

Reference Guide

Version 1.13

Website at <http://www.demarctech.com>

Downloads / Updates

- For firmware downloads and updated information, Please visit: <http://www.demarctech.com/> on the software downloads page

Frequently asked Questions (FAQ) & Support

- For a listing of Frequently Asked Questions, Please visit: <http://www.demarctech.com.com/>

General Overview

System Types

Demarc's RWV product line can be used for a variety of applications.

- All Modes (RWV-2/3/4XXX) act as a **Client unit**, which enables the end user to access the Internet connection from more than one machine with either standard or NAT IP addresses.
- All Models (RWV-2/3/4XXX) act as an AP (**Access Point**) unit, which allows wireless connections and routing on the ISP side of the Internet service.
- RWV Servers (RWV-4XXX) only acts as an IS (**Internet Server**) with the following services: DNS, Transparent caching-Proxy, Routing, NAT, DHCP, Firewall, and Bandwidth Control.
- All Models (RWV-2/3/4XXX) act as a **Router** with the following services: Routing, NAT, DHCP, Firewall, and Bandwidth Control.

Features

- Each interface can contain up to 255 IP addresses with the ability to enable, disable and add comments to each one
- One interface can be selected to be configured by DHCP.
- Bandwidth shaping based IP and/or Protocol with optional Auto Fallback.
- Firewall scripting interface provides the ability to set up and protect your network in no time
- Up to 255 static routes are supported, ability to enable, disable and add a comment to each route
- Full support for the 802.1d Spanning Tree Protocol
- Ability to set up large amounts of static and dynamic NAT rules
- Support for 250 simultaneous wireless station associations
- Signal Strength Meter, for easy client antenna alignment or signal level troubleshooting.
- Ability to monitor both noise level and connection rate for each link to the AP
- Ability to monitor each client's MAC address, and assign a name for easy tracking
- Monitor last used IP address, so you can see in an instant what IP your customer is using
- RX and TX data transfer statistics for both Ethernet and Radio interfaces
- Remote firmware Upgrade
- DHCP server with the ability to group, manage and assign IP's dynamically or statically
- DHCP Proxy to forward DHCP requests to a remote DHCP server
- SSH (v2) server is provided to allow for remote configuration of the server
- Remote Report Viewing via telnet ports of system specific information
- Proxy Server with the ability to do Web and FTP caching (Internet Server)
- Recursive DNS Server to help preserve valuable bandwidth (Internet Server)
- Eezee configuration
- "Captive Portal" web login hotspot
- RIP, OSPF and BGP4+ routing
- PPPoE, PPTP Tunneling protocols
- Radius server and authentication for PPPoE, PPTP and Hotspot authentication (Internet Server)

RWV Base Station - Router Setup Quick Start Guide

Step 1: **Logging in:** Using a SSH you will be provided with a login prompt. The default username is "**admin**" and the default password is "**1234**". You should change this as soon as possible (see section 7 for instructions).

```
login as: admin
Sent username "admin"
admin@192.168.1.1's password: 1234
```

Step 2: **Setting up the Ethernet cards:** Under the **Interfaces** menu choose **Ether1** then **IP Assignments** menu. Click the **Create** button to give the card an IP address. The IP you provide will be the address that the RWV will use to connect to the up-stream network. Continue by choosing **Ether2** as needed for local networks that will be connecting to the RWV through Ethernet ports. Under each interface click the **Create** button to give the card an IP address. The IP you provide will be the address that the machines on each of these local networks will use as their gateway address.

Step 3: **Setting up the Wireless cards:** Under the **Wireless** menu, select the wireless card you wish to setup, and then select **Config Current Card**. If this wireless card is to be an **Access Point** Set the ESSID you wish to use and select **Access Point** in the **Network Type** field. If this wireless card is **NOT** to be an Access Point Set the ESSID field to the ESSID of the Access Point that it will be connecting to and select **Infrastructure** in the **Network Type** field.

Step 4: **Continue setting up the Wireless cards:** Under the **Interfaces** menu choose the wireless interface wish to setup then **IP Assignments** menu. Click the **Create** button and provide the wireless card with the IP address and subnet mask. The IP you provide will be the address that the RWV on your wireless networks will use as their gateway address.

Step 5: **Set up routing:** Under the **Routing** menu, select **Static and Default Routes**. Click on the 0.0.0.0/0 route and click on **Edit**. Enter your gateway address and click on **Make Default Route**. Click on OK and close window. Also setup a static router for each IP subnet that was set for each interface.

Step 6: Select the **File** menu and **Save Change**. Select the **File** menu and **Activate Changes**

RWV Base Station - Bridge Setup Quick Start Guide

Step 1: **Logging in:** Using a SSH you will be provided with a login prompt. The default username is "**admin**" and the default password is "**1234**". You should change this as soon as possible (see section 7 for instructions).

```
login as: admin
Sent username "admin"
admin@192.168.1.1's password: 1234
```

Step 2: **Setting up the Ethernet cards:** Under the **Interfaces** menu choose **Ether1** then **IP Assignments** menu. If needed select the default IP 192.168.1.1 then click the **Edit** button to change the card the IP address. The IP you provide will be the address that the RWV will use to connect to the up-stream network. On the bottom of this screen change the **Ethernet Bridge Number** to **1**.

Step 3: **Setting up the Wireless cards:** Under the **Wireless** menu, select the wireless card you wish to setup, and then select **Config Current Card**. If this wireless card is to be an **Access Point** Set the ESSID you wish to use and select **Access Point** in the **Network Type** field. If this wireless card is **NOT** to be an Access Point Set the ESSID field to the ESSID of the Access Point that it will be connecting to and select **Infrastructure** in the **Network Type** field.

Step 4: **Continue setting up the Wireless cards:** Under the **Interfaces** menu choose the wireless interface wish to setup then **IP Assignments** menu. On the bottom of this screen change the **Ethernet Bridge Number** to **1**. *Note: in bridge mode only the Ethernet interface will have an IP not the wireless.*

Step 5: Select the **File** menu and **Save Change**. Select the **File** menu and **Activate Changes**

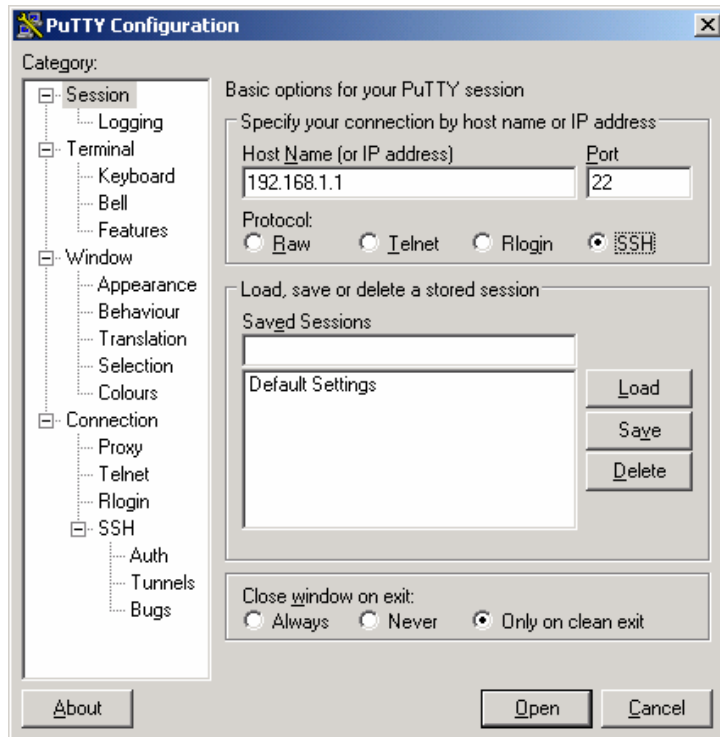
User Interface

First Login

The factory default IP for the system is 192.168.1.1. You can interface with the device by connecting to your computer via the Ethernet port. You will require a SSH client in order to access the user interface. PuTTY, a freeware SSH client, is available for download via a link on our tech support page (<http://www.demarctech.com>).



Execute the putty program. In the **Host Name (or IP address)** box, type in the default IP address (192.168.1.1). Make sure that the **SSH** radio button is active. **S**ave your session and then click the **O**pen button.



The following instructions for the User Interface are for both methods of connection. In order to make changes, you will need to login to the device using 'admin' as your username and '1234' as your password. (You will be able to change your password once you enter the configuration utility)

```
login as: admin
Sent username "admin"
admin@192.168.1.1's password:
```

Once the correct username and password are entered, the configuration screen will appear.

System Configuration

```
file wireless interfaces routing advanced hotspot services system

Demarc Technology Groups Reliakave OS - Station Router
[ kustom.ap1.com ]

System Information:
Ethernet Ports: 2
Wireless Ports: 1 wpci card, and 1 pcmcia socket
Server Uptime: 1 day, 19 hours and 57 minutes
Swap Memory: No drive available
System Memory: Total: 60MB, Used: 30MB, Free: 30MB, Total Free: 30MB
SSHv2 [ ACTIVE ] OSPFv2 [INACTIVE] IPv6 [INACTIVE]
BGPv4+ [INACTIVE] HotSpot [INACTIVE] DHCP Relay [INACTIVE]
DHCP Server [INACTIVE] PPTP Server [INACTIVE] PPPoE Server [INACTIVE]
SNMP Service [ ACTIVE ] Radius Server [INACTIVE] Ping Watchdog [INACTIVE]
Remote Report [ ACTIVE ] IP Accounting [INACTIVE] Remote Syslog [ ACTIVE ]


System Key:
TRGKB3-QKMNLJ-HF1BR6-HQIGS9

Wireless Devices:
Qual Signal Noise Rate Freq Mode Link Information
wpci1: ar5212 KUSTOM5 5825 ap-mode 0 associations (F1)
wlan1: prism 2.5 KUSTOM1 2412 ap-mode 0 associations (F2)
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device

Alt-X Exit CPU Load: 6.6% | Router Edition v1.13.3 (build 3993)
```

This is the main display. It provides a “heads-up” of the system’s current status including memory usage, CPU utilization, active services and network usage.

The top of the screen has several menu options that are used to configure and manage the system. You may navigate the menus using either your keyboard, or a mouse.

 If you are using an SSH program such as Putty or SecureCRT you can navigate the menu system using your mouse!

Several hot-keys are also available in the main screen and throughout the RWV’s interface:

- **F1-F10** will display a list of users currently associated with each Wireless interface on your system. For example, pressing F2 would display associated users on the second Wireless NIC.
- **F9** brings up the kernel message log. This displays low-level information about the system and is useful for debugging.
- **F10** will activate the **file** menu.

Using the keyboard

Please note, you may use a mouse to point, click, double click, and select text but you can also navigate through the system faster by using these shortcuts:

- Alt + [differently colored letter] will bring up the main menus
- Menu options can be selected by typing the red character.
 - The arrow keys can also be used to select the appropriate menu choice,

```
routing  advanced hotspot  services  system
1 ip accounting
2 802.1d bridging
3 pcmcia irq options
4 dns server list
5 connection table size
6 kernel message log (dmesg)
7 scripts (cbq, firewall, nat, ...)
1 class based queuing (cbq / bw management)
2 advanced firewall and port forwarding
3 nat and static nat (1:1 ip mapping)
4 activate script changes
3 ap-mode 0 associations
```

Pressing **ALT-A 7 2** will bring up the advanced firewall and port forwarding screen

- The 'Esc' key will close the active window and allow you to back out of menu choices
- The 'Enter' key will choose the currently highlighted selection
- When selecting text, 'Ctrl+K+B' will begin the text block. You may use the arrow keys to move the selection area to the desired size.
- 'Ctrl+C' is the command for Copy, 'Ctrl+X' is the command for Cut, 'Ctrl+V' is the command for Paste, and 'Ctrl+Y' is the command for delete line.
- When text is selected, the 'Del' key will delete the selected text.
- Because the user interface is text based, when selecting text with a mouse, you will not see the selection until *after* the mouse button is let up.
- Whenever you make changes to Ethernet card setting, Wireless card setting, or any other settings (routing, DHCP, NAT, DNS, etc.) you need to *save and activate your changes* before the services or settings will take effect.

A note about making, saving and activating changes.

Any changes you make will not be made, or saved, immediately. You must use the **Activate Changes** command located in the File Menu for changes to come into effect.

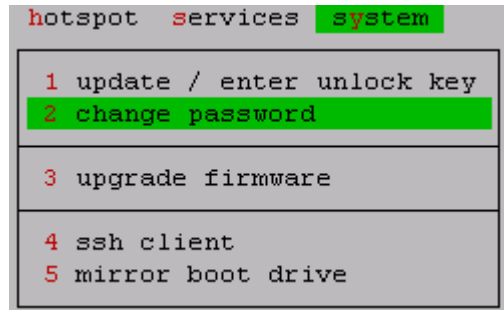
Likewise, any changes you make will not be saved. If the system is rebooted, the changes will be lost. You must **Save Changes** for your new settings to take effect the next time the system is rebooted.

All of these functions are located under the File Menu:

File Menu	Action
Save Changes	This menu choice will save any changes that you have made. It will NOT activate the changes. This is handy for deferred activation during a maintenance window.
Activate Changes	This menu choice saves and activates any changes that you have made.
Reboot Machine	This menu choice will ask if you wish to save any changes and then will reboot the system.
Exit	This menu choice will save any changes and then quit. The changes are NOT activated on exiting.

Changing the Admin Password

The admin password *must* be changed when you have logged in. To do this, select the **System menu** and choose **Change Password**.



The software will ask for you to confirm the **Change Password** choice. Once you confirm your choice, you will be led through the steps of changing your password.

Please enter the old password:

Enter new password:

Again to verify:

Passwords changed. press enter to continue:

Please be sure to save your changes under **File** menu, **Save Changes**.



Failing to change the admin password from the default of 1234 is a sure way of having someone tamper with your system! Change it!

Updating RWV's

- New versions of the firmware are released on a fairly regular basis. To update the software, you will need a copy of `rwv-util-xx.exe` available from <http://www.demarctech.com/> on the software downloads page

Step 1: Download the latest .bin firmware update release and `rwv-util-xx.exe` from our website.

Step 2: Run `rwv-util-xx.exe` command, example:

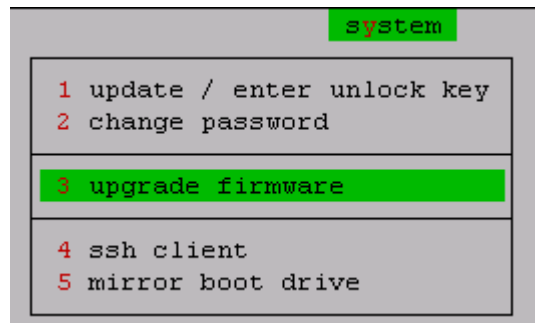
- `rwv-util-19.exe 192.168.1.1 MyPass -f dtrwv3xxx-1.13.3.bin`

Step 3: The firmware will upload to the RWV system. When the new firmware has been uploaded you will see a message similar to, "Please select the 'Upgrade Firmware' option on the server to finish."

Step 5: Login to the RWV system and select **Upgrade Firmware** from the System menu. You will be asked to confirm your decision to upgrade the existing software.

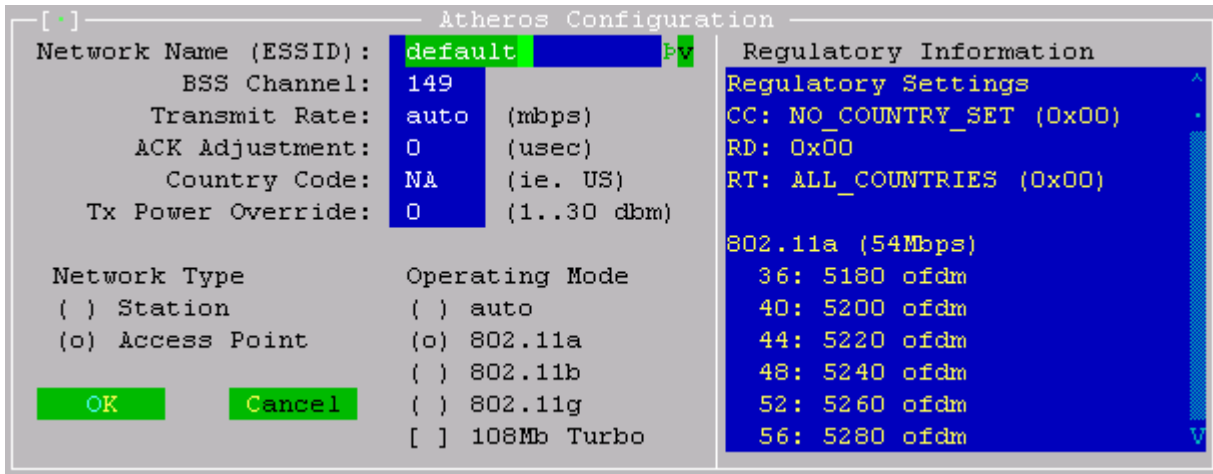
Step 6: The software will perform a CRC check and automatically update the firmware.

Step 7: Reboot the machine for the new firmware to take effect.



Wireless Network Configuration

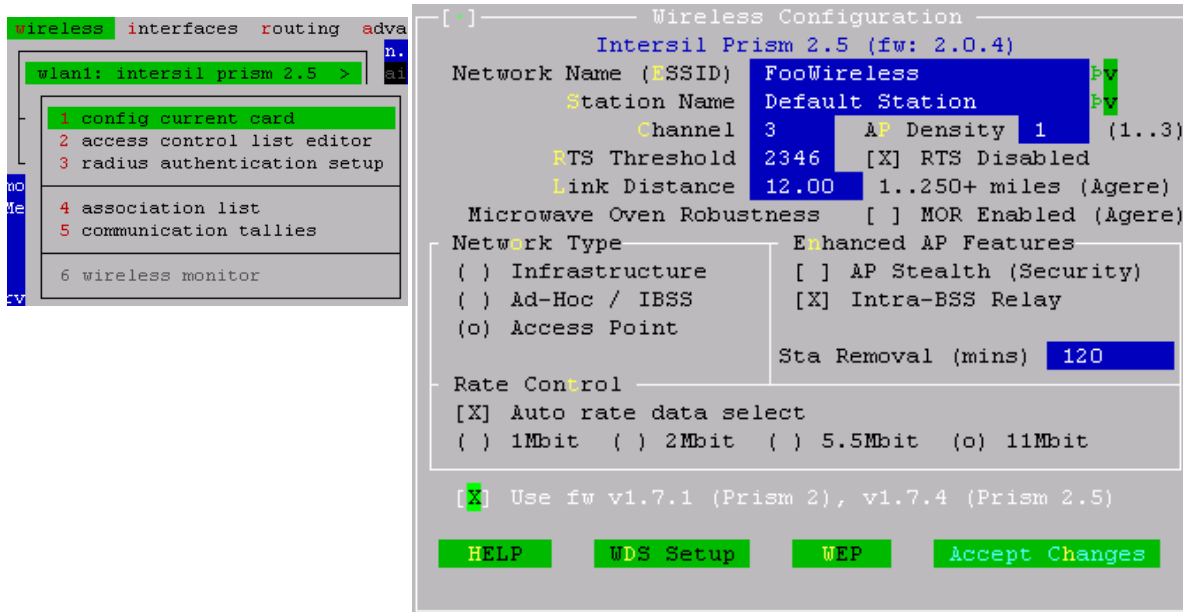
Atheros 802.11b/g/a Wireless NIC



ESSID	The name of the Wireless Network.
BSS Channel	The channel or frequency for this network card to operate on. Refer to the Regulatory Information window for a list of channel numbers and their respective operating modes, or refer to the 802.11 Channel List .
Transmit Rate	The speed (in Mbps) this card should operate at. Specify auto to have the card select the best rate based on connection quality.
ACK Adjustment	<p>The values above represent the hardware defaults for the cards we have. When you wish to adjust for a longer link, increase the numbers beyond the values shown. Setting the value back to 0 will use the card's default.</p> <p>Atheros ar5212 cards - default ACK values:</p> <p>802.11b mode: 450 802.11a mode: 180 802.11g mode: 180</p> <p>Atheros ar5211 cards - default ACK values:</p> <p>802.11a mode: 180 802.11b mode: 230</p> <p>For example, if you wish to extend a 5.8 link, try using a value of 400 or more as a starting point.</p> <p>All values are 1/4 of a microsecond (usec). 100usec equals an ACK value of 400</p>
Country Code	Specifies the regulatory region that the system is operating in. Please refer to the Regulatory Country Codes table for a list of supported regions.
TX Power Override	Override the card's default power output. Valid values are 1 to 30 dBm. <i>Note: Max values will only be what the radio is capable of and not more.</i>
Network Type	Sets the card to act as either an Access Point, or a Station which connects to an access point. Ad-Hoc is presently not supported.
Operating Mode	This determines what protocols the card will operate in. By default, <i>auto</i> mode is enabled.

Setting up an Access Point with the Prism 2.5 Radio

From the **Wireless** menu click the *wlan* device you want to act as the Access Point and select the **1 config current card** menu option.



ESSID	The name of your Wireless Network that clients will connect to.
Station Name	A descriptive name of this device, suggested examples include "lobby AP", "internet gateway", etc.
RTS Threshold	For advanced users only! Adjusts the RTS fragmentation threshold. Click on the HELP button for more information on what this does.
Network Type	Specifies the mode this Access Point will operate in. Select Access Point to have this radio act as a master repeater in the Wireless Network. Select Ad-Hoc/IBSS if you want this radio to act in a Peer to Peer network that does not use an Access Point.
AP Stealth	Turns off beacons that announce the presence of your network. This function can help deter some war drivers but should <u>not</u> be solely relied upon for security.
InterBSS Relay	Allows associated wireless clients to communicate between each other.
Rate Control	Specifies the maximum speed that your clients can connect to this access point at.
Use fw v1.71 and v1.74	(Intersil Prism cards only!) Some cards may exhibit problems acting as an access point. If you have difficulties using a Prism based radio as an AP, check this box.

Setting up as a Client (CPE) device

When configuring RWV on a client or CPE device you should only need to change the following settings:

1. The **SSID** should be set to the same name as the *Access Point* you are connecting to.
2. The **Network Type** should be set to *Infrastructure* (or *Station*, if you are using an Atheros device).

If you are connecting to an *Ad-Hoc* network, set the **Network Type** to *Ad-Hoc/IBSS*. Please note that *Ad-Hoc* is not supported with Atheros.

IP Address Configuration

You will need to assign an IP address to each Network interface (Ethernet and Wireless) in your RWV system when setup as a router. Your Internet Service Provider may have provided a range of addresses for you to use. If you do not have IP addresses from your ISP, you can also use addresses out of the *Private Internet Address Space*:

10.0.0.0 - 10.255.255.255	(10/8 prefix)
172.16.0.0 - 172.31.255.255	(172.16/12 prefix)
192.168.0.0 - 192.168.255.255	(192.168/16 prefix)

By default, the first Ethernet adapter in your RWV system will be configured to use the following settings:

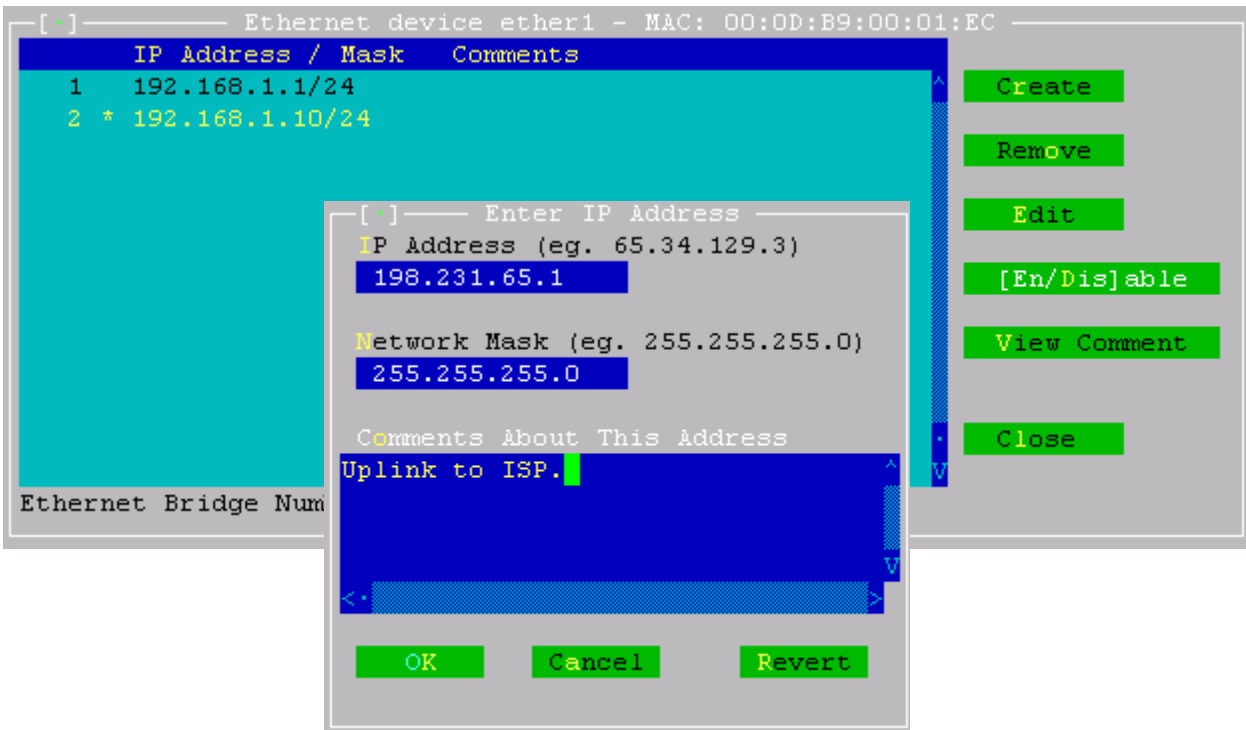
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Default Gateway: none

IP Address settings are configured from the **interfaces** main menu. From the interfaces menu, select the network interface to configure, and then choose the **ip assignments** option.

A list of IP Addresses on the Network Interface will be displayed. From here, you may **Create**, **Remove**, **Edit** or **Enable/Disable** an address.

- Addresses listed with a * beside them are Disabled. This can occur for a variety of reasons:
 - The Address is already in use by another system on the network.
 - The address may be configured on another interface in the same RWV system.
 - You manually disabled the address.

When editing or adding an address, a dialog similar to the one below will be shown. Enter the IP Address, the Network Mask and an optional comment.



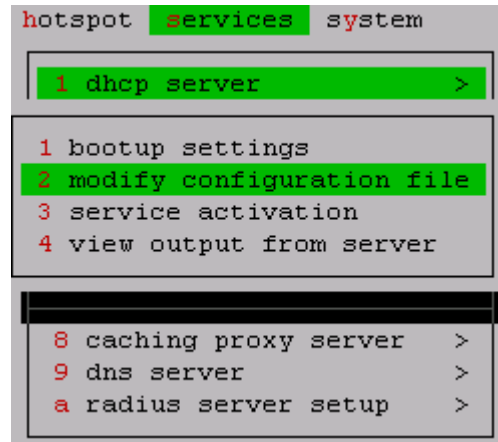
Assigning IP addresses to your users

Using DHCP

DHCP (Dynamic Host Configuration Protocol) is a system that allows client systems to automatically configure themselves on a TCP/IP network.

The DHCP server is configured from the **services -> dhcp -> modify configuration file** menu item.

The DHCP Server configuration is a text file. A comprehensive list of configuration commands is available from <http://www.demarctech.com/XXXXX>



1. Set your domain-name using the option domain-name command.
2. Set your DNS servers using the option domain-name-servers command.
3. Define the subnet's you wish to service with DHCP
4. Configure the DHCP parameters to be handed out to clients.

Example:

```
option domain-name "domain.com";
option domain-name-servers 192.168.1.254, 192.168.1.253;

subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.10 10.0.0.100;
    option routers 10.0.0.1;
};
```

This configuration will automatically configure client computers to use the following parameters:

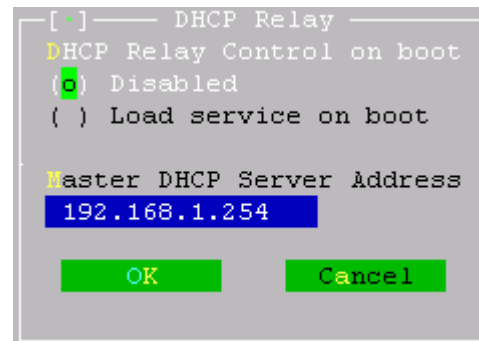
- o Domain Name: domain.com
- o Name Servers: 192.168.1.254 and 192.168.1.253
- o An IP address from 10.0.0.10 through 10.0.0.100
- o A default router address of 10.0.0.1

Statically assigning IP addresses using DHCP

Some customers may need a static IP address (for example: they may run an Email or Web server). You can do so by adding a configuration block similar to:

```
host customers.name.foowireless.net {
# Your customer's MAC address
    hardware ethernet 00:4F:4E:0D:12:FF;
# IP address to assign - not part of
dynamic IP group above
    fixed-address 10.0.0.200;
}
```

to the dhcp server's configuration file.



Configuring a DHCP relay service

The DHCP relay service is used to forward DHCP requests from your clients to a DHCP server somewhere else. For example, you may have a many access points that provide connectivity to your clients, but you run a single central DHCP server.

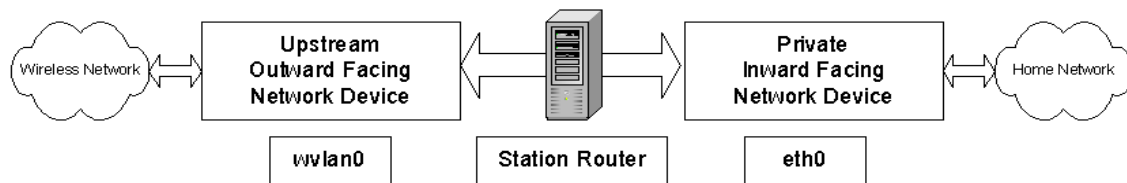
To configure the DHCP relay server, select "configure service" from the **dhcp relay server** menu under **services**.

Specify "Load service on boot" to have the service start at bootup time, and enter in the IP address of your DHCP server.

NAT (IP Masquerading)

All hosts on the Internet must use "internet routable" IP addresses. This let's other hosts on the 'net send data back to you.

IP Masquerading provides a mechanism for relaying a packet from your private network out to the Internet by encapsulating it in a packet with a valid public IP number. Masquerading stuffs your local workstation's real (private) IP address inside the packet, along with the rest of the packet's data, and then puts a public IP address on the outside of the packet. Hence your workstation's packet is said to "masquerade" as a packet with a valid IP address.



When the RWV is being used as a CPE (Customer Premise Equipment) with the wireless card being the connection to the Internet via a RWV Base Station Server / Base Station Router or other AP device.

The eth0 device is "inward facing", to the home network, and wlan0 device is "outward facing", to the Internet. These two devices can be configured so that packets are permitted to flow, or be "forwarded", from one device to the other. However, you don't want raw packets to be forwarded between the two network devices without intervention.

We want to process the packets as they pass through the router by using software that will masquerade our internal packets so they can travel to the Internet and then inspect the return packets and then relaying the packets to the correct PC on the home network.

In addition you may want to inspect incoming packets for packets that shouldn't be coming in. That is, you may want to establish a set of rules under Advanced Firewall and Port Filtering that define which packets to let in, and which not to. You want to protect your internal network by filtering packets through a set of firewall / filtering rules.

Configuring IP Masquerading and Forwarding

The assumption being made from this point on is that you have your two network devices working properly. Your inward-facing NIC (e.g., eth0) is connected to your internal LAN and you can ping the Station Router from all the workstations on your home network. Your outward-facing NIC (e.g. wlan0) is connected to your via a RWV Base Station Server / Base Station Router or other AP device and you can ping the Station Router from a location external to your local network.

In order to route, or forward, network packets from your inward-facing device to your outward-facing device, and vice versa, you must modify the configuration files under the Advances section in both the Nat and Static Nat and Advanced Firewall and Port Filtering sections following instructions included in those files.

Configuring the Caching Proxy Server (Server Only)

The Proxy Caching manages web requests from your clients and keeps a local copy of web pages and their content. The cache can reduce the amount of bandwidth to the Internet by serving your clients a local copy of a web page instead of having to retrieve it on each request.

A comprehensive list of configuration settings for Proxy Caching system is available from: <http://www.demarctech.com/XXXXX>

Preparing a hard drive for Proxy and Radius use

You must have a hard drive installed into the system running the Proxy and/or Radius, the RWV Server can not store this information on the flash device.

To prepare a drive for use, select the “prepare a hdd for proxy and radius use” from the **services** -> **caching proxy server** menu.

A new screen will appear displaying detected hard drives in your system:

```
----- 1 Disk found -----
1) IDE DISK (/dev/hdc) size 406MB, blksize 512
0) Exit utility, do not touch any hard disks.
```

```
-----
Which disk do you wish to use for a caching
proxy and radius? [0 - 1]:
```

Select the disk and answer the following question carefully:

Are you sure you wish to repartition the selected hard disk? [y/n]:

Answering ‘y’ will setup the disk for RWV Servers’s use. This will also delete any existing data on the drive.

You will be asked if you want to create a SWAP partition. If you plan on running a heavily loaded server without much memory, answer “Y”, otherwise answer “N”.

Finally, answer “y” to the following question:

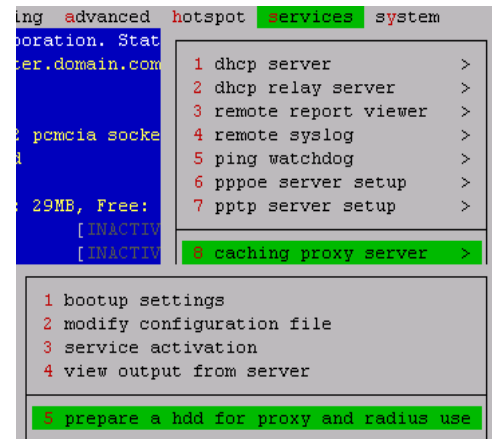
```
Ready to partition hard disk, do you wish to continue? [y/n]:
```

The RWV Server will start formatting the drive, you should see message similar to:

```
Partitioning disk...
Formatting disk...

Building the proxy cache structures...
Saving your new configuration...

Press any key to continue:
```



User authentication through Radius

Radius is an authentication protocol used by many network devices.

RWV Server includes a Radius and simple user management interface for use with PPPoE, PPTP and the system. You will need to prepare a hard drive for use by Radius and the Proxy server first. See the chapter on preparing a [hard drive for proxy/radius use](#).

```
1 bootup settings
2 users database (usernames, passwords, cbq settings, etc)
3 clients database (list of allowed NAS clients and their secrets)

4 service activation
5 prepare a hdd for proxy and radius use
```

- The **bootup settings** menu specifies whether the Radius server should be started on boot-up. You probably want to enable this.
- The **service activation** menu allows you to Stop, Start and Restart the Radius server immediately. You will need to restart the radius server for changes to the user or client database to come into effect.

The users database is a plain text file which stores user entries in the following format:

```
# fullname: John Smith
jsmith    Auth-Type := Local, User-Password == "moocow"
          DTG-PPPoE-CBQ-RX = 128000,
          DTG-PPPoE-CBQ-TX = 128000,
          Session-Timeout = 86000,
          Idle-Timeout = 900
```

The username is specified in the first column, while the rest of the user attributes are spaced away from the beginning of the line. These are known as *radius* attributes.

This file also contains the line:

```
##### ENTRIES BELOW THIS LINE ARE MAINTAINED BY USER INTERFACE #####
```

All entries below this line are modified by the web based user interface. You should not adjust these entries unless you are confident of what you are doing.

Configuring the Radius server to service other servers.

Other access points on your network can also use the radius server. Each Radius client (not end-user, but each access point) must be configured with a *secret*. The secret guarantees that only authorized access points can communicate with the radius server.

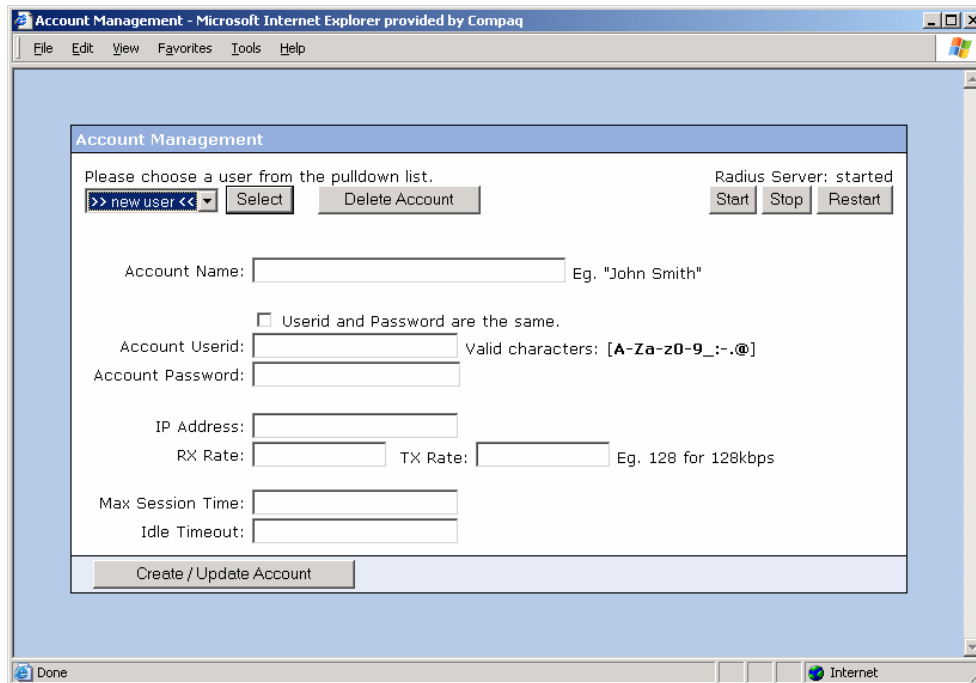
The format of the clients file is:

Client Name	Secret Key
#-----	-----
127.0.0.1	MySecret
#192.168.1.254	SampleEntry

Managing users through the built-in web interface

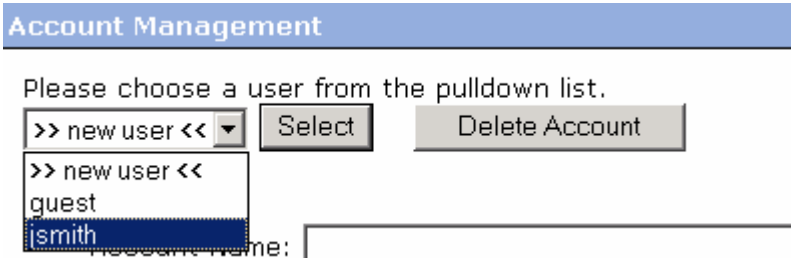
Before you can use the web interface, you must give yourself access to port 10000 on the RWV Server. See the [advanced firewall](#) chapter for more information on how to adjust the firewall.

From your web browser, enter go to <http://yourap.domain.com:10000/> (where yourap.domain.com is either the IP address or hostname of the RWV device). Login as admin with your password.



- The Account Name is the user's full name.
- The Account Userid is the username the user will use to login to the hotspot, PPTP or PPPoE.
 - 💡 You can specify a MAC address in the User ID field, just set the password to "" and they will be automatically logged into the hotspot using the restrictions you specify here!
- The IP Address is the address the user will be assigned, leave it blank if you want to assign the user a DHCP address.
- The RX and TX rate is the speed at which the user will be able to download and upload. This is specified in Kbps.
- The Maximum session time (in seconds) restricts the amount of time the user can stay logged in per session. The Idle timeout specifies when the user should be logged out if they have not done anything.

To modify or delete an existing user, just select the username from the top left drop down box, and click either "Select" or "Delete Account".



IP Accounting

RWV's can keep track of the number of Bytes and Packets transmitted and received for hosts on your network. IP Accounting will present you with a summary based on source and destination IP address that can be retrieved using an HTTP client or a custom tool that you have written yourself.

To configure IP Accounting, select the **ip accounting** option from the **advanced** menu.

```
[*] IP Accounting
[X] Enable IP Collections      OK      Cancel
[ ] Format for easy reading
Collection Mode: (o) Both ( ) Forward only ( ) Local only
TCP Port to collect current IPs: 800 [X] Mimic HTTP
TCP Port to collect previous IPs: 801 [X] Mimic HTTP

Limit to this number of IPs between collection periods to
help protect against possible DoS IP flood attacks.
IP Limit: 20000
```

- Check off Enable IP Collections to enable accounting.
- Check off “Format for easy reading” to display the records in a human readable format.
- Set collection mode to “Both” if you want to account for all traffic, “Forward Only” to display accounting for packets that are routed through your system or “Local Only” for traffic within your network.
- The “TCP port to collect current IP’s” is the TCP port number that RWV will display current accounting activity on.
- The “TCP port to collect previous IP’s” is the TCP port that RWV will display older accounting data on.
- The “Mimic HTTP” option has RWV act as a web server. Enabling this option allows you to view the summary using a web browser, or a command line tool such as “curl” which can be used to integrate RWV’s accounting into your existing system.

Here is an example of RWV’s IP Accounting output:

SOURCE DST	DESTINATION	BYTES	PACKETS	PPPOE-SRC	PPPOE-
204.50.0.178	24.82.83.183	81110	228	*	*
24.82.83.183	204.50.0.178	10755	240	*	*
204.49.171.17	204.50.0.178	188	3	*	*
204.50.0.178	204.49.171.17	292	4	*	*
204.49.171.17	192.168.2.199	92	1	*	*
204.49.76.203	204.50.0.178	236	4	*	*
204.50.0.178	204.49.76.203	252	3	*	*
204.49.76.203	192.168.2.199	92	1	*	*
204.50.0.178	204.50.0.178	800	5	*	*

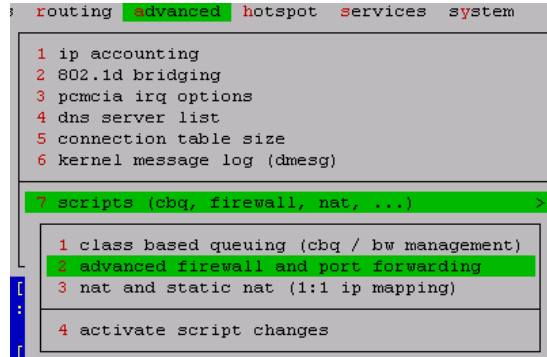
Firewall and port forwarding

The **advanced firewall and port forwarding** section of the **advanced -> scripts** menu allows you restrict access to certain network services and forward tcp and udp ports across firewalls and nat systems.

The firewall and port forwarding configuration is a text file consisting of one command per line. Comments can be added after the '#' sign.

The firewall can act on packets based on the following criteria:

- Source IP address
- Destination IP address
- Source TCP or UDP port number
- Destination TCP or UDP port number
- Whether the packet is coming "in" or "out"
- Whether the packet is traversing a specific network interface.



Allowing

By default the RWV is configured to allow traffic from anywhere to anywhere with a few exceptions. You may find it necessary to restrict all traffic with only a few exceptions to one of your sub-networks such as a commercial VPN customer or a sensitive accounting network.

The allow command is used to explicitly allow traffic through. Some of the RWV's built in services such as IP Accounting are configured to deny traffic. If you wanted to allow your accounting server, 192.168.1.3 to collect statistics you could add the line:

```
allow tcp from 192.168.1.3 to any 800 in
```

Denying

This will specifically deny a certain type of traffic. A popular (and present in the default installation of the RWV) rule is to deny all TCP and UDP traffic destined ports 135 coming in from the Internet:

```
deny tcp from any to any 135 in via $net # RPC port, used by many worms  
deny udp from any to any 135 in via $net # RPC port, used by many worms
```

Another common rule is dealing with a person on the Internet who is causing problems for one of your clients.

```
deny tcp from 12.129.23.16 to 192.168.2.154 in via $net
```

Logging

Firewall logging can be done to a remote syslog server using the 'log' command.

Example:

```
log tcp from any to 192.168.3.1/24 31337
```

Would log all TCP packets going to the 192.168.3.1 network destined for port 31337.

Forwarding

The **forward** command can be used to redirect traffic to another system. This could be used to redirect clients to a caching proxy server to reduce bandwidth on your Internet feed, or to have a service available to the Internet on a different port number not attached to the server itself.

Variables

The “not” (pronounced “not”, not “exclamation mark”) boolean operator can be used in conjunction with variables to setup flexible firewall and forwarding rules.

For example, the RWV is preconfigured to allow access from 127.0.0.1 (the system's local address) to the services using ports 791-801.

```
admin_ip = "127.0.0.1" # ie. 64.124.65.19 or 64.124.65.0/24 for the entire
                    # class C

ldeny tcp from ! $admin_ip to any 791 in      # CBQ Report
ldeny tcp from ! $admin_ip to any 792 in      # Firewall and NAT Report
ldeny tcp from ! $admin_ip to any 793 in      # W/LAN Device statistics
ldeny tcp from ! $admin_ip to any 794 in      # System ARP Table
ldeny tcp from ! $admin_ip to any 795 in      # Active Routing Table
ldeny tcp from ! $admin_ip to any 800 in      # IP Accounting collection
ldeny tcp from ! $admin_ip to any 801 in      # Results from previous IP
                                                # Accounting
ldeny tcp from ! $admin_ip to any 10000 in    # Web based user management
```

Instead of changing each and every one of these lines to give access to your account system you can simply change \$admin_ip to the IP address of the server.

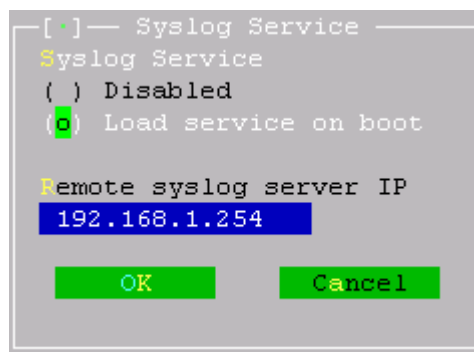
Remote logging

The RWV supports remote logging to syslog hosts. *syslog* is a Unix and Unix flavoured logging daemon that comes with most variations of Unix including Linux and FreeBSD.

To configure the RWV's syslog relay, go into the **services** menu -> remote syslog and select “configure service”.

Select “Load service on boot” so that logging will continue after you reboot the system.

Enter the IP address of the remote syslog server.



Configuring syslogd

Most Unix variants including Linux and FreeBSD ship with ‘syslogd’, the system logging daemon.

You may wish to keep the RWV's logs separately from the rest of your main logs. Most syslogd's can be configured to log messages from specific hosts.

Please consult the syslog.conf man page that ships with your operating system.



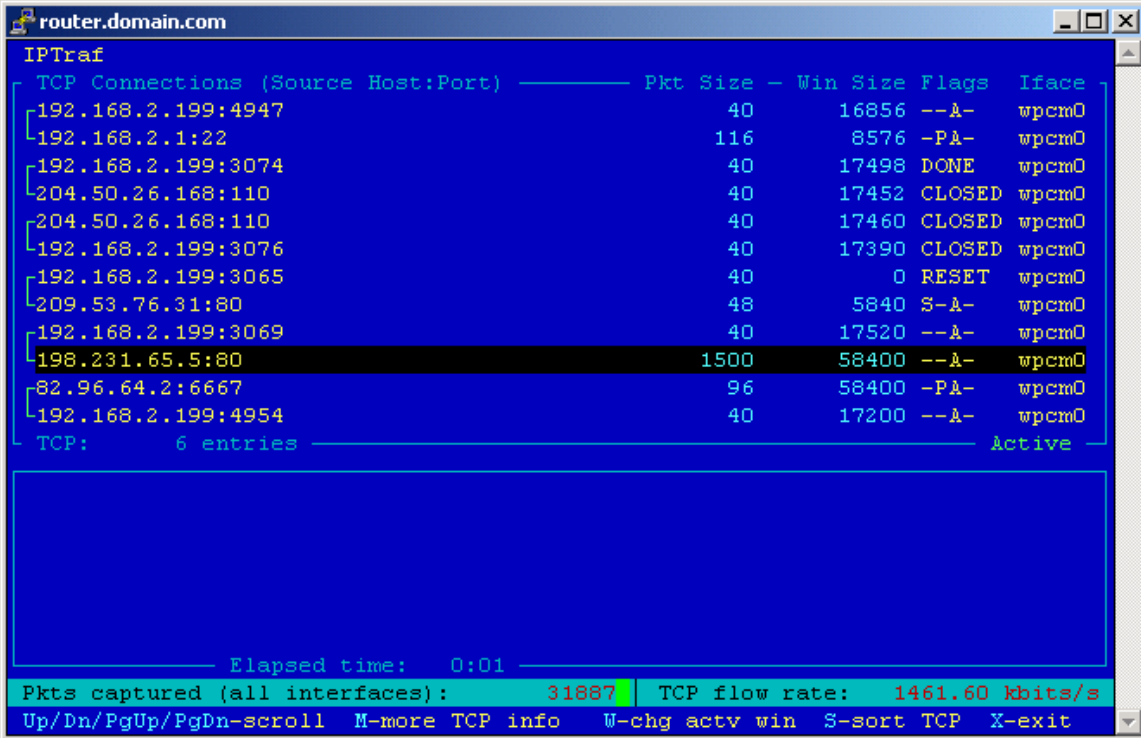
A free syslog service for Windows is also available from <http://www.winsyslog.com/en/>

Monitoring traffic

The RWV's has several monitoring tools you can use to view the current activity over any network interface in the system.

Traffic Monitor

The traffic monitor displays current TCP and UDP sessions on the particular interface.



The screenshot shows a terminal window titled "router.domain.com" running the "IPTraf" utility. The window displays a list of TCP connections with columns for Source Host:Port, Pkt Size, Win Size, Flags, and Iface. The connection between 192.168.2.199 and 192.168.65.5 is highlighted in yellow. At the bottom, a status bar shows "Pkts captured (all interfaces): 31887" and "TCP flow rate: 1461.60 kbits/s".

TCP Connections (Source Host:Port)	Pkt Size	Win Size	Flags	Iface
192.168.2.199:4947	40	16856	--A-	wpcm0
192.168.2.1:22	116	8576	-PA-	wpcm0
192.168.2.199:3074	40	17498	DONE	wpcm0
204.50.26.168:110	40	17452	CLOSED	wpcm0
204.50.26.168:110	40	17460	CLOSED	wpcm0
192.168.2.199:3076	40	17390	CLOSED	wpcm0
192.168.2.199:3065	40	0	RESET	wpcm0
209.53.76.31:80	48	5840	S-A-	wpcm0
192.168.2.199:3069	40	17520	--A-	wpcm0
192.168.2.199:4954	40	17200	--A-	wpcm0
198.231.65.5:80	1500	58400	--A-	wpcm0
82.96.64.2:6667	96	58400	-PA-	wpcm0

TCP: 6 entries Active

Elapsed time: 0:01

Pkts captured (all interfaces): 31887 TCP flow rate: 1461.60 kbits/s

Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit

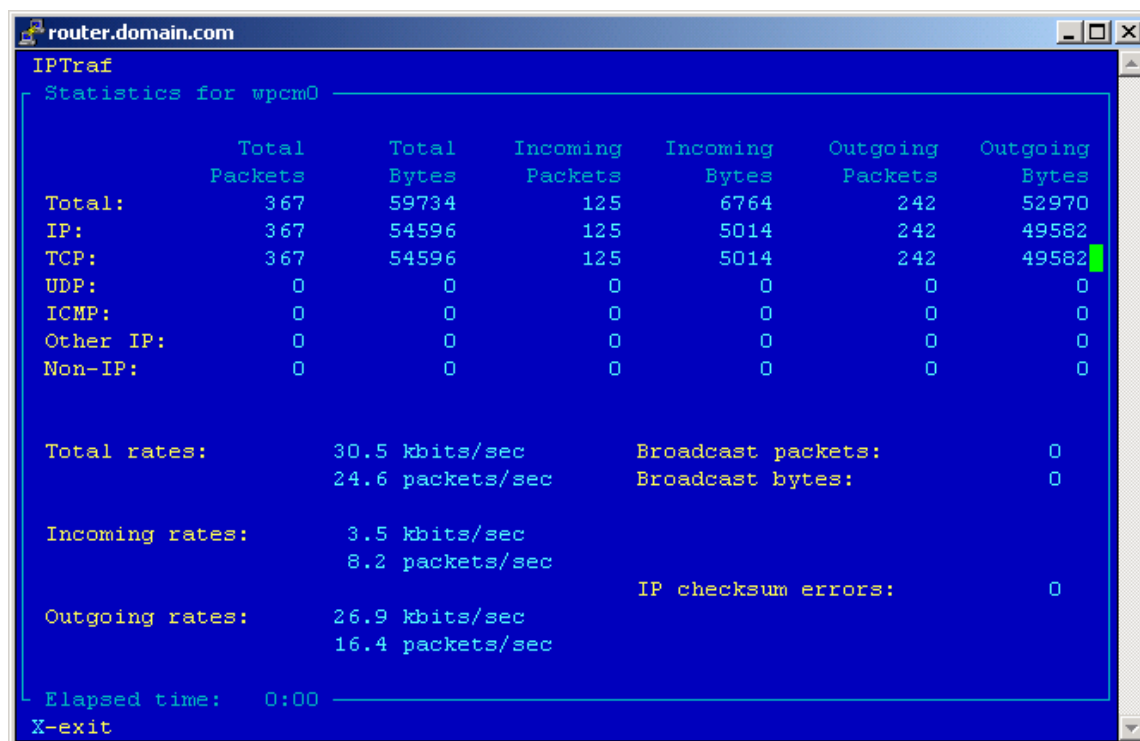
While in this screen, you can:

- Press **W** to toggle between Packet / Byte count and current packet size and window size.
- Press **S** to sort by Packet and Byte count.

This is particularly useful for identifying which users are placing an extra load on your network. In the picture above you see that the flow rate is 1461 kbit/s, a little under 1.5Mbps. You see a connection between 192.168.2.199 and 192.168.65.5 with a constant packet size of 1500 and a window size of 58400 indicating that this client is using a fair bit of network bandwidth.

Traffic Statistics

The traffic statistics screen gives you an overall view of what protocols, packet rates and throughput are going across a particular interface.



```
router.domain.com
IPTraf
- Statistics for wpcm0 -

```

	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
Total:	367	59734	125	6764	242	52970
IP:	367	54596	125	5014	242	49582
TCP:	367	54596	125	5014	242	49582
UDP:	0	0	0	0	0	0
ICMP:	0	0	0	0	0	0
Other IP:	0	0	0	0	0	0
Non-IP:	0	0	0	0	0	0

Total rates:	30.5 kbits/sec	Broadcast packets:	0
	24.6 packets/sec	Broadcast bytes:	0

Incoming rates:	3.5 kbits/sec		
	8.2 packets/sec		

Outgoing rates:	26.9 kbits/sec	IP checksum errors:	0
	16.4 packets/sec		

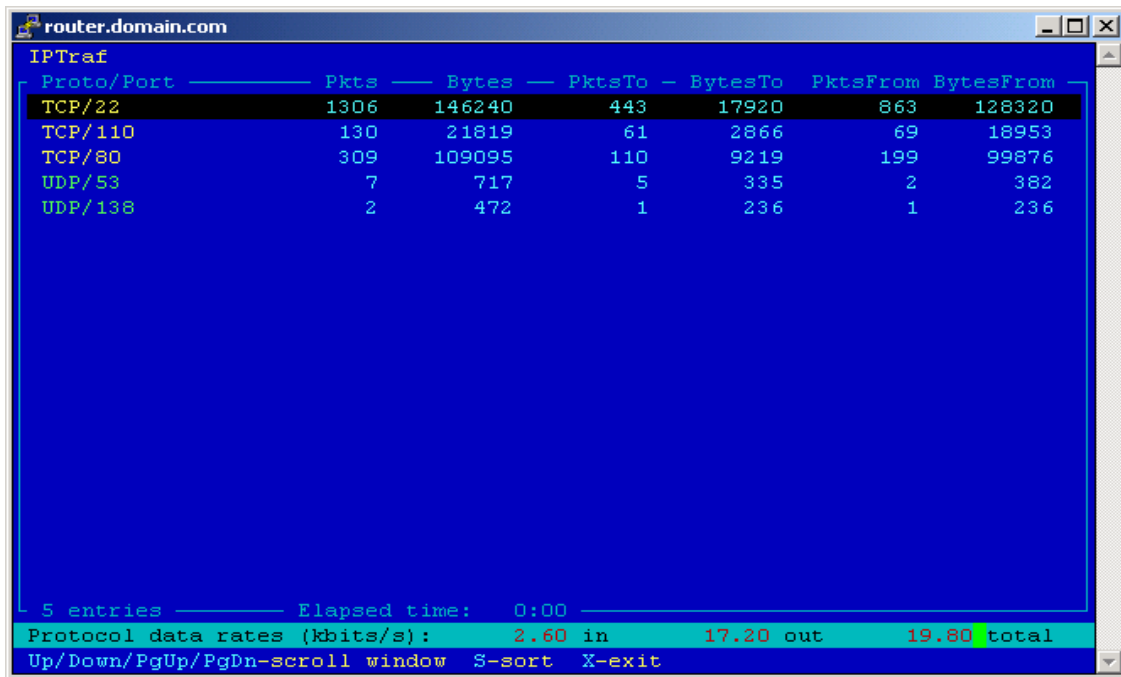

```
- Elapsed time: 0:00 -
X-exit
```

udp/tcp monitor

The UDP/TCP Monitor displays a packet and byte count based on TCP and UDP port numbers. You can sort the display by one of:

- Port Number
- Total Packets
- Total Bytes
- Packets to, or packets coming into the interface.
- Bytes to, or bytes coming into the interface
- Packets from, or packets sent from the interface
- Bytes from, or bytes sent from the interface

The protocol display is particularly useful in diagnosing network problems that may be caused by excessive use of a particular protocol, such as Kazza or another Peer to Peer application.



The screenshot shows a window titled "router.domain.com" with a blue background. The main content is a table of network traffic statistics. At the bottom, there is a summary line for protocol data rates and a control bar with instructions.

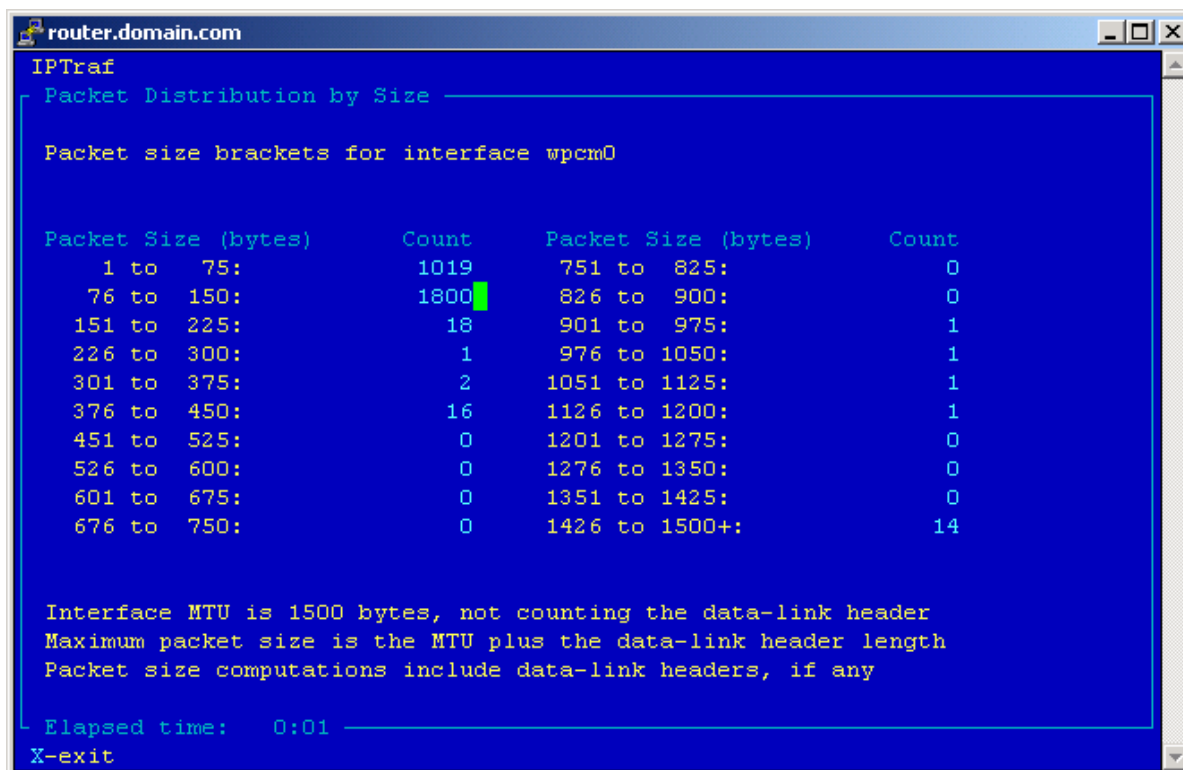
Proto/Port	Pkts	Bytes	PktsTo	BytesTo	PktsFrom	BytesFrom
TCP/22	1306	146240	443	17920	863	128320
TCP/110	130	21819	61	2866	69	18953
TCP/80	309	109095	110	9219	199	99876
UDP/53	7	717	5	335	2	382
UDP/138	2	472	1	236	1	236

5 entries Elapsed time: 0:00
Protocol data rates (kbits/s): 2.60 in 17.20 out 19.80 total
Up/Down/PgUp/PgDn-scroll window S-sort X-exit

Packet Size Counts

This allows you to gauge the use of your system. Generally lots of small packets will result in lower system throughput. The radios have a specification called packets per second and it does not matter whether the packet is small or the maximum size. Therefore a system that is passing predominately small packets will pass less traffic than a system with large packets.

The packet size monitor displays counts based on size of packets traveling through the interface.



```
router.domain.com
IPTraf
Packet Distribution by Size
Packet size brackets for interface wpcm0

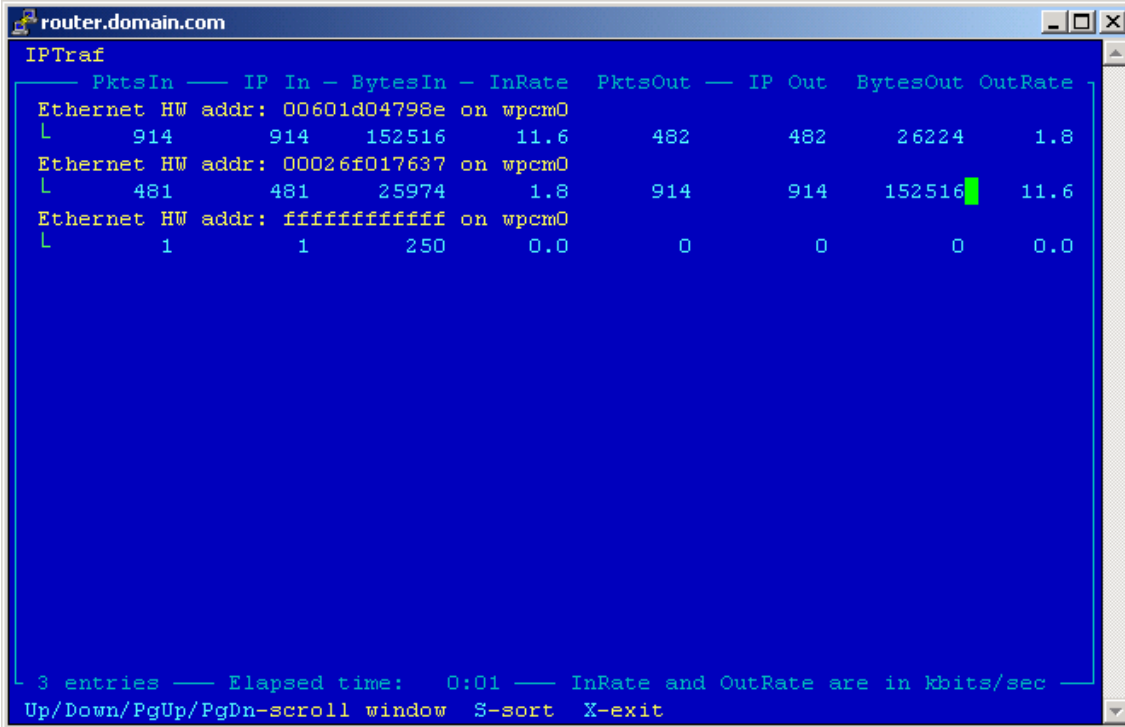
Packet Size (bytes)      Count      Packet Size (bytes)      Count
  1 to   75:             1019      751 to  825:              0
 76 to  150:             1800      826 to  900:              0
151 to  225:              18        901 to  975:              1
226 to  300:               1        976 to 1050:              1
301 to  375:               2       1051 to 1125:              1
376 to  450:              16       1126 to 1200:              1
451 to  525:               0       1201 to 1275:              0
526 to  600:               0       1276 to 1350:              0
601 to  675:               0       1351 to 1425:              0
676 to  750:               0       1426 to 1500+:             14

Interface MTU is 1500 bytes, not counting the data-link header
Maximum packet size is the MTU plus the data-link header length
Packet size computations include data-link headers, if any

Elapsed time:   0:01
X-exit
```

Lan Station monitoring

The Lan Station monitor displays Packet, IP packet, and Byte counts To and From each station on the local area network. Statistics are aggregated to each user's MAC address, not IP address.



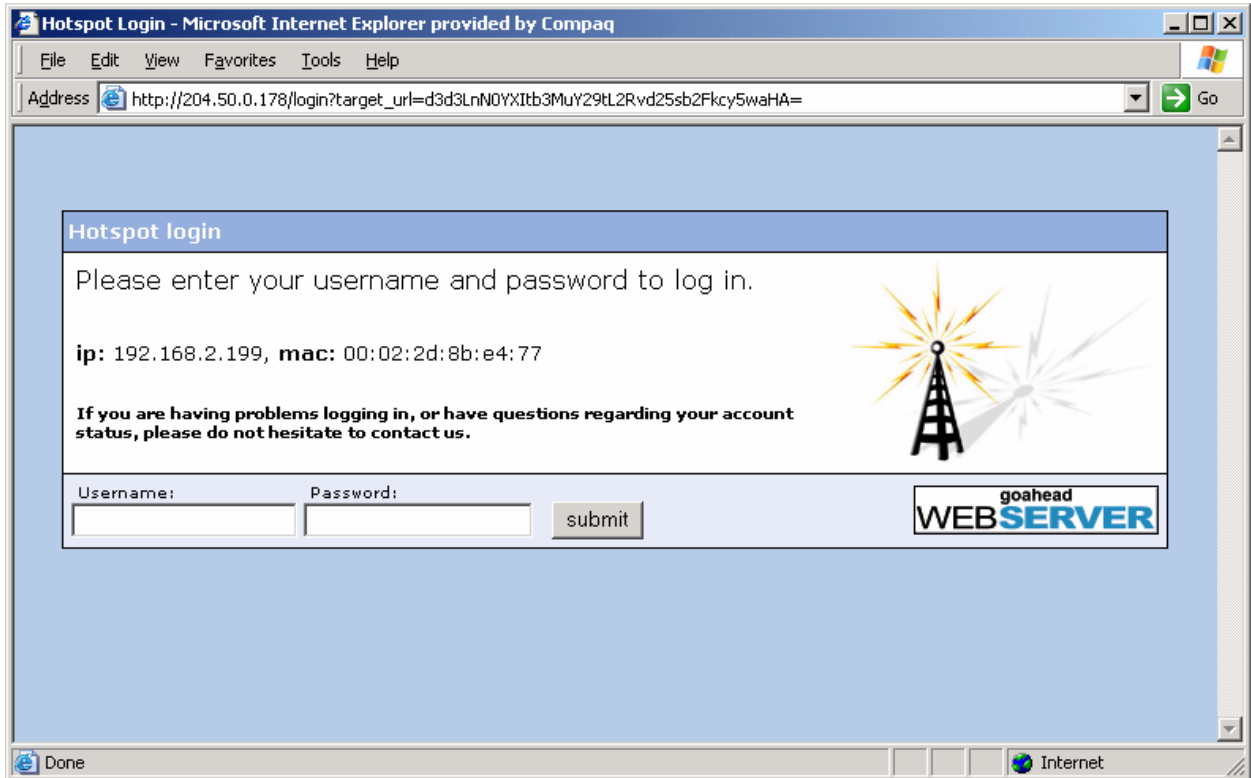
```
router.domain.com
IPTraf
----- PktsIn ----- IP In - BytesIn - InRate  PktsOut --- IP Out  BytesOut  OutRate
Ethernet HW addr: 00601d04798e on wpcm0
L      914      914    152516    11.6      482      482     26224     1.8
Ethernet HW addr: 00026f017637 on wpcm0
L      481      481    25974     1.8      914      914    152516    11.6
Ethernet HW addr: ffffffff on wpcm0
L       1       1      250      0.0       0       0         0         0.0

3 entries --- Elapsed time: 0:01 --- InRate and OutRate are in Kbits/sec ---
Up/Down/PgUp/PgDn-scroll window S-sort X-exit
```

Setting up a “Hotspot”

A “captive portal” is a Web Browser based login system that forces your users to enter a Username and Password to gain access to the rest of your network (in most cases a Captive portal is used to limit access to the Internet).

When a user associates to your wireless access point and tries to visit a website, they are greeted with a login page similar to:



Provided the user has a username and password with you, they would simply enter in their information and the hotspot would allow them through to the Internet. You could also provide a signup link by editing the hotspot login page to take them to a website with an account creation page, for example.

The Hotspot Menu

The **hotspot** -> **hotspot** menu controls the system's hotspot core functionality including:

- Enabling/Disabling the core hotspot system.
- Assigning a default CBQ rate to users,
- Session timeouts
- Whether or not to authenticate a user based on their MAC address.

```
iced hotspot services system
1 hotspot >
1 configuration
2 radius setup
3 hotspot whitelists >
4 edit hotspot pages >
5 restore factory hotspot pages
6 hotspot session list
```

The **default CBQ** rate is the speed at which your customers will be able to transfer data through the hotspot.

The **session timeouts** determine how long a user can stay "idle" for, after which the user is logged out of the system and must re-enter their username and password. Maximum session time determines how long a user can stay logged in at a time.

The hotspot uses any radius server to authenticate users with, and shares the same radius profile as the PPTP and PPPoE services.

Once you have configured the core hotspot system, you must tell each network interface to listen to hotspot requests. This is done from the **interfaces** -> **[interface name]** -> **interface features** menu.

```
Interfaces routing advanced hotspot
802.1q virtual lan (vlan) setup
pptp client setup
dhcp client information
1 ether1: 00:0A:E6:47:B0:A3 ips: 2, b
2 wlan1: 00:02:6F:01:76:38 ips: 1, b
1 ip assignments
2 interface features >
1 listen to pppoe requests: no
2 enable hotspot: no
3 enable ezee client: no
4 enable dhcp auto-auth: no
5 enable dhcp client: no
9 lan station monitor
```

Advanced Hotspot Features

The hotspot supports both server and client white lists. A server white list specifies IP addresses that un-authenticated users may visit. This is particularly useful if you want to provide a “new user signup page”, for example.

The client white list specifies MAC addresses of clients who will never be captured by the portal. These addresses will have complete access through your hotspot regardless of whether they have a username and password.

Providing a “new user signup” link on the hotspot login page.

First, add the IP address of the website that hosts the new user signup page. For example, if you your website IP address 192.168.5.100 then you would add:

```
192.168.5.100
```

into the hotspot -> hotspot whitelists -> server whitelist setup screen.

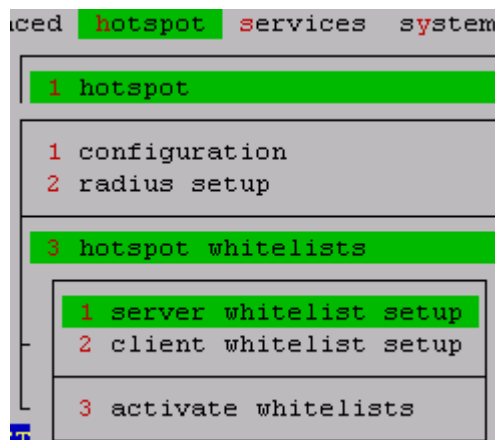
Giving yourself free reign on the MAC address.

You might want to give yourself unfettered access to the hotspot’s you are setting up. Just add your MAC address to the client whitelist setup:

```
# Each client listed will not be prompted for a hotspot  
# login, and will have unrestricted access to the  
# network.
```

```
# Add one MAC address per line. Up to 255 are  
# supported.
```

```
00:02:2D:32:54:A4
```



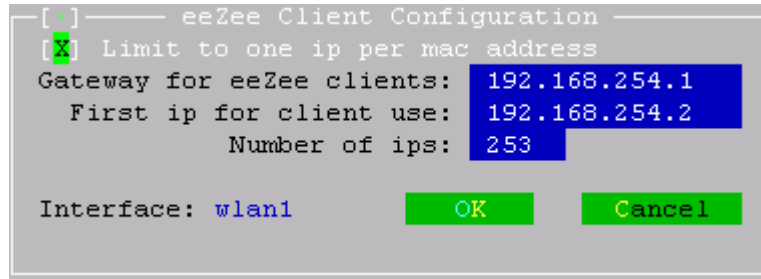
Setting up eeZee configuration

eeZee configuration is a special option supported by the RWV's that enables clients to access the network regardless of their IP settings. This is especially useful in hotspot environments where users may have any sort of IP networking configuration and is invaluable if you ever have to redesign your IP layout and some customers are not using DHCP.

eeZee configuration will put a client onto the network even if they have hard-coded their TCP/IP settings.

To configure eeZee client configuration, go to the **interfaces** menu, select the wireless interface you want eeZee to function on and finally select "configuration".

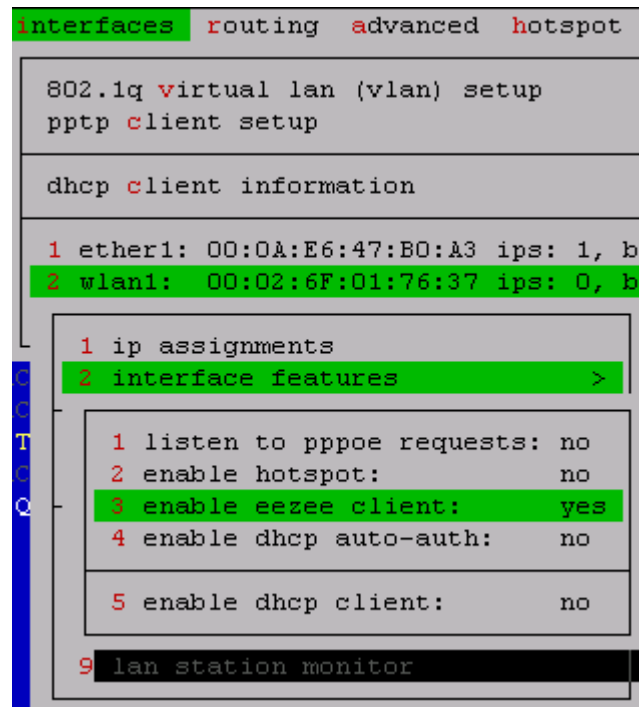
- Limit to one IP per MAC address should be checked.
- The Gateway for eeZee clients is an IP address that will be used as a default gateway.
- The First IP for client use is the starting range of IP addresses that will be assigned to individual users.
- The number of IP's is the amount of addresses that should be used for eeZee client.



NOTE: The IP Addresses you enter in **must not** be used anywhere else on your network, otherwise routing and assignment conflicts may occur.

Click OK to exit and enable eeZee client configuration on the Interface.

From the **interfaces** menu, select the wireless interface to enable eeZee on, go to **interface features** and select the **enable eezee client** option.



Setting up a VPN Server using PPTP

[.] PPTP Server Setup

PPTP Bootup
 Enabled
 Disabled

CBQ Defaults
 Assign a default CBQ rate to users
RX: 128k TX: 128k

IP Address Range (245 IPs)
10 . 100 . 2 . 10 First IP
10 . 100 . 2 . 254 Last IP

PPTP Host IP
10.100.2.1
From Gateway Device

Auth Methods: PAP CHAP MS-CHAP MS-CHAPv2
Encryption: MPPE 40-Bit MPPE 128-Bit
MPPE Mode: MPPE Stateful MPPE Stateless
 Adjust MTU for VLANs

Restart OK Cancel

Setting up a PPPoE server

PPPoE Server Setup

PPPoE Bootup
 Enabled
 Disabled

Access Concentrator: PPPoE

Service Name: Server

Random ID

Assign a default CBQ rate to users
RX: 128k TX: 56k

IP Address Range: (040 IPs)
192 . 168 . 1 . 10 First IP
192 . 168 . 1 . 49 Last IP

PPPoE Host IP: 192.168.1.1
From Gateway Device

Auth Methods: PAP CHAP MS-CHAP MS-CHAPv2
 Adjust MTU for VLANs

Restart OK Cancel

Trouble shooting

Are you running the latest stable firmware release for the RWV? If your system is more than 6 months old, please consider upgrading to the latest stable version before reporting a problem.

Here are some commonly known issues and their resolutions.

The network is to slow!

We suggest you check that:

- You are using CBQ/Bandwidth limiting to prevent one or a handful of users from using all of your available bandwidth.
- That any “sporadic” or marginal links to customers are resolved. A customer with a marginal link may be causing your AP to re-train to a slower speed affecting other users on the network.
 - You may want to lock the speed of your AP to 5 Mbps to keep off users incapable of maintaining a strong enough link.

Tables

802.11b Frequency Range 2,400 – 2500 MHz

Center Frequency chart

Channel ID	FCC	ETSI	France	Japan
1	2412	2412		2412
2	2417	2417		2417
3	2422	2422		2422
4	2427	2427		2427
5	2432	2432		2432
6	2437	2437		2437
7	2442	2442		2442
8	2447	2447		2447
9	2452	2452		2452
10	2457	2457	2457	2457
11	2462	2462	2462	2462
12		2467	2467	2467
13		2472	2472	2472
14				2484

Channel Selection

As each DSSS channel is 22 Mhz wide the best channel selection without overlap would only give you 3 usable channels in most cases you can use 4 channels with overlap.

Best Channel Selection Possible

Channel ID	Center Frequency	Bottom	Top	Width
1	2412	2401	2423	22 Mhz
6	2437	2426	2448	22 Mhz
11	2462	2451	2473	22 Mhz

Usable Channel Selection

Channel ID	Center Frequency	Bottom	Top	Width
1	2412	2401	2423	22 Mhz w/Overlap
4	2427	2416	2438	22 Mhz w/Overlap
7	2442	2431	2453	22 Mhz w/Overlap
10	2457	2446	2468	22 Mhz w/Overlap

802.11 Channel List

This is a list of channels used by 802.11 (a, b and g) devices. These channels may be entered into the Atheros configuration page.

Channel	Frequency	Operating Mode/Modulation
1	2412	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
2	2417	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
3	2422	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
4	2427	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
5	2432	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
6	2437	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps 802.11g Turbo / OFDM / 108 Mbps
7	2442	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
8	2447	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
9	2452	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
10	2457	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
11	2462	802.11b / CCK / 11 Mbps 802.11g / OFDM / 54 Mbps
36	5180	802.11a / OFDM / 54 Mbps
40	5200	802.11a / OFDM / 54 Mbps
42 Turbo	5210	802.11a Turbo / OFDM / 108 Mbps
44	5220	802.11a / OFDM / 54 Mbps
48	5240	802.11a / OFDM / 54 Mbps
50 Turbo	5250	802.11a Turbo / OFDM / 108 Mbps
52	5260	802.11a / OFDM / 54 Mbps
56	5280	802.11a / OFDM / 54 Mbps
58 Turbo	5290	802.11a Turbo / OFDM / 108 Mbps
60	5300	802.11a / OFDM / 54 Mbps
64	5320	802.11a / OFDM / 54 Mbps
149	5745	802.11a / OFDM / 54 Mbps
152 Turbo	5760	802.11a Turbo / OFDM / 108 Mbps
153	5765	802.11a / OFDM / 54 Mbps
157	5785	802.11a / OFDM / 54 Mbps
160 Turbo	5780	802.11a Turbo / OFDM / 108 Mbps
161	5805	802.11a / OFDM / 54 Mbps
165	5825	802.11a / OFDM / 54 Mbps

Regulatory Country Codes

These two-letter codes can be entered on the Atheros configuration dialog to enable certain bands for that country.

Country codes can be used on cards with Regulatory Type (RT): ALL_COUNTRIES as shown in the regulatory information box.

NA - NO_COUNTRY_SET	FR - FRANCE	PT - PORTUGAL
AL - ALBANIA	GE - GEORGIA	PR - PUERTO RICO
DZ - ALGERIA	DE - GERMANY	QA - QATAR
AR - ARGENTINA	GR - GREECE	RO - ROMANIA
AM - ARMENIA	GT - GUATEMALA	RU - RUSSIA
AU - AUSTRALIA	JO - JORDAN	SA - SAUDI ARABIA
AT - AUSTRIA	KZ - KAZAKHSTAN	SG - SINGAPORE
AZ - AZERBAIJAN	KP - NORTH KOREA	SK - SLOVAK REPUBLIC
BH - BAHRAIN	KR - KOREA REPUBLIC	SI - SLOVENIA
BY - BELARUS	K2 - KOREA REPUBLIC2	ZA - SOUTH AFRICA
BE - BELGIUM	KW - KUWAIT	ES - SPAIN
BZ - BELIZE	LV - LATVIA	SE - SWEDEN
BO - BOLIVIA	LB - LEBANON	CH - SWITZERLAND
BR - BRAZIL	LI - LIECHTENSTEIN	SY - SYRIA
BN - BRUNEI DARUSSALAM	LT - LITHUANIA	TW - TAIWAN
BG - BULGARIA	LU - LUXEMBOURG	TH - THAILAND
CA - CANADA	MO - MACAU	TT - TRINIDAD & TOBAGO
CL - CHILE	MK - MACEDONIA	TN - TUNISIA
CN - CHINA	MY - MALAYSIA	TR - TURKEY
CO - COLOMBIA	MX - MEXICO	UA - UKRAINE
CR - COSTA RICA	MC - MONACO	AE - UNITED ARAB EMIRATES
HR - CROATIA	MA - MOROCCO	GB - UNITED KINGDOM
CY - CYPRUS	NL - NETHERLANDS	US - UNITED STATES
CZ - CZECH REPUBLIC	NZ - NEW ZEALAND	UY - URUGUAY
DK - DENMARK	NO - NORWAY	UZ - UZBEKISTAN
DO - DOMINICAN REPUBLIC	OM - OMAN	VE - VENEZUELA
EC - ECUADOR	PK - PAKISTAN	VN - VIET NAM
EG - EGYPT	PA - PANAMA	YE - YEMEN
SV - EL SALVADOR	PE - PERU	ZW - ZIMBABWE
EE - ESTONIA	PH - PHILIPPINES	
FI - FINLAND	PL - POLAND	

Netmask Table

Netmask 255.255.255.0 /24 (11111111.11111111.11111111.00000000)

1 subnet

LOW IP	HI IP
x.x.x.0	x.x.x.255

Netmask 255.255.255.128 /25 (11111111.11111111.11111111.10000000)

2 subnets

LOW IP	HI IP
x.x.x.0	x.x.x.127
x.x.x.128	x.x.x.255

Netmask 255.255.255.192 /26 (11111111.11111111.11111111.11000000)

4 subnets

x.x.x.0	x.x.x.63
x.x.x.64	x.x.x.127
x.x.x.128	x.x.x.191
x.x.x.192	x.x.x.255

Netmask 255.255.255.224 /27 (11111111.11111111.11111111.11100000)

8 subnets

x.x.x.0	x.x.x.31
x.x.x.32	x.x.x.63
x.x.x.64	x.x.x.95
x.x.x.96	x.x.x.127
x.x.x.128	x.x.x.159
x.x.x.160	x.x.x.191
x.x.x.192	x.x.x.223
x.x.x.224	x.x.x.255

Netmask 255.255.255.240 /28 (11111111.11111111.11111111.11110000)

16 subnets

x.x.x.0	x.x.x.15
x.x.x.16	x.x.x.31
x.x.x.32	x.x.x.47
x.x.x.48	x.x.x.63
x.x.x.64	x.x.x.79
x.x.x.80	x.x.x.95
x.x.x.96	x.x.x.111
x.x.x.112	x.x.x.127
x.x.x.128	x.x.x.143
x.x.x.144	x.x.x.159
x.x.x.160	x.x.x.175
x.x.x.176	x.x.x.191
x.x.x.192	x.x.x.207
x.x.x.208	x.x.x.223
x.x.x.224	x.x.x.239
x.x.x.240	x.x.x.255

Netmask 255.255.255.248 /29 (11111111.11111111.11111111.11111000)

32 subnets

x.x.x.0	x.x.x.7
x.x.x.8	x.x.x.15
x.x.x.16	x.x.x.23
x.x.x.24	x.x.x.31
x.x.x.32	x.x.x.39
x.x.x.40	x.x.x.47
x.x.x.48	x.x.x.55
x.x.x.56	x.x.x.63

x.x.x.64	x.x.x.71
x.x.x.72	x.x.x.79
x.x.x.80	x.x.x.87
x.x.x.88	x.x.x.95
x.x.x.96	x.x.x.103
x.x.x.104	x.x.x.111
x.x.x.112	x.x.x.119
x.x.x.120	x.x.x.127
x.x.x.128	x.x.x.135
x.x.x.136	x.x.x.143
x.x.x.144	x.x.x.151
x.x.x.152	x.x.x.159
x.x.x.160	x.x.x.167
x.x.x.168	x.x.x.175
x.x.x.176	x.x.x.183
x.x.x.184	x.x.x.191
x.x.x.192	x.x.x.199
x.x.x.200	x.x.x.207
x.x.x.208	x.x.x.215
x.x.x.216	x.x.x.223
x.x.x.224	x.x.x.231
x.x.x.232	x.x.x.239
x.x.x.240	x.x.x.247
x.x.x.248	x.x.x.255

Netmask 255.255.255.252 /30 (11111111.11111111.11111111.11111100)

64 subnets

LOW IP	HI IP
x.x.x.0	x.x.x.3
x.x.x.4	x.x.x.7
x.x.x.8	x.x.x.11
x.x.x.12	x.x.x.15
x.x.x.16	x.x.x.19
x.x.x.20	x.x.x.23
x.x.x.24	x.x.x.27
x.x.x.28	x.x.x.31
x.x.x.32	x.x.x.35
x.x.x.36	x.x.x.39
x.x.x.40	x.x.x.43
x.x.x.44	x.x.x.47
x.x.x.48	x.x.x.51
x.x.x.52	x.x.x.55
x.x.x.56	x.x.x.59
x.x.x.60	x.x.x.63
x.x.x.64	x.x.x.67
x.x.x.68	x.x.x.71
x.x.x.72	x.x.x.75
x.x.x.76	x.x.x.79
x.x.x.80	x.x.x.83
x.x.x.84	x.x.x.87
x.x.x.88	x.x.x.91
x.x.x.92	x.x.x.95
x.x.x.96	x.x.x.99
x.x.x.100	x.x.x.103
x.x.x.104	x.x.x.107
x.x.x.108	x.x.x.111
x.x.x.112	x.x.x.115
x.x.x.116	x.x.x.119
x.x.x.120	x.x.x.123
x.x.x.124	x.x.x.127
x.x.x.128	x.x.x.131

x.x.x.132	x.x.x.135
x.x.x.136	x.x.x.139
x.x.x.140	x.x.x.143
x.x.x.144	x.x.x.147
x.x.x.148	x.x.x.151
x.x.x.152	x.x.x.155
x.x.x.156	x.x.x.159
x.x.x.160	x.x.x.163
x.x.x.164	x.x.x.167
x.x.x.168	x.x.x.171
x.x.x.172	x.x.x.175
x.x.x.176	x.x.x.179
x.x.x.180	x.x.x.183
x.x.x.184	x.x.x.187
x.x.x.188	x.x.x.191
x.x.x.192	x.x.x.195
x.x.x.196	x.x.x.199
x.x.x.200	x.x.x.203
x.x.x.204	x.x.x.207
x.x.x.208	x.x.x.211
x.x.x.212	x.x.x.215
x.x.x.216	x.x.x.219
x.x.x.220	x.x.x.223
x.x.x.224	x.x.x.227
x.x.x.228	x.x.x.231
x.x.x.232	x.x.x.235
x.x.x.236	x.x.x.239
x.x.x.240	x.x.x.243
x.x.x.244	x.x.x.247
x.x.x.248	x.x.x.251
x.x.x.252	x.x.x.255

net mask:

1111 1100 == 252

Pozar's two-bit(tm) addressing

4-bit m m m m

2-bit m m

(.1)	0 0 0 0	0 0 0 1	(.2)	0 0 0 0	0 0 1 0
(.17)	0 0 0 1	0 0 0 1	(.18)	0 0 0 1	0 0 1 0
(.33)	0 0 1 0	0 0 0 1	(.34)	0 0 1 0	0 0 1 0
(.49)	0 0 1 1	0 0 0 1	(.50)	0 0 1 1	0 0 1 0
(.65)	0 1 0 0	0 0 0 1	(.66)	0 1 0 0	0 0 1 0
(.129)	1 0 0 0	0 0 0 1	(.130)	1 0 0 0	0 0 1 0
(.193)	1 1 0 0	0 0 0 1	(.194)	1 1 0 0	0 0 1 0
(.225)	1 1 1 0	0 0 0 1	(.226)	1 1 1 0	0 0 1 0

Younker's tables

Here's a table showing the relationship between the / notation, the byte

notation, and the corresponding binary numbers (with a dot every eight digits) for the 32 bit addresses. I've thrown in a count of how many Class A/B/C networks the larger networks encompass.

/ Notation	Binary	Byte Notation	#Class
/0	00000000.00000000.00000000.00000000	0.0.0.0	256 A
/1	10000000.00000000.00000000.00000000	128.0.0.0	128 A
/2	11000000.00000000.00000000.00000000	192.0.0.0	64 A
/3	11100000.00000000.00000000.00000000	224.0.0.0	32 A
/4	11110000.00000000.00000000.00000000	240.0.0.0	16 A
/5	11111000.00000000.00000000.00000000	248.0.0.0	8 A
/6	11111100.00000000.00000000.00000000	252.0.0.0	4 A
/7	11111110.00000000.00000000.00000000	254.0.0.0	2 A
/8	11111111.00000000.00000000.00000000	255.0.0.0	1 A
/9	11111111.10000000.00000000.00000000	255.128.0.0	128 B
/10	11111111.11000000.00000000.00000000	255.192.0.0	64 B
/11	11111111.11100000.00000000.00000000	255.224.0.0	32 B
/12	11111111.11110000.00000000.00000000	255.240.0.0	16 B
/13	11111111.11111000.00000000.00000000	255.248.0.0	8 B
/14	11111111.11111100.00000000.00000000	255.252.0.0	4 B
/15	11111111.11111110.00000000.00000000	255.254.0.0	2 B
/16	11111111.11111111.00000000.00000000	255.255.0.0	1 B
/17	11111111.11111111.10000000.00000000	255.255.128.0	128 C
/18	11111111.11111111.11000000.00000000	255.255.192.0	64 C
/19	11111111.11111111.11100000.00000000	255.255.224.0	32 C
/20	11111111.11111111.11110000.00000000	255.255.240.0	16 C
/21	11111111.11111111.11111000.00000000	255.255.248.0	8 C
/22	11111111.11111111.11111100.00000000	255.255.252.0	4 C
/23	11111111.11111111.11111110.00000000	255.255.254.0	2 C
/24	11111111.11111111.11111111.00000000	255.255.255.0	1 C
/25	11111111.11111111.11111111.10000000	255.255.255.128	
/26	11111111.11111111.11111111.11000000	255.255.255.192	
/27	11111111.11111111.11111111.11100000	255.255.255.224	
/28	11111111.11111111.11111111.11110000	255.255.255.240	
/29	11111111.11111111.11111111.11111000	255.255.255.248	
/30	11111111.11111111.11111111.11111100	255.255.255.252	
/31	11111111.11111111.11111111.11111110	255.255.255.254	
/32	11111111.11111111.11111111.11111111	255.255.255.255	

Here's an example of how to get from the binary number 11000000 to the decimal number (192).

$$\begin{aligned}
 11000000 &=> 128*1 + 64*1 + 32*0 + 16*0 + 8*0 + 4*0 + 2*0 + 1*0 \\
 &= 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0 \\
 &= 128 + 64 \\
 &= 192
 \end{aligned}$$

Another example (using an arbitrarily chosen binary number):

$$\begin{aligned}
 10000100 &=> 128*1 + 64*0 + 32*0 + 16*0 + 8*0 + 4*1 + 2*0 + 1*0 \\
 &= 128 + 0 + 0 + 0 + 0 + 4 + 0 + 0 \\
 &= 128 + 4 \\
 &= 132
 \end{aligned}$$