

WR650a FIRMWARE (LAST UPDATE: 04/Sep/2006)

=> CONTACT INFO

=>Version 6.1

Requirements:

- > Realtek RTL 8186 chipset based equipment
- > At least 16 Mbytes Ram and 2 Mbytes Flash

=> CHANGELOG FROM VERSION 6.0a

- * **5 operation modes: Gateway, Bridge, WISP Client, Router (Ethernet WAN), Router (Wireless WAN)**
- * **MAC Address traffic control when acting as BRIDGE Access Point**
- * **Faster traffic control execution**
- * **Corrections regarding DNS**
- * **Real time RSSI measure, showing dBm signal**

Features:

- > 5 main operational modes: Gateway, Gateway, Bridge,WISP Client, Router(Ethernet WAN) and Router (Wireless WAN).
- > Telnet (client) added
- > /etc/cbu.conf file editing via WEB
- > Enable/Disable SSH server
- > New Configuration method: Save and Apply
- > Clone WAN MAC option
- > ACK Timeout control
- > MESH (OLSR) support: <http://www.olsr.org>
- > SSH Client support
- > Easy personal script /etc/script.sh file editing via web interface
- > Region Domain selection via WEB (11 or 14 channels)
- > Easy /etc/ethers file editing via web interface
- > Tx power control
- > Ipraf Utility
- > Tcpdump Utility
- > Remote access via SSH2
- > Cron daemon
- > Prende o MAC ao IP e fornece ip estaticamente baseado no MAC
- > Freedom to edit your own scripts
- > Bandwidth control (IP, MAC and Interface) with groups option
- > Ping based Watchdog
- > Block Relay
- > PPPoE Relay

- > DHCP Relay
- > Config Wizard
- > Auto Discovery Tool
- > 802.1x, WPA and Radius
- > Mac, ip, ports filter
- > DMZ Host
- > PPPoE-Client
- > PPTP Protocol
- > DDNS Protocol
- > IAPP Protocol
- > Hide SSID
- > WEB Interface
- > Signal meter
- > AP, Client, WDS+AP, WDS and Ad Hoc modes
- > Site Survey
- > DHCP server
- > DHCP Client
- > Up to 5 IP Alias via WEB interface
- > uPNP
- > Spanning Tree Protocol
- > WAN Management protection
- > MAC clone (for just one machine)
- > System commands via WEB interface
- > Log system (local and remote)

=> TESTED MODELS

OBS.: It's supposed to work with any RTL8186 device.

=> NOTES ABOUT TX POWER CONTROL

Tx power control setting was currently tested on WR650A up to 100mW. Tx power setting only works for 802.11b mode.

NOTE: WE DO NOT RECOMMEND HIGH TX POWER OUTPUT. It MAY CAUSE OVERHEATING AND/OR REDUCE EQUIPMENT LIFE TIME.

=> VERSION NOTES

There are as well, special editions with SNMP and VTUN (VPN system) enabled versions.

=> NOTES ABOUT MAIN OPERATION MODES

- There are 5 main operation modes:

- Gateway
- Bridge
- Wireless ISP
- Router (Ethernet WAN)
- Router (Wireless WAN)

-- Gateway mode:

- With this mode, eth0 interface + Wireless will be LAN (br0) Segment. LAN2 (eth1 interface) will be WAN port. NAT will be enabled.

-- Bridge mode:

- All interfaces (ETH0 + ETH1 + Wireless) will be LAN (br0). All firewall functions will be disabled. NAT will be disabled.

-- Wireless ISP mode:

- eth0 + eth1 will be LAN (br0). Wireless (wlan0) will be WAN. NAT will be enabled.

-- Router (Ethernet WAN):

- Eth0 + Wireless will be LAN (br0) Segment. Eth1 interface will be WAN port. NAT will be disabled.

-- Router (Wireless WAN):

- eth0 + eth1 will be LAN (br0). Wireless (wlan0) will be WAN. NAT will be disabled.

=> HOW TO USE BANDWIDTH CONTROL

NOTE: This control uses QoS with HTB.

BAndwidth control it's done through Traffic Control menu, via web interface or via /etc/cbu.conf file. You can limit all traffic via Interface control or you can control via IP and/or MAC basis. Further more, you can create QoS groups and share the group rate among the members of that group. You can as well, guarantee minimum rate for group member.

Ex:

CASE 1:

You are going to install this equipment for a Wireless ISP client, which has maximum 256 kbit download speed and 128 kbit upload. Go to traffic control menu and enable "Interface traffic control", with the values:

LAN Output rate: 256 -> LAN control downloads
WAN Output rate: 128 -> WAN control uploads

With interface based traffic control, you can control maximum interface speed, regardless NAT function enabled or not.

CASE 2:

You are going to install this equipment for an inn establishment, which have 3 clients. Each client wants to have their own speed rate.

With this scenario, you can control them via IP or MAC address. To do it so, enable you desired option (IP/MAC control) and put your client's IP/MAC address. One entry for each client. This way, you will limit desired speed for each individual client. Further more, you can activate firewall option to block any other machine not listed.

To use IP/MAC control, you must disable interface traffic control.

=> HOW TO USE BANDWIDTH CONTROL WITH QoS GROUP OPTION

QoS groups are used to limit a group of users, and share the total rate. The idea here is simple:

- Any member of the group can reach the total rate of the group
- The total sum of all member's traffic together, will not exceed the total rate of the group
- Any member of the group can have guaranteed bandwidth
- Equal bandwidth sharing

Ex:

Let's back to our example above. Inn establishment, which have 3 clients. All clients have 256 kbit speed contract. One of the clients has 2 machines, which he likes to use internet on both. How to solve this case, if he has 256 kbit speed and two machines? Simple. Let's enable QoS group option.

Go to traffic control and enable QoS group option. Create a group as follow:

Group ID: 1
LAN Out rate: 256 -> Total rate for download
WAN Out rate: 256 -> Total rate for upload

Next thing to do is to put the two machines of that client inside the group (via IP or MAC control), as follow:

Group ID: 1 -> Member of QoS group ID 1
IP: 192.168.x.x -> machine's 1 IP

LAN Out rate: 0 -> 0 for equal sharing
WAN Out rate: 0 -> 0 for equal sharing

Group ID: 1 -> Member of QoS group ID 1
IP: 192.168.x.x -> machine's 2 IP
LAN Out rate: 0 -> 0 for equal sharing
WAN Out rate: 0 -> 0 for equal sharing

This is the example for equal sharing between those 2 machines. Now, let's suppose that, this client wants to have at least 200 kbit guaranteed to machine 1. Simple to do it, as follow:

Group ID: 1 -> Member of QoS group ID 1
IP: 192.168.x.x -> machine's 1 IP
LAN Out rate: 200 -> 200 kbit guaranteed
WAN Out rate: 200 -> 200 kbit guaranteed

Group ID: 1 -> Member of QoS group ID 1
IP: 192.168.x.x -> machine's 2 IP
LAN Out rate: 0
WAN Out rate: 0

The other 2 clients, will have no group:

Group ID: 0 -> Does not belong to any group
IP: 192.168.x.x -> Client 2
LAN Out rate: 256
WAN Out rate: 256

Group ID: 0 -> Does not belong to any group
IP: 192.168.x.x -> Client 3
LAN Out rate: 256
WAN Out rate: 256

=> HOW TO GUARANTEE BANDWIDTH FOR A VOIP SYSTEM

We will use this example to show how easy is to guarantee bandwidth for a voip system for instance. The main objective here is, to set up simple scenario with no effort. The scenario is:

- Internet connection of 300 kbit
- Guarantee 64 kbit for Voip machine
- Don't need to enter every single machine as group member

You are going to install this equipment, for some company which has a voip system and some small network (let's say, 30 computers). We want that all machines have internet access.

Let's set up our QoS group:

Group ID: 1
LAN Out rate: 300 -> Internet Total download rate
WAN Out rate: 300 -> Internet Total upload rate

Now, the first thing to do is to put our voip machine in first place:

Group ID: 1 -> Member of QoS group ID 1
IP: 192.168.x.x -> Voip machine IP address
LAN Out rate: 64 -> 64 kbit guaranteed
WAN Out rate: 64 -> 64 kbit guaranteed

Next, instead of put every single machine inside the control list, we will put this rule:

Group ID: 1 -> Member of QoS group ID 1
IP: 0.0.0.0 -> 0.0.0.0= the entire network
LAN Out rate: 0
WAN Out rate: 0

Simple as that.

How dos it work?

- When there is no VOIP traffic, the entire network can reach 300 kbit internet connection. As soon as the voip system starts to operate, the QoS system will reserve 64 kbit for the voip.

But, if the boss machine wants to have 128 kbit guaranteed as well? Proceed as follow:

Group ID: 1
LAN Out rate: 300 -> Internet Total download rate
WAN Out rate: 300 -> Internet Total upload rate

Group ID: 1 -> Member of QoS group ID 1
IP: 192.168.x.x -> Voip machine IP address
LAN Out rate: 64 -> 64 kbit guaranteed
WAN Out rate: 64 -> 64 kbit guaranteed

Group ID: 1 -> Member of QoS group ID 1
IP: 192.168.x.x -> Boss ip address
LAN Out rate: 128 -> 128 kbit guaranteed
WAN Out rate: 128 -> 128 kbit guaranteed

Group ID: 1 -> Member of QoS group ID 1
IP: 0.0.0.0 -> 0.0.0.0= the entire network

LAN Out rate: 0
WAN Out rate: 0

=> TRAFFIC CONTROL VIA CONFIG FILE INSTEAD OF WEB INTERFACE

This version allow unlimited IP or MAC address traffic control, via /etc/cbu.conf file. Via WEB interface you can only control up to 40 entries. The file /etc/cbu.conf uses the same idea as via WEB interface. After you're done with file changes, you have to type the following commands in order, to save and activate the changes:

```
# save  
# /bin/cbu.sh  
# /bin/firewall.sh
```

NOTE: REMEMBER TO ACTIVATE TRAFFIC CONTROL VIA WEB INTERFACE.

=> NOTES ABOUT SSH ACCESS

This firmware version comes with SSH2 server. As default, we have the user "root" with password "root".

To change the root's password, proceed as follow:

- Access the equipment through SSH terminal (putty for example)
- type: "passwd"
- Type your new password and confirm
- Now, to permanet save the change, type: "save"

This version comes with SSH client program. You can use it to remotelly connect to another equipment.

=> FREEDOM TO CHANGE/EDIT PERSONAL SCRIPT VIA WEB

Since version 5.1a, it's possible to edit your personal script via WEB! The procedure is really simple:

Go to menu Management -> Edit Script File. You can change the way you want. After that, just press Save button. Now your script will be saved and executed!

=> FREEDOM TO CHANGE/EDIT/CREATE SCRIPTS VIA SSH TERMINAL

When connected via SSH, you can edit/create scripts inside /etc structure. To do it, there is a popular linux editor: "vi".

All files from /etc, will be permanently saved if you type "save". So, be carefull with your changes...

The main script file is /etc/init.sh, which is responsible for the entire system. You can create your own script inside /etc and call it from /etc/init.sh.

NOTE: DO NOT FORGET TO TYPE "save" AFTER ANY CHANGE TO PERMANENTLY SAVE IT INSIDE THE FLASH MEMORY! AGAIN, BE EXTRA CEREFULL WITH YOUR CHANGES!

=> HOW TO FIX MAC ADDRESS TO CERTAIN IP AND STATIC LEASE VIA DHCP (VIA SSH TERMINAL)

With just one file it's possible to lease static ip based on mac addr and to tie-up this pair mac/ip. To do it, you have to edit this file /etc/ethers like that:

```
# John
00:12:34:51:fd:ea 192.168.2.100
# Jhony
00:4f:23:fb:ce:3d 192.168.2.101
```

After that, save it. Now, type "save". To put it to work straightaway, type: "init.sh gw all"
With this file, the DHCP server will give IP ADDR based on MAC ADDR. Further more, the equipment will only respond for that IP ADDR with that MAC ADDR.

=> HOW TO FIX MAC ADDRESS TO CERTAIN IP AND STATIC LEASE VIA DHCP (VIA WEB INTERFACE)

It's simple, fast and easy to edit /etc/ethers file. To do it, just go to Management - Edit ethers file menu. Once you're done, press "save" button, to apply your changes.

=> HOW TO USE CROND

This firmware version comes with the popular job scheduler CROND. The file responsible for that is located at: /etc/crontabs/root. Use the following format:

```
minute hour day_of_month month day_of_week script_or_command
```

Ex: To schedule a ping command for every 5 minutes.

Edit the file and put the line as follow:

```
*/5 * * * * ping -c 5 192.168.2.40
```

Save the file. Now type: "save" and "init.sh gw all"

=> MESH SYSTEM WITH OLSRD SOFTWARE

This firmware version has OLSRD software, used to create MESH system (<http://olsr.org>). Config file is located at: /etc/olsrd.conf.

Basically, you have to config your wireless settings acting as CLIENT AD-HOC and run OLSRD daemon, via SSH.

If you need further details, please consult OLSR's home page.