

# **User's Manual**

This is the new designer of the AP Router firmware version 8.3. From now on we will show the settings for each part of the AP.

The Status screen is the most complete and modern. Some things we can see now that it had in previous versions.



AP Router Status LAN Settings IP Alias & Routes Wireless Settings Clients Database Services Firewall QoS Site Survey Associated Stations Signal Setup Logout

#### Status Information.

##### System

Model SmartAP-2 → **1**

Alias

Uptime 0days:0h:1m:11s

Firmware Version 8.3 → **2**

NTP Client Disabled

Date & Time Sat Jan 01 00:01:11 UTC 2000

Operation Mode Bridge ← **3**

##### Wireless Information

Mode AP

Band b

SSID AirWAN

Channel 14

Crypt Disabled

BSSID 00:23:d3:00:f9:89

Status Initialized

Associated Stations 0

TX Power - 802.11b 18 dBm → **4**

TX Power - 802.11g 20 dBm

Tx Power 20 dBm

Wireless MAC 00:23:d3:00:f9:89

##### TCP/IP Settings - LAN

IP Address 192.168.2.1

Netmask 255.255.255.0

Gateway 192.168.2.254

MAC Address 00:23:d3:00:f9:87

##### DHCP Settings

DHCP Server Enabled

BANDwidth Control

Interface Control Disabled

IP Control Disabled

MAC Control Disabled

Comes with the model of equipment **01 02**.

When the equipment is in the Bridge **03**, the WAN interface is hidden and only appears the LAN interface settings (see next figure).

NTP client information, power of wireless interface **04**.

### Status Information.

#### System

Model	SmartAP-2
Alias	
Uptime	0days:0h:0m:21s
Firmware Version	8.3
NTP Client	Disabled
Date & Time	Sat Jan 01 00:00:21 JTC 2000
Operation Mode	Gateway → 5

#### Wireless Information

Mode	AP
Band	b
SSID	AirWAN
Channel	14
Crypt	Disabled
BSSID	00:23:d3:00:f9:89
Status	Initialized
Associated Stations	0
TX Power - 802.11b	18 dBm
TX Power - 802.11g	20 dBm
Tx Power	20 dBm
Wireless MAC	00:23:d3:00:f9:89

#### TCP/IP Settings - LAN

IP Address	192.168.2.1
Netmask	255.255.255.0
MAC Address	00:23:d3:00:f9:87

#### TCP/IP Settings - WAN

IP Configuration Type	DHCP
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
MAC Address	00:23:d3:00:f9:88

#### DHCP Settings

DHCP Server	Enabled
-------------	---------

#### BANDwidth Control

Interface Control	Disabled
IP Control	Disabled
MAC Control	Disabled

Continuing to talk about that hide the WAN interface. We note that the equipment for Gateway 05, so it is replaced by the WAN interface 06 as shown.

Here is where we define the TCP / IP **07**, a portion of the utmost importance and requires a little knowledge. The ID field equipment **08**, already speaks by itself. Serves only to identify the equipment. This name will appear in the Status screen. Mode of Operation **09** is very important, is through him that we define how the equipment will behave in our network. There are five modes of operation of the equipment: Gateway, Bridge, Client ISP, Ethernet Router and Wireless Router. Taking the Bridge mode, all they release access.

With the new version, you can have up to three separate interfaces, different from the earlier versions that were even two. As shown in the Advanced Settings **05**, you can for exam, have entered the Internet via the WAN port Ethernet, the Ethernet LAN ports have customers with different IPs that are in the Wireless LAN port.

It is the same logic of a VLAN. The computers that are connected to the wireless interface will not see those on the Ethernet interface (via cable). And best of all is that each interface will have its DHCP server.

AP Router Status | LAN Settings | IP Alias & Routes | Wireless Settings | Clients Database | Services | Firewall | QoS | Site Survey | Associated Stations | Signal | Setup | Logout

**LAN Settings**

Alias:  **8**

Operation Mode: **7** Gateway **9**

**LAN Settings**

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

802.1d Spanning Tree

DHCP Server: Server

DHCP Server Range: 192.168.2.100 - 192.168.2.200

Domain:

DHCP Lease Time: 7200

[Show lease table](#)

**WAN Settings**

**Advanced Settings**

**DNS Settings**

Save Reset

**WAN Settings**

IP Configuration Type: Fixed IP

IP Address: 192.168.100.1 **10**

Netmask: 255.255.255.0

Default Gateway: 192.168.100.254

WAN MAC Clone: 000000000000

**Advanced Settings**

Wlan0 **11**

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

DHCP Server: Disabled

**DNS Settings**

DNS Mode: Manual

DNS Server 1: 208.67.222.222 **12**

DNS Server 2: 208.67.220.220

DNS Server 3: 0.0.0.0

Save Reset

IP settings for the other interfaces. Configuring the WAN **10**, which is the entrance of internet settings avocados **11**, lets you put an IP in Wireless interface separating it from other interfaces and DNS settings **12**.



13

AP Router Status LAN Settings **IP Alias & Routes** Wireless Settings Clients Database Services Firewall QoS Site Survey Associated Stations Signal Setup Logout

## IP Alias

Ip	Mask	Interface	Options
0.0.0.0	0.0.0.0	Lan	
192.168.0.1	255.255.255.0	Lan	

14

## Static Routes

Ip	Mask	Gateway	Comment	Options
0.0.0.0	0.0.0.0	0.0.0.0		
10.10.10.1	255.255.255.0	192.168.0.10	RoutesA / RouB	

15

16

17

**IP Alias and Route 13** are features of specific use. For example if you want to put more than one IP address on the LAN interface for separating two or more networks. Just enter the IP, mask and to select which interface will be created, LAN or WAN, this nickname, alias or as many know. After filling out the required fields, you must click the green arrow next to **14** that this action will continue. The rule automatically goes down **15** giving start to a table. If you need to change this IP, you just modify it's own table and pressed the edit button **16** and to delete an alias IP simply click the **X 17**.  
**Note:** Those names are not good at doing VLAN. Because computers will be on the same bus network they will not fail to see.

Static routes are mainly used when the equipment is part of the router. For this, just put the IP of the destination host or network, its proper mask and the gateway to reach the desired network. The rules of the buttons **15**, **16** and **17** is the same for the table of routes.



AP Router Status LAN Settings IP Alias & Routes **Wireless Settings** Clients Database Services Firewall QoS Site Survey Associated Stations Signal Setup Logout

### Wireless Settings

#### Basic

Enable Wireless Interface

Operational Mode: AP  
 Band: 11b/g  
 Network Type: Infrastructure  
 SSID: AirWAN  
 Country: Japan  
 Channel: Auto

#### Advanced

In the configuration of the wireless here is the part of Basic and Advanced. In Basic is where we configure the wireless features. We can simply turn it off page 18 and it is hidden. Otherwise, choose a mode of operation that can be 19 AP, Client, WDS, AP + WDS or Repeater Universal, 20 Band 11b 11M to 2.4GHz, and 2.4GHz band for 54M 11g. In advanced we Fragment Threshold: Standard size for sending packets in networks with high traffic or have many packages with error it is advisable to be reduced RTS Threshold: Size of the send request packet if the network is unstable this value should be reduced.

Operational Mode: AP



#### Advanced

Fragment Threshold: 2346 ( 256-2346 )  
 RTS Threshold: 2346 ( 0-2347 )  
 Beacon Interval: 100 ( 20-1024 ms )  
 Fixed Rate: Auto  
 Preamble: Long Preamble  
 802.11g Protection:  Active  
 IAPP:  Active  
 Turbo Mode:  Active  
 Tx Power (CCK): 18dbm(63mW)  
 Tx Power (OFDM): 20dbm(100mW)  
 Broadcast SSID:  Active  
 Block Relay:  Active  
 TX Burst:  Active  
 ACK Timeout: 0 ( 0-255 ) Default = 0

**IAPP:** Mesh Network Protocol. **Turbo Mode:** Only works with equipment from the same manufacturer. **TX Power (CCK):** Refers to the power of Band B. **TX power (OFDM):** Refers to the power of the Band A / G **Broadcast SSID:** Enable or disable the SSID issue. **Block Relay:** Allows or not the visualization of other network equipment. **ACK Time Out:** In order resumed, is the adjustment of transmission time between two APs.

**Beacon Interval:** Packages sent by the timing Access Point. **Basic Rates, Rates and Fixed Rates Supported:** Are all speed options of the radio. **Preamble Type:** These are control bytes and sync that comes before sending dados. **Portico 802.11g:** In transmissions B / G G assures customers work on their speed and their customers is not level B.

## Wireless Settings

Basic

Advanced

Security

Authentication:

Crypt:

Access Control

Open System  
Open System  
Shared Key  
Automatic  
802.1x (WEP)  
WPA  
WPA2  
WPA-PSK  
WPA2-PSK

Save

Reset

On the Security menu, configure encryption. What is Open System: no encryption, shared key: WEP64 and WEP128 encryption, ASCII or HEX, Auto: WEP64 and WEP128 encryption, ASCII or HEX, 802.1x (WEP): RADIUS authentication requires the appointment to a server via port, IP and password, WPA and WPA2: with TKIP, AES and RADIUS, WPA-PSK and WPA2-PSK: TKIP and AES pass phrase.

Access Control is disabled by default, but we can allow listed MAC block listed or Authenticate via RADIUS. The difference of Access Control in relation to other equipment, is that registering the MACs are not made in this part but on Customer Database. MACs granddaughter table appear automatically when the client is registered.

## Wireless Settings

Basic

Advanced

Security

Access Control

ACL Mode:

MAC Address:

Allow list  
Disabled  
Allow list  
Deny list  
MAC Address through Radius

Save

Reset

21

22

23

AP Router Status LAN Settings IP Alias & Routes Wireless Settings **Clients Database** Services Firewall QoS Site Survey Associated Stations Signal Setup Logout

Automatically attach clients into QoS root group\*

\* When enabled, new clients inserted below will be added to QoS root automatically.

Save Save & Apply

Insert IP  :

Client	Ip	Min Download	Min Upload	Max Download	Max Upload	ACL Active	Options
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	---

Entry list:

Client	Ip	End Ip	Mask	MAC	Min Download	Min Upload	Max Download	Max Upload	ACL Active	Active	Options
Camera	60.251.56.31	0.0.0.0	0.0.0.0	00:23:D3:00:00:01	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

Insert client  
 Change client  
 Delete client

ACL When enable, this entry is at Access Control List.

This is a register of customer base, which will be used in other modules of the firmware as Bandwidth Control (QoS) **21**, Access Control (wireless) **22**, Firewall and tie the IP to MAC. The addition, modification and removal is always done on this screen. **23** If you change any settings here in the customer master, for example, the name, or even the MAC, will be changed automatically in another module that it is being used without disturbing anything on the run.

There are five modes of customer base: by IP, MAC, IP and MAC, Network and IP range. Regardless of the type of registration that was chosen in all the fields will be displayed after you register, Client, IP, IP End Mask, MAC.

## Tying the IP to the MAC:

To tie the IP to MAC just register the MAC and IP option in the client registry of IP and MAC. It is logical that the equipment in question must be a DHCP server and for this he can not be in Bridge mode.

## Firewall:

The Firewall also depends on the Registration of Client to have meaning in paging XX demonstrate how to use the Firewall with customers registered here.

## Access Control:

Access Control is used when the equipment is in Access Point mode. It's a way we can protect our network of clients registering the MAC has allowed access. When you tick the ACL on the Register Client automatically switches to the MAC Access Control in Wireless tab. The moment you activate the Access Control tab and apply the changes wireless access control comes into play.

## Bandwidth Control:

First and foremost it is important to know that the bandwidth control is done on QoS but the band profile for each client is determined at the time of registration. The bandwidth control can be done individually for each client, therefore, this account must be related to the root group, or the client may be part of a group pre-created for us on the QoS Rules tab of the group are prominent on all the other rules.

Before you begin to register customers via MAC, IP ... Or whatever the mode, you'd know the reason for the registration of download and upload speeds, minimum and maximum ...

When you register values for download and upload, this does not mean that the control bandwidth has to happen. These values are only valid if you come to relate these customers in the QoS that is the case where the bandwidth control. If you leave the minimum and maximum values at zero and enroll these customers in a group of QoS, the calculation will be done automatically according to the availability of the group.

Using our examples, the Commercial Department was registered with 0kbps (zero) to download and 0kbps minimum (zero) from minimum to upload, up to 400kbps for download and 200kbps for uploading. Lets see how this customer would be in control of the band.

By default is already set up a group of QoS that is the root group, so if you registered the Commercial Department in this group (root) values created in the database of customers is going to be worth, since the root group comes with all values download and upload max in caso 100Mbps. But if we create a group and register the Commercial Department of this group, automatically download and upload values we create for the group is what will prevail over all members of this group, for example, create a group and this group registrations a maximum download and upload of 128kbps. In this group we will register the Commercial Department, remember that the customer base Rep. Commercial was registered with 400kbps download and 200kbps upload. Well, if he is in a group with a maximum of 128kbps download and upload, the values we place at the time we've registered Rep. Commercial not become worth more as the Commercial Department is a member of a group and is always characteristics of the group prevails. In addition there will be a mistake to relational the client, we'll forward this error.

You may be wondering why we put the customer base values of download and upload? These values can serve for an organization within the group, for example: We created a group of 1024kbps and registered 10 clients in this group, but each client in this group can download a maximum of 500kbps. The values of register would be as follows: for each client cadastraríamos 0kbps (zero) for minimum download and upload 500kbps for maximum download and upload. The group would 0kbps (zero) as a minimum, download and upload and 1000kbps for the maximum download and upload. In this case by more than a client to invoke your connection it will never use all the bandwidth of the group harming other customers as he is confined in a maximum of 500kbps.

Another interesting example to be analyzed is the minimum download and upload that may be registered in the Register of Clients. If we have a client of a VoIP user, we must take into consideration that for the smooth operation of voice over IP we have to guarantee a minimum bandwidth for this service, so that minimum registered as in the example VoIP Management, which has a minimum of 100kbps for Download and upload and a maximum of 400kbps for download and upload. When this client is part of a group where the client is online is a guaranteed minimum bandwidth for this client. The care that we have on record that the minimum is the sum of all minimal accounts does not exceed the maximum group, for example: if we have a group of 400kbps download with six customers VoIP users in the group and register a minimum to 100kbps for each client, will give error in the group, since the sum of the minimum ( $100 \times 6 = 600$ kbps) is greater than the maximum of the group which is 400kbps. Solution for this case:

- 1) Increase the maximum group to 600kbps.
- 2) Move two clients of the group.
- 3) Reduce the minimum of each customer in the Customer Database.

**Note:** Decreasing the minimum of each client would not be more correct procedure, as you solve one problem and create another. For decreasing the minimum download and upload each client, would not mistake the group, but you would not guarantee a good VoIP service to your customer.

Then we'll see each type of registration, IP, MAC, IP and MAC, Network, and Range of IPs:

Client	Ip	Min Download	Min Upload	Max Download	Max Upload	ACL	Active	Options
Camera	60.251.56.31	0	0	512	512	---		

**Control over IP: will the Client Name, IP, minimum and maximum speed. ACL in this case there is no point scoring, because the access control is by MAC and not IP.**

Client	MAC	Min Download	Min Upload	Max Download	Max Upload	ACL	Active	Options
Camera	00:23:D3:00:00:01	0	0	512	512	---		

**Control by MAC: will the Client Name, MAC, the minimum and maximum speed. In this case, the ACL can be checked, if you want this client / MAC part of Access Control.**

AP Router Status LAN Settings IP Alias & Routes Wireless Settings **Clients Database** Services Firewall GoS Site Survey

Automatically attach clients into QoS root group\*

*\* When enabled, new clients inserted below will be added to QoS root automatically.*

Save Save & Apply

Insert IP & MAC :

Client	Ip	MAC	Min Download	Min Upload	Max Download	Max Upload	ACL Active	Options
Camera	60.251.56.31	00:23:D3:00:00:01	0	0	512	512	<input type="checkbox"/>	---

**Register by IP and MAC:** is to merge the two examples above and beyond the IP and MAC must also be registered. Marking the MAC ACL is now part of Access Control and is also so that the MAC is tied to the IP.

**Control by Network:** The networked control, generalizes an entire IP network, for which the network is managed correctly, your mask is essential. Sign the minimum and maximum speed and the ACL does not help check this case.

AP Router Status LAN Settings IP Alias & Routes Wireless Settings **Clients Database** Services Firewall GoS Site Survey

Automatically attach clients into QoS root group\*

*\* When enabled, new clients inserted below will be added to QoS root automatically.*

Save Save & Apply

Insert Network :

Client	Ip	Mask	Min Download	Min Upload	Max Download	Max Upload	ACL Active	Options
Camera	60.251.56.31	255.255.255.0	0	0	512	512	<input type="checkbox"/>	---

**By IP Range:** A limited group or rather a range of IPs given by the administrator using the fields starting IP and End IP, plus the minimum and maximum speed and ACL does not help scoring.

AP Router Status LAN Settings IP Alias & Routes Wireless Settings **Clients Database** Services Firewall GoS Site Survey

Automatically attach clients into QoS root group\*

*\* When enabled, new clients inserted below will be added to QoS root automatically.*

Save Save & Apply

Insert IP Range :

Client	Ip	End Ip	Min Download	Min Upload	Max Download	Max Upload	ACL Active	Options
Camera	60.251.56.31	60.251.56.41	0	0	512	512	<input type="checkbox"/>	---

## Services

- General
- VPN (VTUN) Settings
- System Log
- WatchDog
- DynDNS
- NTP Client
- Cron Scheduler
- MESH (OLSR)
- Personal Script

Salvar

## Services

### General

- PPPoE Relay
  - DNS Relay (dnrd)
  - DHCP Relay
- DHCP Server IP Address: 192.168.2.254

24

**General: 24** This menu is very simple to configure. The PPPoE Relay is an event marked another device or computer that is connected to it is responsible for PPPoE authentication. Relay (DNS dnrd) streamlines the cache of DNS zones and allows the equipment to be the DNS server to host online. Relay DHCP: The DHCP relay is a machine capable of receiving packets from DHCP clients on your network, and forward these requests to another server. For this, just enter the IP through the DHCP server.

## VPN (VTUN) Settings

VPN Service (VTUN): Client

Connection Name: AirLinkWiFi

Server Address: 125.65.112.13

File:

25

**Configuring VPN (VTUN): 25** You can use the AP Router to a VPN, it can be both a client and can be a server. Make the script VTUN in a simple text editor and send this file over the Send button configuration file.



System Log

System Log

Send to remote log server with IP

26

**System Log: 26** Are any events generated by the system that you can follow on-screen setup AP Router or forward to a server log indicating the server's IP.



WatchDog

WatchDog

IP Address

Time Interval  Seconds

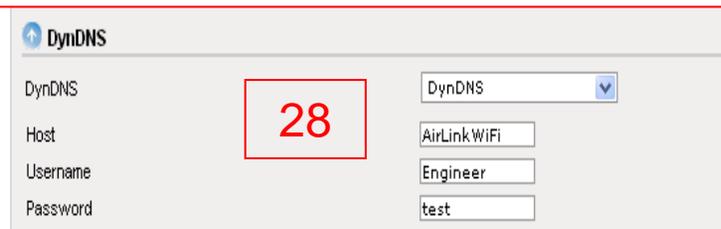
WatchDog 2

IP Address

Time Interval  Seconds

27

**WatchDog per IP: 27** The IP WatchDog by nothing more than a simple ping test to an address or two IP configured below. This case (s) do not respond (m), the unit restarts automatically. Checking interval is in seconds. To disable the function, just put in 0.0.0.0 (s) field (s) address (s) IP.



DynDNS

DynDNS

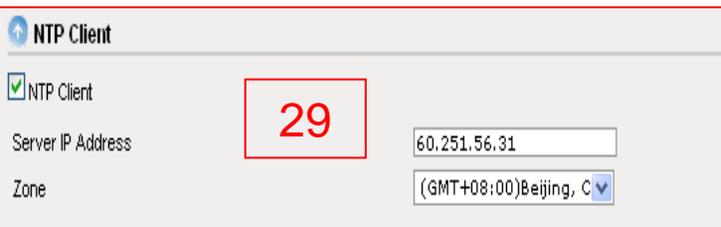
Host

Username

Password

28

**DynDNS server: 28** DNS Domain Name provides services that had resolved names for dynamic IP simplifying access to these hosts, so it is not necessary to know the IP but the host name. Enrollment into DynDNS and TZO servers are free.



NTP Client

NTP Client

Server IP Address

Zone

29

**NTP Client: 29** Next page you may configure your system to synchronize the time with a public NTP server on the Internet, with a particular server or yours.

**Cron Scheduler**

Cron Scheduler

File: 30

Scheduled Tasks (cron): **30** a program that executes scheduled commands in **Unix-like operating systems**. The cron will be in charge of verifying the time and determine whether or not any program to be run. If there is it will run on the hour and date requested.

**MESH (OLSR)**

MESH (OLSR)

File: 31

MESH System (olsrd): **31** A mesh network consists of multiple nodes / routers, which are to behave as a single large network, enabling the client to connect to any one of us. Communication between the points / APs is via the OLSR protocol in ad hoc mode. All facilities participating in the network must have this protocol (OLSR) running.

**Personal Script**

File: 32

Script Staff: **32** This page is used for editing your personal script, which will be called from within / etc / init.sh.

**Firewall general options**

- Ativa ping na WAN **33**
- netbios block **34**
- p2p block **35**

Buttons: Save, Save & Apply

**Firewall groups**

Group name	Options	A
Client	<input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <b>36</b>
Office	<input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/>

**Firewall Rules - [add rule](#)**

Rule Name	Type	Details	Function	Groups	Options
No entry found.					

**37**

**Clients associated to firewall groups - [link client to group](#)**

Groups	Client	Options
No entry found.		

**38**

Enables the WAN Ping: **33** Allows you to send a ping command remotely from the WAN interface.

**NetBIOS Block : 34** Enabling NetBIOS Block causes the packets regarding this protocol not to flow between networks, where the AP Router is configured in bridge mode.

**P2P Blocking: All 35** packets of P2P are blocked by the firewall, but if the package travel from P2P network in encrypted form, in this case the firewall can not identify it.

**Groups firewall: Group of 36** created to enable different firewall rules in firewall rules **37**. For example, one group may have a firewall rule blocking MSN and other group may have a rule to limit connections. Customers connected in groups of **38** can add a firewall client denied access to MSN but I do not need to worry about the number of connections the same. If this customer has these two restrictions, just add it to both groups. We can create as many groups as necessary.

The image shows a screenshot of the 'Firewall Rules - add rule' window. The window is divided into several sections:

- Rule Name:** A text input field with a red callout **39** pointing to the 'add rule' button above it.
- Type:** A dropdown menu currently set to 'String Control', with a red callout **40** pointing to it.
- String Control:** A text input field for keywords, with a red callout **40** pointing to it.
- Groups attached to rule:** A section with 'Available Groups' and 'Selected Groups' lists, with a red callout **42** pointing to the 'Available Groups' list.
- Program List:** A separate window titled 'MSN Messenger - Chat' showing a list of programs, with a red callout **41** pointing to it.

The dropdown menu for 'String Control' is expanded, showing the following options:

- String Control
- String Control
- Program (Layer7) Control
- P2P (Emule, BitComet...) Control
- IP Control
- Mac Address Control
- Connection limit
- Port forwarding
- Port/IP Forwarding
- Port Control
- DMZ
- URL Control

The program list in the 'MSN Messenger - Chat' window includes:

- POCO e PP365 - P2P software
- POP3
- Tencent QQ
- Quake 1
- Half Life 1 - HL 1 - Quake 2/3/World - Counterstrike 1.6
- RDP
- rlogin
- RTSP
- Shoutcast e Icecast
- SIP
- Skype para telefone
- Skype para Skype
- Samba/SMB
- SMTp
- SNMP
- SOCKS Versão 5
- Soribada - P2P software
- Soulseek - P2P software
- SSDP
- SSH

**Firewall rules:** When we click add rule **39**, a window opens. In this window we'll name the rule and select the type of rule that we create. For each type of rule, the window frames so that we can fill the fields correctly. For example if you choose Control words (strings) **40** opens into a field you enter the site or the content to be controlled, but if you choose Control Program, a list **41** with more than ninety programs appears. All these rules are based on IP tables and are already pre-configured. For special rules, you can use the script tab staff services. With the rule set, we can add the groups that can or should do this part (s) rules (s). The group will be pre-created Groups appear in the window **42** free.

Clients associated to firewall groups - [link client to group](#)

Groups

44

45

46

47

45

47

customers connected to groups of firewalls: Now let's connect 43 clients who should be part of a firewall rule, or rather a group. All customers that were added in Registration Client will appear in the list of 44 clients and 45 free Groups window, all 46 groups previously created will be listed, just select the group to which the customer must take part in, click the arrow in right that these groups begin to appear in the window of Selected Groups 47.

AP Router Status LAN Settings IP Alias & Routes Wireless Settings Clients Database Services Firewall GoS Site Survey Associated Stations Signal Setup Logout

**Firewall general options**

Ativa ping na WAN  
 netbios block  
 p2p block

Save Save & Apply

**Firewall groups**

Group name	Options	A
		48

**Firewall Rules - [add rule](#)**

Rule Name	Type	Details	Function	Groups	Options
No entry found.					

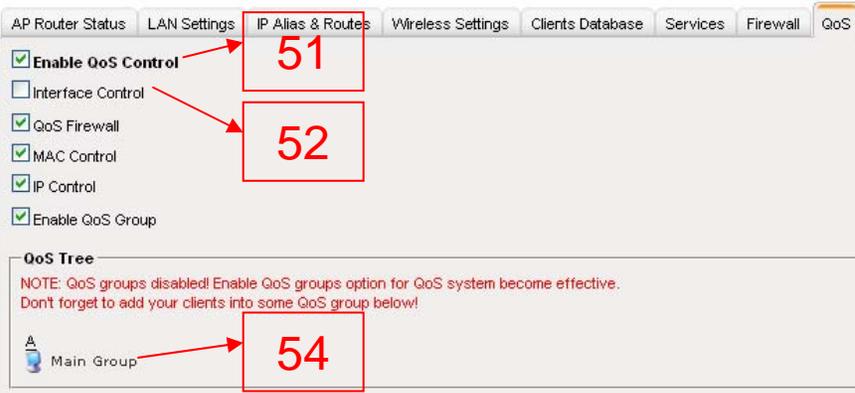
49

**Clients associated to firewall groups - [link client to group](#)**

Groups	Client	Options
No entry found.		

50

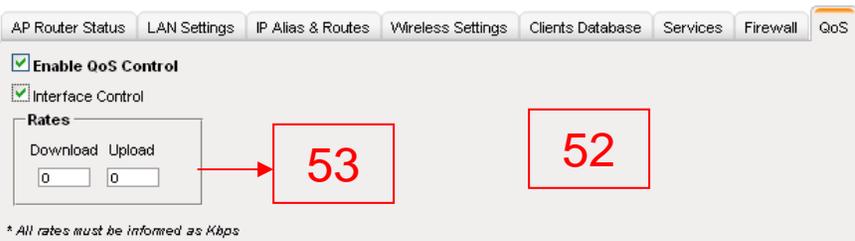
In order to screen the firewall is as follows: List all groups 48, 49 firewall rules created in every detail with the name, type of rule, details the role and groups that make up the rule and 50 guests linked to a particular group are also listed.



QoS tab is where the true bandwidth control. When we access the tab of QoS, the system is off **51**, to enable QoS, some further options that can be enabled or not appear.

The bandwidth control can be done with the data that were registered in Customer Register or can be done by interface **52**. In this case the whole band is controlled in the input and output interface regardless of the number of devices that it is connected. Just enter the maximum download and upload **53**. The bandwidth control by the interface is simpler, does not require much knowledge on the part of QoS

By default QoS tab already exists a group which is the root group **54** and that comes with the maximum bandwidth that can be traveled by the equipment that is 102,400 Kbps (100Mbps), which corresponds to this speed transfer rate used by large Most standard 10/100 network cards.



In the following pages we will illustrate how to make the bandwidth control by IP or MAC. The data bandwidth for each customer must be made in the Customer Database tab (look páginasXX). The examples will be based on customers who are registered in the Register of Clients tab.

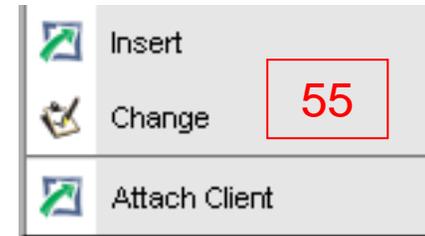
**Firewall QoS:** The QoS Firewall serves to block users have registered to access the Internet. When this option is enabled, only clients connected will be able to surf the internet. If it is not enabled, the bandwidth control will work fine for registered customers, but those who are not registered will have free access and without bandwidth control.

**Control by MAC:** Makes the QoS control the band by MAC address.

**Control over IP:** Makes the QoS control the band by IP address

**Groups enable QoS:** Allows the network administrator to create groups of QoS as are necessary.

**NOTE:** How to Control for IP and MAC Control, we pay attention to the Customer Database, because if we have different types of entries we have to enable the two types of control here in the QoS



When I press the left button on the Root menu, the submenu appears **55** left with the options of Add, Change, and customer relationship. When clicked on will include the option to create a group **56** with the minimum and maximum download and upload a minimum and maximum. In a simple group do not care about the minimum but always with the maximum of the band. In a simple group we have no need to register the minimum download and upload at least. These values can be left at 0 (zero). But if this group is a special group, a group type of equipment that require a minimum of up and down, like VoIP, in which case we must then register these values.

QoS Groups					
Group name	Min Upload	Max Upload	Min Download	Max Download	Options
<input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>				
					<b>56</b>

You can simply relate Clients. Clicking Relate clients, a list of pre-registered customers in Customer Database will appear. To give you a good understanding of the control band, it is essential to read the previous pages on Customer Database and Bandwidth Control.

**Site Survey**

Mode	Channel	SSID	BSSID	Encryption	Signal	Select
AP	5	SmartAP (Engineer)	00:23:d3:01:c8:7c	WEP		<input type="radio"/>
AP	6	WiFi-11N Router	00:23:d3:01:a2:7d	WEP		<input type="radio"/>
AP	5	RT305x_AP	00:0c:43:56:11:eb	no		<input type="radio"/>
AP	11	AirLinkWiFi.Net	00:23:d3:01:e8:21	WEP		<input type="radio"/>
AP		S2	00:11:d8:24:55:ad	WEP		<input type="radio"/>

Search Connect

1 2 3 4 9 5 6 7 8

The Site Survey lists the networks it finds on the frequency that your equipment is configured. In this case the scan list mode the equipment is **01**, channel **02** that is, the network name (SSID) **03**, MAC **04** of its wireless interface (BSSID), whether or not encryption and type **05**, a graph with the signal level **06**, the value at **07** dBm and that your equipment is configured in client mode, you can still select **08** and to connect this AP if all other settings are correct.

The Site Survey is interesting for you to have a sense of number of access points that are emitting the signal and main channel in which they are serving. This makes it easy to choose the best frequency to be used in your link. This table is updated every time you click the Browse button **09**

**Associated Stations**

MAC ADDRESS	Client	Tx Rate	Signal

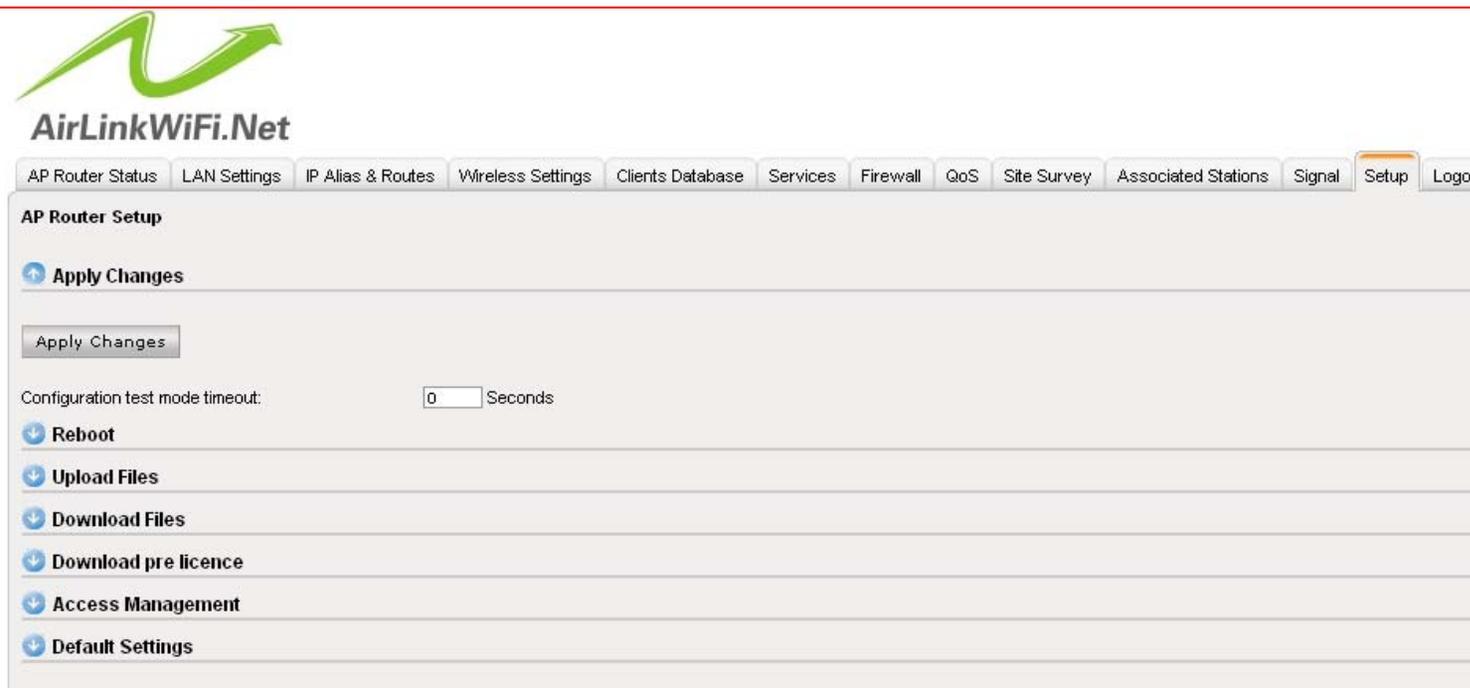
Refresh

10 11 12

The tab shows all connected clients customers who are active, is same as using the command arp-n in Linux to list the arp table. This table lists the user's IP **10**, **11** and its MAC interface **12** Tx Rate.

The Setup tab in addition to having some kind of firmware management options, password change, firmware upgrade .... is the space that always used to do that with all the modifications made to the settings of the radio into operation.

Every tab has a save button when this button is pressed, the setup tab starts flashing red, this means that the amendment should be made and is applied through the Apply button to save the changes it is done. Now a very interesting part of this release is the time to validate the new configuration. If you make a configuration doubtful that you can lose access to radio, then you should set a lifetime for these new settings must have. Say you have configured for 300 seconds (five minutes). One in five minutes you can no longer access the settings of the AP, he returns to the previous configuration. But if the new settings were successful, you have to implement the changes again so that they come into force, otherwise the equipment will reinitialize the same way.



AirLinkWiFi.Net

AP Router Status LAN Settings IP Alias & Routes Wireless Settings Clients Database Services Firewall QoS Site Survey Associated Stations Signal Setup Logout

AP Router Setup

Apply Changes

Apply Changes

Configuration test mode timeout:  Seconds

Reboot

Upload Files

Download Files

Download pre licence

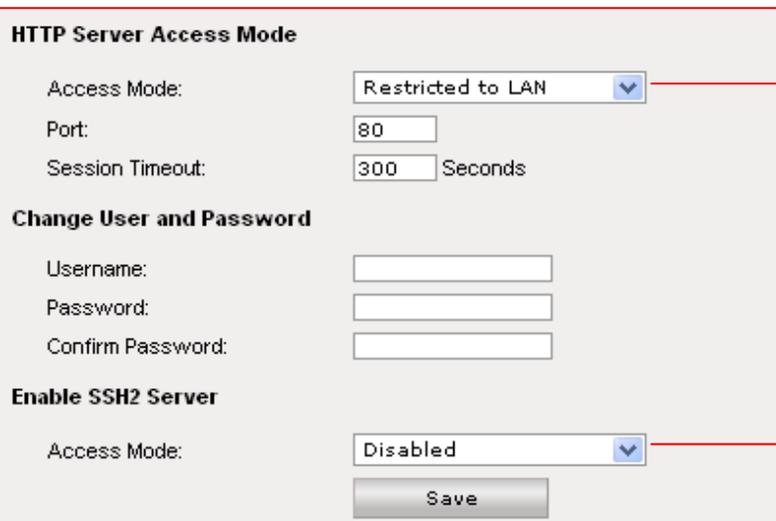
Access Management

Default Settings

The Reset button equipment is the same as a reboot. The option to upload file has three options, upgrade the firmware, apply the license and download the configuration file done Downloading files. The download file is to just save the current configuration of your equipment to speed up if you need future maintenance. The Download pre license is only used when the 8x version is installed by the user. In this case the generated file should be forwarded to our support so that we can generate the license to use the firmware.

In addition to Access Manager we can register a password for access via the Web and via SSH, we can define if access can be done only by LAN interface, the two interfaces - WAN and LAN and can still leave off any access.

Something that happens frequently in how we are accessing the settings and the expiration time of access. This time is also configured in the Access Management in the Session Timeout and serves as a safety. If the user stay indefinitely without doing anything, the session is automatically terminated. But this is configurable.



**HTTP Server Access Mode**

Access Mode:

Port:

Session Timeout:  Seconds

**Change User and Password**

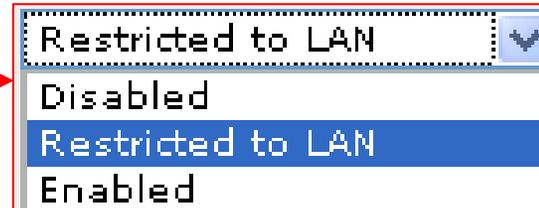
Username:

Password:

Confirm Password:

**Enable SSH2 Server**

Access Mode:



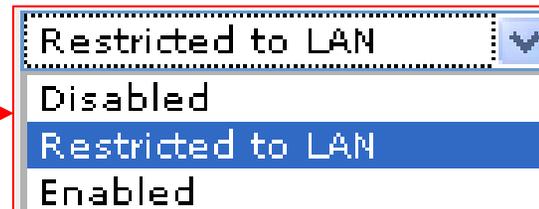
Restricted to LAN

Disabled

Restricted to LAN

Enabled

In the model AirWAN access via the web by default comes with a user is "admin" but that may change.



Restricted to LAN

Disabled

Restricted to LAN

Enabled

The SSH access is disabled by default. And to enable it to be created a password. Already a user has no way be changed. By default the user's SSH access is "root" without quotes.