If no OID is specified all SNMP request to the controller will be redirected to a specific host.

SNMP Trap Table:

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

Figure 192 – SNMP Trap Table

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

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

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

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

System | Access | Web Auth

Web auth controls all the built-in AAA web authentication method.

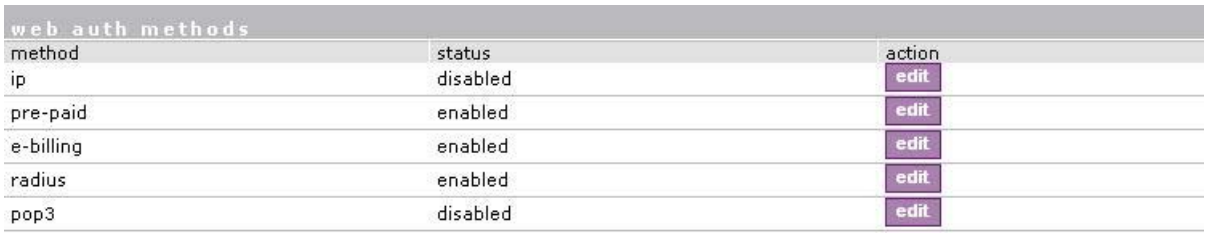

Figure 193 – Web Authentication methods

IP: IP authentication method. it means every client who has an IP address can be authenticated. Before client authentication, its first web access of client will be redirected to a confirm/login page, Need not any username or password, user just press confirm or OK button then client will be automatically authenticated and client's MAC address will be act as the username of login session.

Pre-paid: If Pre-paid authentication was disabled, BW1330 would not use pre-paid database to authenticate clients.

e-billing: If e-billing authentication was disabled, BW1330 would not use E-Billing built-in database to authenticate clients.

RADIUS: BW1330 would use extern RADIUS server to do authenticate client if RADIUS authentication setting was enabled.

POP3: By using pop3 mail address for user authentication.

BW1330 executes the web authentication with the below web authentication method order: IP auth, Pre-paid auth, e-billing Auth and RADIUS auth. If one auth method failed (including setting of the auth method is disabled), try next.

System | Access | Mac List

The MAC list is a client pass-through table. If MACACL (***system | Access | AAA***) is enabled and the client's MAC address is belong to this table. Then the client will be authorized transparently. (Please refer to MACACL item in ***System | Access | AAA***.

Press the "NEW" button to add a new MAC address to the table. The format of a MAC address can be:

xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx or xxxxxxxxxx

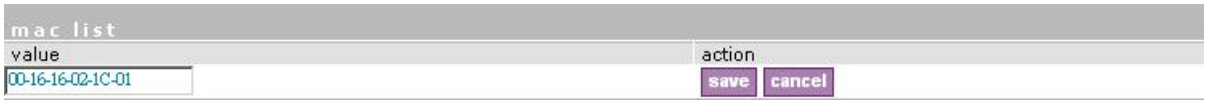

figure 194-MAC format

Figure 195 – MAC List for MAC-ACL

Press the "apply changes" button to save the changes to flash after you finish your input..

Figure 196 – Add new MAC address

System | Access | HTTPC

For web authentication, this item configure whether redirect web logon user to a HTTPS logon page or HTTP page.

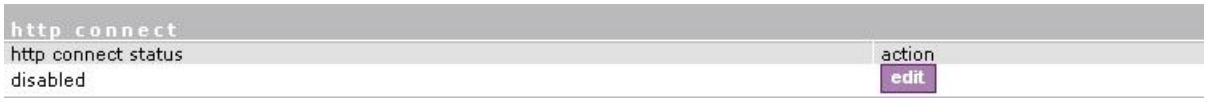

Figure 197 – HTTPC configuration for web logon.

Default configuration is disabled. It means web logon client will be redirected to a HTTPS logon page for more security.

System | Status

Use the **system | status** menu to check the BW1330 current status:

- **Device statistics** (including device name, model, firmware version, status, logged administrators, general uptime, memory, load, connected clients)

device statistics	
description	value
device name:	BROWAN Inc. , SMB PAC, model: BW1330
firmware version:	BW1330.BRO.2.22.0015
device status:	running
currently connected administrators:	admin @ 192.168.3.2 Idling: 00:00:00
uptime:	01:38:12
software runtime:	01:37:49
total memory:	63220 kB
free memory:	30324 kB
average load:	1min: 1.04
	5min: 1.10
	15min: 1.06
connected clients number:	1
connected clients input bytes:	8.76 MB
connected clients output bytes:	546.75 KB

Figure 198 – Device Statistics

Device Name – full device name and model.

Firmware Version – the current version of the firmware.

Device Status – current device status: running/warning.

Currently Connected Administrators – logged administrators list in format: [administrator name, IP address, and idling time in hours/minutes/seconds].

Uptime – indicates the time, expressed in days, hours and minutes since the system was last rebooted [days/hours/minutes/seconds].

Software Runtime – indicates the time, expressed in days, hours and minutes since the software reboot. The system itself can restart the software without rebooting the device [days/hours/minutes/seconds].

Total Memory – total operational memory of your BW1330 [kB].

Free Memory – indicates the memory currently available in the controller [kB].

Average Load – indicates the average load of the BW1330 processor in the period of the last 1minute, 5 minutes and 15 minutes (a larger value means a larger average load on the processor).

Minimum load – 1.0
Normal load – should not exceed 2.0 (including)
Processor is busy – more than 2.0

Connected Clients Number – total number of current connected clients. Click on the settings and get detailed connected clients list (clients page under the **connection | user**):

users						
no	user	interface	user IP	time length	idle time	action
01.	gary	br1	192.168.3.2	00:36:16	00:00:54	details logout user
						refresh

Figure 199 – Connected Clients Detailed List

Connected Clients Input Bytes – current connected clients' total Input bytes [K, KB, MB, GB].

Connected Clients Output Bytes – current connected clients' total Output bytes [K, KB, MB, GB].

- **WAN interface (ixp1**) (including the IP address, netmask, gateway, MAC address of the WAN interface, DNS servers, RX/TX statistics)

WAN (ixp1)	
description	value
IP address:	192.168.0.66
netmask:	255.255.255.0
gateway:	192.168.0.1
MAC:	00:16:16:02:21:A1
DNS servers:	202.96.209.5
	202.96.209.133
RX/TX:	9165987/663590

Figure 200 – WAN Interface Statistics

- **RX** – indicates data volume received on the WAN interface since reboot.
- **TX** – indicates data volume transmitted to the WAN interface since reboot.

- **LAN interface (br1)** (including the IP address, netmask, MAC address of the LAN interface, RX/TX statistics)

LAN (br1)	
description	value
IP address:	192.168.3.1
netmask:	255.255.255.0
MAC:	00:16:16:02:21:A0
RX/TX:	619949/9387439

Figure 201 – LAN Interface Statistics

- **RX** – indicates data volume received on the LAN interface since reboot.
- **TX** – indicates data volume transmitted to the LAN interface since reboot.

- **Services** (all services list with its status: enabled/disabled)

services	
description	value
VLAN:	enabled
management subnet:	disabled
route:	disabled
port forwarding	disabled
DHCP servers:	enabled
RADIUS proxy:	disabled
remote authentication:	disabled
walled garden:	disabled
web proxy:	enabled
NTP status:	enabled
default access control status:	allow
telnet:	enabled
SSH:	enabled
UAM:	enabled
EAP802.1X:	disabled
MAC authentication:	disabled
universal address translation:	disabled
user isolation:	disabled
NAT:	enabled
client authentication status:	enabled
visitor access:	disabled
SNMP service status:	enabled
e-mail redirection:	disabled
	refresh

Figure 202 – Services

Services are displayed as a link to the respective menu where status can be configured.

Refresh – click the button to refresh device status statistics.

System | Reset

If you need to reboot your device or reset to factory defaults select the **system | reset** menu:

reset/reboot	
description	action
reset configuration to factory defaults	reset
reboot device	reboot

Figure 203 – Reset and Reboot

Reset – reset device to factory default values.

Keep in mind that resetting the device is an irreversible process.
Please note that even the administrator password will be set back to the factory default.

Reboot – reboot device with the last saved configuration.

System | Update

Check for new product updates at the Browan Communications website: http://www.browan.com

To update your device firmware, use only the original firmware image and under **system | update** menu click the **upload** button:

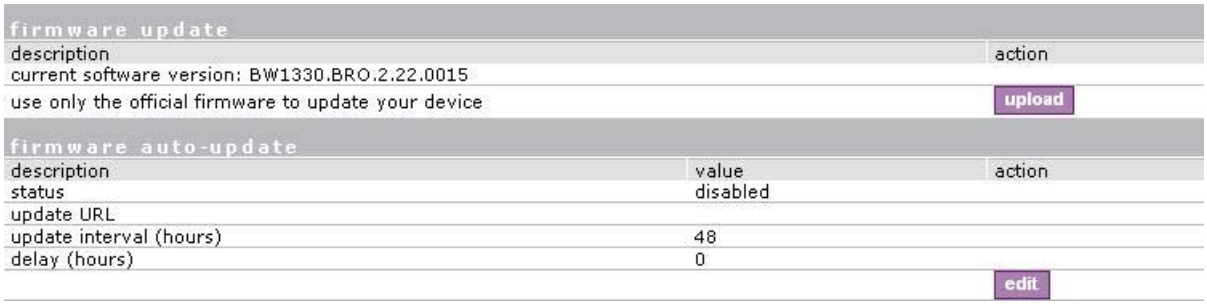

Figure 204 – Firmware Update

Specify the full path to the new firmware image and click the **upload** button:

Figure 205 – New Firmware Upload

Firmware Image – enter the firmware image using the full path.

Browse – click the button to specify the new image location.

Upload – upload with new firmware.

Cancel – cancel the upload process.

New firmware image is uploaded into the controller. Now you need to upload this new firmware into the controller's FLASH memory, click the **flash** button:

Figure 206 – Flash New Image

Flash – flash new image, reboots the system.

Do not switch off and do not disconnect the BW1330 from the power supply during the firmware update process because the device could be damaged.

Firmware auto-update:

Auto-update function allows update device firmware automatically. This function will help for large enterprises, having hundreds of AC's, to keep them up to date.

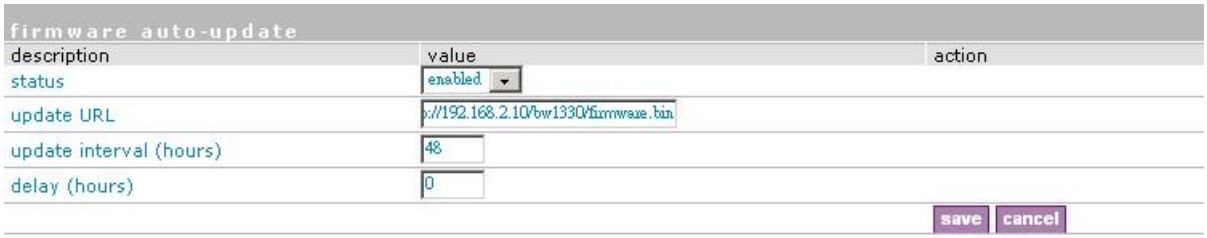

Figure 207 – Firmware Auto-update Configuration

Status - defines if auto-update is enabled or disabled. Default value disabled.

Update URL - defines where firmware should be downloaded from. It points directly to firmware update file. URL should be accessible without any user authentication. URL can use HTTP, HTTPS and FTP protocols. Default value - empty string.

Update interval – define the time interval between each update in hours [1-9999]. Time is counted from last device boot-on. Default value is 48 hours.

Delay – delays update process by given amount of hours. This should prevent from getting hundreds requests for firmware download at the same time [0-24]. Default value is 0.

Save - save new firmware auto-update settings.

On boot auto-update feature checks for available updates on specified server at given URL. If there is different version - device downloads, installs firmware update and reboots. If firmware version matches current version on device - no update takes place.

Connection

Use the **connection** menu to view the connected user's statistics, set outgoing mail server or observe the connected station availability.

Figure 208 – Connection Menu

Connection | Users

The **users** menu is for viewing the connected users' statistics. Also ability to **logout user** from the system is implemented here:

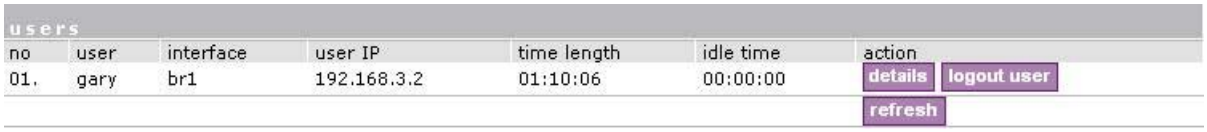

Figure 209– Users' Statistics

The users' statistics parameters are as follows:

No – number of the user's session connection.

User – username of the connected client.

Interface – name of interface, through which client is connected [br1].

User IP – IP address, from which the user's connection is established. Address is presented in digits and dots notation.

Time length - session duration since the user login.

Idle Time - amount of user inactivity time [hours: minutes: seconds].

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

Figure 210 – User's Details

User – the username of the connected client.

Interface – name of interface, through which client is connected.

User IP – IP address, from which the user's connection is established. Address is presented in digits and dots notation.

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

Authentication mode – authentication method which user uses to connect.

WISP – WISP domain name where the user belongs.

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

Time length – session time duration since user login [hours: minutes: seconds/unlimited].

Remaining Time length– remaining user's session time [hours: minutes: seconds/unlimited]. Session time for user is defined in the RADIUS server.

Idle Time - amount of user inactivity time [hours: minutes: seconds].

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

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

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

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

Back – returns to connected client's statistics list.

Logout User – click this button to explicitly logout user from the network.

Refresh – click the button to refresh users' statistics.

Connection | E-mail Redirection

The outgoing mail (SMTP) server redirection is performed using the **e-mail redirection** menu. By default such redirection settings is displayed:

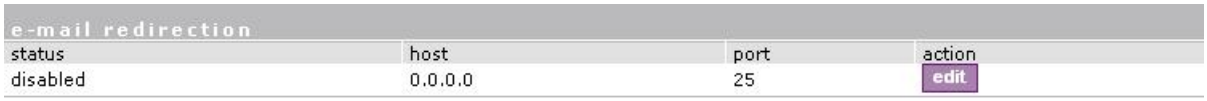

Figure 211 – E-mail Redirection Settings

Click the **edit** button to specify your outgoing mail server settings.

Figure 212 – Edit E-mail Redirection

Status – enable/disable e-mail redirection function.

Host – SMTP server address where to redirect the outgoing clients e-mails [enter host name or host IP address].

Port – port number [number, by default: 25].

Save – save new e-mail redirection settings.

Connection | Station Supervision

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

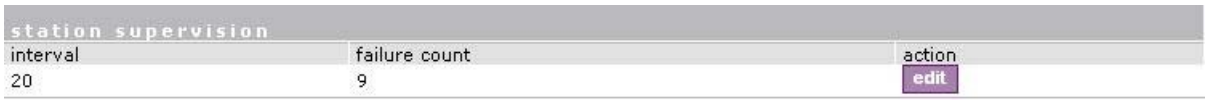

Figure 213 – Station Supervision

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

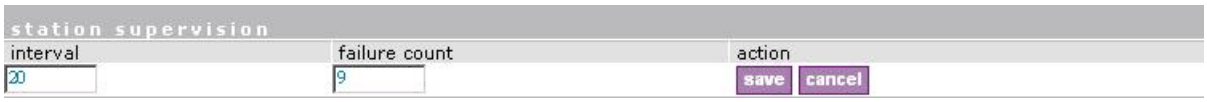

Figure 214 – Edit Station Supervision

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

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

Save – save station supervision settings.

Cancel – cancel changes.

Built-In AAA

Use built-in AAA to configure the post-paid account (e-billing) and pre-paid account (pre-paid) of built-in AAA system.

Figure 215 – Built-In AAA Menu

Built-in AAA | E-Billing

Hotspot owner can use this function to create E-Billing user account, set the E-Billing account billing policy and price. With this feature, hotspot owner can setup public access service without external RADIUS server.

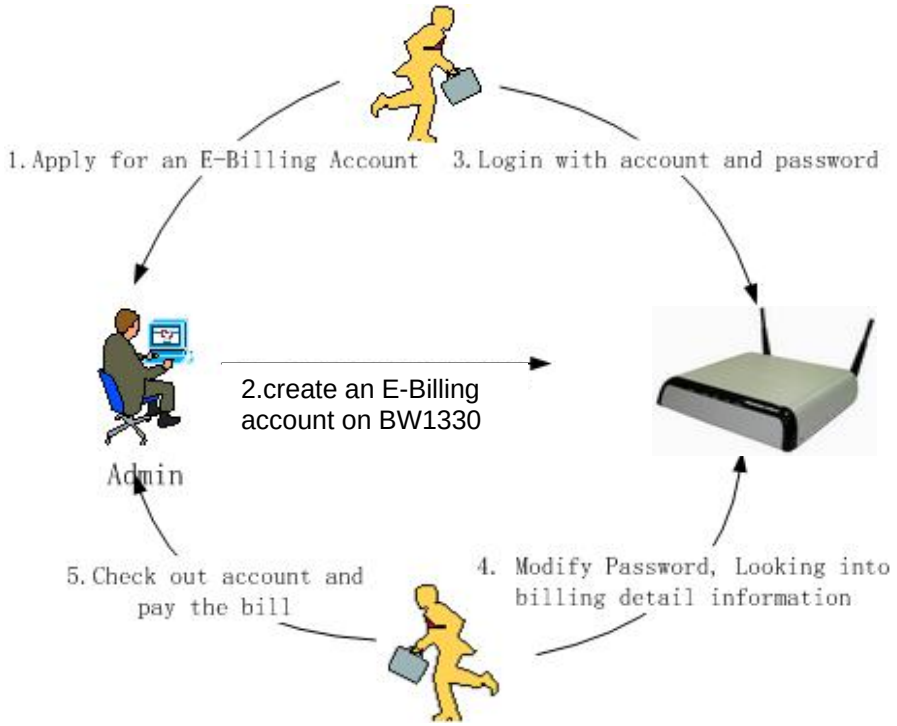

Figure 216 – E-Billing operate mode

Built-in AAA | E-Billing | User Control

"User control" provides an interface to manage E-Billing user accounts.

Figure 217 – Ebilling accounts

You can edit or delete exist E-Billing accounts, change their password or check account's billing information. Click the "new" button will create a new E-Billing account.

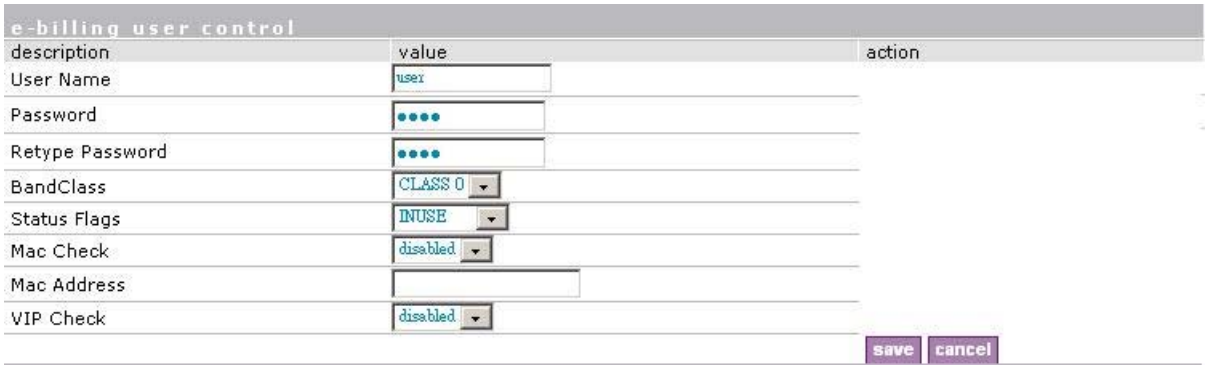

Figure 218 – Create new ebilling account

New created account need fill out below item:

1. User Name – user of e-billing account.
2. password – Password of the user to be logged on.
3. retype password – re-enter the new password to verify its accuracy
4. Band Class: means account priority, BW1330 support 3 priority class for E-Billing account, each priority class relevant to different bandwidth. Detail will descript in **Built-in AAA| E-Billing| Band Clas**s
5. Status flags: **InUse**, **Suspend** and **NoUse**.

   InUse: This account is normal, user can use this account to login.

   Suspend: This account will be temporary suspend for some reason such as this account will not be use for some days.

   NoUse: This account will be NoUse. Account recycle will delete this account after 72 hours.

   If E-Billing account status flags are **NoUse** or **Suspend**, this logon process by this account will be failed.

   The different of **NoUse** and **Suspend** is for administrator's facility to distinguish E-Billing accounts status.
   Suggestion: If an account is check-out, it is better to change the account status to **NoUse** and keep for some days rather than delete this account to for user re-check the account detail.
6. Mac check and Mac address: If "Mac Check" is enabled, This account will bind a special MAC address for more security. Other clients with different MAC address will not be login success even use the right account and password.
7. VIP Check: if this account is a VIP account, the VIP Check status must be enabled. The billing policy of the account will be daily policy.

   It is suggested that the VIP account class is higher than the normal account for example class 1 for 2M bps bandwidth.
   If an account was changed from Normal to VIP or VIP to Normal, BW1330 will count charge of this account as totally VIP/Normal account when he check-out.

Once a new account has been created, an account receipt will be output from the account printer (A720 and printer converter A-721)) which connected to BW1330.

If a E-Billing account needs to be checked out, just click the "checkout" button, and the detail billing receipt of this account which record the total cost and total using time will be output from the account printer and the status of this account will be set to NOUSE. After 72 hours, this account will be automatically removed.

Below is the printed receipt of account (for user and for counterfoil) when user check-in and user bill receipts (for user and for counterfoil) when user checkout.

Figure 219 – Account receipt (for user)

Figure 220 – Account receipt (counterfoil)

Figure 221 – Bill Receipt (for user)

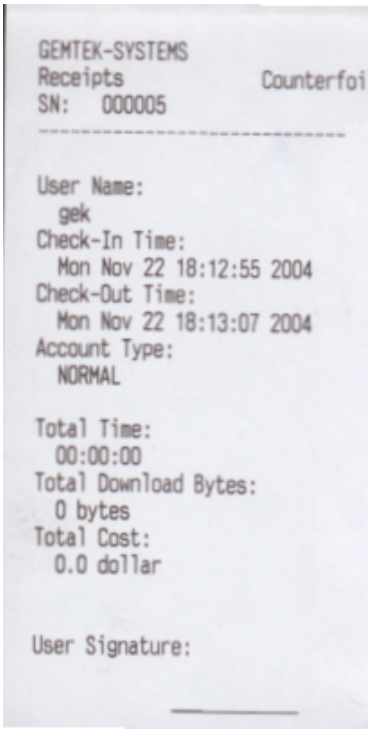

Figure 222 – Bill receipt (Counterfoil)

Built-in AAA | E-Billing | Band Class

BW1330 provide three bandwidth class, administrator can define each class bandwidth:

Figure 223 – Bandwidth class

There are three class level in default.

Class Level — Define the different user level for the download and upload bandwidth.

Max Up-Bandwidth — Maximum upload data for the specified user class level.

Max Down-Bandwidth — Maximum download data for the specified user class level.

Click edit button to change the upload and download bandwidth.

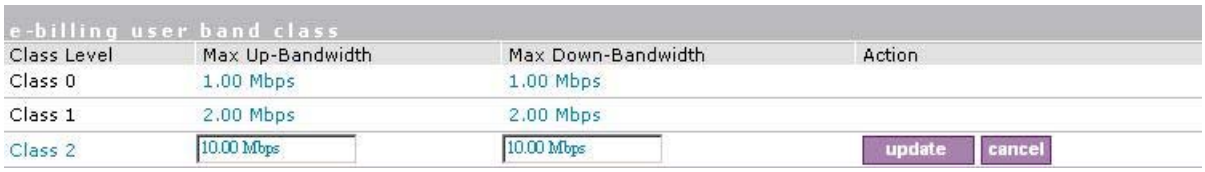

Figure 224 – Bandwidth class

Click the update button to apply change or the cancel button to cancel the modification.

Built-in AAA | E-Billing | Bill setting

Administrator can set the E-Billing billing policy through this sub-menu:

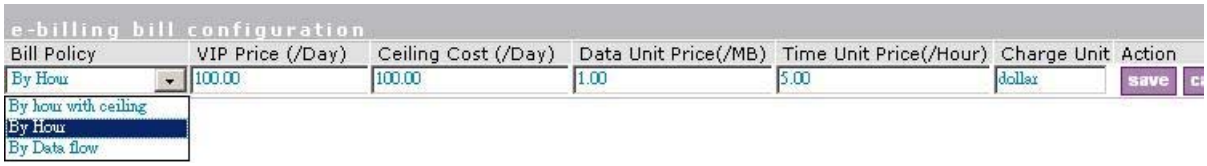

figure 225 – Billing policy

BW1330 supports billing policy of billing **by Hour**, **by Data flow** and **by hour with ceiling policy**. Administrator need fill a price of each billing unit; the price can be accuracy to two places of decimals. For time the unit is hour and for data it is Mbytes.

If the "By hour with ceiling" policy is selected, the daily cost of an account will be limit to the ceiling cost, (PM12:00 as the start time and ending time of one day).

BW1330 will only compute the download data flow if the policy is billing by data flow.

In "Charge Unit" administrator need fill out the currency unit of the local country.

Administrator and logon user can look into user's detail billing list via **Built-in AAA | E-Billing | user control** menu and click the "bill" button for the detail.

Bill

username:	gary (NORMAL)
check in time:	Sun Sep 10 10:09:24 2006
total time:	06:09:30
total download bytes:	665.11 MB
total cost:	31.08 dollar

detailed bill:

no	ip	start time	time length	download bytes	upload bytes	policy	price	charge
01.	192.168.3.2	Sun Sep 10 10:12:02 2006	01:05:54	648.34 MB	18.90 MB	time	5.00	5.50
02.	192.168.3.2	Sun Sep 10 16:09:42 2006	00:14:43	429.57 KB	113.41 KB	time	5.00	1.25
03.	192.168.3.2	Sun Sep 17 16:52:48 2006	00:12:10	580.11 KB	148.24 KB	time	5.00	1.08
04.	192.168.3.2	Sun Sep 17 18:25:48 2006	00:04:48	575.80 KB	66.12 KB	time	5.00	0.42
05.	192.168.3.2	Sat Sep 23 11:32:28 2006	01:19:04	9.26 MB	8.75 MB	time	5.00	6.67
06.	192.168.3.2	Sat Sep 23 19:37:42 2006	00:21:18	467.01 KB	107.22 KB	time	5.00	1.83
07.	192.168.3.2	Sat Sep 23 21:16:47 2006	02:51:33	5.51 MB	689.63 KB	time	5.00	14.33

Figure 226 – Bill detail of an ebilling account

"Start time" means the time when user start this session.

"Time length" means the total time of this session.

"Download bytes" and "upload bytes" means the flow of this session.

The column "charge" show the user cost of each session.

If the bill policy is by hour, the minimum time unit will be minutes, less or equal to one minute will count as one minute.

After administrator modify the billing policy, sessions only after the time of modification will take effect while sessions before the time of modification will still use the old policy to billing.

Built-in AAA | E-Billing| Power cut protection

If power cut protection is disabled, BW1330 only record E-Billing account's accounting data when user logout. If there has an accidental power cut-off, the accounting data of this session will be lost; If the power cut protection is enabled, BW1330 will update each online E-Billing account's accounting data to flash disk every "User Accounting Update" which configured in ***Network Interface | RADIUS | RADIUS Settings*** and if BW1330 will automatic restore the last session's accounting data if an accidental power cutoff happened.

BillRecord Power Cut Protection

Power Cut Protection	Action
Disable	edit

Figure 227 -- Power cut protection

For power cut protection will frequently write data to flash, so if it is enabled, please make sure the "user accounting update" which configured in **Network Interface | RADIUS | Settings** not less than 600 seconds.

If you don't need the lost accounting data when accidental power cut off, set the power cut protection setting to disabled.

Built-in AAA | pre-paid

With Browan Communications A-720/A-721 (account printer and converter), user can use the pre-paid feature. With the scenario descript in the below figure. Venue owner can use this feature create a Public access operate mode by BW1330 with its printer/A-720 and converter/A-721.

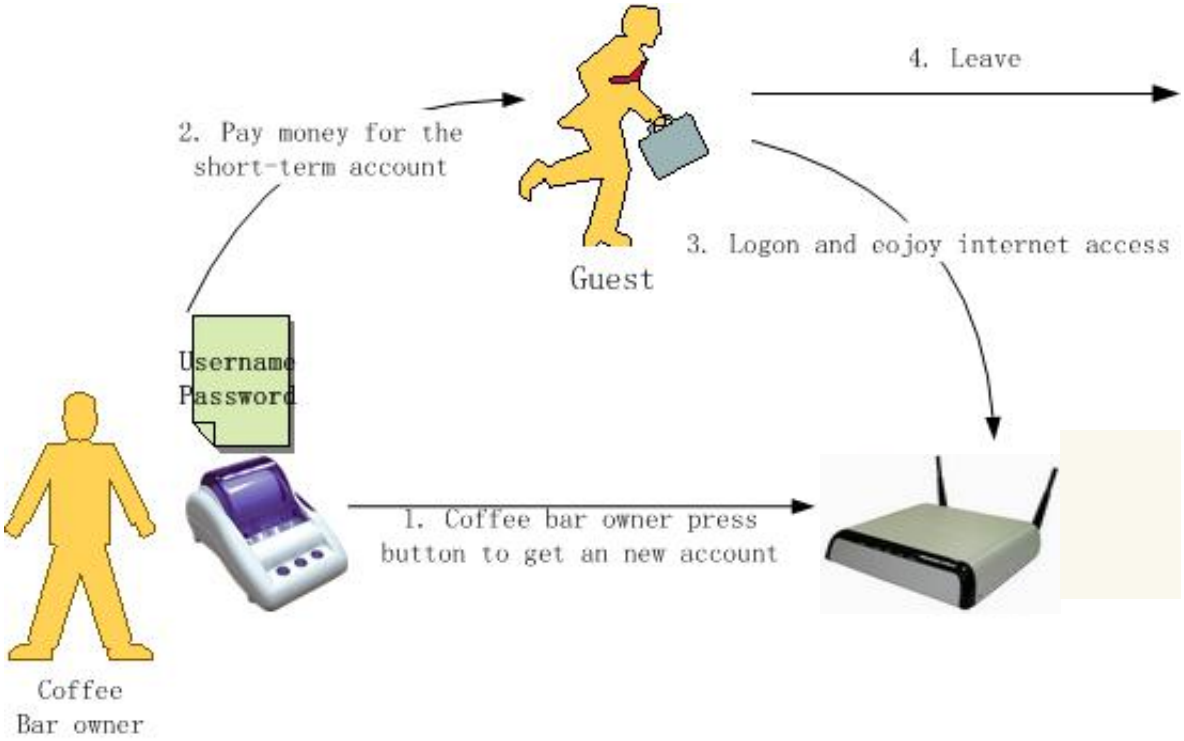

Figure 228 – Pre-paid scenario

Built-in AAA | pre-paid | user account

User account shows the receipts status which has been printed and not expired now.

user accounts

user	time length	charge	open time	remain time	connect ip	online
BRO_0925_001	2.0hours	10.00	Mon Sep 25 14:59:48 2006	02:00:00	192.168.3.66	no
BRO_0925_002	1.0hours	5.00	Mon Sep 25 14:59:52 2006	01:00:00	192.168.3.66	no
BRO_0925_003	1.0hours	5.00	Mon Sep 25 15:01:47 2006	01:00:00	192.168.3.66	no

refresh

Figure 229 – Pre-paid user account

User: show the printed pre-paid account name.

Pre-paid account is composed with three parts.

1. The first part is the prefix (first there characters) of Title configuration;
2. The second part is the date when print this receipt;
3. The last part is a sequence number which will increase automatically.

Time length: the total session time of the receipt has.

The session time of a receipt has decided the price of the receipt. The session time is 0.5, 1.0, 2.0, and 3.0 hours and so on. A-710 only can generate receipt with session time of 1 hour; A-720 can generate receipt with session time from 0.5 to 9 hours.

Charge: show the total charge of the receipt.

Open time: The time when the receipt is generated.

Remain time: Remain time of the pre-paid account.

Pre-paid account session time can be consumed by server times. Before the receipt expired time, this account can logon and logout. And each logon session time will be accumulated. For example, if a customer buy one hour. He logon and use 20 minutes then he logout and have a phone call for 20 minutes. After the phone call he can logon and has 40 minutes session time left.

Online: show if this receipt is in using.

The pre-paid has power cut-off protection function. If there has an accidental power cut-off, the pre-paid account which generated before accident cut-off can be restored and still can use.

Built-in AAA | pre-paid | price/unit

Price/unit configure the price of pre-paid account.

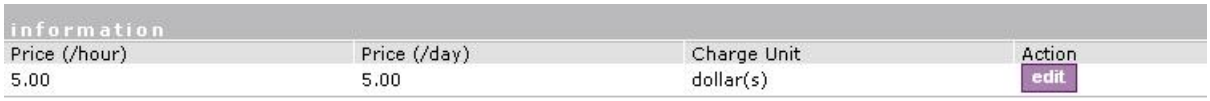

Figure 230 – Pre-paid price/unit

Price(/hour) – the price of each hour.(Maximum value is 100,000,000)

Price(/day) – the price of each day. (Maximum value is 1,000,000,000)

Charge Unit: the cash unit.

Click the edit button to change the policy and save it.

Built-in AAA | pre-paid | account life

Account life is to configure the expired time of user.

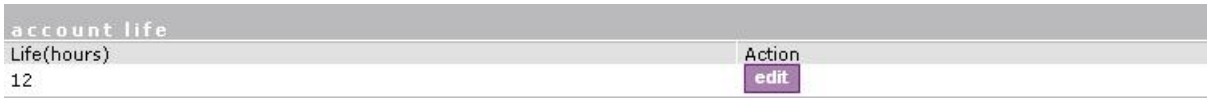

Figure 231 – Pre-paid account life

Life(hours) – the expire time of user. (Maximum value is 720 hours)

Click edit button to specify the life value and then save it.

Built-in AAA | pre-paid | receipts

Receipts show the printed pre-account, and computed the total cost. It is a history record for printed receipts, include expired and un-expired receipts. User can delete each history record of receipt.

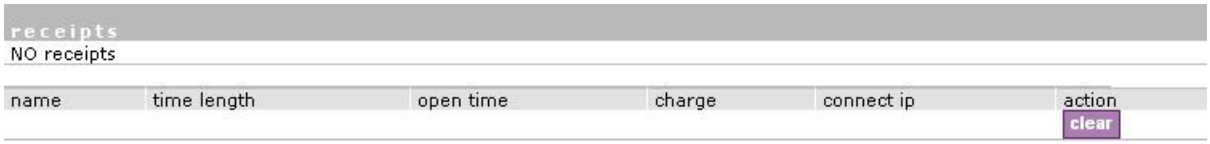

Figure 232– Pre-paid receipts

Built-in AAA | pre-paid | timeunit

Hotspot owner can define the charge time by hour or day for the pre-paid user via **Built-in AAA | pre-paid | timeunit** menu.

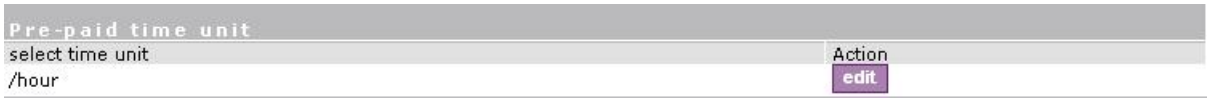

Figure 233– timeunit

Click the "edit" button to set up the timeunit.

Figure 234– timeunit setting

hour — The charge is by hour. Corresponding to the A-720 printer the keypad 0~9.(0 means half hour while the keypad 1~9 mean 1~9 hours respectively.)

misc — mix mode by hour and day.Corresponding to the printer keypad which 0 means half hour and 1~5 means 1~5 hours respectively. The keypad 6~9 means 1~4 days respectively.

Built-in AAA | pre-paid | account reminder

The account reminder feature is for reminding hot spot owner to check the income of prepaid accounts. (Please refer to the **Built-in AAA | pre-paid | receipts)**.

Administrator can set the rating of cash and remind times for reminding himself (herself) to check the income which bring by prepaid account. After checking, administrator need delete the recorded receipts history to avoid BW1330 remind again.

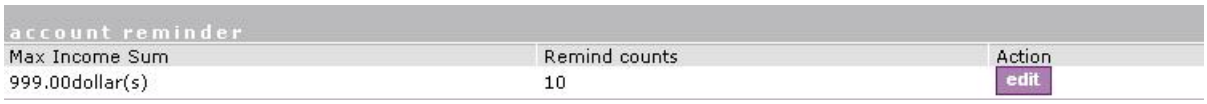

Figure 235 – account reminder

Built-in AAA | pre-paid | manage net print

BW1330 supports its account printer with converter to print receipt. Without RS232 DB-9 Connector, you must connect the printer to BW1330 through the converter connected to the LAN port.

For more detail please refer to the production CD of the converter for the setting and connection.

Figure 236– net print default IP address

IP address — the IP address of converter(default IP address:192.168.3.250).

delete — delete IP setting.

new — specify a new IP address of converter.

Up to three IP address can be specified in the net print menu.

Built-in AAA | Configuration

For more detail information showed on the receipt such as the SSID,WEP key,language or title of receipt use **Built-in AAA | Configuration** to make configuration.

Built-in AAA | Configuration | Language

The language of printed receipt: Chinese or English.

Figure 237 – Pre-paid receipt language

Built-in AAA | Configuration | Backup and restore

You can save user information locally using the **backup and restore** menu under the **Built-in AAA | configuration** menu:

Click "download" button to backup the E-billing and pre-paid Billing information.

Click "upload" button to restore the backup information.

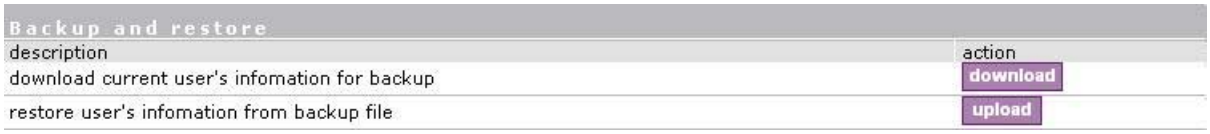

Figure 238 – E-Billing information backup and restore.

Built-in AAA | pre-paid | WEP key and SSID

The configuration of WEP key and SSID will be printed on the receipt.

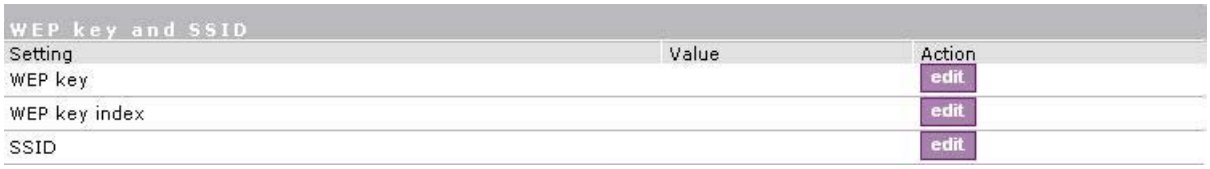

Figure 239 – Pre-paid WEP key and SSID configuration

Click the edit button for every column to specify the WEP key and SSID.

Built-in AAA | Configuration | title

Title is the name of a venue. Venue owner can print their venue name and description on each printed receipt.

title

Title	Description	Action
BROWAN	BROWAN Communications	edit

Figure 240 – Printed receipts title

Pre-paid name will use the format: "Prefix three characters of title name + date + serial number"

Below is an example of printed receipts.

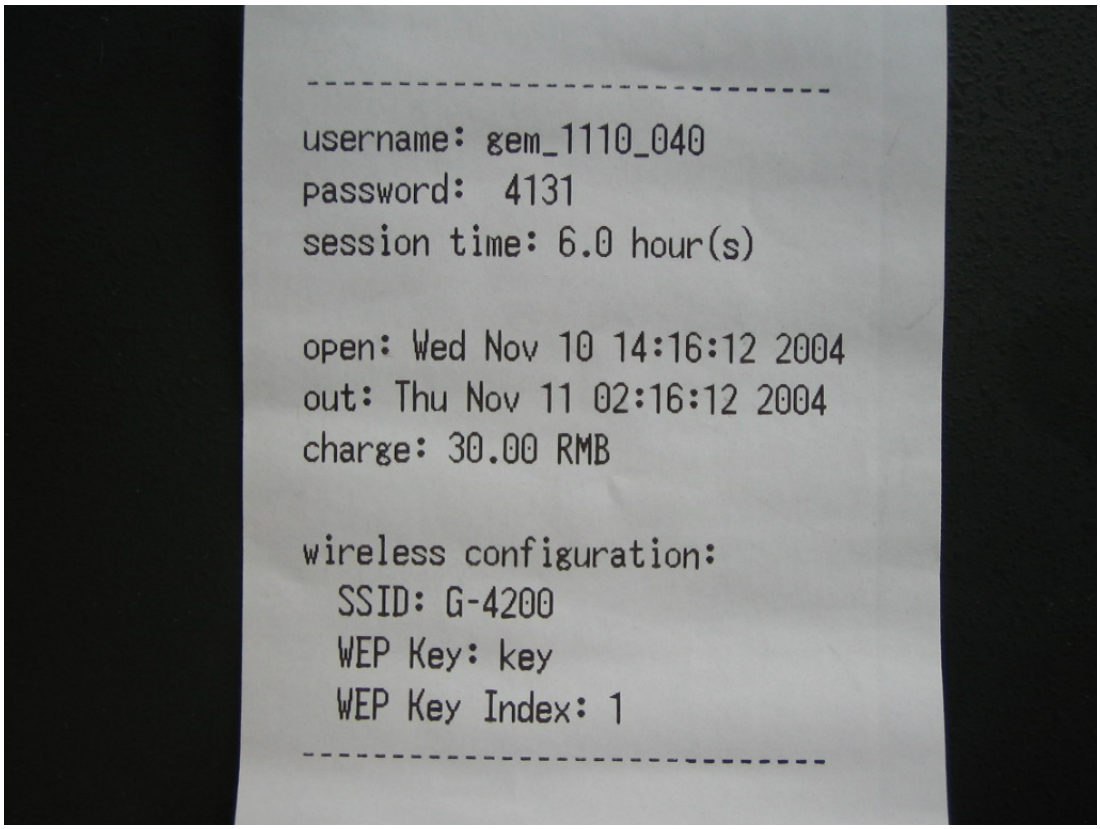

Figure 241 – Pre-paid receipt example

Appendix

A) Access Controller Specification

Technical Data

Wireless	
Standard	IEEE 802.11g (OFDM), IEEE 802.11b (DSSS), 2.4GHz ISM band, Wi-Fi certified
Data Rate	802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps, 802.11b: 11Mbps, 5.5Mbps, 2, 1Mbps (auto fall back)
Client Stations	Max. 100 simultaneous client stations(wireless+LAN)
Typical range	50 meters in indoor environments, up to 300m outdoors
Transmit Power	Max. 19 dBm
Antennas	Two 2.33 dBi dipole antennas, R-TNC connectors.
Encryption	WPA, WPA2, WPA-PSK, WEP64, WEP128
WDS	Wireless Distribution System
Network and Hotspot Access Control	
▪ IP Router with NAT/NAPT, configurable firewall filters	▪ Hotspot access controller with web browser log-on (UAM) and 802.1x/EAP support, Smart Client support, MAC authentication, WISPr compliant (Wi-Fi alliance)
▪ AAA RADIUS client and proxy server with EAP support	▪ Extended Universal access method (web browser log-on) with XML support and walled garden (free web sites)
▪ Universal address translation and web proxy support (any client configuration is accepted)	▪ WISPr compatible log-on via web browser, SSL/TLS support UAT
▪ VPN client (GRE)	▪ IEEE 802.1x authenticator with EAP-SIM, MD-5, TLS, TTLS, PEAP
▪ WPA support	▪ DHCP server, DHCP relay gateway, DHCP client
▪ VPN pass-through	▪ Layer 2 user isolation
▪ E-mail redirection	▪ Bandwidth management via RADIUS
Interface	
WAN	One 10/100Mb Ethernet, auto sensing (speed, duplexity, MDI/MDIX), RJ-45
LAN	One 10/100Mb Ethernet port, auto sensing (speed, duplexity, MDI/MDIX), RJ-45, 802.1q VLAN support
WLAN	Two R-TNC antenna connectors
Management	
Interfaces	HTTPs, SSH, Telnet, SNMP (MIB II, Ethernet MIB, bridge MIB, private MIB)
Software Update	Remote software update via HTTP, HTTPs or FTP
Reset	Remote reset / Manufacturing reset
Console	RS-232 DB-9 Connector
Physical Specification	

Dimension	195 mm x 160 mm x 27 mm	
Weight	450g	
Environment Specification		
	Temperature	Humidity
Operating	0 to 55°C	10 % to 95%, non-condensing
Power Supply		
External	Input:100-230V AC, 50/60Hz/Output:12V/1A DC	
LEDs		
5 LEDs	Power, Online, WAN, LAN, WLAN	
Warranty		
3 years		
Package Contents		
▪ **BW1330** Hotspot Access Point x 1	▪ External power supply, 100-230 V, 50/60 Hz x 1	
▪ RJ-45 Ethernet cable x1	▪ Printed warranty note x 1	
▪ Detachable antenna(R-TNC connector)x2	▪ US power cord x 1	
▪ CD-ROM with software and documentation x 1	▪ EU power cord x 1	
Related Products		
Access Points:	**P-520r** 54Mb Operator Access Point **BW1250** Dual radio Operator Access Point	**BW2250** Outdoor dual radio Operator Access Point/Bridge

B) Regulatory Domain/Channels

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	European Union (CE/ETSI)	WORLD (CE/FCC)	France	China	Japan	Manual
1	2412	•	•	•	—	•	•	•
2	2417	•	•	•	—	•	•	•
3	2422	•	•	•	—	•	•	•
4	2427	•	•	•	—	•	•	•
5	2432	•	•	•	—	•	•	•
6	2437	•	•	•	—	•	•	•
7	2442	•	•	•	—	•	•	•
8	2447	•	•	•	—	•	•	•
9	2452	•	•	•	—	•	•	•
10	2457	•	•	•	•	•	•	•
11	2462	•	•	•	•	•	•	•
12	2467	—	•	—	•	•	•	•
13	2472	—	•	—	•	•	•	•
14	2484	—	—	—	—	—	•	•
Maximum Power Levels		**18**dBm	20dBm	20dBm	20dBm	20dBm	20dBm	20dBm

Mexico is included in the Americas regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of Mexico.

C) CLI Commands and Parameters

Network Commands

network	
configuration	Network Interfaces configuration.
dhcp	Dynamic Host Configuration Protocol services configuration.
dns	DNS Server settings.
radius	Configuration set for changing RADIUS Server settings.
tunnels	Tunnels configuration commands.
network configuration	
bridge	Bridge configuration
interface	Network Interfaces configuration.
portforward	Port forwarding setup.
routes	Static IP routing settings.
subnet	Management subnet configuration.
vlans	VLANs configuration.
network configuration bridge	
configuration	Bridge configuration.
ports	Bridge ports configuration.
network configuration bridge configuration	
<action>	Action to take upon a bridge interface: A(dd), E(dit), D(elete).
<id>	Bridge interface identifier (number)
-a <aging>	Bridge aging time.
-g <garbage>	Garbage collector interval.
-t <stp>	Spanning Tree Protocol status: enabled or disabled.
-p <priority>	Bridge priority: low, medium or high.
-d <delay>	Bridge forward delay.
-h <hello>	Bridge hello time.
-e <age>	Bridge maximum age.
network configuration bridge ports	
<bridge>	Bridge name to add or delete interface (port) from.
<action>	A(dd) or D(elete) interface(port) from bridge.
-i <interface>	Interface (port) name.
-c <cost>	Port path cost in the bridge interface.
-p <priority>	Port priority in the bridge interface.
network configuration interface	
<interface>	Standard UNIX interface name. This name cannot be changed.

-s <status>	The interface status. Possible values are enabled and disabled.
-a <ip_address>	Interface IP address in digits and dots notation, e.g. 192.168.2.27.
-m <netmask>	Interface subnet mask e.g. 255.255.255.0.
-g <gateway>	Interface gateway in digits and dots notation or name of other interface.
-d <dhcpclient>	The status of dhcp client for the interface. May have values enabled and disabled. Can be used with WAN interface only.
-q <masquerade>	Masquerade status for interface: enabled or disabled.
-u <authentication>	Authentication status on interface: enabled and disabled.
-v <visitor_access>	Visitor access for interface: values enabled and disabled.
network configuration portforward	
<action>	Action to take upon Port Forwarding entry: A(dd), E(dit), D(elete).
<id>	Port Forwarding entry id. Needed with actions E(dit) and D(elete).
-s <status>	PortForwarding rule status: enabled or disabled.
-p <protocol>	Rule protocol.
-a <ip>	Source ip address.
-l <port>	Source port.
-d <ip>	Destination ip address.
-r <port>	Destination port.
network configuration routes	
<action>	Action to take upon the route. May have values A(dd), E(dit), D(elete).
<id>	Route id. Needed only with actions E and D
-s <status>	Route status. May have values enabled or disabled.
-d <device>	Interface name.
-t <target>	Target ip address.
-m <netmask>	Target netmask.
-g <gateway>	Gateway for the target address.
network configuration subnet	
<interface>	Interface name on which the management subnet is configured.
-s <status>	Interface ip address for management subnet.
-a <ip_address>	Interface ip address for management subnet.
-m <netmask>	Interface netmask for management subnet.
-n <filterNetwork>	Network from which users are allowed to access management subnet.
-t <filterNetmask>	Netmask of network from which users are allowed to access management subnet.
network configuration vlans	
<action>	Action to take upon VLAN interface: A(dd), E(dit), D(elete).
<id>	VLAN interface id. Needed only with action A.
<interface>	Name of LAN interface on which VLAN interface exists. Needed only with action A.
<name>	Name of VLAN interface. Needed only with actions E and D.

<dedicate>	Switch control dedicated port: disabled/LAN1/LAN2/LAN3/LAN4. Needed only with actions A and E.
network dhcp	
<interface>	Interface name for DHCP server instance.
-s <status>	Status of DHCP server for interface. May be server, relay or disabled.
-f <from>	Start of IP address range supported for DHCP service. Needed only with server status.
-t <to>	End of IP address range supported for DHCP service. Needed only with server status.
-w <wins>	WINS Address (Windows Internet Naming Service Address) if it is available on the network. Needed only with server status.
-l <lease_time>	DHCP Server lease time. Needed only with server status.
-d <domain>	DHCP domain name. Needed only with server status.
-c <circuit_id>	Circuit ID - a unique NAS identifier. MAC address will be used by default. Needed only with relay status.
-n <dns_list>	List of up to two DNS servers IP addresses.
network dns	
-p <nameserver>	DNS primary Server IP address.
-s <nameserver>	DNS secondary Server IP address.
-d <nameserver>	DNS Domain Name.
-h <nameserver>	DNS Host Name.

Network Radius Commands

network radius	
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.
network accounting_log	
-r <status>	Remote accounting log status. Possible values are enabled or disabled.
-a <host>	The host IP address where to send the accounting information.
network radius proxy	
-s <status>	RADIUS Proxy status: enabled or disabled.
-a <port>	RADIUS Proxy authentication port.
-c <port>	RADIUS Proxy accounting port.
-t <time>	RADIUS Proxy accounting detection timeout
network radius servers	
accounting	Accounting RADIUS servers' configuration.
authentication	Authentication RADIUS servers' configuration.
backup	Accounting information backup servers configuration.
network radius servers	

accounting	
<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).
network radius servers authentication	
<action>	Action to take uppon radius server. May have values A(dd), E(dit), D(elete).
<id>	RADIUS server id.
-n <name>	RADIUS server name.
-a <ip_address>	RADIUS server IP address.
-p <port>	RADIUS server port.
-s <secret>	Shared secret key (must be the same on RADIUS server and RADIUS client).
-d <default>	Sets the server as default. Possible values: yes. Note: there can be only one default Radius server.
-r <status>	Reverse accounting. May have values enabled or disabled.
-w <status>	Strip WISP name before sending to RADIUS. May have values enabled or disabled.
-u <method>	UAM authentication method for RADIUS server. May have values pap, chap, mschap1 and mschap2.
network radius servers backup	
<id>	RADIUS server id.
-b <status>	If RADIUS Backup Server feature is on. May have values enabled or disabled.
-a <ip_address>	Backup RADIUS server IP address used for Radius accounting.
-p <port>	Backup RADIUS server port used for Radius accounting.
-s <secret>	Shared secret key for backup server(must be the same on RADIUS server and RADIUS client).
network radius settings	
-r <retries>	Retry count of sending RADIUS packets before giving up.
-t <timeout>	Maximal amount of time before retrying RADIUS packets (in seconds).
-n <nas>	NAS Server identification string.
-o <user_timeout>	Amount of time from user side (no network carrier) before closing the connection (in seconds).
-a <acct_update>	Period after which server should update accounting information (in seconds).
-c <acct_retry>	Retry time period in which server should try to update accounting information before giving up (in seconds).
-i <idle>	Amount of user inactivity time, before automatically disconnecting user from the network (in seconds).
-u <bandwidth>	Default Radius user upload bandwidth.

-d <bandwidth>	Default Radius user download bandwidth.
network radius wisp	
<action>	A(dd), D(elete)
<id>	WISP Id. Usable only with D action.
<name>	WISP name. Usable only with A action.
<radius_id>	WISP Radius server id (from Radius authentication server list). Usable only with A action.
<interface>	Interface name to which the WISP should be bound or none. Usable only with A action.

Network Tunnels Commands

network tunnels	
gre	GRE client setup.
ppp	PPTP, PPPoE and GRE setup.
pptp4vpn	PPTP for VPN setup.
network tunnels gre	
<action	Action to take upon GRE tunnel: A(dd), E(dit), D(elete).
<id>	GRE tunnel id. Needed only with action E and D.
<status>	GRE tunnel status. Needed only with action A and E.
<remote>	Remote host ip. Needed only with actions A and E.
network tunnels ppp	
-s <status>	Status: disabled/PPTP/PPPoE/GRE.
-n <name>	PPPoE/PPTP username.
-p <password>	PPPoE/PPTP password.
-e <encryption>:	PPPoE/PPTP encryption status: enabled or disabled.
-a <server>	PPTP server ip address/GRE remote address.
-i <ip>	GRE interface address.
-m <netmask>	GRE interface netmask.
network tunnels pptp4vpn	
<action>	A(dd), D(elete) or E(dit) entry.
-c <channel>	PPTP channel. Used only with A and E actions.
-s <server>	PPTP server ip address. Used only with A and E actions.
-u <username>	PPTP username. Used only with A and E actions.
-p <password>	PPTP password. Used only with A and E actions.
-e <encryption>	PPTP encryption status: enabled or disabled. Used only with A and E actions.
-a <network>	PPTP remote network address. Used only with A and E actions.
-m <netmask>	PPTP remote network netmask. Used only with A and E actions.

User Commands

user	
administrator	Administrator login and password change.
connected	Connected users list.

start_page	Definition of first URL after user login.
walled_garden	Free Web sites list.
webproxy	Web proxy configuration.
user administrator	
Enter for wizard	Follow the wizard and complete administrator settings changes.
user connected	
<action>	D(etail) user statistics for or L(ogout) user with specified ip.
<ip>	User ip address.
user start_page	
<url>	The web page to which the user is redirected after login.
user walled_garden	
autoupdate	Configures automated walled garden update.
host	Configures free web sites that are not displayed to users.
url	Configure free web sites that are displayed to users.
user walled_garden autoupdate	
-s <status>	Automated update status: enabled or disabled.
-u <url>	Update URL.
-i <interval>	Update interval in hours.
user walled_garden host	
<action>	Action to take on free web site. May have values A(add), E(edit), D(delete).
<id>	Walled Garden entry id. Used only with E(dit) and D(elete) actions.
-h <host>	Host address.
-p <port>	Network port, or port range i.e. 25-50, or use '0' or 'all' for all ports that may be used to reach the host.
-t <type>	Used protocol type. May have values tcp or udp.
-m <netmask>	Host subnet mask e.g. 255.255.255.255.
user walled_garden url	
<action>	Action to take on free web site. May have values A(add), E(edit), D(delete).
<id>	Walled Garden entry id. Used only with E(dit) and D(elete) actions.
-u <url>	URL address used for link.
-s <display>	URL description visible for user.
user webproxy	
-s <status>	Web proxy status: enabled or disabled.
-a <port> [<port>... [<port>]]	Add list of Web proxy ports.
-d <port> [<port>... [<port>]]	Delete list of Web proxy ports.

System Commands

system	
access	System access configuration.
configuration	System configuration.
system access	
aaa	Multimode settings.
control	Allow or deny management access depending on user network address.
firewall	Firewall configuration.
iplogging	Enabling or disabling IP request logging.
snmp	Configuration of SNMP service.
telnet	Enabling or disabling of telnet protocol.
uat	Universal Address Translation of all IP and proxy settings.
system configuration	
clock	Manual setting of internal device clock
ntp	Configuration of Network time Protocol service.
pronto	Pronto compatibility agent configuration.
syslog	For sending system and debug messages via syslog protocol.
trace	Displays the last logged messages.
upgrade	Auto firmware upgrade configuration.

System Access Commands

system access aaa	
<interface>	Interface to set AAA on.
-m <mode_list>	Either disabled or space separated list of modes. Modes may be: uam, 8021x, mac, proxy.
-u <use_password>	Mac authentication mode password usage: 'radius' - use radius shared secret key, 'user' - use user defined password.
-p <password>	User defined mac authentication password.
system access control	
<action>	Action to take upon management access entry: A(dd), E(dit), D(elete) or default.
<id>	Management access entry id. Needed only when editing or deleting entry.
-s <service>	Services for which the policy should be set: ssh, snmp, telnet or all.
-a <ip/bitmask>	'all' or network ip address and bitmask to (dis)allow service to.
-p <policy>	Management access policy: allow or deny(default is deny).
system access firewall	
<action>	Action to take upon the rule: A(dd), I(nsert), E(dit), R(emove), move U(p), move D(own).
<id>	Firewall rule index. Not needed when adding a new rule.
-c <type>	Rule type: input, output, forward.

-t <policy>	Rule policy: accept, reject, drop.
-p <protocol>	Rule protocol: tcp, udp, icmp, all.
-si <interface>	Rule source interface.
-sa <ip_address>	Rule source Ip address.
-sm <netmask>	Rule source netmask.
-sp <port>	Rule source port.
-di <interface>	Rule destination interface.
-da <ip_address>	Rule destination Ip address.
-dm <netmask>	Rule destination netmask
-dp <port>	Rule destination port.
-s <status>	Firewall status: enabled or disabled. Must be the only parameter used with command.
system access iplogging	
<status>	Change IP request logging service status: enabled or disabled.
system access snmp	
proxies	SNMP proxies settings.
settings	SNMP service settings.
traps	SNMP traps settings.
users	SNMP users settings.
system access snmp proxies	
<action>	Action to take upon SNMP proxy entry: A(dd), E(dit) or D(elete).
<id>	Entry id. Needed only with Edit and Delete actions.
-t <type>	Proxy type. May have values v1, v2c. Can be used only when adding or editing proxy.
-a <ip_address>	Proxy ip address.
-c <community_name>	Proxy community name.
-l <oid_local>	Proxy local OID.
-r <oid_target>	Proxy target OID.
system access snmp settings	
-s <status>	Status of SNMP service.
-n <name>	System name.
-l <location>	Location of the device.
-c <contact>	Contact information.
-b <public_name>	Public name of SNMP service.
-r <private_name>:	Private name of SNMP service.
system access snmp traps	
<action>	Action to take upon SNMP trap entry: A(dd), E(dit) or D(elete)
<id>	Entry id. Needed only with Edit and Delete actions.
-c <community>	SNMP community string.
-a <ip_address>	SNMP trap host address.
-p <port>	SNMP trap port.
-t <type>	SNMP trap type: v1, v2 or inform.

system access snmp users	
<id>	User id.
-n <name>	SNMP user name.
-p <password>	SNMP user password.
system access telnet	
<status>	Change telnet service status: enabled or disabled.
system access uat	
<interface>	Active LAN interface.
-s <status>	UAT status on interface.
-a <ip_from>	UAT address pool start.
-m <ip_to>	UAT address pool end.

System Configuration Commands

system configuration	
clock	Manual setting of internal device clock.
ntp	Configuration of Network time Protocol service.
syslog	For sending system and debug messages via syslog protocol.
trace	Displays the last logged messages.
system configuration clock	
<date>	New date values in YYYY.MM.DD format.
<time>	New time in hh:mm format.
<zone>	New time zone (time from GMT in minutes).
system configuration ntp	
<action>	Action: A(dd), E(dit), D(elete) server or set NTP S(tatus).
<id>	Server id. Needed only with E and D actions.
-a <server>	NTP server address.
-s <status>	NTP service status: enabled or disabled. Needed only with S action.
system configuration pronto	
-s <status>	Pronto compatibility agent status: enabled or disabled.
-u <server_url>	HNS server url in format host:port.
-h <interval>	Heartbeat interval in seconds, 'disabled' or 'server' to obtain it from the server.
-a <remote_host>	Remote host ip address.
-p <remote_port>	Remote host port.
system configuration syslog	
-s <status>	Syslog status. Possible values are enabled or disabled.
-h <host>	The host IP address where to send the syslog. Needed only when enabling syslog.
-l <level>	The lowest level of messages that will be logged. Possible levels: debug, info, warning, error, fatal.
system configuration trace	

clear	Clears trace history.
size <number>	Sets trace history size.
level <level>	Sets level of trace messages. Possible levels: debug, info, warning, error, fatal.
system configuration upgrade	
-s <status>	Firmware auto-upgrade status: enabled or disabled.
-u <url>	URL to get firmware for autoupgrade from.
-i <interval>	Interval in hours between auto-upgrade checks.
-d <delay>	Delay in hours after the interval has passed.

Status Commands

status	
device	General system information.
network	Network information.
service	Services information.

Connection Commands

connection	
email	Outgoing Main (SMTP) Redirection settings.
supervision	Settings for station availability monitoring with ARP-Pings.
connection email	
<status>	SMTP redirection status: enabled or disabled.
<host>	New SMTP server host IP address.
<port>	New port number.
connection supervision	
<seconds> <number>	ARP-Ping interval in seconds and failure number after reaching which user is automatically logged out.

D) Location ID and ISO Country Codes

This list states the **country names** (official short names in English) in alphabetical order as given in ISO 3166-1 **and** the corresponding **ISO 3166-1-alpha-2 code elements**.

It lists 239 official short names and code elements.

Location ID	Country	Location ID	Country
AF	Afghanistan	LI	Liechtenstein
AL	Albania	LT	Lithuania
DZ	Algeria	LU	Luxembourg
AS	American Samoa	MO	Macao
AD	Andorra	MK	Macedonia, the former Yugoslav republic of
AO	Angola	MG	Madagascar
AI	Anguilla	MW	Malawi
AQ	Antarctica	MY	Malaysia
AG	Antigua and Barbuda	MV	Maldives
AR	Argentina	ML	Mali
AM	Armenia	MT	Malta
AW	Aruba	MH	Marshall islands
AU	Australia	MQ	Martinique
AT	Austria	MR	Mauritania
AZ	Azerbaijan	MU	Mauritius
BS	Bahamas	YT	Mayotte
BH	Bahrain	MX	Mexico
BD	Bangladesh	FM	Micronesia, federated states of
BB	Barbados	MD	Moldova, republic of
BY	Belarus	MC	Monaco
BE	Belgium	MN	Mongolia
BZ	Belize	MS	Montserrat
BJ	Benin	MA	Morocco
BM	Bermuda	MZ	Mozambique
BT	Bhutan	MM	Myanmar
BO	Bolivia	NA	Namibia
BA	Bosnia and Herzegovina	NR	Nauru
BW	Botswana	NP	Nepal
BV	Bouvet island	NL	Netherlands
BR	Brazil	AN	Netherlands Antilles
IO	British Indian ocean territory	NC	New Caledonia
BN	Brunei Darussalam	NZ	New Zealand
BG	Bulgaria	NI	Nicaragua
BF	Burkina Faso	NE	Niger

BI	Burundi	NG	Nigeria
KH	Cambodia	NU	Niue
CM	Cameroon	NF	Norfolk island
CA	Canada	MP	Northern Mariana islands
CV	Cape Verde	NO	Norway
KY	Cayman islands	OM	Oman
CF	Central African republic	PK	Pakistan
TD	Chad	PW	Palau
CL	Chile	PS	Palestinian territory, occupied
CN	China	PA	Panama
CX	Christmas island	PG	Papua new guinea
CC	Cocos (keeling) islands	PY	Paraguay
CO	Colombia	PE	Peru
KM	Comoros	PH	Philippines
CG	Congo	PN	Pitcairn
CD	Congo, the democratic republic of the	PL	Poland
CK	Cook islands	PT	Portugal
CR	Costa Rica	PR	Puerto Rico
CI	Côte d'ivoire	QA	Qatar
HR	Croatia	RE	Réunion
CU	Cuba	RO	Romania
CY	Cyprus	RU	Russian federation
CZ	Czech republic	RW	Rwanda
DK	Denmark	SH	Saint Helena
DJ	Djibouti	KN	Saint Kitts and Nevis
DM	Dominica	LC	Saint Lucia
DO	Dominican republic	PM	Saint Pierre and Miquelon
EC	Ecuador	VC	Saint Vincent and the grenadines
EG	Egypt	WS	Samoa
SV	El Salvador	SM	San Marino
GQ	Equatorial guinea	ST	Sao tome and Principe
ER	Eritrea	SA	Saudi Arabia
EE	Estonia	SN	Senegal
ET	Ethiopia	SC	Seychelles
FK	Falkland islands (malvinas)	SL	Sierra Leone
FO	Faroe islands	SG	Singapore
FJ	Fiji	SK	Slovakia
FI	Finland	SI	Slovenia
FR	France	SB	Solomon islands
GF	French Guiana	SO	Somalia
PF	French Polynesia	ZA	South Africa
TF	French southern territories	GS	South Georgia and the south

			sandwich islands
GA	Gabon	ES	Spain
GM	Gambia	LK	Sri Lanka
GE	Georgia	SD	Sudan
DE	Germany	SR	Suriname
GH	Ghana	SJ	Svalbard and Jan Mayan
GI	Gibraltar	SZ	Swaziland
GR	Greece	SE	Sweden
GL	Greenland	CH	Switzerland
GD	Grenada	SY	Syrian Arab republic
GP	Guadeloupe	TW	Taiwan, province of china
GU	Guam	TJ	Tajikistan
GT	Guatemala	TZ	Tanzania, united republic of
GN	Guinea	TH	Thailand
GW	Guinea-Bissau	TL	Timor-leste
GY	Guyana	TG	Togo
HT	Haiti	TK	Tokelau
HM	Heard island and McDonald islands	TO	Tonga
VA	Holy see (Vatican city state)	TT	Trinidad and Tobago
HN	Honduras	TN	Tunisia
HK	Hong Kong	TR	Turkey
HU	Hungary	TM	Turkmenistan
IS	Iceland	TC	Turks and Caicos islands
IN	India	TV	Tuvalu
ID	Indonesia	UG	Uganda
IR	Iran, Islamic republic of	UA	Ukraine
IQ	Iraq	AE	United Arab emirates
IE	Ireland	GB	United kingdom
IL	Israel	US	United states
IT	Italy	UM	United states minor outlying islands
JM	Jamaica	UY	Uruguay
JP	Japan	UZ	Uzbekistan
JO	Jordan	VU	Vanuatu
KZ	Kazakhstan		Vatican city state see holy see
KE	Kenya	VE	Venezuela
KI	Kiribati	VN	Viet nam
KP	Korea, democratic people's republic of	VG	Virgin islands, British
KR	Korea, republic of	VI	Virgin islands, u.s.
KW	Kuwait	WF	Wallis and Futuna
KG	Kyrgyzstan	EH	Western Sahara
LA	Lao people's democratic republic	YE	Yemen

LV	Latvia	YU	Yugoslavia
LB	Lebanon		Zaire see Congo, the democratic republic of the
LS	Lesotho	ZM	Zambia
LR	Liberia	ZW	Zimbabwe
LY	Libyan Arab Jamahiriya		

E) User Pages Templates Syntax

In this section you will find syntax for the writing of the user pages with examples for the writing of XSL templates. The BW1330 web server creates XML, having data inside its structure:

Example:

```
<?xml version="1.0"?>
<Gemtek>
<Header Script_Name="login.user" Title="Login" charset="; charset=ISO8859-
1" language="en"/>
<Data nasid="TestLab" version=" BW1330" help="images/help.html"
ip="192.168.4.1"
mac="00923456789A" original_url="https://192.168.4.4:7777/login.user";
type="2" username="g1">
<entry descr="Gemtek Baltic" id="0" url="http://www.gemtek.lt"/>;
<entry descr="Gemtek Systems, Inc." id="1" url="http://www.gemtek-
systems.com"/>;
</Data>
<WISPAccessGatewayParam MessageType="120" ResponseCode="100">
<entry ReplyMessage="Your password has expired."/>
</WISPAccessGatewayParam>
<Errors id="4102"/>
</Gemtek>
```

Current script filename (to be used in forms action attribute) can be located in the XML tree at: `/Gemtek/Header/@Script_Name`

Page title at:

`/Gemtek/Header/@Title`

Custom char set (if enabled on administration pages) for user pages at:

`/Gemtek/Header/@charset`

Welcome.xsl

Welcome page is the first page that the user sees while not registered on the network. This page provides welcome text to the user who is connected to the controller and supplies a link to the login page.

Attribute in XML tree at `/Gemtek/Data/@cmd` defines the link to the **login** page. This link should be used to point the user from the **welcome** screen to login screen. The **Welcome** page also lists defined walled garden entries, informing the user where to browse without registering on the network.

Walled Garden information is located in the XML tree under `/Gemtek/Data` with multiple "`entry`" branches. These branches have the following attributes:

`descr` - website description;

`url` - website URL;

`id` - website id for BW1330 configuration, which is not needed for the user connecting to the network through the BW1330.

Login.xsl

Login page appears when the user is not registered to the network and tries to open a webpage. The user proceeds to the **login** page, following the link from the welcome page. The **Login** page has variables that can be used:

`/Gemtek/Header/@Script_Name` - script name to send back to the BW1330 user login information;

`/Gemtek/Data/@username` - the username to be entered into the user name field – usually the name the user entered before while unsuccessful in registering on the network;

`/Gemtek/Data/@ip` - detected user IP from which he/she tries to register on the network;

`/Gemtek/Data/@mac` - detected users MAC address;

`/Gemtek/Errors/@id` - returned error code, which can be as follows:

error	description
4101	Failed to authorize.
4102	Login or/and password incorrect.
4103	Network connection failed.
4104	Accounting error.
4105	Unknown authorization error.
4106	Could not get redirection URL.
4107	Already logged in.

`/Gemtek/Data/@type` - returns to BW1330 response for login request. Type values are as follows:

error	description
0	Ok - logged in, redirect user to start page
1	Failed to authorize
2	Login or/and password incorrect
3	Network connection failed
4	Accounting error
5	User already logged in

It is advisable to first check the error codes, because they return more precise information. Branch "Type" returns RADIUS server response, which gives additional information about the user status. This can help in detecting whether the user is just logged in or has come to this page while already logged-in.

`/Gemtek/WISPAccessGatewayParam/entry/@ReplyMessage` - the RADIUS server response message on user logon [optional]. This parameter supports multiple messages.

This optional RADIUS Reply-Message's could provide more detailed information, why user logon failed.

`/Gemtek/Data/@cmd` - link to **logout** page. The logout page displays network usage statistics and provides the logout from the network function.

`/Gemtek/Data/@url` - the URL of **start** page to where the user is redirected after successful login. Usually it can be the website of the company or organization providing the BW1330 controller and configuring the users to visit their website.

`/Gemtek/Data/@help` - link to **help** page regarding how the user should register on the network.

When the user clicks the **login** button, information is sent to: `/Gemtek/Header/@Script_Name` location with following information:

username - user name to register to network;

password - user password.

When the form is submitted, user information is checked and indication of success or failure is returned.

Logout.xsl

The **logout** page displays network usage statistics and the user ability to logout from the network. The **Logout** page is displayed after the successful login and with usage statistics which are automatically refreshed after a defined time period.

Logout page has variables:

/Gemtek/Header/@Script_Name - current script name, to send command to logout or refresh the statistics on page.

/Gemtek/Data/entry/@auth - authentication method.

/Gemtek/Errors/@id - returned error code. Error code is a follows:

error	description
4107	Already logged in. This error code usually comes from login screen, when redirecting.

Following error codes are sent when other than the LOGOUT command is submitted:

error	description
4201	Failed to authorize.
4202	Login failed.
4203	Network connection failed.
4204	Accounting error.
4205	Undefined error return from RADIUS client on BW1330.
4206	Already logged in.

Following error codes are sent when other than LOGOUT command is submitted:

error	description
4210	Already logged in.
4211	Failed authorization.
4212	Login failed.
4213	Network connection failed.
4214	Accounting error.
4215	Undefined error return from RADIUS client on BW1330.

/Gemtek/Data/@cmd - link to **logout** page.

/Gemtek/Data/@login - link to **login** page. This is used when the user is logged-off and to provide a quick link to be used to register again.

/Gemtek/Data/entry/@username - username with which user is logged in.

/Gemtek/Data/entry/@ip - detected user IP address from which the user has made his attempt to register on the network.

/Gemtek/Data/entry/@mac - detected users MAC address.

/Gemtek/Data/entry/@time - session time.

/Gemtek/Data/entry/@idle - idle time.

/Gemtek/Data/entry/@in - input bytes sent.

/Gemtek/Data/entry/@out - output bytes sent.

/Gemtek/Data/entry/@remain_down - input bytes left.

/Gemtek/Data/entry/@remain_up - output bytes left.

/Gemtek/Data/entry/@remain_total - total bytes left.

/Gemtek/Data/entry/@remain_time - session time remaining.

/Gemtek/Data/entry/@down - bandwidth downstream.

/Gemtek/Data/entry/@up - bandwidth upstream.

If there is no /Gemtek/Data/entry in XML tree, it indicates that the user is not logged in.

Logout page has two purposes:

- Log off the user
- Show the user usage statistics.

To log off the user, call the script defined in `/Gemtek/Header/@Script_Name` with variable cmd set to logout. This could be done trough POST or simply GET methods supplying simple link with parameters:

```
<a href="/logout.user?cmd=logout">.
```

To get user usage statistics, simply refresh the script defined in `/Gemtek/Header/@Script_Name` with no variables set. This could be done by defining the simple link:

```
<a href="/logout.user">.
```

Help.html

This is a HTML file with no embedded cgi prepared. It is advisable to write instructions for the user on how to register to the network or what to do in the case of troubleshooting.

Unauthorized.html

This page appears if the user is not registered on the network or the web authentication is not provided on the AC. It is recommended to include information on how to contact the network administrator (e.g. phone number).

Smart Client

The BW1330 cannot only be used with a browser, but with a smart client connected to the BW1330 through HTTPS connection; thus, retrieving information given as XML in the same login.user output. To support a smart client, the following lines should be included in all user XSL templates:

```
<xsl:import href="xml-in-comments.xsl"/>
<xsl:apply-templates select="Gemtek/WISPAccessGatewayParam"/>
```

Commands for User Pages

A user who is not logged in and trying to browse the Internet will be redirected to the welcome page automatically.

The **welcome** page address is:

`https://` BW1330_ip_address`/welcome.user`

The **login** page address is:

`https://` BW1330_ip_address`/login.user`

The **logout** and session information page address is:

`https://` BW1330_ip_address`/logout.user`

For the user who is logged in, the form should be posted to `/login.user` address and the form should have the following parameters:

username - username to log on;

password - user password;

'cmd' with value 'login'.

To receive connected user session information, the following address should be used:

`https://` BW1330_ip_address`/logout.user`

To disconnect a user who is currently connected, the following address should be used:

`https://` BW1330_ip_address`/logout.user` with parameter 'cmd' with value 'logout'.

Entering the following address into the browser will disconnect the currently logged in user:

```
https:// BW1330_ip_address/logout.user?cmd=logout
```

Upload Templates

All user pages files (welcome.xsl, login.xsl, logout.xsl, help.html, unauthorized.html) can be on an external server or on the BW1330. Which templates are to be used is found in **user interface | configuration | pages**. The BW1330 has default user templates that can be replaced by uploading new templates. Any uploaded templates and images overrides the default templates.

Next to predefined templates, there are supported image types:

- PNG
- GIF
- JPG

Supported cascading style sheets:

- CSS

Uploaded file types are detected by their extension.

Use of cascading style sheets (css) is not required, but recommended.

The Wireless PAC administrator is responsible to conduct tests to ensure that all uploaded templates are correct and work as expected. After the upload, the controller does not verify the correctness of the uploaded templates. If the controller is not able to load the uploaded xsl template, it will use the default build-in templates.

Image Location

Designers who prepare custom user templates should take note of the location of the images used. All uploaded images, style sheets and static HTML pages (help.html and unauthorized.html) are located at the virtual directory 'images'. Uploaded image example.gif will be accessible at the following path: 'images/example.gif'

Using other paths like 'webserver/example.gif' or 'example.gif' will redirect to images/unauthorized.html' or if UAM is enabled to user page (welcome.user, login.user or logout.user depending on device configuration and user status).

This is an example of how to use an image in a XSL template:

```
<img name="example" src="images/example.gif" />
```

Glossary

Symbols:

802.11: 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The original specification provides for an Ethernet Media Access Controller (MAC) and several physical layer (PHY) options, the most popular of which uses GFSK modulation at 2.4GHz, enabling data rates of 1 or 2Mbps. Since its inception, two major PHY enhancements have been adopted and become "industry standards".

802.11b adds CCK modulation enabling data rates of up to 11Mbps, and 802.11a specifies OFDM modulation in frequency bands in the 5 to 6GHz range, and enables data rates up to 54Mbps.

A

AAA: Authentication, Authorization and Accounting. A method for transmitting roaming access requests in the form of user credentials (typically user@domain and password), service authorization, and session accounting details between devices and networks in a real-time manner.

authentication: The process of establishing the identity of another unit (client, user, device) prior to exchanging sensitive information.

B

backbone: The primary connectivity mechanism of a hierarchical distributed system. All systems, which have connectivity to an intermediate system on the backbone, are assured of connectivity to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.

Bandwidth: Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit. For example, typical Ethernet has a bandwidth of 100Mbps.

bps: bits per second. A measure of the data transmission rate.

D

DHCP: Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, ÿn IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DNS: Domain Name Service. An Internet service that translates a domain name such as browan.com to an IP address, in the form xx.xx.xx.xx, where xx is an 8 bit hex number.

E

EAP: Extensible Authentication Protocol. Defined in [RFC2284] and used by IEEE 802.1x Port Based Authentication Protocol [8021x] that provides additional authentication methods. EAP-TLS (Transport Level Security) provides for mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints [RFC2716]. EAP-TTLS (Tunneled TLS Authentication Protocol) provides an authentication negotiation enhancement to TLS (see Internet-Draft <draft-ietf-pppext-eap-ttls-00.txt>).

ERP: Extended Rate PHY. The 802.11g enhancement to the Physical Layer definition that introduces OFDM as a mandatory coding scheme for mandatory 6, 12 & 24Mbps bit rates and 18, 36, 48 & 54Mbps optional bit rates. The ERP retains backward compatibility with 802.11b coding and modulation mechanisms.

G

gateway: A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

H

hotspot: A hotspot is wireless public access system that allows subscribers to be connected to a wireless network in order to access the Internet or other devices, such as printers. Hot-spots are created by WLAN access points, installed in public venues. Common locations for public access are hotels, airport lounges, railway stations or coffee shops.

hotspot operator: An entity that operates a facility consisting of a Wi-Fi public access network and participates in the authentication.

HTTP: The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

HTTPS: HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

I

ICMP: ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

IEEE: Institute of Electrical and Electronics Engineers. The IEEE describes itself as the world's largest professional society. The IEEE fosters the development of standards that often become national and international standards, such as 802.11.

IP: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

IPsec: IPsec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPsec will be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Cisco has been a leader in proposing IPsec as a standard (or combination of standards and technologies) and has included support for it in its network routers.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

ISP: An ISP (Internet Service Provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

L

LAN: A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network).

M

MAC: Medium Access Control. In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packet formatting and addressing, and error detection.

N

NAT: NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses.

NAT is included as part of a router and is often part of a corporate firewall.

P

POP3: POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netmanage suite of Internet products and one of the most popular e-mail products, Eudora. It's also built into the Netscape and Microsoft Internet Explorer browsers.

PPP: PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

PPPoE: PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. PPPoE can be used to have an office or building-full of users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame.

PPPoE has the advantage that neither the telephone company nor the Internet service provider (ISP) needs to provide any special support. Unlike dialup connections, DSL and cable modem connections are "always on." Since a number of different users are sharing the same physical connection to the remote service provider, a way is needed to keep track of which user traffic should go to and which user should be billed. PPPoE provides for each user-remote site session to learn each other's network addresses (during an initial exchange called "discovery"). Once a session is established between an individual user and the remote site (for example, an Internet service provider), the session can be monitored for billing purposes.

PPTP: Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. This kind of interconnection is known as a virtual private network (VPN).

R

RADIUS: RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

S

SNMP: Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMP is described formally in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157 and in a number of other related RFCs.

SSL: The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

T

TCP: TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

Telnet: Telnet is the way to access someone else's computer, assuming they have given permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. On the Web, HTTP and FTP protocols allow to request specific files from remote computers, but not to actually be logged on as a user of that computer.

U

UAM: Universal Access Method is the current recommended methodology for providing secure web-based service presentment, authentication, authorization and accounting of users is a WISP network. This methodology enables any standard Wi-Fi enabled TCP/IP device with a browser to gain access to the WISP network.

W

WAN: A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (MAN).

X

XSL (Extensible Style sheet Language), formerly called Extensible Style Language, is a language for creating a style sheet that describes how data sent over the Web using the Extensible Markup Language (XML) is to be presented to the user.