interface Configuration Settings part.1

Interface - standard interface name. This name cannot be edited and is assigned by the operating system during startup. Interface name cannot be changed because the hardware drivers define it.

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



Do not disable the interface through which you are connected to the BW1330. Disabling such interface will lose your connection to the device.

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;

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:

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled	LAN	<input type="text" value="192.168.3.1"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="ixp1"/>	update cancel
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	

Figure 70 – Edit Interface Configuration Settings part.2

IP Address – specify new interface IP address [in digits and dots notation, e.g. 192.168.5.1].



IP address of each interface should be from a 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 can only be defined as WAN interface gateway. The gateway of the WAN interface is usually the gateway router of the ISP or other WAN network. [Default gateway is marked with “*”].

Update – update old values with entered ones.



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

Warning: DHCP settings were adjusted to match network settings.

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled	LAN	192.168.5.1	255.255.255.0	ixp1	edit
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	edit

[apply changes](#) [discard changes](#)

Figure 71 – Apply or Discard Interface Configuration Changes

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

Discard changes – restore all previous values.

For such general changes as interface settings change, the Wireless PAC server needs to be restarted. Request for restart server appears:

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled	LAN	192.168.5.1	255.255.255.0	ixp1	edit
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	edit

Server software needs to be reboot. [reboot](#)

Figure 71 – Restart Server

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

Network Interface | Configuration | Bridge

A bridge transparently relays traffic between multiple network interfaces. This means that a bridge connects two or more physical LAN interfaces together to form one bigger (logical) network interface. There are some restrictions for bridge management that shall be taken into account:

- There is special bridge **br1** in BW1330 that cannot be removed. This bridge initially contains two interfaces: wlan1_0 and ixp0.
- Interfaces (physical, VLAN or GRE tunnel) can be included only in one bridge.
- The WAN interface cannot be included into a bridge.
- VLAN's cannot be created on bridge interfaces they can only be added to them.
- A Bridge cannot be included into another bridge.

By default the enabled bridge (ixp0 and wlan1_0) on br1 interface exists on the system:

bridge									
ID	status	ageing	garbage	STP	priority	delay	hello time	max. age	action
br1	enabled	0	0	disabled	low	0	0	0	edit

figure 72 - Default Bridge

To set up bridge on the AC click **edit** button and enter following parameters:

bridge									
ID	status	ageing	garbage	STP	priority	delay	hello time	max. age	action
1	enabled	<input type="text" value="0"/>	<input type="text" value="0"/>	disabled	low	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	continue cancel

figure73 - setting parameters

Ageing – define the Ethernet (MAC) address ageing time, in seconds [0-65535]. The ageing time is the number of seconds a MAC address will be kept in the forwarding database after having received a packet from this MAC address. The entries in the forwarding database are periodically timed out to ensure they won't stay around forever. Default value is 0.

Garbage – specify the interval in seconds between garbage collector runs [0-65535]. Garbage collector periodically checks MAC table for timed out entries and removes them from the table. Default value is 0.

STP –define the STP (Spanning Tree Protocol) status [enabled/disabled].

Priority – define the bridge's priority [high,medium,low]. Default value is low.

Delay – specify the bridges' forward delay time in seconds [0-65535]. Delay is the time spent in each of the Listening and Learning states before the Forwarding state is entered. Default value is 0.

Hello Time – specify the interval between hello packets in seconds [0-65535]. Hello packets are used to communicate information about the topology throughout the entire Bridged LAN. Default value is 0.

Max. Age – specify the maximum bridge message age in seconds [0-65535]. If the last received hello packet is more than this value, the bridge in question will initiate the Root Bridge election procedure. Default value is 0.

Click **continue** button to finish the parameters setting and click **new** button if needs new interfaces adding into bridge.

bridge									
ID	status	ageing	garbage	STP	priority	delay	hello time	max. age	action
br1	enabled	0	0	disabled	low	0	0	0	

bridge ports			
port (interface)	cost	priority	action
ixp0	low	low	edit delete
wlan1_0	low	low	edit delete
			new
			back

figure – 74 bridge setting

Click new button to add interfaces into bridge and specify the bridge ports (interfaces):

bridge									
ID	status	ageing	garbage	STP	priority	delay	hello time	max. age	action
br1	enabled	0	0	disabled	low	0	0	0	

bridge ports			
port (interface)	cost	priority	action
wlan1_0	low	low	
wlan1_1	low	low	
<input type="text" value="wlan1111"/>	<input type="text" value="low"/>	<input type="text" value="low"/>	save cancel

figure – 75 add interface

Port (interface) – select the interface name to be bound into bridge .

Cost – specify the port's path cost on this interface. This value is used in the designated port and root port selection algorithms. Default value is low.

Priority – specify the priority of ports with equal cost. You can use this to control which port gets used when there are redundant paths.

If you want to remove interface from bridge click delete button. e.g remove ixp0 from bridge.

Click delete button on the ixp0 column.

bridge ports			
port (interface)	cost	priority	action
ixp0	low	low	edit delete
wlan1_0	low	low	edit delete
			new
			back

figure 76 – remove interface

Click apply changes button and then reboot system to finish the removing.

bridge ports			
port (interface)	cost	priority	action
wlan1_0	low	low	edit delete
			new
			back
		apply changes	discard changes

figure 77- apply and reboot

Network Interface | Configuration | VLAN



Up to **4094** VLANs can be created in the system.

Virtual Local Area Networks (**VLANs**) are logical groupings of network resources. You can create your own VLANs on your AC using the network **interface | configuration | VLAN** menu. By default no VLANs are defined on the system:

VLAN						
interface	status	ID	IP address	netmask	gateway	action
no VLAN entries are defined on system						
						new

Figure 78 – VLAN

To create a VLAN on the AC click the new button and enter following parameters:

VLAN						
interface	status	ID	IP address	netmask	gateway	action
ixp0	disabled	<input type="text" value="1111"/>	-	-	-	save cancel

Figure 79 – Create New VLAN

Interface – select interface for your VLAN network. VLANs cannot be created on a bridge.

Status – non-editable, by default is disabled.

ID – assign ID for your VLAN network [1 to 4094]. Client devices that associate using the ID are grouped into this VLAN.



You can not create VLANs which interface includes in bridge such as ixp0.If you want to create VLANs on the interface ixp0 you must separate ixp0 from bridge(br1 interface) via **network interface| configuration| Bridge** menu. Refer to **Chapter 8 Network Interface | Configuration | Bridge**

Please note after remove ixp0(LAN) it is DHCP server disabled as default.You will connect BW1330 either via WAN port(fix IP:192.168.2.66) or wlan1_0 wireless connected which DHCP server enabled(ip:192.168.3.x) as default.

Other VLAN settings cannot be changed. Click on the **disabled** link to continue specifying settings for your VLAN. The network interface configuration page is opened and VLAN settings are ready for editing:

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled	LAN	192.168.3.1	255.255.255.0	ixp1	
ixp0	enabled	LAN	192.168.5.1	255.255.255.0	ixp1	
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	
vlan1111 (ixp0)	disabled	LAN	0.0.0.0	0.0.0.0	0.0.0.0	continue cancel

Figure 80 – Configure VLAN

Status – enable/disable your VLAN network. Select [enable] and click the **continue** button to configure the VLAN settings:

interface configuration						
interface	status	type	IP address	netmask	gateway	action
br1	enabled	LAN	192.168.3.1	255.255.255.0	ixp1	edit
ixp0	enabled	LAN	192.168.5.1	255.255.255.0	ixp1	edit
ixp1	enabled	WAN	192.168.2.66	255.255.255.0	*192.168.2.1	edit
vlan1111 (ixp0)	enabled	LAN	192.168.100.1	255.255.255.0	ixp1	edit

apply changes **discard changes**

Figure 81 – Configure VLAN

Type – cannot be edited, depends on selected interface for VLAN [ixp0].

IP Address – enter the network address of your VLAN [format: digits and dots].

Netmask – enter the netmask for your VLAN network [format: digits and dots].

Gateway – select gateway for VLAN network [default: ixp1].

Click the **update** and **restart** and **apply changes** to save your new VLAN. Check the **interface | configuration | VLAN** menu for new created VLAN:

VLAN						
interface	status	ID	IP address	netmask	gateway	action
ixp0	enabled	vlan1111	192.168.100.1	255.255.255.0	ixp1	delete

new

Figure 82– Enable New VLAN

Network Interface | Configuration | Route

Under the **network interface | configuration | route** menu, static routes for the Ethernet interfaces can be set. By default no static routes are defined on the system:

route						
interface	status	gateway	target IP address	netmask	action	
no routes are defined on system						

new

Figure 83 – Route

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:

route						
interface	status	gateway	target IP address	netmask	action	
ixp0	enabled	0.0.0.0	192.168.3.0	255.255.255.0	save	cancel

Figure 84 – Add New Route



If you want to set static routes on the interface ixp0 you must separate ixp0 from bridge (br1 interface). Refer to **Chapter 8 Network Interface | Configuration | Bridge**

Interface – choose device interface for the route: [br1/ixp0/ixp1/vlan[n]].

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].

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

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

Save – save the new route.

Cancel – restore all previous values.

route						
interface	status	gateway	target IP address	netmask	action	
ixp0	disabled	0.0.0.0	192.168.3.0	255.255.255.0	edit	delete
						new

Figure 85 – Save New Route



Up to **255** static routes can be set between each interface.

Network Interface | Configuration | Port Forwarding

Port Forwarding is required when NAT is configured. NAT translates all internal addresses to one official IP address (WAN IP address). With port forwarding enabled it is possible to access internal services and workstations from the WAN interface.

Port forwarding forwards TCP or UDP traffic through the BW1330 controller's local port to the specified remote port. Use the **network interface | configuration | port forwarding** menu to specify such a port forwarding rule. By default no port forwards are defined on the controller:

port forwarding							
status	type	local IP address	local port	remote IP address	remote port	action	
no port forwards defined							
							new

Figure 86 – Port Forwarding Rules

Click the new button to add a port-forwarding rule:

port forwarding							
status	type	local IP address	local port	remote IP address	remote port	action	
enabled	TCP	192.168.2.248	8080	1.2.3.4	8080	update	cancel

Figure 87 – Add Port Forwarding Rule.

Status – select status: [enabled/disabled].

Type – select type of forwarding traffic: [TCP/UDP].

Local IP Address – BW1330 device interface address from which the selected traffic should be forwarded.

Local Port – BW1330 device interface port from which the selected traffic should be forwarded.

Remote IP Address/Port – internal IP address and port no (LAN ports) to which the selected traffic shall be forwarded.

Example:

Create rule as follow:

Type = TCP, local IP address/port = 192.168.2.248:8080 remote IP address/port = 1.2.3.4:8080.

With such a rule all traffic coming to port 8080 on the BW1330 interface local address 192.168.2.248 will be forwarded to port 8080 on the server (host) 1.2.3.4.



Port forwarding is limited to **255** rules.

Network Interface | Configuration | DHCP Relay

If BW1330 use DHCP relay on its LAN interface, administrator can designate the DHCP relay server.

DHCP Relay		
setting	value	action
DHCP Server Address	255.255.255.255	edit

Figure 88 – DHCP Relay Server

The default value is “255.255.255.255”, it means BW1330 will broadcast client's DHCP request to its WAN interface. Administrator can designate an only server's IP address.

Network Interface | Configuration | User ACL

User ACL provide high flexibility for administrator to define the rules for BW1330 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	Destination IP	Destination Netmask	Destination Port	Action
No acls are defined on system.											
											new

Figure 89 – User ACL

To add a new rule, just click the “new” button

User ACL											
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source Ip	Source Netmask	Source Port	Destination IP	Destination Netmask	Destination Port	Action
1	DROP	all	any	any	-	-	-	-	-	-	continue cancel

Figure 90 – 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).Then decide the incoming and outgoing interfaces(any/br1/ixp1).

User ACL											
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source Ip	Source Netmask	Source Port	Destination IP	Destination Netmask	Destination Port	Action
1	ACCEPT	udp	any	any	Special IP	-	-	Special IP	-	-	continue cancel

Figure 91 – 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	Destination IP	Destination Netmask	Destination Port	Action
1	ACCEPT	udp	any	any	special	-	Special Port	any	-	Special Port	continue cancel

Figure 92 – 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	Destination IP	Destination Netmask	Destination Port	Action
1	ACCEPT	udp	any	any	192.168.5.0	255.255.255.255	12	any	-	45	save cancel

Figure 93 – 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 do not need 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 do not need fill out the port).

User ACL											
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source Ip	Source Netmask	Source Port	Destination IP	Destination Netmask	Destination Port	Action
1	ACCEPT	udp	any	any	192.168.5.0	255.255.255.0	12	any	-	45	delete sort

Figure 94 – 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. Click the “sort” button to change the index.

User ACL											
Index	Policy	Protocol	In Interfaces	Out Interfaces	Source Ip	Source Netmask	Source Port	Destination IP	Destination Netmask	Destination Port	Action
1	ACCEPT	udp	any	any	192.168.5.0	255.255.255.0	12	any	-	45	
2	DROP	tcp	any	any	192.168.3.7	255.255.255.255	80	any	-	80	save cancel

Figure 95 – re-order rules

Click the “sort” button of one rule to re-order its priority and then select the index number; click “save” button to save your changes.

Network Interface | Configuration | Management Subnet

Each network interface can have a **management subnet**. Use the **network interface | configuration | management subnet** menu to configure this feature on selected interface.



When **management subnet** is enabled, **port forwarding will NOT WORK** when connecting from IP addresses that are in the management subnet's **remote administrator's network**. This is because the **management subnet** allows connecting to the client computer without using **port forwarding**.

The administrator can enable or disable management subnet for each interface. By default no management subnet is enabled on the controller:

management subnet						
interface	status	IP address	netmask	remote network	remote netmask	action
br1	disabled	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	edit
ixp0	disabled	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	edit
vlan1111	disabled	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	edit

Figure 96 – Management Subnet

To specify new subnet management click the **edit** button on the selected interface:

management subnet						
interface	status	IP address	netmask	remote network	remote netmask	action
br1	disabled	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	edit
ixp0	enabled	10.0.0.1	255.255.255.0	10.0.0.0	255.255.255.0	edit
vlan1111	disabled	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	edit

Figure 97 – Add Management Subnet

IP Address and **Netmask** – specify the IP address and netmask of the management subnet. **IP address** will be set on the network interface as an alias, so you can connect to the BW1330 using this address. This IP address should be used on access points as the gateway address.

Remote Network and **Netmask** –specify the remote network that is allowed to access the local management subnet. Only addresses that are from the remote network will be accepted [dots and digits].

If you do not specify any remote network all stations with IP addresses from the management LAN are routed to the WAN port even without being authenticated.

Clients using an IP address from the management subnet can browse the Internet without authorization, and no accounting will be done. Thus, it is strongly recommended to allow traffic only from the administrative remote network (no 0.0.0.0/0.0.0.0 in remote specification).

Example:

Interface configuration for ixp0:

```

type:          LAN
IP address:    192.168.3.1
netmask:      255.255.255.0
gateway:      ixp1

```

Management subnet on ixp0:

```

IP address:    10.0.0.1
netmask:      255.255.255.0
remote network: 10.10.0.1
remote netmask: 255.255.255.0

```

With these settings applied, the administrator will be able to connect to devices behind the BW1330 on interface ixp0, if these devices use address in the range: 10.0.0.2 ... 10.0.0.254. The administrator is connecting via the Internet (from ixp1 interface).

The administrator's computer can have an address from 10.10.0.1 to 10.10.0.254.



Please note that devices which are using 10.0.0.2 – 10.0.0.254 addresses have access to the administrative network too!

In this example, the administrative network uses the reserved IP address (10.x.x.x) – they are not routed in the Internet, so the administrator should setup routers in a path between the BW1330 and the administrator's computer to recognize 10.x.x.x addresses and route them correctly. This is not comfortable and sometimes it is impossible. There is a solution – the administrator can use GRE tunnel(see: **Network Interface | Tunnels**) to setup a tunnel between the administrator's computer and the BW1330. The only addresses visible on the Internet will be the BW1330 WAN IP address and the administrator's computer (or router) IP address.

Network Interface | DNS

DNS (Domain Name Service) service allows AC subscribers to enter URLs instead of IP addresses into their browser to reach the desired web site.

DNS		
type	IP address	action
primary	202.96.209.5	edit
secondary	202.96.209.133	edit

Figure 98 — DNS Settings Configuration

You can enter the **primary** and **secondary DNS** servers settings under the **network interface | DNS** menu.

DNS		
type	IP address	action
primary	202.96.209.5	
secondary	<input type="text" value="168.95.1.1"/>	save cancel

Figure 99—Edit DNS Redirection Settings

The **DNS server** or **DNS address** can be obtained dynamically if DHCP, PPPoE (for DSL) service is enabled. To add **DNS** server manually click the **edit** button in the **action** column and type in the **DNS** server's IP address:

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

Save – click to save the new DNS server's settings.

Network Interface | DHCP

The **BW1330** controller can act as a **DHCP server** and/or as a **DHCP relay gateway**. The **DHCP** (Dynamic Host Configuration Protocol) service is supported on the LAN interfaces [ixp0/vlan[n]]. 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					
status	interface	IP address from	IP address to	WINS address	action
DHCP server	br1	192.168.3.1	192.168.3.254	0.0.0.0	details edit

Figure 100 – DHCP Configuration



By default the AC is configured to act as a **DHCP server**.

Each LAN interface runs a different instance of the **DHCP** service. This service is configured by defining an IP address range and WINS address for client workstations. Other settings, such as the default gateway and DNS server address are configured automatically according to the interface settings.

To see the complete **DHCP** service configuration, click the **details** button in the action column:

DHCP		
description	value	action
status	DHCP server	
interface	br1	
IP address from	192.168.3.1	
IP address to	192.168.3.254	
WINS address	0.0.0.0	
lease time (seconds)	300	
domain		
DNS address	202.96.209.5	
DNS secondary address	0.0.0.0	
		back edit

Figure 101 – DHCP Settings Details

To edit the **DHCP** service configuration [DHCP server/DHCP relay], click the **edit** button in the **action** column:

DHCP		
description	value	action
status	<input type="text" value="DHCP server"/>	update cancel
interface	br1	
IP address from	192.168.3.1	
IP address to	192.168.3.254	
WINS address	0.0.0.0	
lease time (seconds)	300	
domain		
DNS address	202.96.209.5	
DNS secondary address	0.0.0.0	

Figure 102 – Edit DHCP Configuration Settings

Status – select status from drop-down menu:

- Disabled** – disable the DHCP service on the selected interface
- DHCP Server** – enabled by default
- DHCP Relay** – to route DHCP through the external server, enable relay service

Case 1 Configure the DHCP server

Select the interface on which you want to configure the DHCP service. Select the **DHCP server** and click the **update** button specify the DHCP server parameters: