MPC8377EWLAN Wireless Router

Software User's Guide

Document Number: MPC8377EWLANSUG
Rev 1.1.2
03/2009

freescale™ semiconductor

How to Reach Us:

Home Page:
www.freescale.com

Web Support:
http://www.freescale.com/support

USA/Europe or Locations Not Listed:
Freescale Semiconductor, Inc.
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
1-800-521-6274 or +1-480-768-2130
www.freescale.com/support

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.freescale.com/support

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064
Japan
0120 191014 or +81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor China Ltd.
Exchange Building 23F
No. 118 Jianguo Road
Chaoyang District
Beijing 100022
China
+86 10 5879 8000
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
1-800-441-2447 or +1-303-675-2140
Fax: +1-303-675-2150
LDCForFreescaleSemiconductor@hibbertgroup.com

Federal Communications Commission Radio Frequency Interference Statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference and
(2) this device must accept any interference received, including interference that might cause undesired operation.
Changes or modifications to this equipment not expressly approved by Freescale could void the user’s authority to operate the equipment.
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

Reminding

1. The installed antennas must not be located in a manner that allows exposure of the general population at a distance of less than 23cm.
2. Mount the antennas in a manner that prevents any personnel from entering the area within 23cm from the central position of the antenna.

This device has been designed to operate with the attached antennas, and having a maximum gain of 2.5dBi. Antennas not identical as that or having a gain greater than 2.5dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

Contents

About This Book

This manual provides information about the MPC8377EWLAN wireless router software. It contains information on how to connect and configure MPC8377EWLAN wireless router.

Audience

The audience for this software manual is the user who wants to become familiar with the MPC8377EWLAN wireless router and who is trying to connect and configure MPC8377EWLAN wireless router. It is assumed that user has basic computer and Internet skills.

Definitions, Acronyms, and Abbreviations

The following list defines the acronyms and abbreviations used in this document.

Abbreviations	Description
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
BSSID	Basic Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DynDNS	Dynamic Domain Name System
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
POE	Power over Ethernet
PPPOA	Point to Point Protocol over ATM
PPPOE	Point to Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Inexpensive Disks
SSID	Service Set Identifier
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol-Internet Protocol

VPN	Virtual Private Network
WAN	Wide Area Network
WDS	Wireless Distribution System
WEP	Wired Equipment Privacy
WPA	Wi-Fi Protected Access
WWAN	Wireless-Wide-Area-Network

1 Package Contents

The package should contain all the items listed in Table 1-1. MPC8377EWLAN is a secure wireless router, one-application build in the Reference Design Solution platform enabled by near-market ready, with BOM-optimized hardware and open-source software support. Check your package for the following contents:

Table 1-1 Package Content

Items	Quantity
MPC8377EWLAN router	1
Power adapter	1
External antennas	3
Wireless card (part of router)	1
CAT-5 Ethernet cable	1
UART cable	1
Documentation CD	1

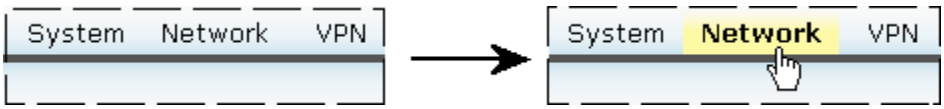
2 Introduction to the Interface

This section introduces various parts of the interface that you will see after you have logged in and are ready to configure the router. Refer to Section 3.4 Configuring the MCP8377EWLAN Wireless Router.

2.1 Hovering the Cursor at an Option

This section explains navigating the options near the top of the page. When you place your cursor over an option, the option becomes bold, with yellow background. Figure 2-1shows an example of an option (Network) being highlighted when a cursor is placed on it.

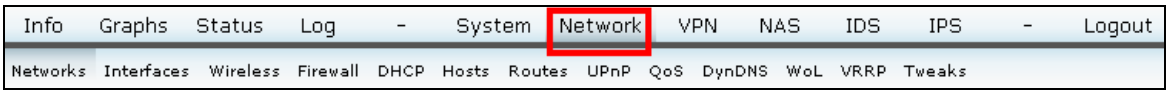
Figure 2-1. Option Cursor Hover



2.2 Clicking an Option and Opening a Submenu

When you click an option: **Network**, in this case—the option's submenu appears below the row of the primary options (See Figure 2-2). Submenu options will also change to highlighted yellow background with bold text when you place the cursor over them.

Figure 2-2. Option Example Selection—Network



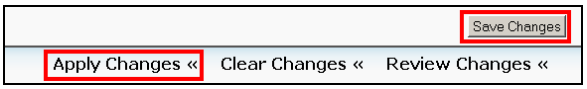
2.3 Saving and Applying Changes to Settings

When you change a setting, scroll to the bottom of the webpage to see **Save Changes** and **Apply Changes** options. Click **Save Changes** and then **Apply Changes** to establish your new settings (Figure 2-3). Other options you can select are reviewing and cancelling the changes.

NOTE

Figures might or might not show the save/apply option. For each page you change, scroll to the bottom and select change option(s) as applicable.

Figure 2-3. Save then Apply



NOTE

Figures need not necessarily reflect the most current system information and software version.

3 Connecting and Configuring the MPC8377EWLAN Wireless Router

This section describes the parameters for your Internet connection and your wireless local area network (WLAN) connection. Details about the connectivity settings, as well as instructions on how to log into the router for further configuration is provided.

Before using MPC8377EWLAN Wireless Router, please ensure that the basic settings to guarantee that it will work in your environment. The MPC8377EWLAN wireless router can be configured to meet various usage scenarios. Some of the factory default settings may suit your usage; however, others may need changing. The recommended sequence for configuration is

Step 1. Configure the IP,

Step 2. Connect the computer to 8377 EWLAN

Step 3. Configure the router, and then

Step 4. Power on the unit.

Configuring MPC8377EWLAN wireless router is done through a web browser. You need a PC connected to the MPC8377EWLAN wireless router (either directly or through a hub) and running a web browser as

a configuration terminal. Verify the TCP/IP settings. Normally, the TCP/IP setting should be on the IP subnet of the MPC8377EWLAN wireless router.

NOTE

Before you start, you should use a wired connection for initial configuration, which will avoid possible setup problem due to wireless uncertainty.

3.1 Connecting the MPC8377EWLAN Wireless Router (Wired Computing)

This section explains the wiring setup for the computer connected to the Internet. The MPC8377EWLAN wireless router has the capability to support usage of power adapter (48 V power supply) and POE (Power over Ethernet).

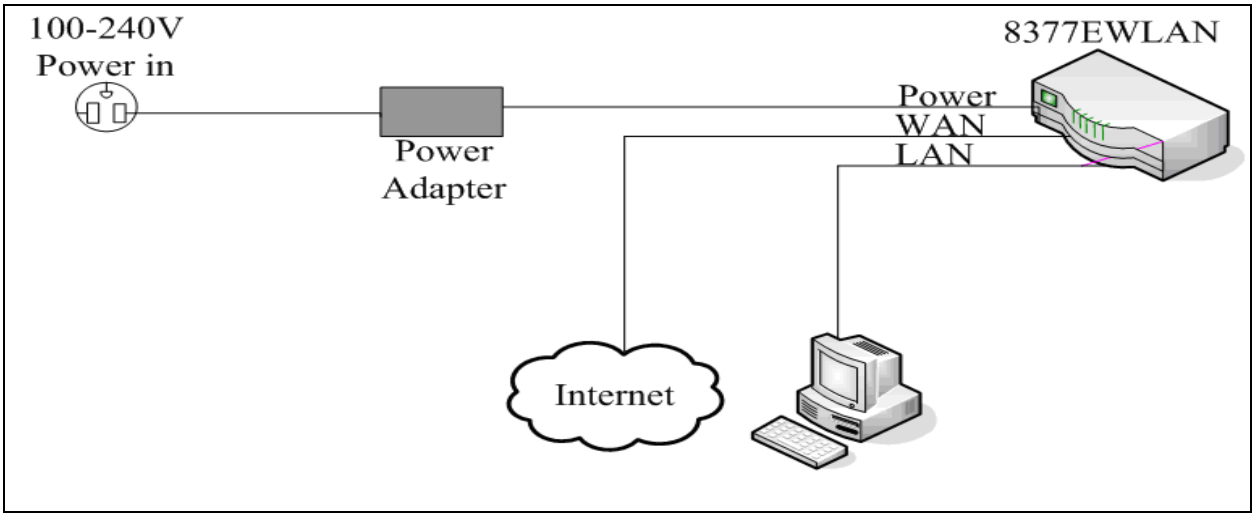
3.1.1 Using the Power Adapter

There must be at least two RJ-45 cables in the MPC8377EWLAN wireless router wiring connection while using a power adapter. Table 3-1 lists the cable connections, and Figure 3-1 depicts them below.

Table 3-1. Cable Connections, Power Adapter

Cable		
Cable #	From	To
1	Router, WAN port	ADSL or computer modem, Ethernet
2	Router, LAN port	Your computer port

Figure 3-1. Cable Connection Layout, Power Adapter



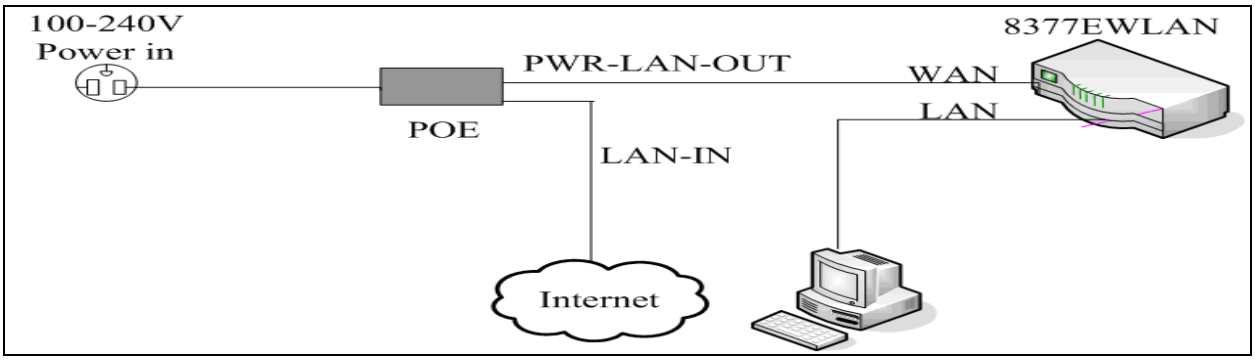
3.1.2 Using the Power over Ethernet (POE)

There must be at least three RJ-45 cables in the MPC8377EWLAN wireless router wiring connection while using POE. Table 3-2 lists the cable connections, and Figure 3-2 depicts them.

Table 3-2. Cable Connections, Power Over Ethernet

Cable		
Cable #	From	To
1	Router, WAN port	POE, PWR-LAN-OUT
2	Router, LAN port	Your computer, Ethernet
3	POE, LAN-IN	ADSL or computer modem, Ethernet

Figure 3-2. Cable Connection Layout, Power Over Ethernet



3.2 Connecting the MPC8377EWLAN Wireless Router (Wireless Computing)

This section explains wiring setup for the computer that has wireless connection to the Internet. The information is similar to the information in Section 3.1 titled Connecting the MPC8377EWLAN Wireless Router (Wired Computing), except, connecting your computer's LAN port to an Ethernet cable, find the SSID **FSL_AP1** (or equivalent), and connect to it. Section 3.4.2.7 Wireless User explains the wireless interface setup, with Figure 3-18 showing SSID setting as FSL_AP1.

3.3 Setting Up the IP Address

This section explains MPC8377EWLAN wireless router capability to automatic and manual setup of the IP address. The IP address setup procedures shown in this document are for Microsoft Windows PCs.

3.3.1 Setting up the IP Address Automatically

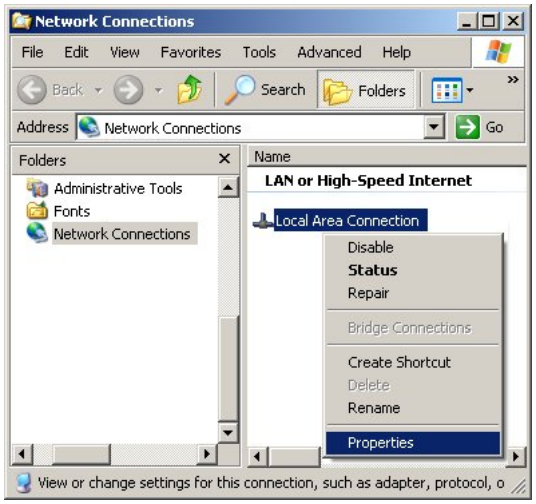
The MPC8377EWLAN wireless router incorporates a DHCP server, hence it is to set your PC to get its IP address automatically and the correct IP address, gateway, DNS can be obtained. Perform the following steps to set your IP address automatically:

1. Right-click **My Network Places** desktop icon and then click **Properties** (Figure 3-3). (Or you can open **Windows Explorer** window, then right click **My Network Places**.)

Figure 3-3. My Network Places > Properties

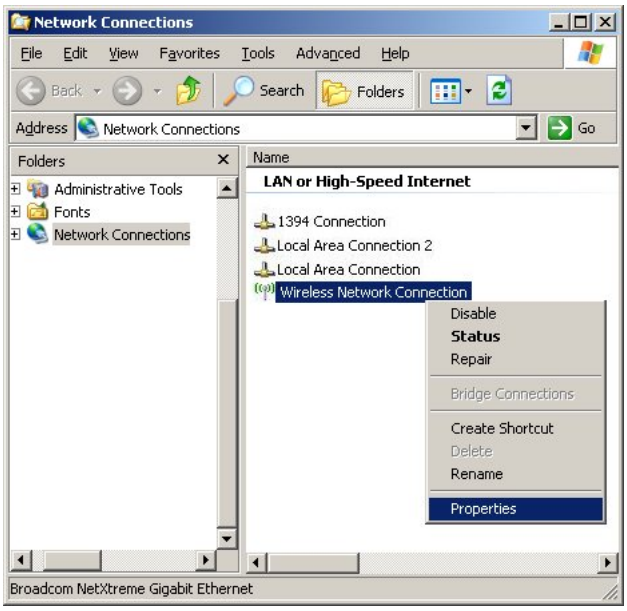
2. In the **Network Connections** window, select one of the following options
   — If you are using a wired connection, right-click **Local Area Connection > Properties** (Figure 3-4).

Figure 3-4. Network Connections, Wired



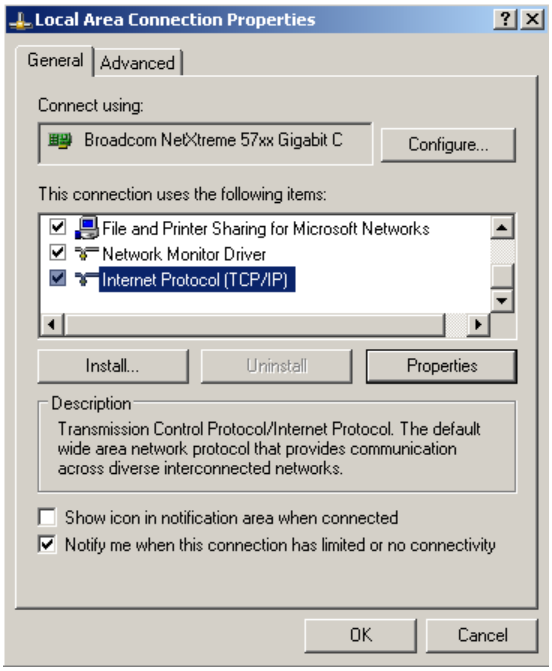
   — If you are using a wireless connection, right click **Wireless Network Connection > Properties** (Figure 3-5).

Figure 3-5. Network Connections, Wireless



3. For wired connection, the following steps apply:
   a. In the **Local Area Connection Properties** window **> General** tab, scroll down to **Internet Protocol (TCP/IP)** (Figure 3-6) then double click it to open the **Internet Protocol (TCP/IP) Properties** window (Figure 3-7).

Figure 3-6. Local Area Connection Properties

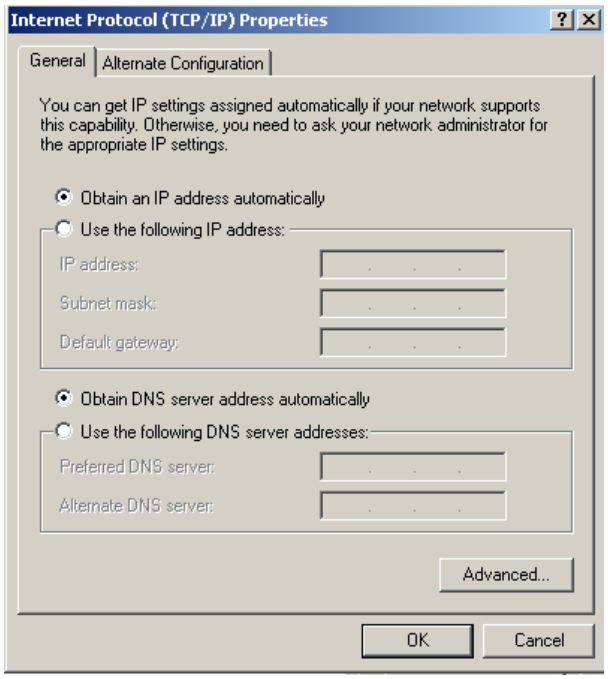


   b. In the **General** tab (Figure 3-7), perform the following steps:
      1.) Click **Obtain an IP** address automatically.

2.) Click **DNS** address automatically.

3.) Click **OK** to close **Internet Protocol (TCP/IP) Properties** window and return to the **Local Area Connection Properties** window.

Figure 3-7. Setting Up the IP Address Automatically



c. At the **Local Area Connection Properties** window, click **OK** to close it.

4. For wireless connection, perform step 3 similar to those of wired connection. (The window titles are different.)

3.3.2 Setting up the IP Address Manually

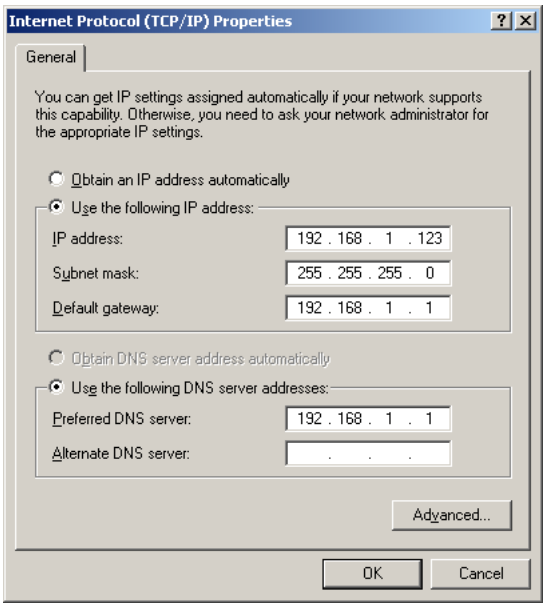
If you want to set your IP address manually, the settings must be set during the same session. The procedure is similar to that of setting up the address automatically. Perform the steps from Section 3.3.1 Setting up the IP Address Automatically until you reach the **Internet Protocol (TCP/IP) Properties** window. Figure 3-8 shows the general settings. Perform the following steps:

1. Click **Use the following IP address**.
   a. In the **IP address**, type **192.168.1.xxx**, where xxx can be any number between 2 and 254.
   b. In the **Subnet Mask**, type **255.255.255.0**.
   c. In the **Default gateway**, type **192.168.1.1**, this is the MPC8377EWLAN wireless router IP address.

2. Click **Use the following DNS server addresses**.
   a. In the **Preferred DNS server**, type **192.168.1.1**, this is the MPC8377EWLAN wireless router IP address or your own.
   b. In the **Alternate DNS server**, leave blank. (See Figure 3-8)

3. Click **OK**.

Figure 3-8. Setting Up the IP Address Manually



3.4 Configuring the MCP8377EWLAN Wireless Router

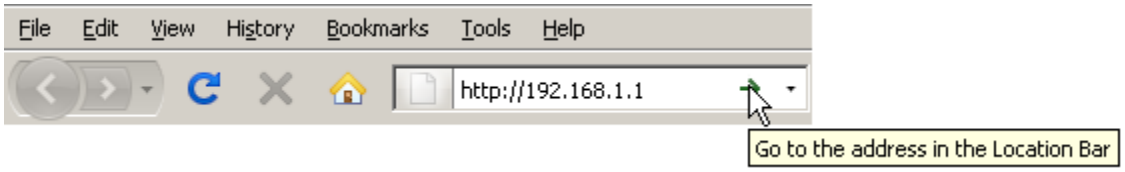
This section explains how to configure your router. The steps consist of opening a browser, going to a website, logging in, and then configuring the router for user equipment.

3.4.1 Logging In to the Router Home Page

Perform the following steps to log in to the router home page:

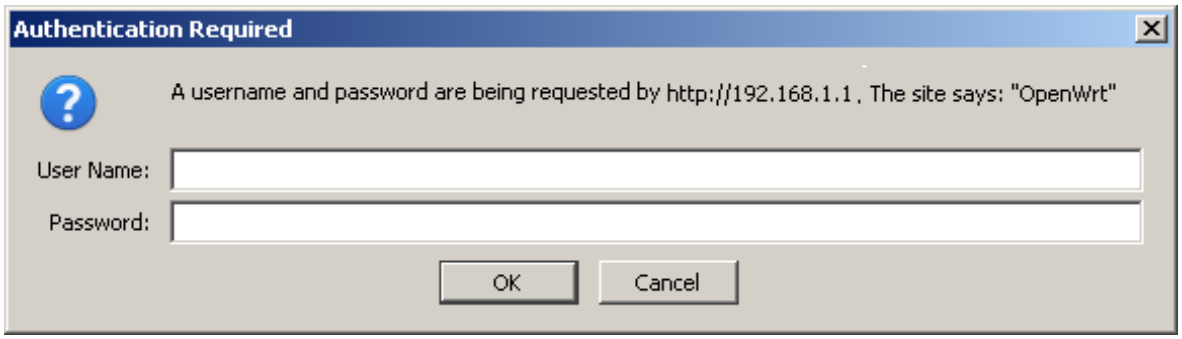
1. Open an Internet browser.
2. Type http://192.168.1.1 in the address bar, then press **Enter** or click the go-to link (Figure 3-9).

Figure 3-9. IP Address in Web Browser



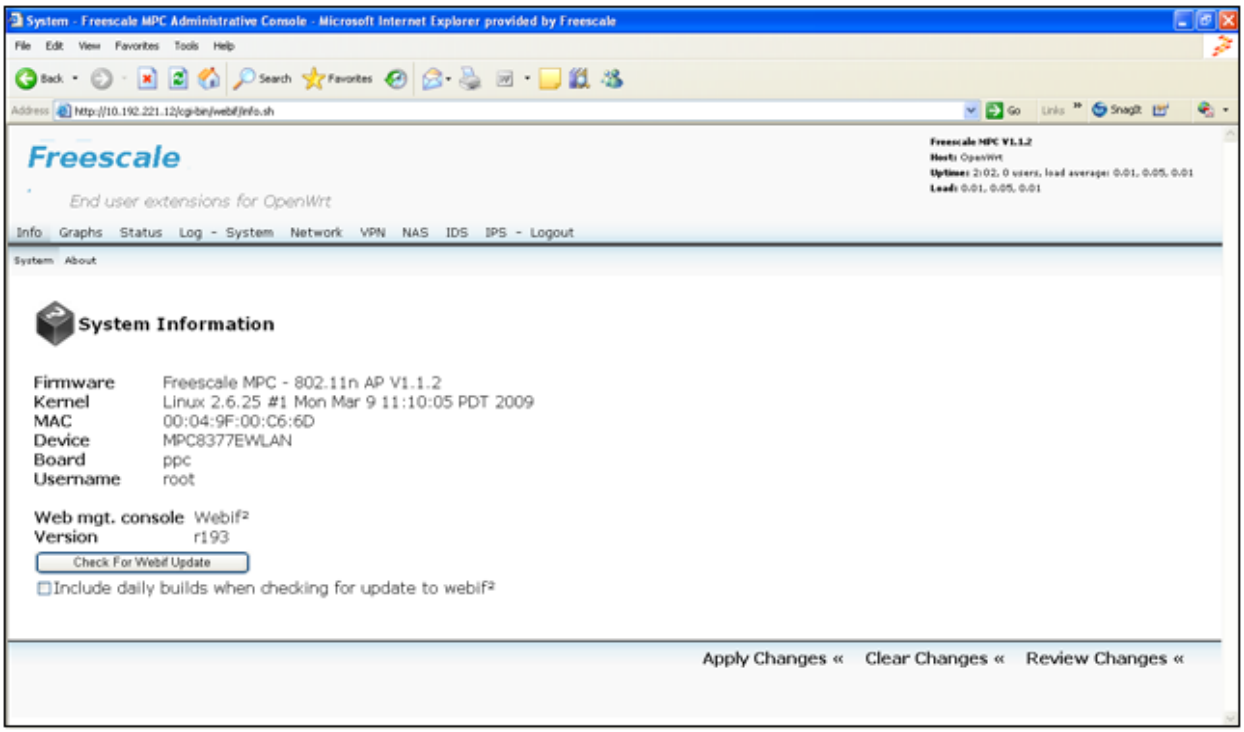
3. In the login window, type `admin` for both **User name** and **Password**, then click **OK** (Figure 3-10).

Figure 3-10. Login



The MCP8377EWLAN wireless router home page appears (Figure 3-11), with default page **Info** > **System**. (For information about the interface, refer to Section 2 titled Introduction to the Interface.)

Figure 3-11. MPC8377EWLAN Wireless Router Home Page



3.4.2 Setting up the Network

The MPC377EWLAN wireless router supports six types of ISP services—static IP address, PPPOE, PPTP, DHCP, PPPOA, and WWAN. Since each service has its own protocols and standards, during the setup process, there are different identity settings demanded by MPC8377EWLAN wireless router.

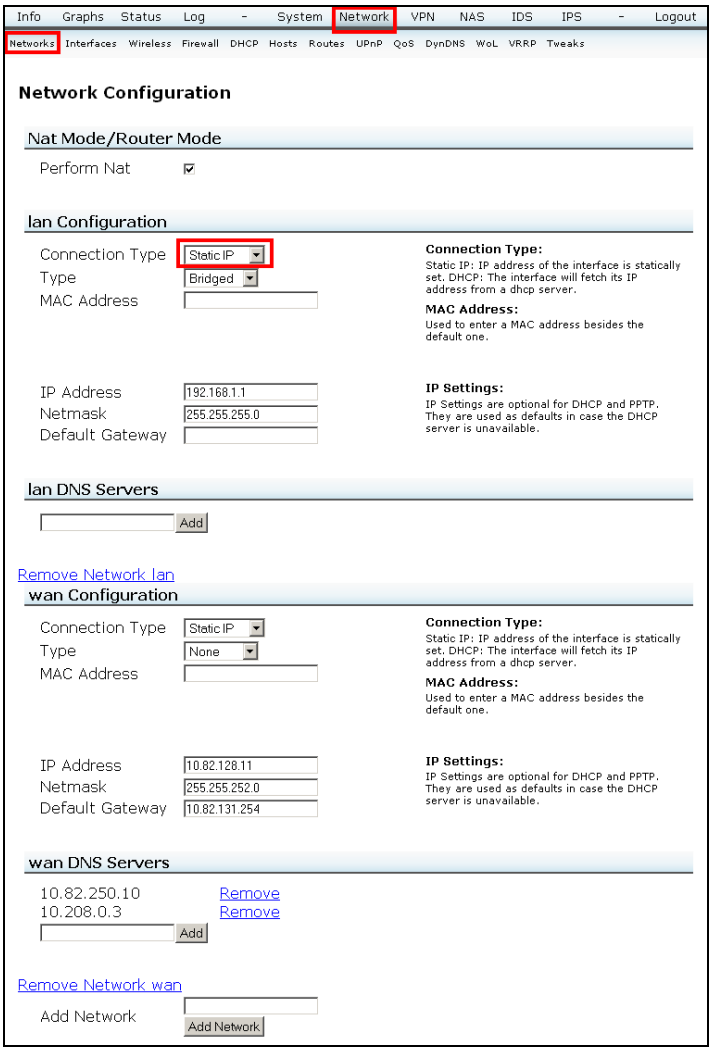
At the MPC8377EWLAN wireless router home page, click **Network**, select the correct connection type, and then follow instructions for the individual sections.

3.4.2.1 Cable User (Static IP)

If you are receiving services from cable or other ISP assigning IP address automatically, select one of the following (Figure 3-12), for which you can type the static IP address:

- **LAN Configuration > Connection Type > Static IP**
- **WAN Configuration > Connection Type > Static IP**

Figure 3-12. Network Setup—Static IP Address (LAN or WAN)



Options include the following:

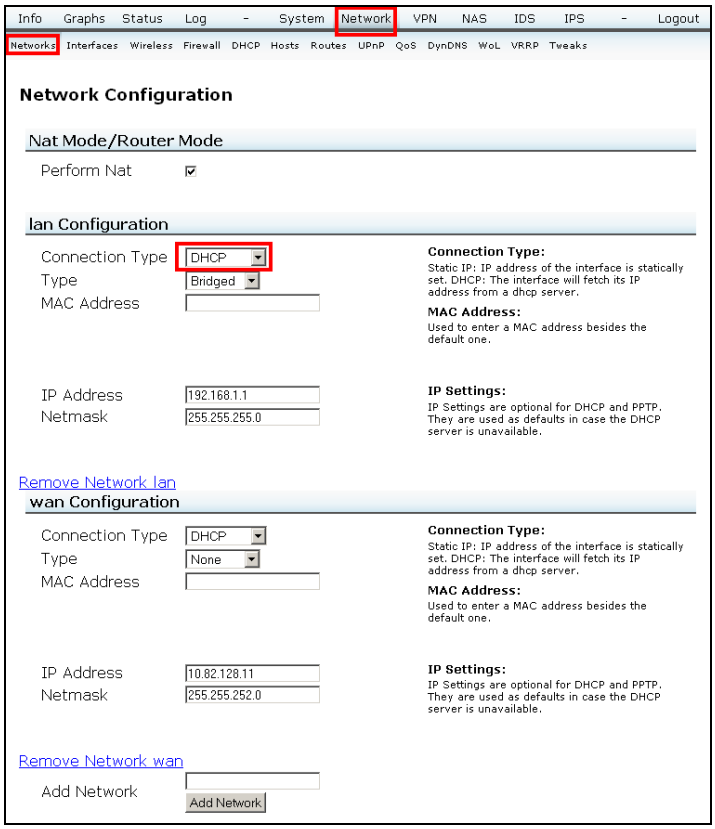
- **LAN DNS Servers** (field and **Add** button). Also, for any LAN server IP shown (if existing), there is a **Remove** link option.
- **Remove Network LAN**, which removes selection options for LAN Configuration.
- **Remove Network WAN**, which removes selection options for WAN Configuration.
- **Add Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

3.4.2.2 DHCP User

If you are a DHCP service user, select one of the following (Figure 3-13):

- **LAN Configuration > Connection Type > DHCP**
- **WAN Configuration > Connection Type > DHCP**

Figure 3-13. Network Setup—DHCP (LAN or WAN)



Options include the following:

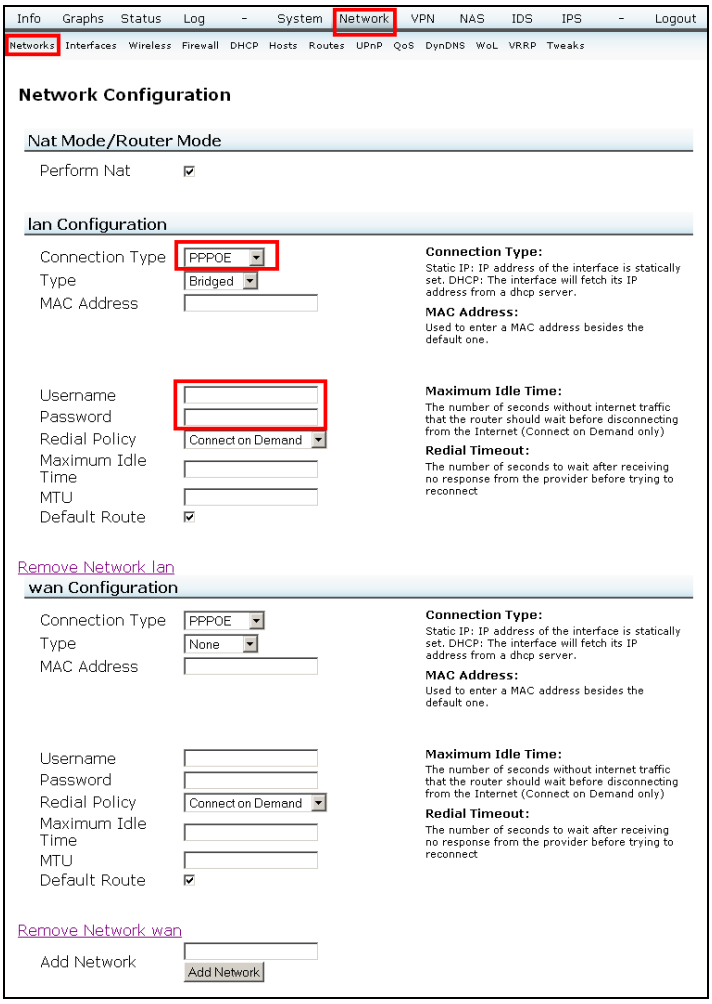
- **Remove Network LAN**, which removes selection options for LAN Configuration.
- **Remove Network WAN**, which removes selection options for WAN Configuration.
- **Add Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

3.4.2.3 PPPOE User

If you are a PPPOE service user, select one of the following (Figure 3-14), for which you must type the **Username** and **Password** provided by your ISP:

- **LAN Configuration > Connection Type > PPPOE**
- **WAN Configuration > Connection Type > PPPOE**

Figure 3-14. Network Setup—PPPOE (LAN or WAN)



Options include the following:

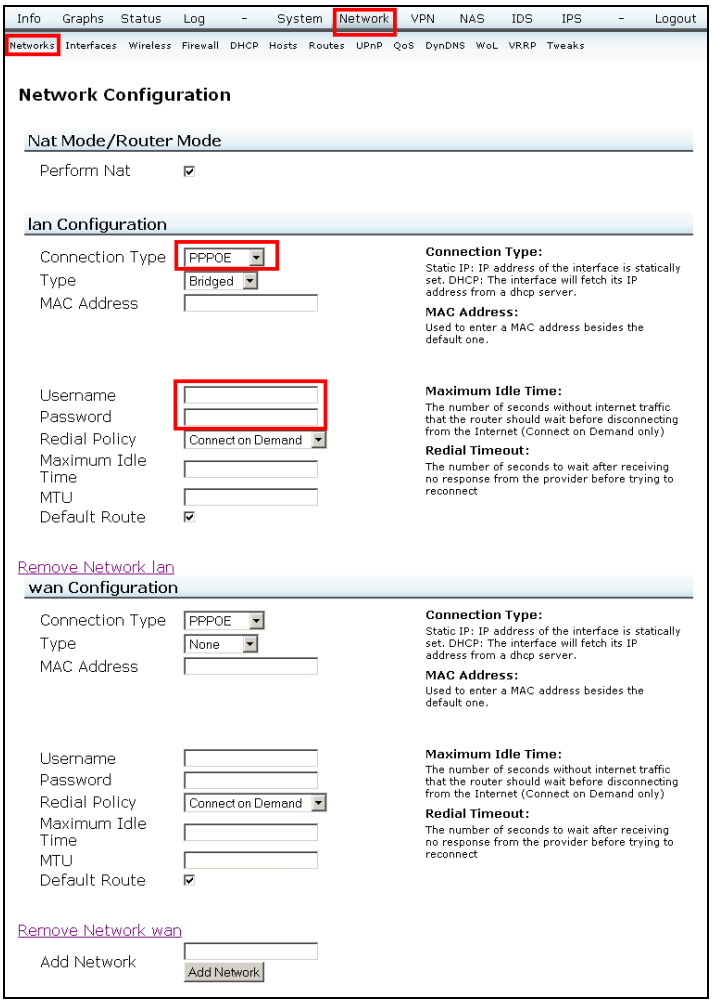
- **Remove Network LAN**, which removes selection options for LAN Configuration.
- **Remove Network WAN**, which removes selection options for WAN Configuration.
- **Add Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

3.4.2.4 PPPOA User

If you are a PPPOA service user, select one of the following (Figure 3-15), for which you must type the **Username** and **Password** provided by your ISP:

- **LAN Configuration > Connection Type > PPPOA**
- **WAN Configuration > Connection Type > PPPOA**

Figure 3-15. Network Setup—PPPOE (LAN or WAN)



Options include the following:

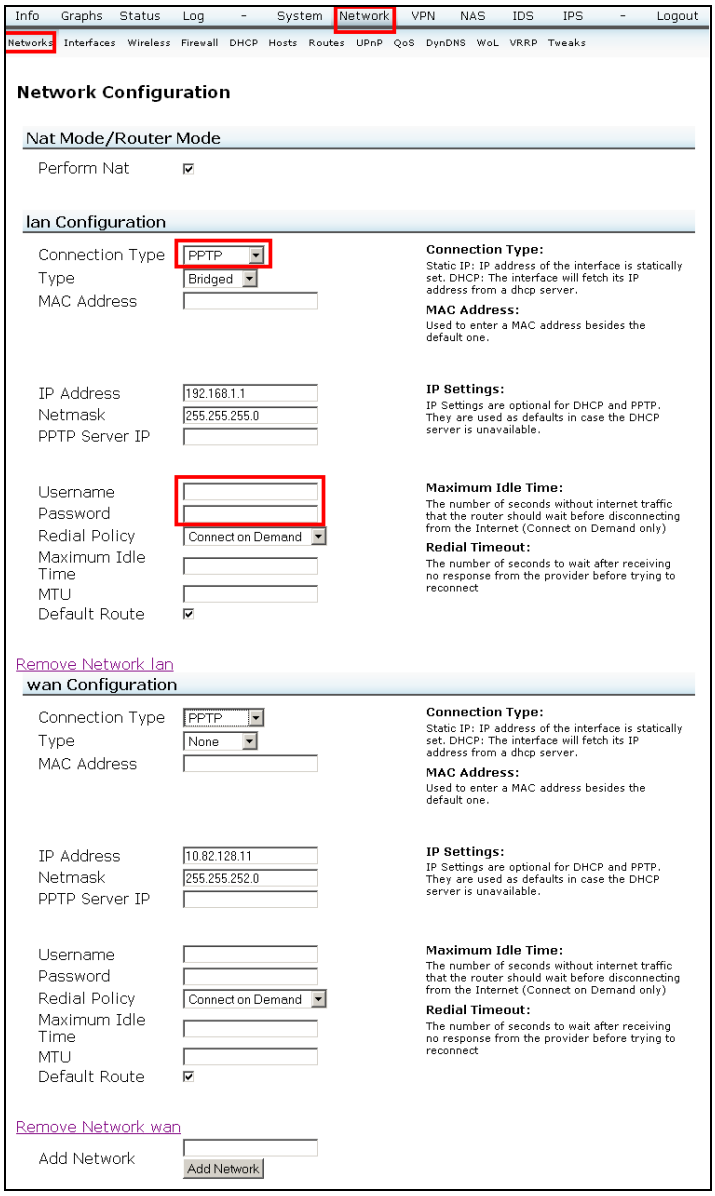
- **Remove Network LAN**, which removes selection options for LAN Configuration.
- **Remove Network WAN**, which removes selection options for WAN Configuration.
- **Add Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

3.4.2.5 PPTP User

If you are a PPTP service user, select one of the following (Figure 3-16), for which you must type the **Username** and **Password** provided by your ISP:

- **LAN Configuration > Connection Type > PPTP**
- **WAN Configuration > Connection Type > PPTP**

Figure 3-16. Network Setup—PPTP (LAN or WAN)



Options include the following:

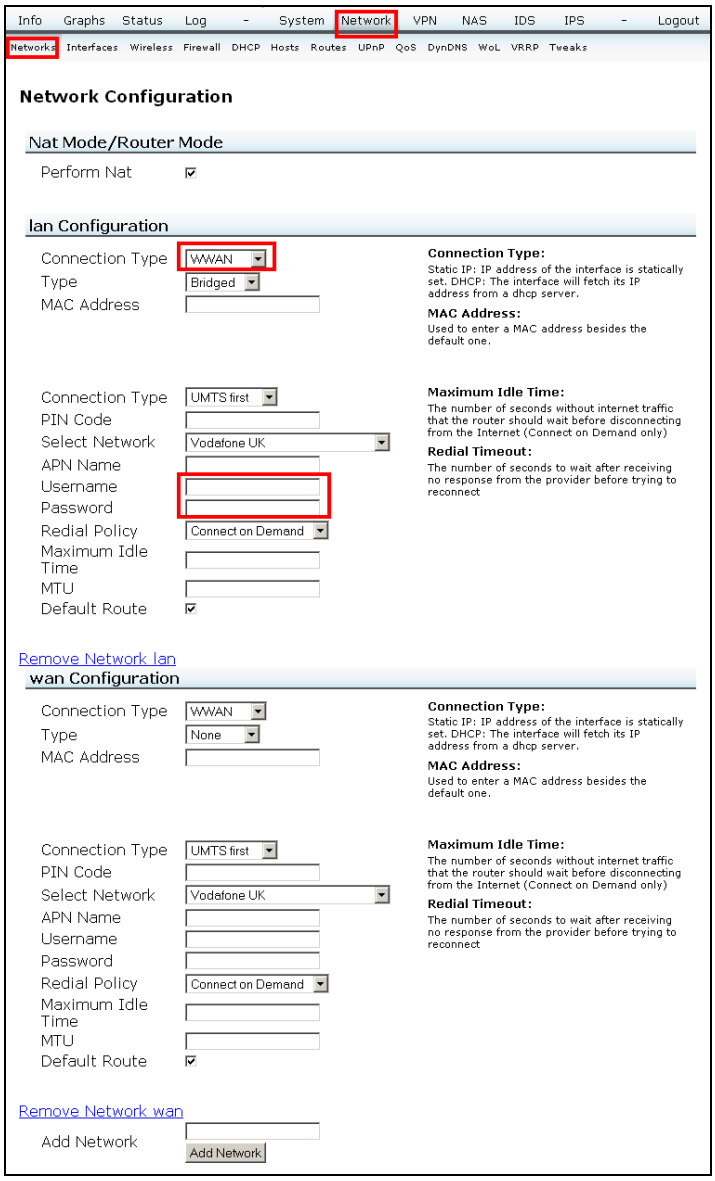
- **Remove Network LAN**, which removes selection options for LAN Configuration.
- **Remove Network WAN**, which removes selection options for WAN Configuration.
- **Add Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

3.4.2.6 WWAN User

If you are a WWAN service user, select one of the following (Figure 3-17), for which you must type the **Username** and **Password** provided by your ISP:

- **LAN Configuration > Connection Type > WWAN**
- **WAN Configuration > Connection Type > WWAN**

Figure 3-17. Network Setup—WWAN (LAN or WAN)



After selecting LAN or WAN configuration, also select the secondary **Connection Type** (UMTS first, UMTS only, GPRS only) from the drop-down list. Make other selections and fill other fields as appropriate.

Options include the following:

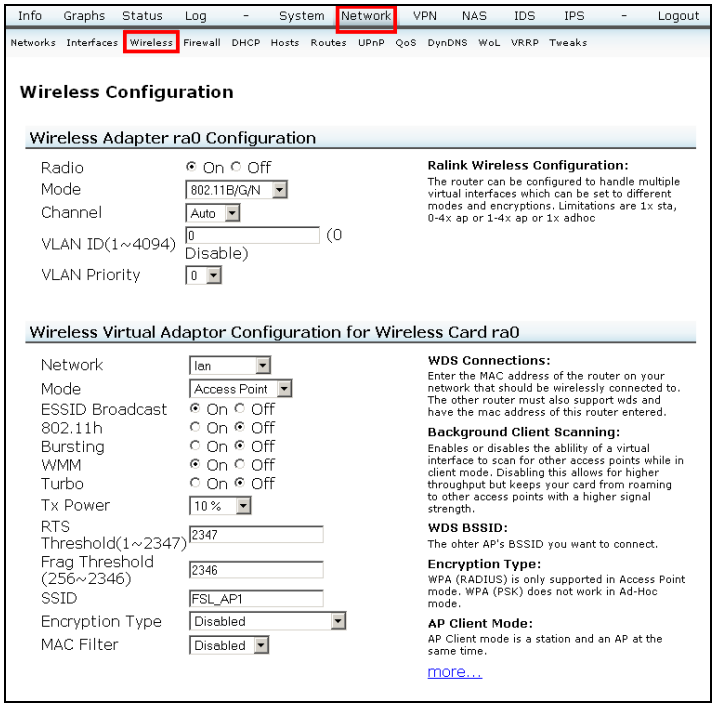
- **Remove Network LAN**, which removes selection options for LAN Configuration.
- **Remove Network WAN**, which removes selection options for WANConfiguration.
- **Add Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

3.4.2.7 Wireless User

The MPC8377EWLAN wireless router supports 802.11b/g/n, you can choose the right criteria which are suitable for your wireless connection. The router supports two wireless cards at the same time. The configuration steps for both the wireless cards are same. After configuring for the first card, you can perform the same steps for the second card.

After setting the connection type in the **Network Configuration** tab page, set up your wireless interface. Click **Wireless** to enter the Wireless configuration page (Figure 3-18).

Figure 3-18. Network > Wireless, RA0 Section Shown



Provide an SSID, which is a unique identifier attached to packets sent over WLAN. Because an SSID distinguishes WLAN from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

If you want to protect transmitted data, a middle (WEP) or high (WPA, WPA2) security level is recommended.

- **Medium**—Only users with same WEP key have permission to connect to this access point and to transmit data using 64bits or 128bits WEP key encryption.
- **High**—Only users with the same WPA/WPA2 pre-shared key have permission to connect to this access point and to transmit data using TKIP encryption.

3.4.2.8 Wireless Encryption Settings

This section explains settings for three families of wireless encryption:

- WEP. WEP is the abbreviation for Wired Equipment Privacy.

- WPA (PSK), WPA2 (PSK), WPA+WPA2 (PSK). WPA is the abbreviation for Wi-Fi Protected Access. PSK is the abbreviation for -Pre-Shared Key.
- WPA (RADIUS), WPA2 (RADIUS), WPA/WPA2 (RADIUS). RADIUS is the abbreviation for Remote Authentication Dial-In User Service.

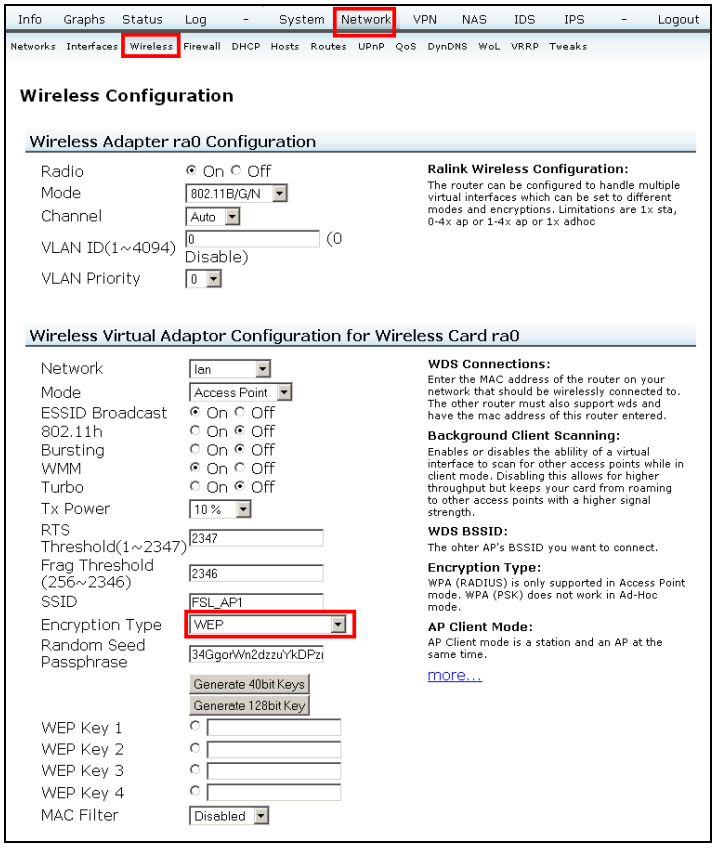
NOTE

In this section, a pair of break lines in a figure indicates a gap between the top of a screen page and the information of interest farther down.

3.4.2.8.1 WEP Encryption

WEP is an encryption method used to protect your data during wireless communications. These settings must be identical to your existing wireless network's WEP settings. You can choose between 64-bit and 128-bit encryption, and select a key to be the active key. Figure 3-19 shows example settings for WEP.

Figure 3-19. Wireless Encryption Setting—WEP, RA0 Section Shown

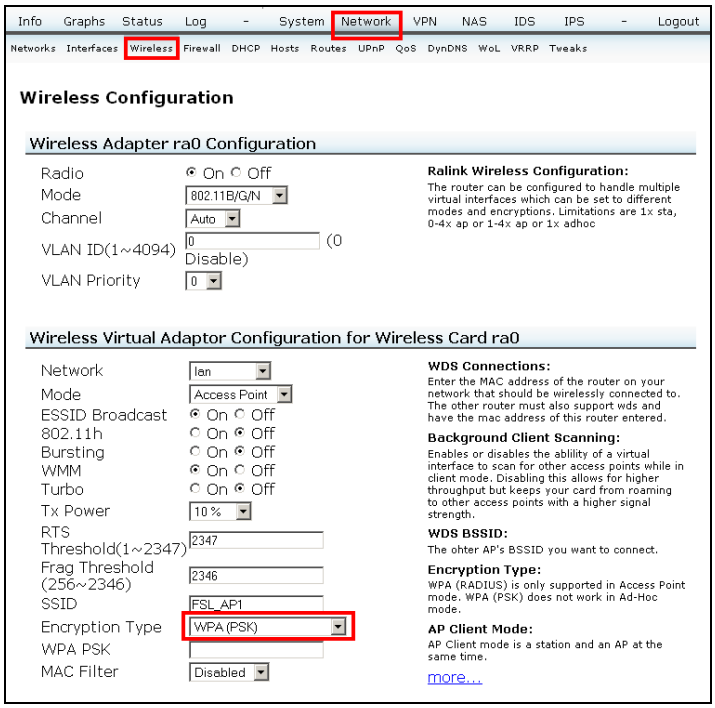


3.4.2.8.2 WPA Encryption

If your network supports WPA/WPA2-PSK security, it is highly recommended that you use those encryptions. WPA and WPA2 are more secure than WEP. Select WPA (PSK), WPA2 (PSK), or

WPA+WPA2 (PSK) from the dropdown menu and type the key in the **WPA PSK** field. Figure 3-20 shows example settings for WPA (PSK).

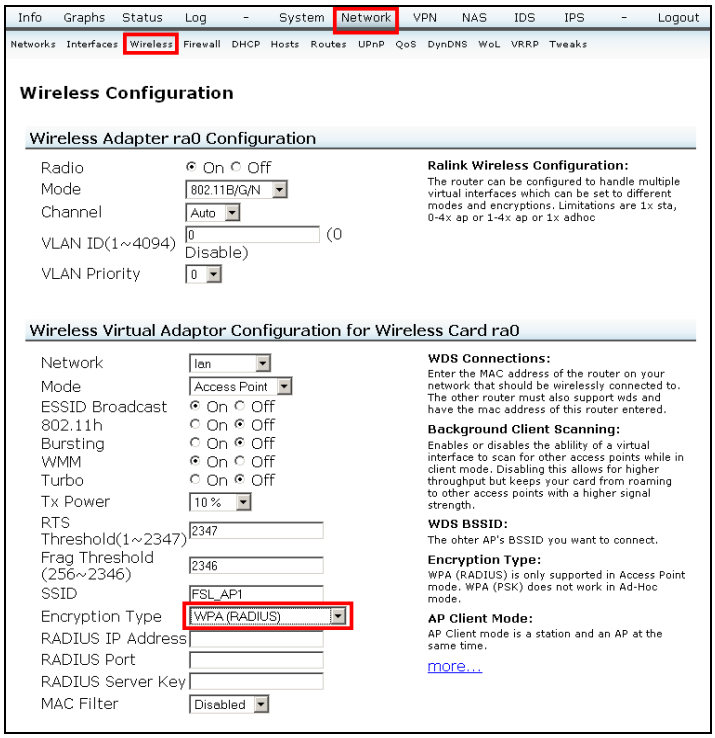
Figure 3-20. Wireless Encryption Setting—WPA-(PSK), RA0 Section Shown



3.4.2.8.3 WPA (RADIUS) Encryption

If your network uses a Remote Authentication Dial-in User Service (RADIUS) server for authentication, select WPA (RADIUS) or WPA2 (RADIUS) or WPA+WPA2 (RADIUS) from the drop-down menu. Type the IP address of your radius server in the **RADIUS IP Address** field, type the authentication port number of your radius server in the **RADIUS Port** field, and type the key for your radius server in the **RADIUS Server Key** field. Figure 3-21 shows example settings for WPA (RADIUS).

Figure 3-21. Wireless Encryption Setting—WPA-(RADIUS), RA0 Section Shown

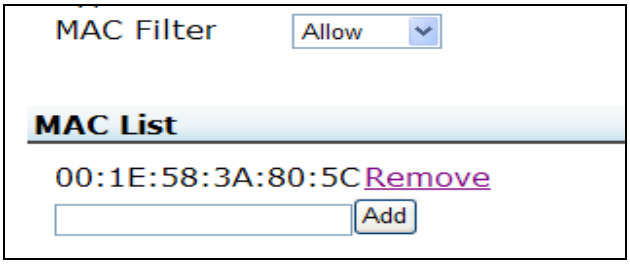


3.4.2.9 MAC (Media Access Control) Filter

MAC filtering is security access control method, in which the 48-bit address assigned to each network card is used to determine access to the network. At the MAC Filter drop-down list, you can control which PCs are permitted or denied communication with the access point depending on their MAC address. See section 5.3 Interfaces for the addresses that apply to your unit.

Figure 3-22 shows a partial view of the configuration page and example settings for MAC Filter. (If there is an existing MAC address, it has a **Remove** link option.)

Figure 3-22. MAC Filter



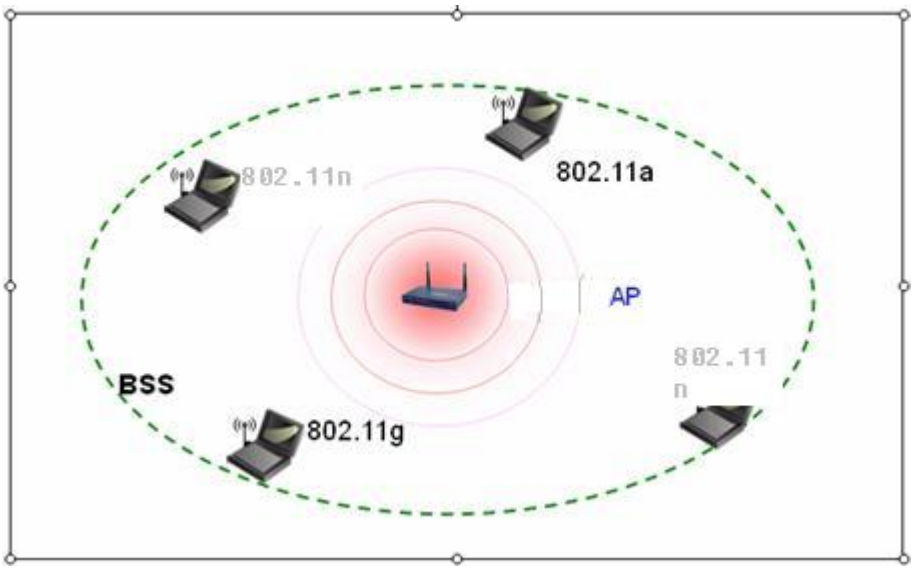
3.5 Changing the Operation Mode

This section explains four types of operation modes: Access Point, WDS (Bridge), Repeater, AP Client.

3.5.1 Configuring for Access Point (AP) Mode

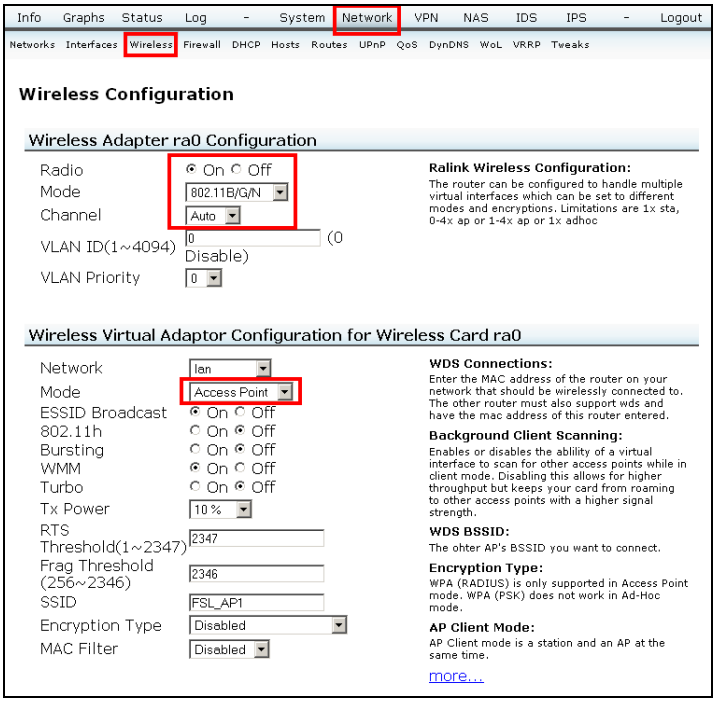
The Access Point mode is the most basic of multi-function modes. It acts as a central hub as depicted in Figure 3-23.

Figure 3-23. Access Point Mode



Configure as shown in Figure 3-24.

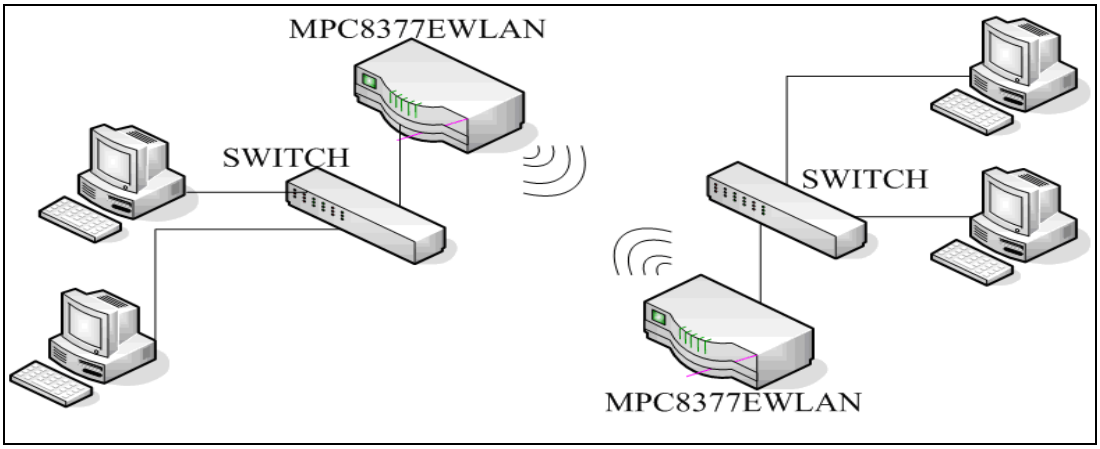
Figure 3-24. Access Point Mode Configuration, RA0 Section Shown



3.5.2 Configuring for WDS (Bridge)

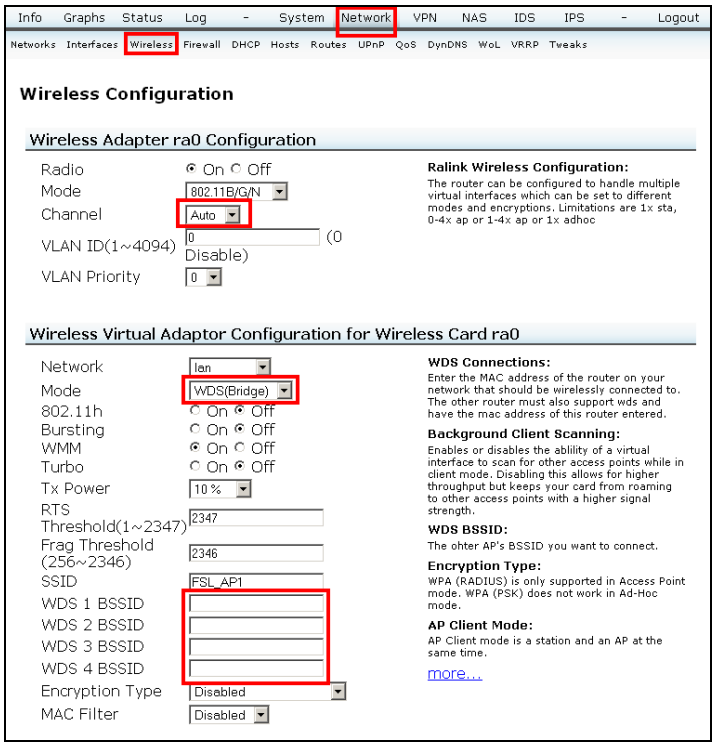
In Wireless Distribution System (WDS) mode, remote access points connect to each other to provide a wireless bridge between LANs. See Figure 3-25 for depiction.

Figure 3-25. WDS Layout



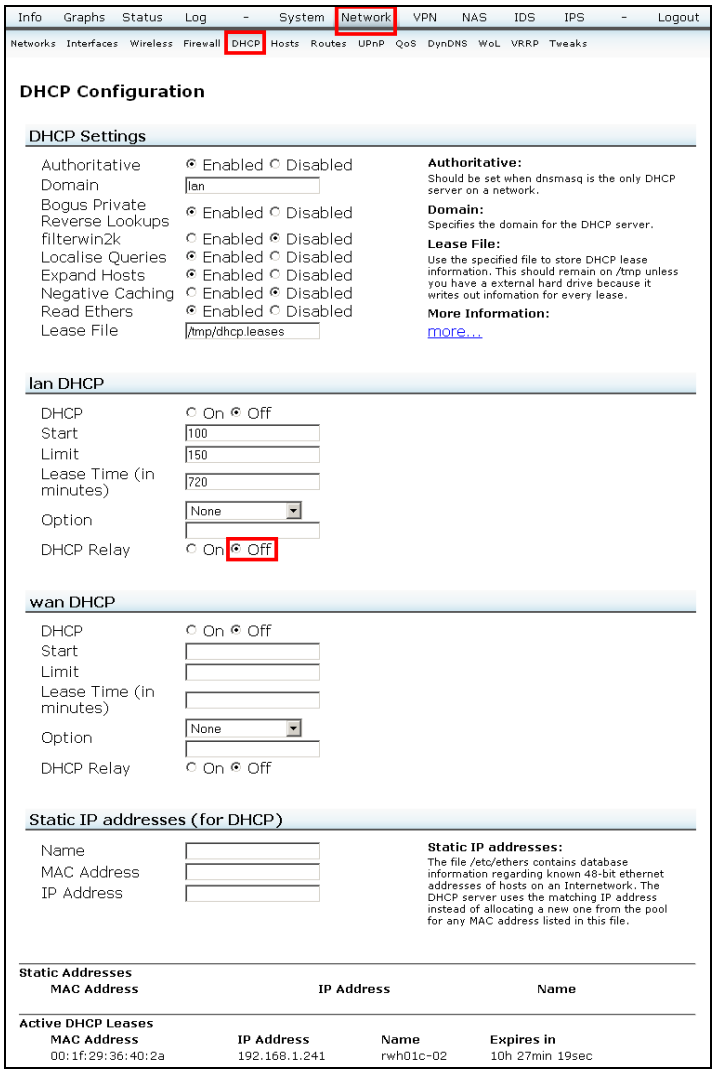
1. Perform the following steps in the **Wireless Configuration** page (Figure 3-26) for both routers. (Navigation: **Network > Wireless**, if necessary.)
   a. From the **Channel** drop-down list, set the two MPC8377EWLAN wireless routers to the same channel.
   b. From the **Mode** drop-down list, select **WDS (Bridge)**.
   c. Copy the MAC address of the remote MPC8377EWLAN wireless router and paste it in the local router's **WDS BSSID** fields.

Figure 3-26. Setting the Same Channel, RA0 Section Shown



2. Click **DHCP** (Dynamic Host Configuration Protocol) to enter the DHCP configuration page, then at the **DHCP** (server) option, click **Off** (Figure 3-27).

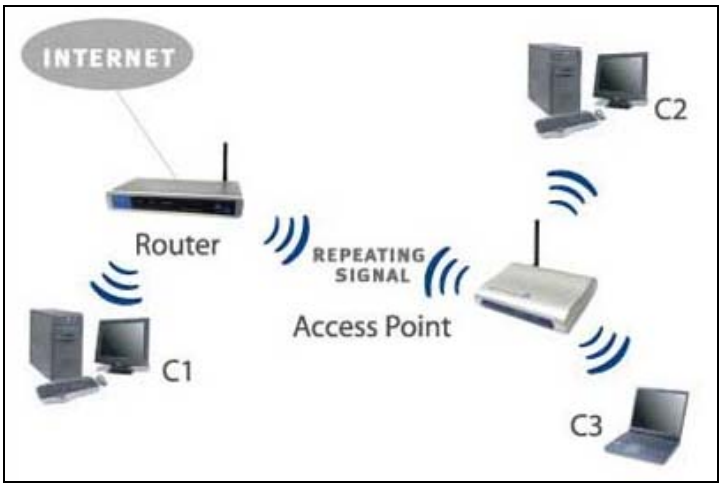
Figure 3-27. DHCP



3.5.3 Configuring for Repeater Mode

A repeater's function is to extend the wireless coverage of another wireless access point or router. For a repeater to work, the remote wireless access point router must also support the WDS/Repeater function. See Figure 3-28 for depiction.

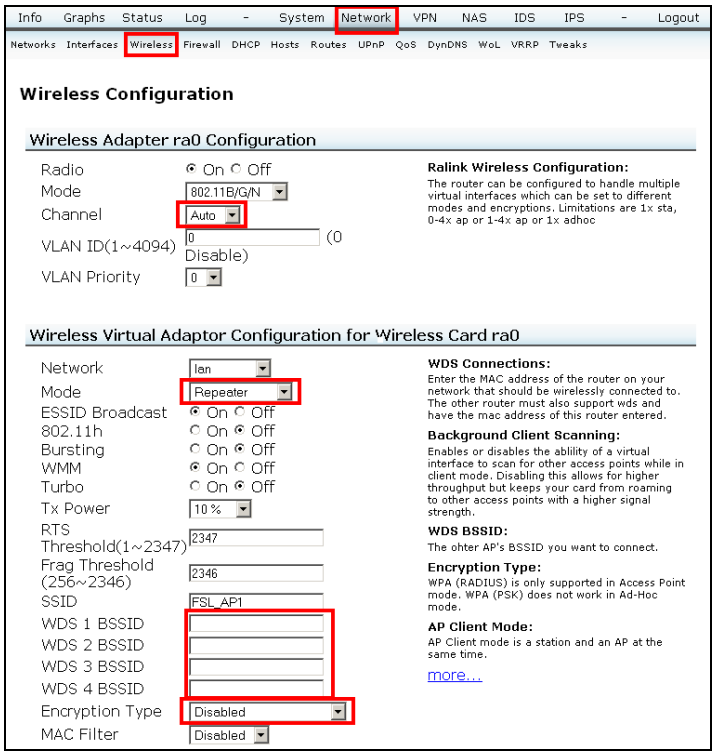
Figure 3-28. Repeater Mode



Perform the following steps in the **Wireless Configuration** page Figure 3-29. (Navigation: **Network** > **Wireless**, if necessary.)

1. From the **Channel** drop-down list, select a channel to match the other EWLAN channel. (The channel setting must be the same for both EWLANs.)
2. From the **Mode** drop-down list, select **Repeater**.
3. In the **SSID** field, type the AP's SSID.
4. In the **WDS [n] BSSID** fields, type the other WDS AP's BSSIDs. (Format: xx:xx:xx:xx:xx:xx)
5. From the **Encryption Type** drop-down list, select the AP's encryption.

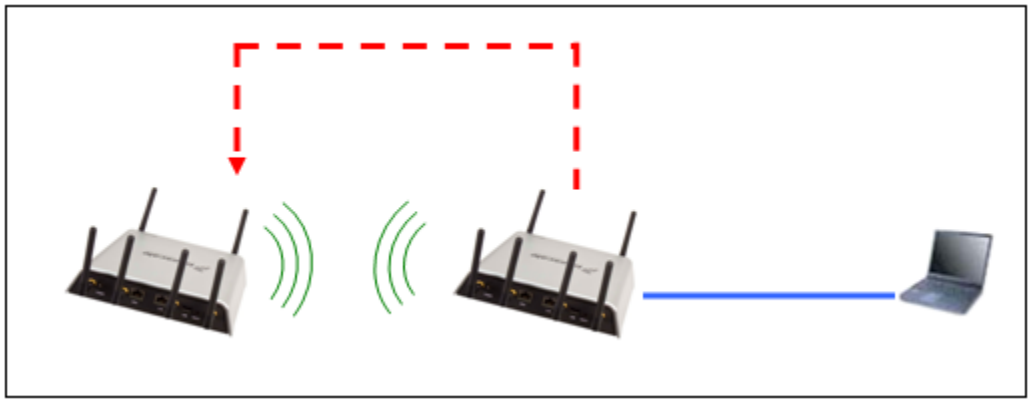
Figure 3-29. Repeater Mode Configuration, RA0 Section Shown



3.5.4 Configuring for AP Client Mode

An AP-Client can extend the wireless coverage of another wireless AP or router. However, AP-Client does not require the remote device to have WDS function. It can work with almost any wireless device. See Figure 3-30 for depiction.

Figure 3-30. AP Client Mode



Perform the following steps in the **Wireless Configuration** page Figure 3-31. (Navigation: **Network** > **Wireless**, if necessary.)

1. From the **Mode** drop-down list, select **AP Client**.

2. In the **SSID** field, type the **SSID** of the AP client unit.
3. From the **Encryption Type** drop-down list, select the **Encryption Type** of the AP client unit.
4. In the **AP's SSID** field, type the **AP's SSID** field of the AP client unit.
5. In the **AP's BSSID** 335 field, type the **AP's BSSID** (MAC address) field of the client unit.
6. From the **AP's Auth Mode** drop-down list, select the **AP's Auth Mode** of the AP client unit.

Figure 3-31. AP Client Mode Configuration

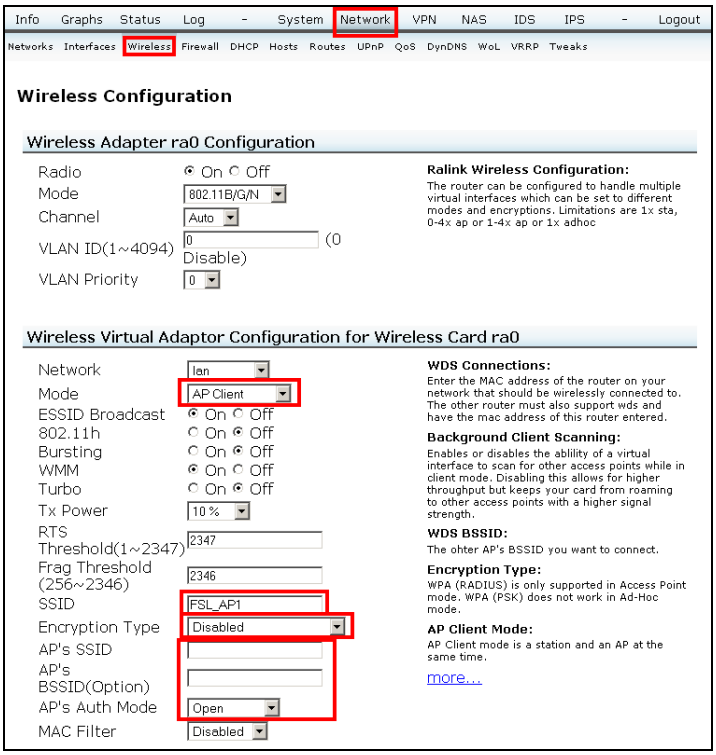
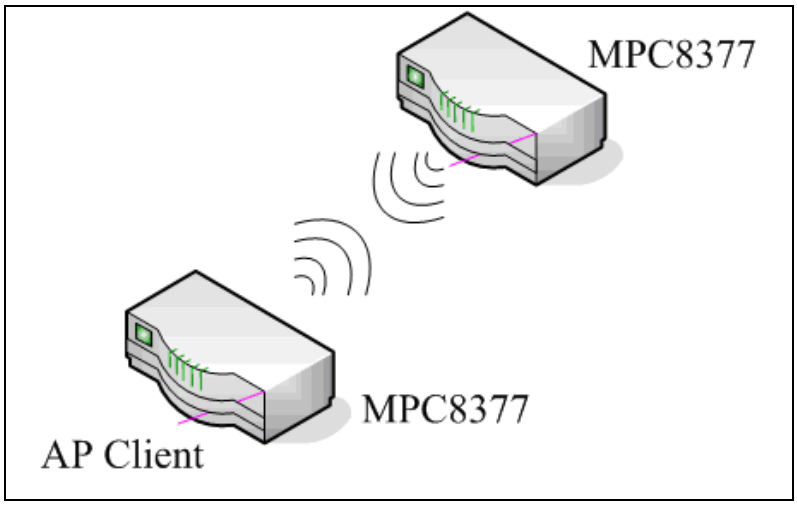


Figure 3-32 depicts an AP Client mode as follows: Two 8377 units are required. The SSID information used at the local 8377 AP Client is the same SSID information as the one used for the remote MPC8377, enabling them so that they can link together.

Figure 3-32. AP Client Mode Layout



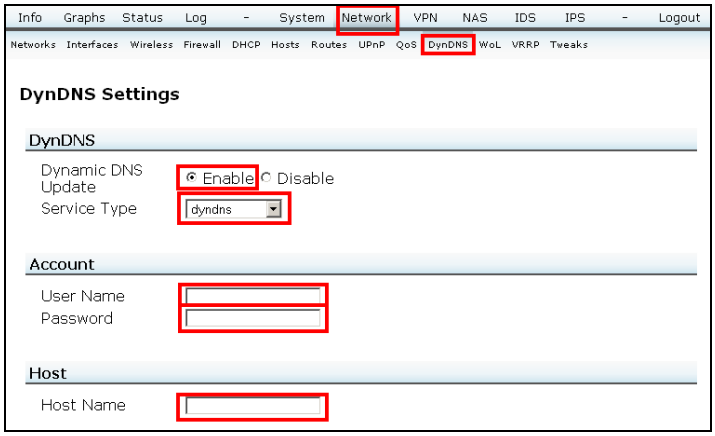
3.6 Selecting DynDNS Settings

Dynamic-DNS (Dynamic Domain Name System, also known as DDNS) allows a user to export a host name to the Internet through a DDNS server provider. Each time the MPC8377EWLAN wireless router connects to the Internet and gets an IP address from the ISP, this function updates your IP address to the DDNS service provider automatically. Any user on the Internet can access it through a predefined name registered in DDNS service provider.

Click **DynDNS** to enter the **DynDNS Settings** page (Figure 3-33), then perform the following steps:

1. Under the DynDNS section, click **Enable** for **Dynamic DNS Update**.
2. From the **Service Type** drop-down list, select **dyndns**.
3. Under the **Account** section, in the **User Name** text box type the user name.
4. In the **Password** text box, type the password.
5. Under the **Host** section, in the **Host Name** text box, type the host name.

Figure 3-33. DynDNS Settings

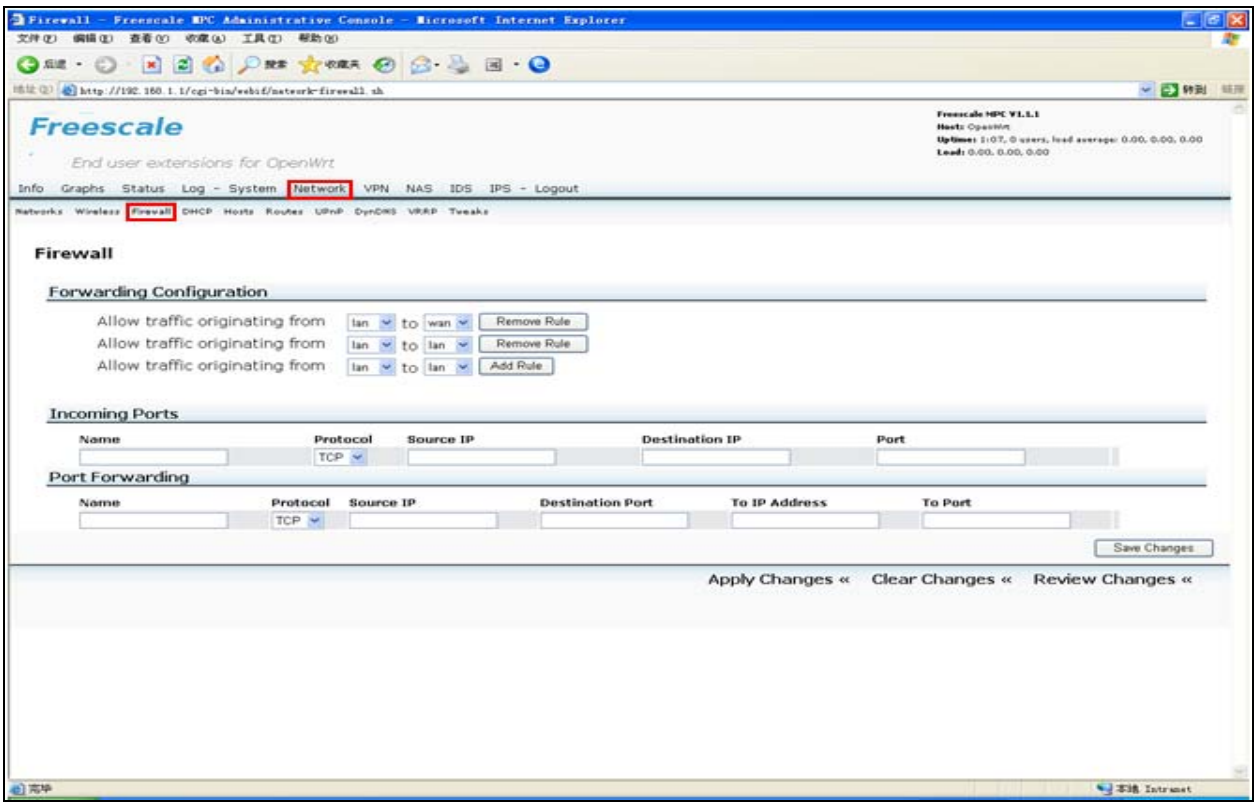


3.7 Firewalls

Firewall prevents unauthorized access to or from a private network. You can configure MPC8377EWLAN as Firewall to prevent unauthorized Internet users accessing your private networks connected to the Internet.

Click **Network** > **Firewall** to open the Firewall configuration page (Figure 3-34).

Figure 3-34. Firewall Configuration



3.7.1 Forwarding Configuration

The forwarding configuration should be set when the package traffic function is effect between ethernet ports. You can add rules from LAN to WAN or from WAN to LAN under Forwarding Configuration section. (See Figure 3-34) For example, to forward internet packets from one network to another, follow the process given below:

1. Add Rule **Allow traffic originating from WAN to LAN** and **Allow traffic originating from LAN to LAN**.
2. In the **Ports Forwarding** column, add PC1 IP address in **Source IP**, add PC2 IP address in **To IP Address** and Port number (set as 69).
3. Setup a tftp sever on PC2 and a tftp client on PC1(fill PC2's IP address in the Host IP column). Both of there ports of tftp are set as 69.
4. Use the tftp software; PC1 can transfer any file to PC2 successfully.

3.7.2 Incoming Ports

The Incoming Port screen allows you to customize incoming ports. (Figure 3-35) The incoming ports configuration should be set when the client on board is using TCP (or other protocol) port XXX, the incoming package data via port XXX would to be allowed.

Figure 3-35 Incoming Ports

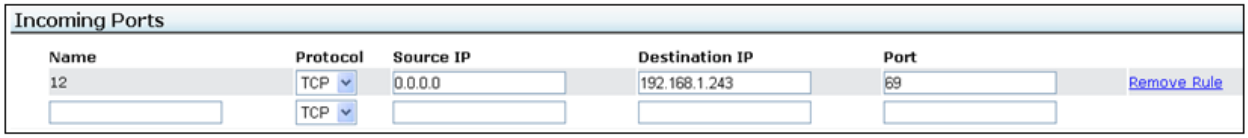


Table 3-3 describes each of the Incoming ports option.

Table 3-3 Incoming Ports

Options	Description
Name	Enter the name of the port.
Protocol	Select the protocol used for this application from the drop-down list. You can select TCP, UDP or Both as a protocol.
Source IP	Enter the source IP.
Destination IP	Enter the destination IP.
Port	Enter the port address.
Remove Rule	Click this link to remove the rule.

3.7.3 Port Forwarding

Sometimes referred to as port mapping, It is the act of forwarding a network port from one network node to another. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside via a NAT-enabled router.

Figure 3-36 Port Forwarding

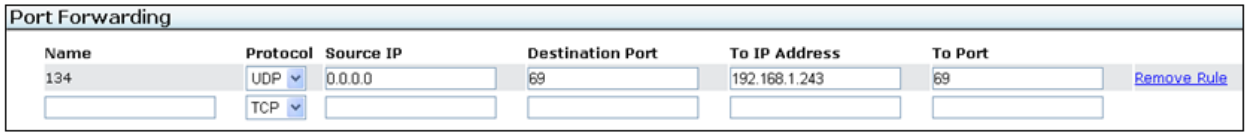


Table 3-4 describes each of the Incoming ports option.

Table 3-4 Port Forwarding

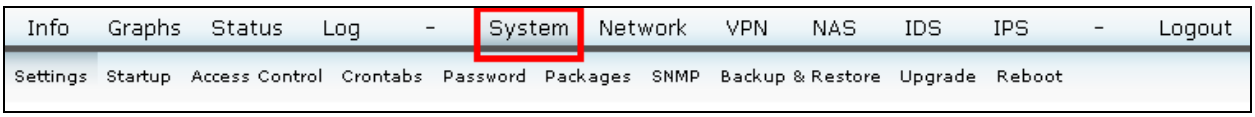
Options	Description
Name	Enter the name of the port.
Protocol	Select the protocol used for this application from the drop-down list. You can select TCP, UDP or Both as a protocol.
Source IP	Enter the source IP.
Destination IP	Enter the destination IP.
To IP Address	Enter the IP address.
Port	Enter the port address.
Remove Rule	Click this link to remove the rule.

Click **Save Changes** to apply your changes.

4 Selecting or Changing System Items

This section explains selecting or changing system items as follows: Settings, Password, Firmware Upgrade, and Reboot. Click **System** (Figure 4-1), then proceed with the respective sections.

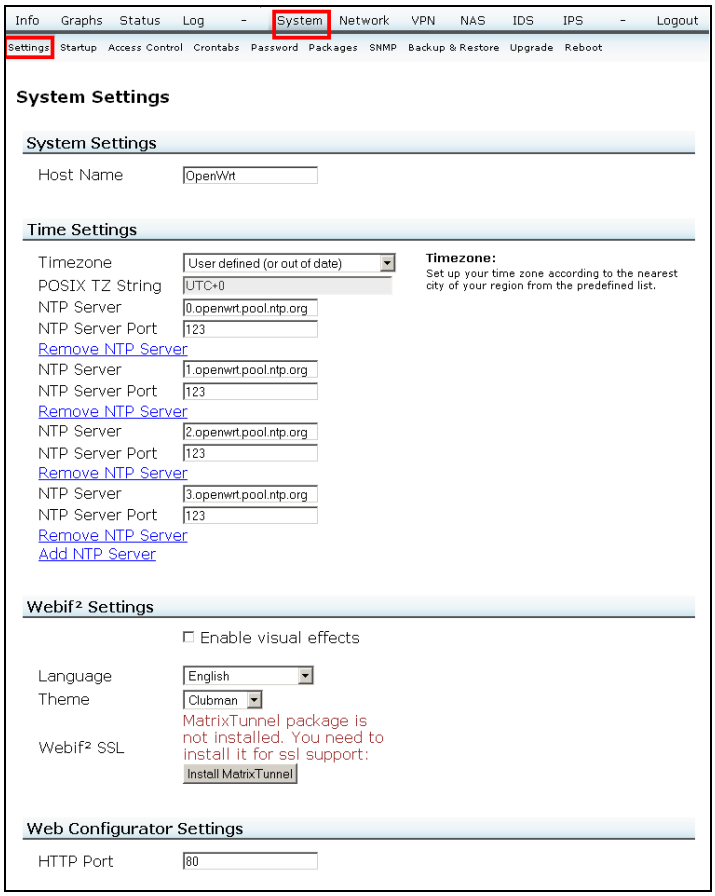
Figure 4-1. System



4.1 Settings

Click **Settings**. Figure 4-2 depicts the **System > Settings** window. Type the host name and select your time zone or closest region.

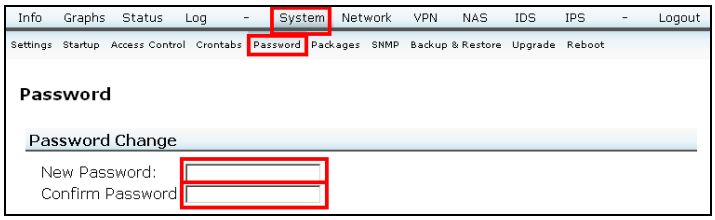
Figure 4-2. System Settings



4.2 Password

Click **Password**. Figure 4-3 depicts the **System > Password** window. Type the new login password in both the **New Password** and **Confirm Password** fields. This is the password used for logging into the web configuration page.

Figure 4-3. Password



4.3 SNMP

The Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment (example, routers), computer equipment and even devices like UPS.

Click **SNMP**. Figure 4-34 depicts the **System > SNMP** window, Configure the Simple Network Management Protocol settings. You can use management software to read or write information from or to the device.

Figure 4-4 SNMP Settings

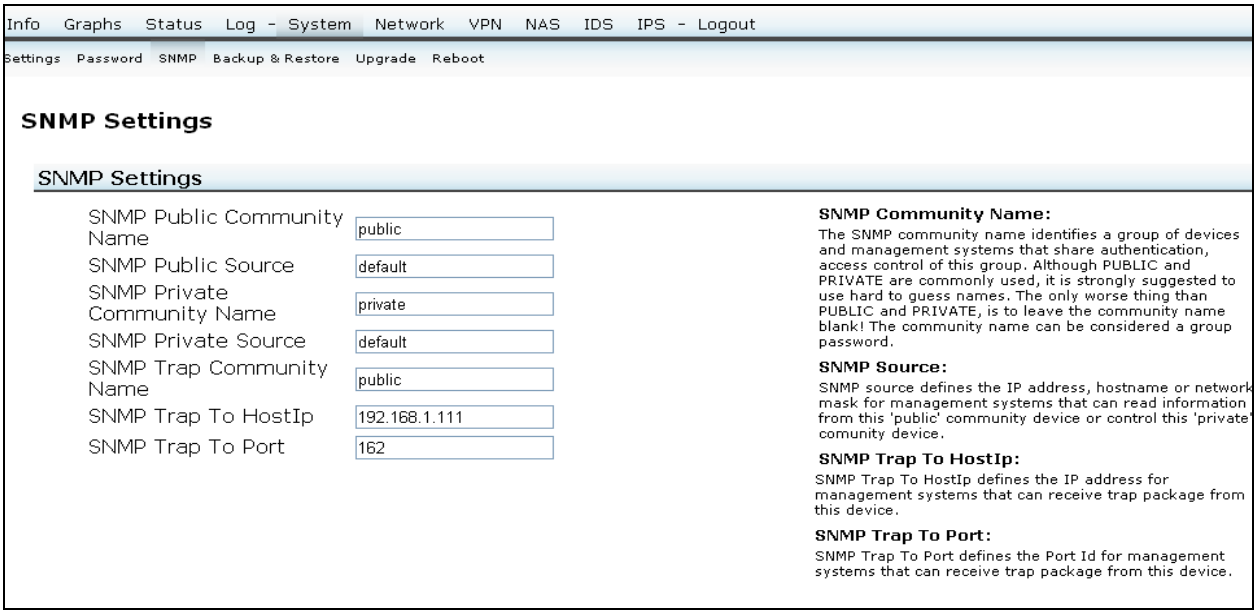


Table 4-1 describes each SNMP setting options in detail.

Table 4-1 SNMP Settings

Options	Description
SNMP Public Community Name	It identifies a group of devices and management systems that can read configure information of system by SNMP “Get” commands.
SNMP Public Source	It identifies the IP address, hostname or network mask for management systems that can read information by this 'public' community.
SNMP Private Community Name	It identifies a group of devices and management systems that can modify configure information of system by SNMP “Set” commands
SNMP Private Source	It identifies the IP address, hostname or network mask for management systems that can modify information by this 'private' community
SNMP Trap Community Name	It identifies the community string to be used when sending traps by SNMP "Trap" commands.
SNMP Trap To HostIp	It defines the IP address for management systems that can receive trap package from this device..
SNMP Trap To Port	It identifies the Port number for management systems that can receive trap package from this

	device at this port.

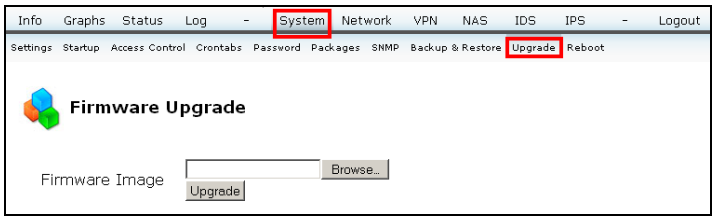
4.4 Firmware Upgrade

Click **Upgrade**. Figure 4-5 depicts the **System > Firmware Upgrade** window. Click **Browse** to locate the new firmware, then click **Upgrade** to change the firmware.

NOTE

Upgrading firmware may take a few minutes. Do not turn off the power nor invoke any resets, such as pressing the reset button).

Figure 4-5. Firmware Upgrade

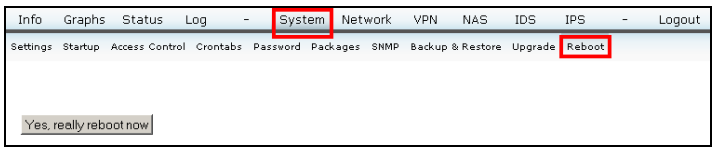


Click **Save Changes**, if certain. (There are also the following options: **Apply Changes**, **Clear Changes**, **Review Changes**.)

4.5 Reboot

Click **Reboot**. Figure 4-6 depicts the **System > Reboot** window. Click **Yes, really reboot now** button to reboot the router.

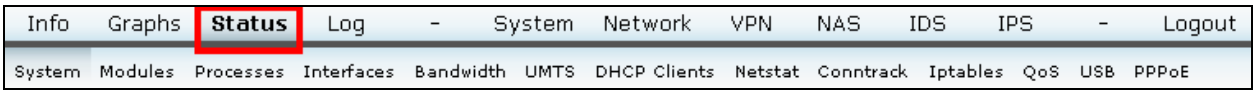
Figure 4-6. Reboot



5 Status

This section explains viewing the unit's status. Click **Status** (Figure 4-1), then proceed with the respective sections.

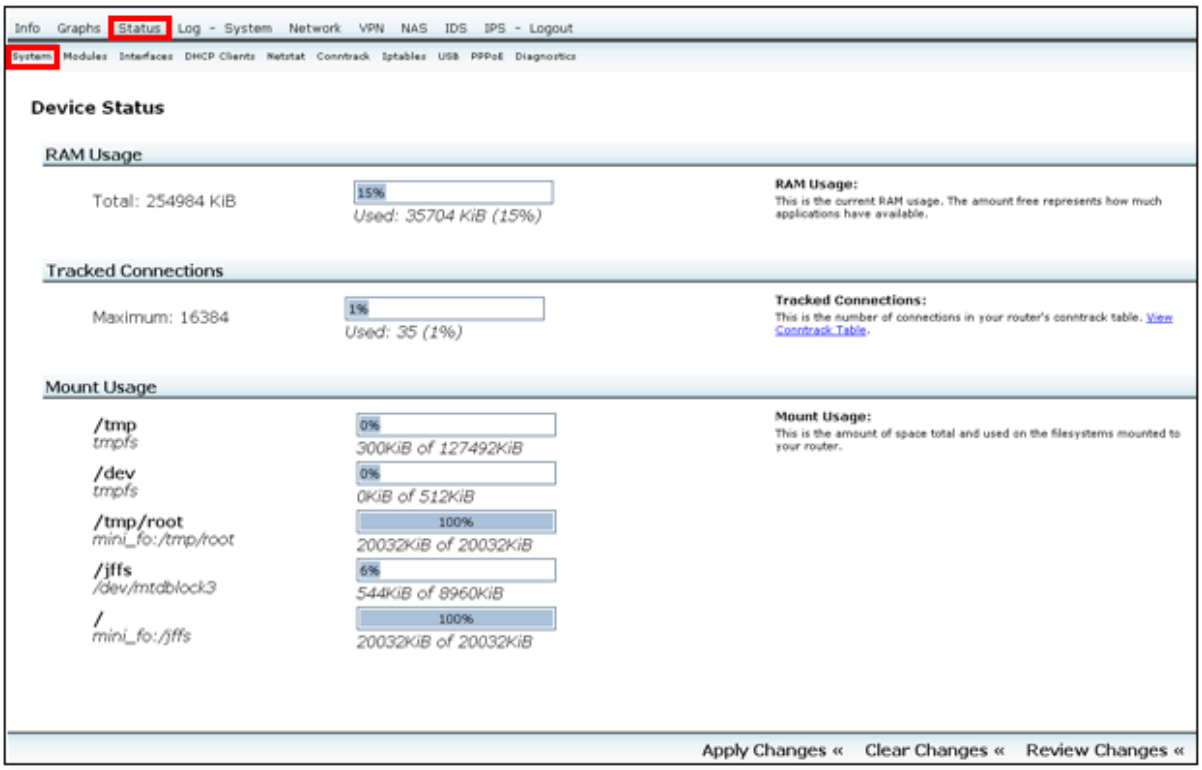
Figure 5-1. System



5.1 System

This section describes the status of device. (Figure 5-2)

Figure 5-2 Device Status



5.1.1 RAM Usage

This section displays the current RAM usage. It also tells the total available RAM and percentage of used RAM. (Figure 5-2)

5.1.2 Tracked Connections

This section displays the number of connections in your router's conntrack table (Figure 5-2). You can click the **View Conntrack Table** link to jump to Conntrack Table page.

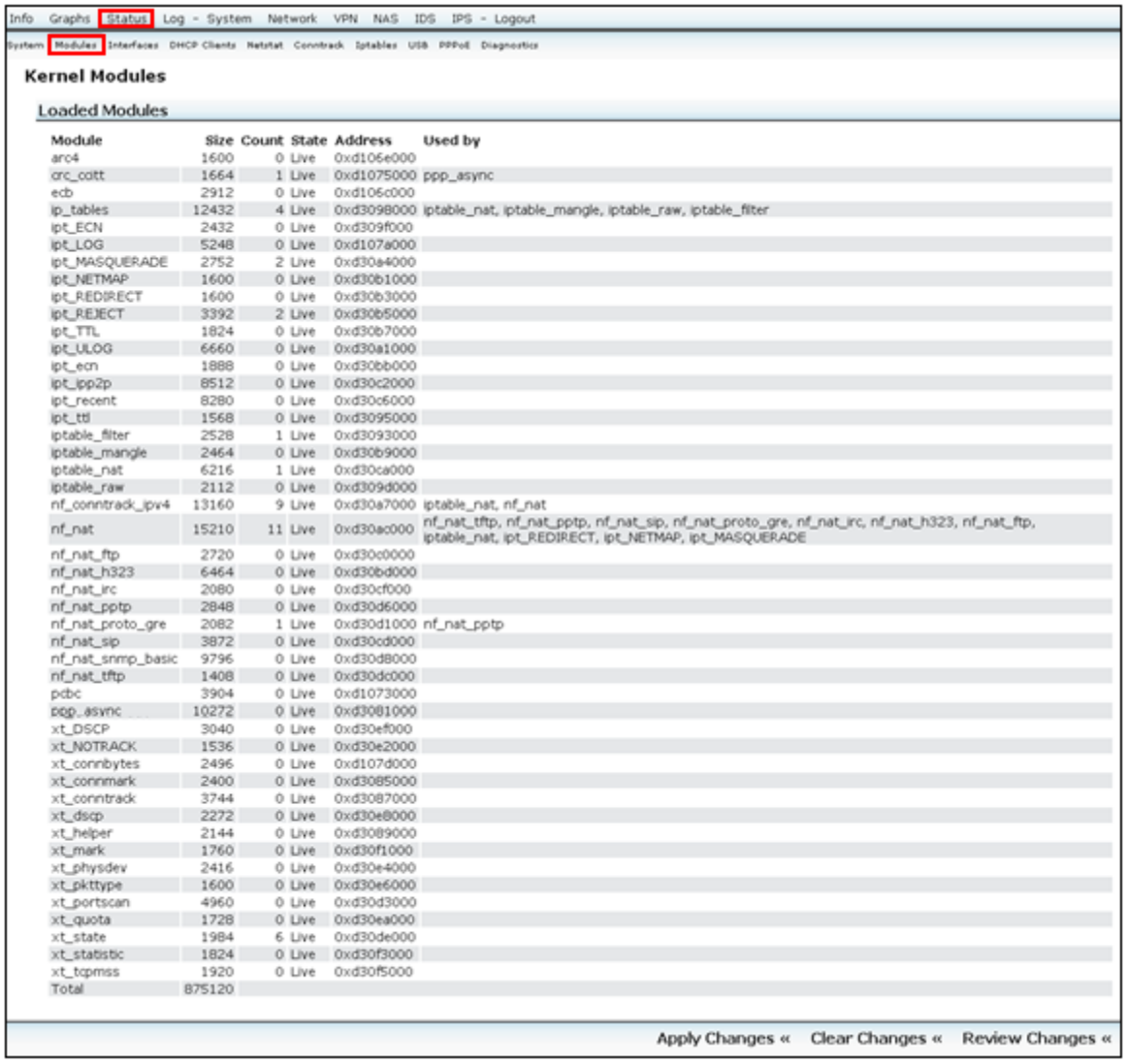
5.1.3 Mount Usage

This section displays the total amount of space and used on the file systems mounted to your router (Figure 5-2).

5.2 Modules

Click **Modules**. Figure 5-3 displays information about kernel modules. It displays all the loaded modules and provide information about module name, size, count, state, address and used by.

Figure 5-3 Kernel Modules



Module	Size	Count	State	Address	Used by
arc4	1600	0	Live	0xd106e000	
crc_ccitt	1664	1	Live	0xd1075000	ppp_async
ecb	2912	0	Live	0xd106c000	
ip_tables	12432	4	Live	0xd3098000	iptable_nat, iptable_mangle, iptable_raw, iptable_filter
ipt_ECN	2432	0	Live	0xd309f000	
ipt_LOG	5248	0	Live	0xd107a000	
ipt_MASQUERADE	2752	2	Live	0xd30a4000	
ipt_NETMAP	1600	0	Live	0xd30b1000	
ipt_REDIRECT	1600	0	Live	0xd30b3000	
ipt_REJECT	3392	2	Live	0xd30b5000	
ipt_TTL	1824	0	Live	0xd30b7000	
ipt_ULOG	6660	0	Live	0xd30a1000	
ipt_ecn	1888	0	Live	0xd30bb000	
ipt_ipp2p	8512	0	Live	0xd30c2000	
ipt_recent	8280	0	Live	0xd30c6000	
ipt_ttl	1568	0	Live	0xd3095000	
iptable_filter	2528	1	Live	0xd3093000	
iptable_mangle	2464	0	Live	0xd30b9000	
iptable_nat	6216	1	Live	0xd30ca000	
iptable_raw	2112	0	Live	0xd309d000	
nf_conntrack_ipv4	13160	9	Live	0xd30a7000	iptable_nat, nf_nat
nf_nat	15210	11	Live	0xd30ac000	nf_nat_tftp, nf_nat_pptp, nf_nat_sip, nf_nat_proto_gre, nf_nat_irc, nf_nat_h323, nf_nat_ftp, iptable_nat, ipt_REDIRECT, ipt_NETMAP, ipt_MASQUERADE
nf_nat_ftp	2720	0	Live	0xd30c0000	
nf_nat_h323	6464	0	Live	0xd30bd000	
nf_nat_irc	2080	0	Live	0xd30cf000	
nf_nat_pptp	2848	0	Live	0xd30d6000	
nf_nat_proto_gre	2082	1	Live	0xd30d1000	nf_nat_pptp
nf_nat_sip	3872	0	Live	0xd30cd000	
nf_nat_snmp_basic	9796	0	Live	0xd30d8000	
nf_nat_tftp	1408	0	Live	0xd30dc000	
pcbc	3904	0	Live	0xd1073000	
ppp_async	10272	0	Live	0xd3081000	
xt_DSCP	3040	0	Live	0xd30ef000	
xt_NOTRACK	1536	0	Live	0xd30e2000	
xt_connbytes	2496	0	Live	0xd107d000	
xt_connmark	2400	0	Live	0xd3085000	
xt_conntrack	3744	0	Live	0xd3087000	
xt_dscp	2272	0	Live	0xd30e8000	
xt_helper	2144	0	Live	0xd3089000	
xt_mark	1760	0	Live	0xd30f1000	
xt_physdev	2416	0	Live	0xd30e4000	
xt_pkttype	1600	0	Live	0xd30e6000	
xt_portscan	4960	0	Live	0xd30d3000	
xt_quota	1728	0	Live	0xd30ea000	
xt_state	1984	6	Live	0xd30de000	
xt_statistic	1824	0	Live	0xd30f3000	
xt_tcpmss	1920	0	Live	0xd30f5000	
Total	875120				

5.3 Interfaces

Click **Interfaces**. Figure 5-4 depicts the **Status > Interfaces** window and various interface settings.

Figure 5-4. Reboot

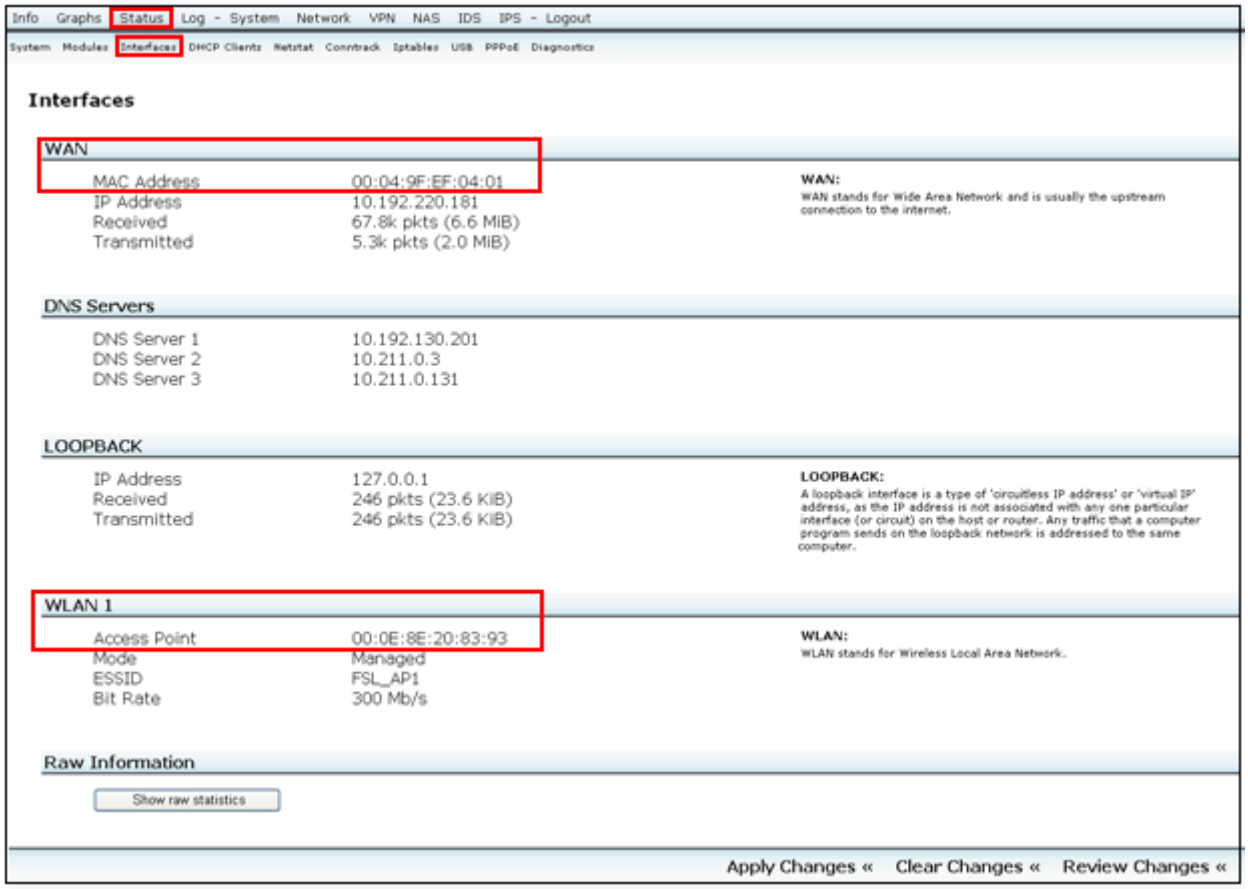


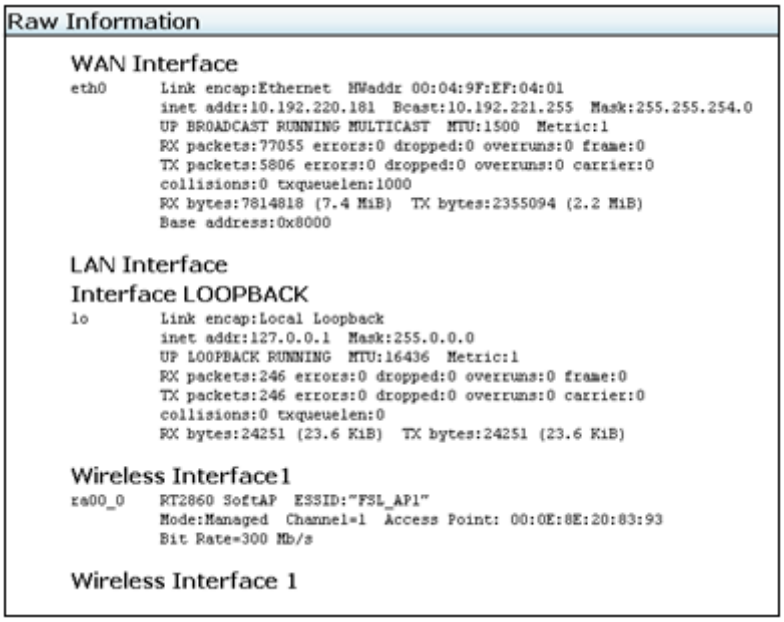
Table 5-1 describes each of the section of Interfaces page.

Table 5-1 Interfaces

Option	Description
WAN	WAN stands for Wide Area Network and is usually the upstream connection to the internet.
DNS Server	It displays the DNS server details.
LOOPBACK	A loopback interface is a type of 'circuit less IP address' or 'virtual IP' address, as the IP address is not associated with any one particular interface (or circuit) on the host or router. Any traffic sent by computer program on the loopback network is addressed to the same computer.
WLAN 1	WLAN stands for Wireless Local Area Network. It displays WLAN 1 details.
RAW Information	It displays the raw information. (Figure 5-5)

Click the **Show raw statistics** button, to view the **Raw Information** page at the bottom of the page. (Figure 5-5)

Figure 5-5 Raw Information



5.4 DHCP Clients

Click **DHCP Clients**. Figure 5-6 displays the DHCP leases.

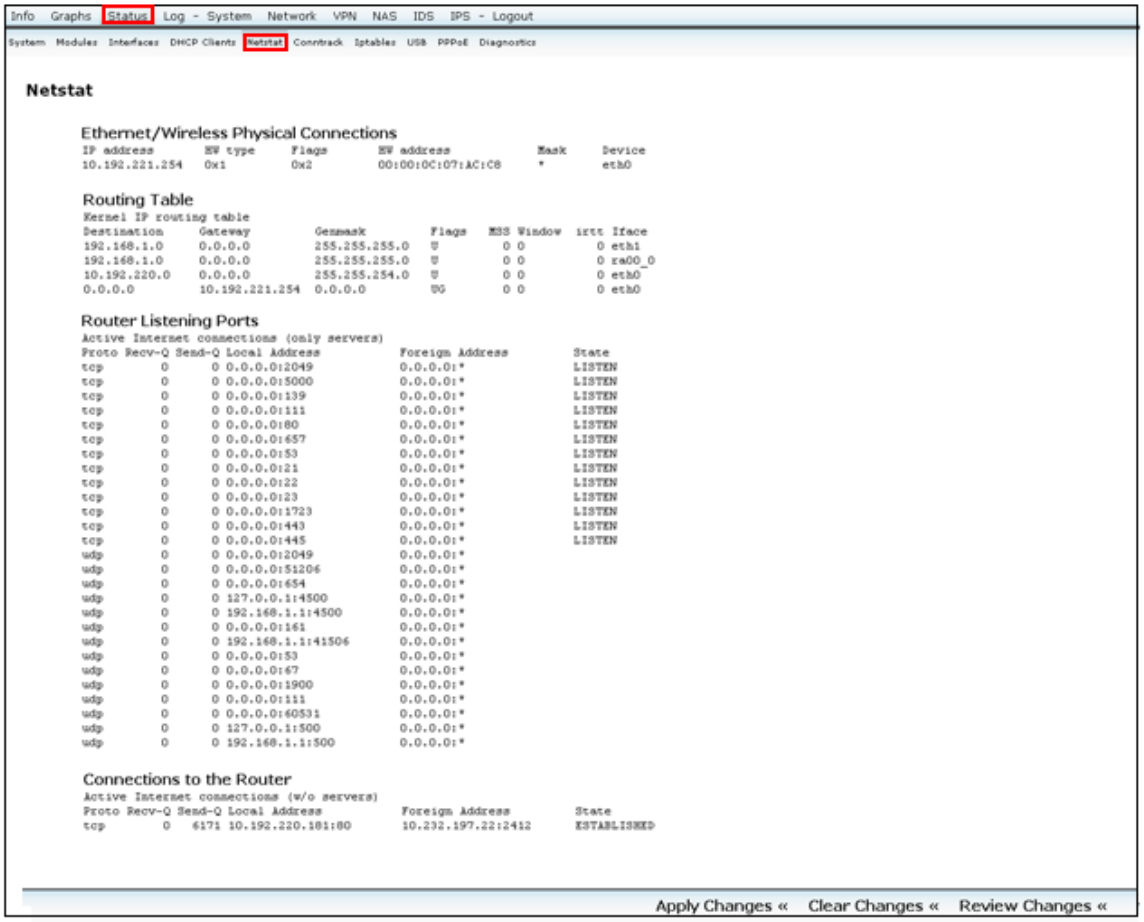
Figure 5-6 DHCP Clients

DHCP leases are assigned to network clients that request an IP address from the DHCP server of the router. Clients, who have requested their IP lease before this router, was rebooted and may not be listed until they request a renewal of their lease.

5.5 Netstat

Click **Netstat**. Figure 5-7 displays the detailed information about Ethernet/Wireless physical connections, routing table, router listening ports and connections to the routers.

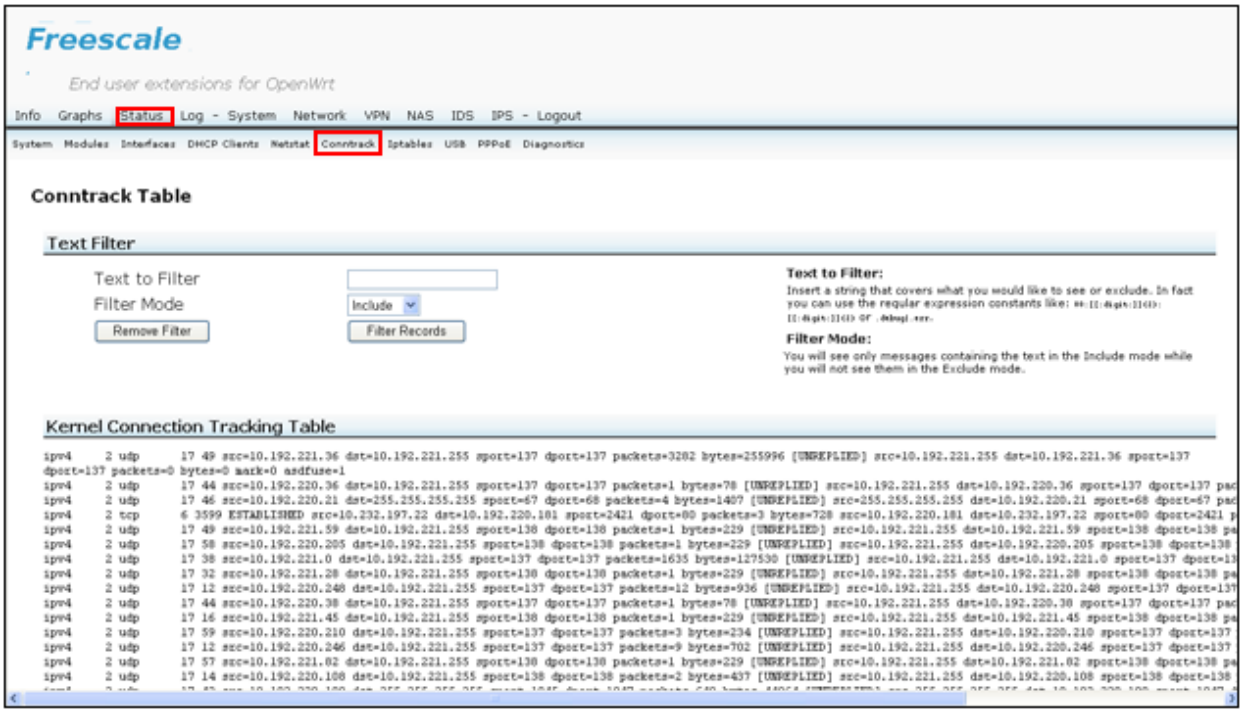
Figure 5-7 Netstat



5.6 Conntrack

Click **Conntrack**. Figure 5-8 displays conntrack table.

Figure 5-8 Conntrack

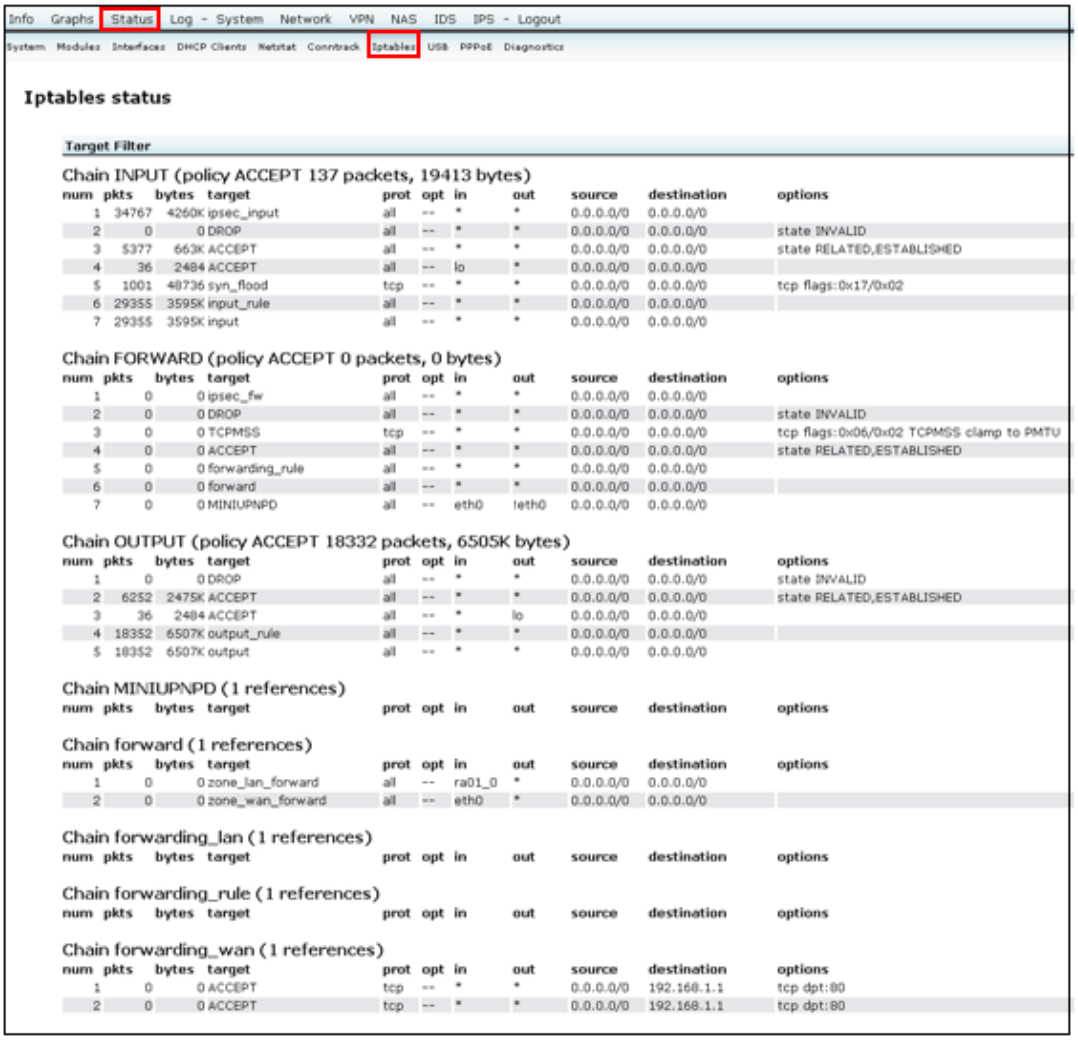


1. Insert a string to include or exclude in the **Text to Filter** text box. You can also type the regular expression constants like: 00:[[:digit:]]{2}:[[:digit:]]{2} or debug|.err
2. From the **Filter Mode** drop-down list, select **Include** or **Exclude** option.
3. Click **Remove Filter** button to remove the filter option that you have selected.
4. Click **Filter Records** button to filter the records.

5.7 Iptables

Click **Iptables**. Figure 5-9 displays iptables status.

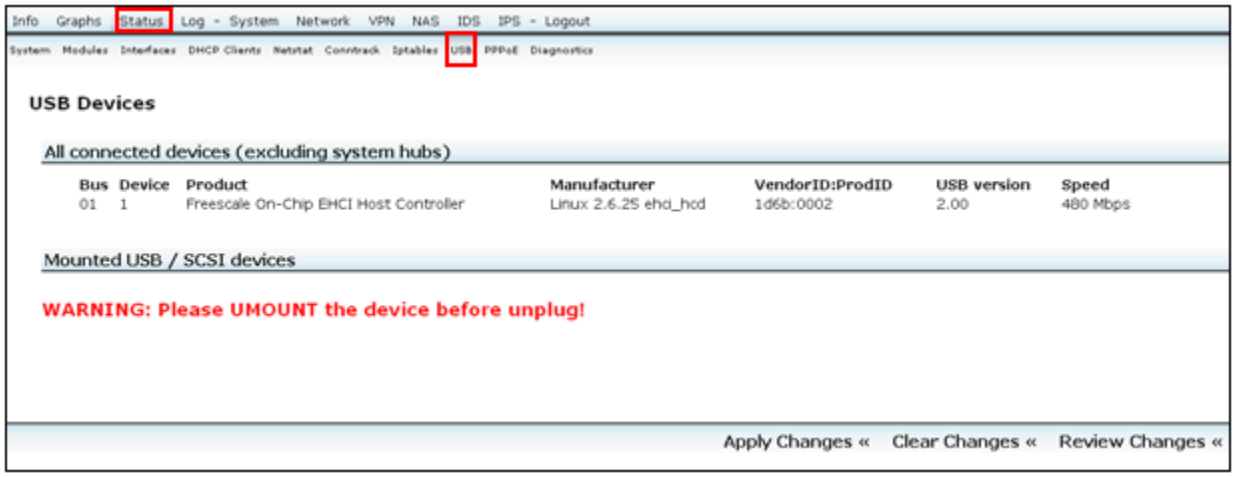
Figure 5-9 Iptables



5.8 USB

Click **USB**. Figure 5-10 displays the information about all the connected devices (excluding system hubs) and mounted USB/SCSI devices.

Figure 5-10 USB



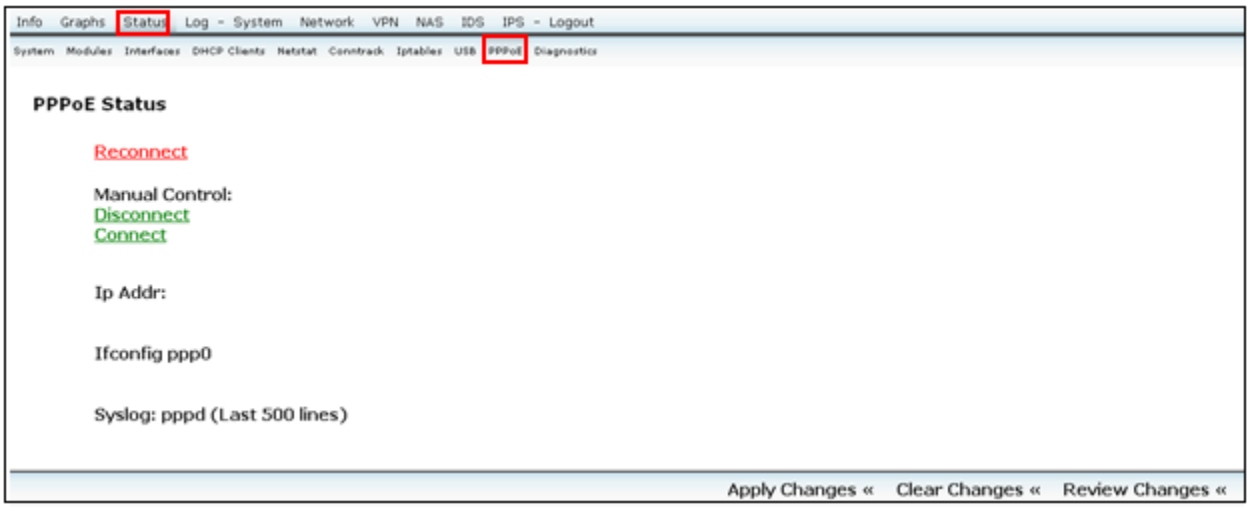
Warning!

You must umount the device before unplug.

5.9 PPPoE

Click **PPPoE**. Figure 5-11 displays the PPPoE status.

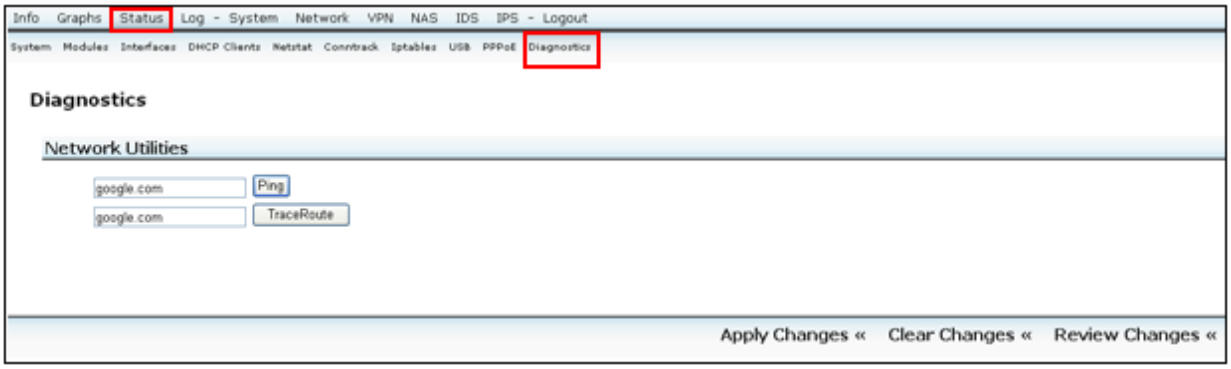
Figure 5-11 PPPoE



5.10 Diagnostics

Click **Diagnostics**. Figure 5-12 displays the network utilities options to ping and trace route.

Figure 5-12 Diagnostics



6 VPN

Virtual Private Network (VPN) is a security measure that creates a secure connection between two remote locations. There are two basic ways to create a VPN connection:

- VPN Router to VPN Router
- Computer (using VPN client software) to VPN Router

VPN Router to VPN Router:

For example, at home, a telecommuter uses his VPN router to connect to the Internet. He configures his router with office VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPN utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he is physically connected.

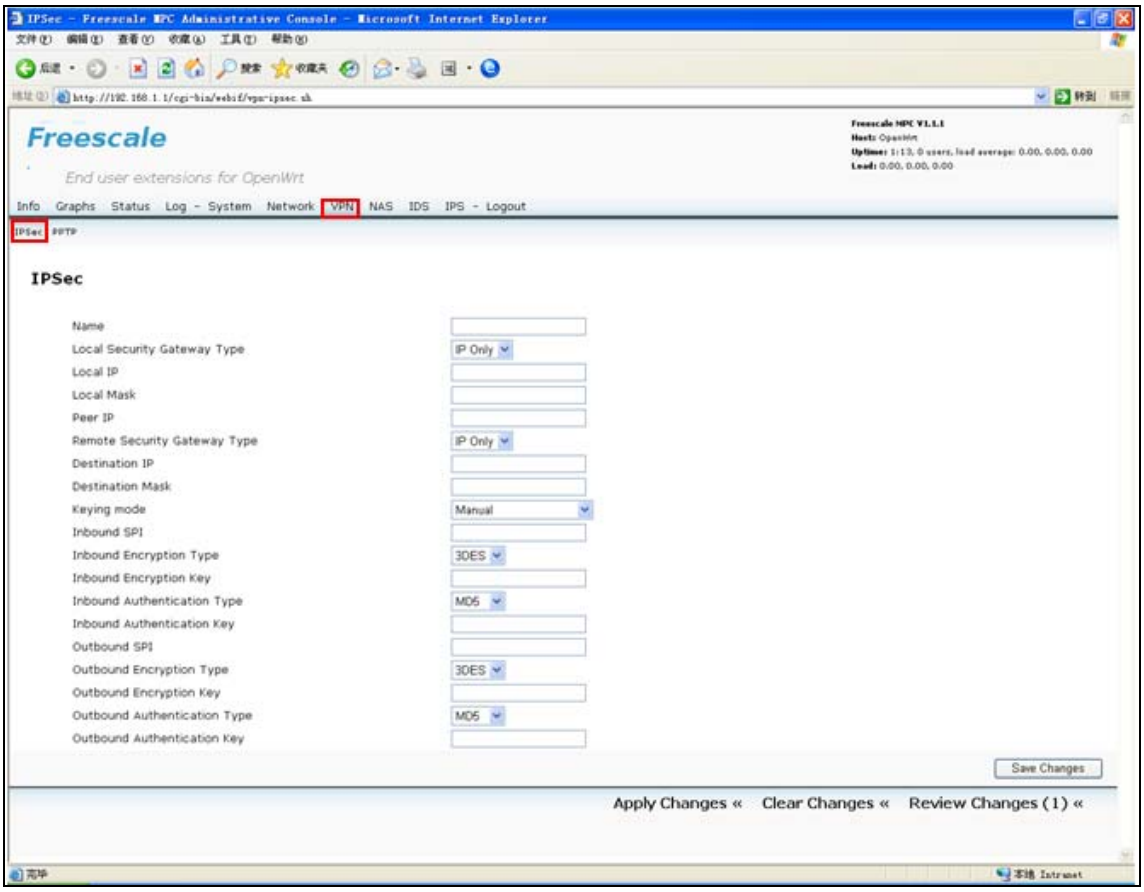
Computer (using VPN client software) to VPN Router:

For example, a traveling businessperson from her hotel room dials up her ISP. Her notebook computer has VPN client software, which is configured with her office's IP address. She accesses the VPN client software and connects to the VPN Router at the central office. Using the VPN, the businessperson now has a secure connection to the central office's network, as if she is physically connected.

Now, configure following settings to create VPN tunnels.

Click **VPN** (Figure 6-1) and then proceed with the respective sections.

Figure 6-1. VPN > IPSec page



6.1 IPSec

The VPN Router can create one or multiple tunnels (or secure channel) that each connect between two endpoints, so that the transmitted data or information between these endpoints is secure.

Virtual Private Network (VPN) is a security measure that creates a secure connection between two remote locations. Configure these settings so the Gateway will create VPN tunnels.

Click **VPN > IPSec** to open the IPSec page (Figure 6-1).

The table below explains each of the option present in IPSec page.

Function	Description
Name	Enter name of tunnel, The name should be unique.
Local Security Gateway Type	Select IP only or IP + domain from the Local Security Gateway Type drop-down list. Incase, you select IP Only, then only the specific IP Address will be able to access the tunnel.

Local IP	Enter the Local IP address.
Local Mask	Enter the mask to determine the IP addresses on the local network.
Peer IP	Enter the peer IP address of tunnel.
Remote Security Gateway Type	Select IP only or IP + domain from the Remote Security Gateway Type drop-down list. Incase, you select IP Only, then only the specific IP Address will be able to access the tunnel.
Destination IP	Enter the destination IP address.
Destination Mask	Enter the mask to determine the IP addresses on the Destination network.
Keying Mode	Select the keying mode from the Keying Mode drop-down list. You can select Manual or Preshared Key mode. See section 6.1.1 Keying Mode for details.

6.1.1 Keying Mode – IKE Config

The router supports both IKE with Preshared Key (automatic) and Manual key management. When choosing automatic key management, IKE (Internet Key Exchange) protocols are used to negotiate key material for SA. If manual key management is selected, no key negotiation is needed. The manual key management is used for small static environments or for troubleshooting purpose. Notice that both sides must use the same Key Management method.

6.1.1.1 IKE with Preshared Key

Select **IKE with preshared key** from **Keying mode** drop-down list. The options changes in the application page as shown in Figure 6-2 below:

Figure 6-2 IKE with Preshared Key

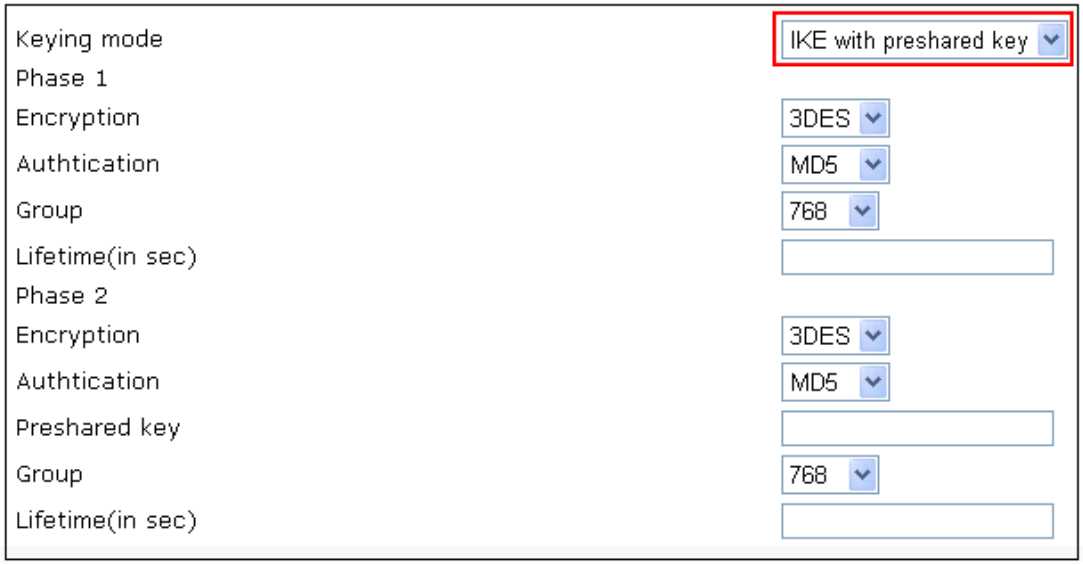


Table 6-1 describes the IKE with preshared key options for phase 1 and phase 2.

Table 6-1 Phase 1 and Phase 2

Function	Description
Phase 1	
Encryption	The encryption method determines the length of the key used to encrypt or decrypt the ESP packets. It supports 3DES. Notice that both sides of the VPN tunnel must use the same Encryption method.
Authentication	Authentication determines a method to authenticate the ESP packets. You can select MD5 or SHA1. Both sides of the VPN tunnel must use the same authentication method.
Group	This is for Diffie-Hellman key negotiation. There are 3 groups available for ISAKMP SA establishment, 768-bit, 1024-bit, 1536-bit. They represent different bits used in Diffie-Hellman mode operation*768-bit Group isn't support*.
Lifetime (in sec)	Specifies the lifetime of the IKE generated key.
Phase 2:	
Encryption	The encryption method determines the length of the key used to encrypt or decrypt ESP packets. It

	supports 3DES. Notice that both sides of the VPN tunnel must use the same encryption method.
Authentication	Authentication determines a method to authenticate the ESP packets. You can select MD5 or SHA1. Both sides of the VPN tunnel must use the same authentication method.
Group	This is for Diffie-Hellman key negotiation. There are 3 groups available for ISAKMP SA establishment; 768-bit, 1024-bit, 1536-bit. It represents different bits used in Diffie-Hellman mode operation. 768-bit Group isn't support.
Preshared Key	IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Only character values are acceptable in this field. Both sides must use the same Pre-shared Key.
Lifetime (in sec)	Specifies the lifetime of the IKE generated key.

6.1.2 Manual

Select **Manual** from **Keying mode** drop-down list. The options changes in the application page as shown in Figure 6-3 below:

Figure 6-3 Manual Keying Mode

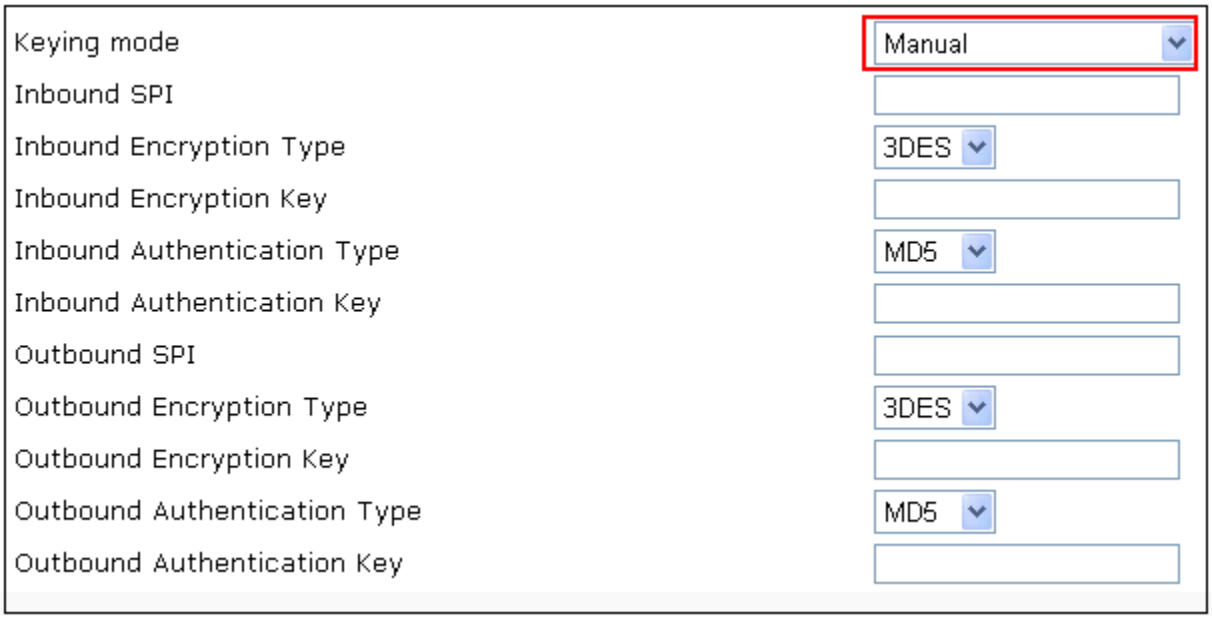


Table 6-2 describes the Manual keying mode.

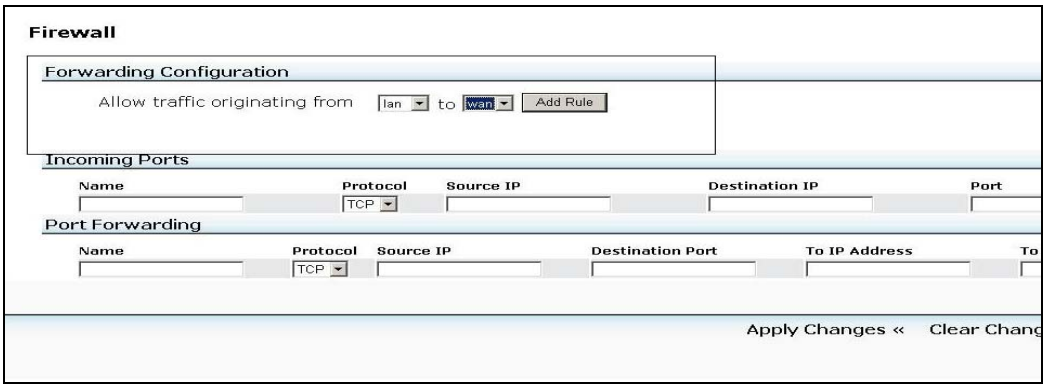
Table 6-2 Manual Keying Mode

Function	Description
Inbound/Outbound SPI	The SPI (Security Parameter Index) is carried in the ESP header. Its range is 256 -65535. Each tunnel must have an unique Inbound SPI and Outbound SPI. Notice that Inbound SPI must match the other router's Outbound SPI.
Inbound/ Outbound Encryption Type	The Encryption method determines the length of the key used to encrypt or decrypt ESP packets. It supports 3DES. Notice that both sides of the VPN tunnel must use the same encryption method.
Inbound/ Outbound Encryption Key	You should input 24 char, 8 char make up of a group, and the char of group should not be the same.
Inbound/ Outbound Authentication Type	Authentication determines a method to authenticate the ESP packets. You can select MD5 or SHA1. Both sides of the VPN tunnel must use the same authentication method
Inbound/ Outbound Authentication Key	This is an authentication Key. You should enter 16 char.

NOTE

Before establishing a VPN tunnel, the tunnel between local network and remote network must be connected. You should add a forward rule from LAN interface to WAN interface at Firewall tab as shown in Figure 6.4 below:

Figure 6-4 Firewall tab



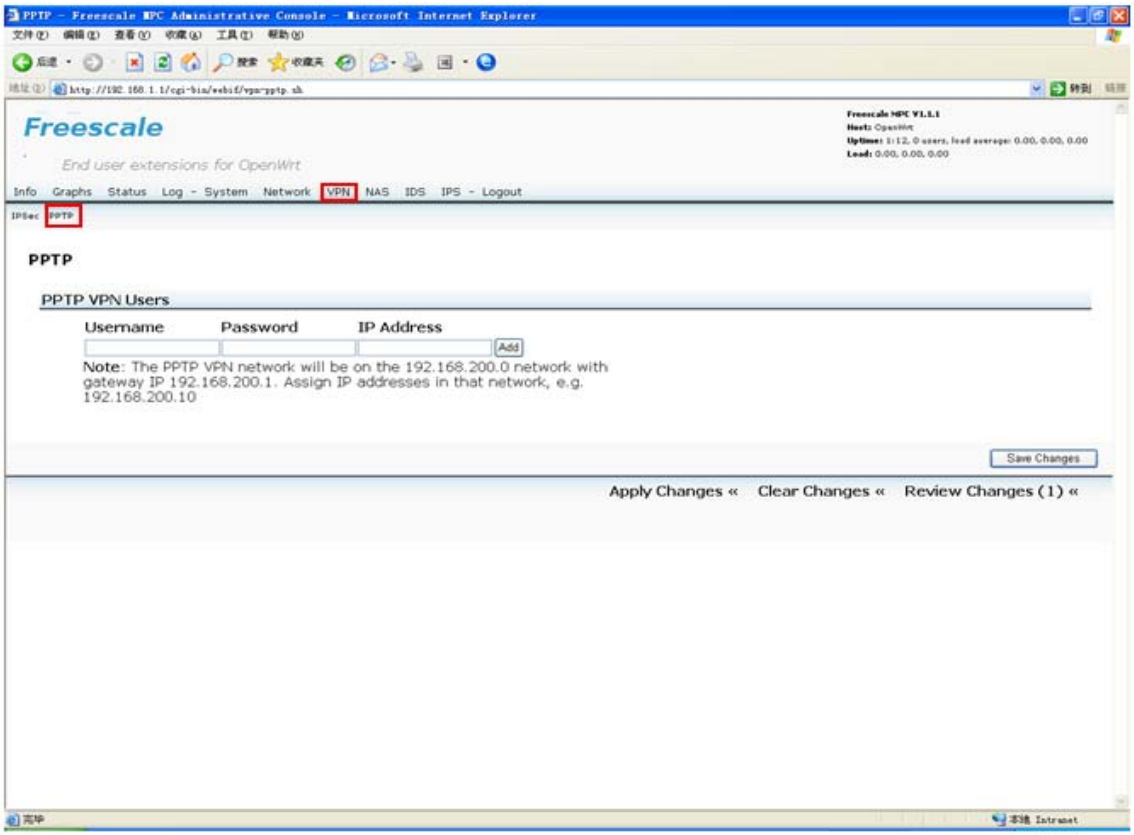
6.2 PPTP

Click **VPN** > **PPTP** to open the PPTP page (Figure 6-5).

Perform the following steps:

1. Enter the user name.
2. Enter the password.
3. Enter the IP Address.
4. Click **Add** to add the configuration
5. Click **Save Changes** to save the configuration data.

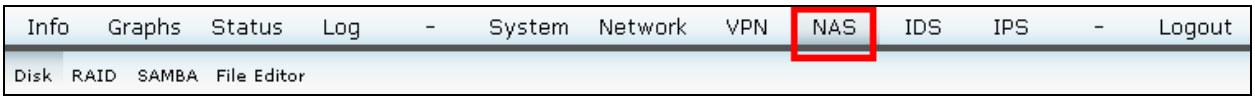
Figure 6-5 VPN > PPTP VPN User page



7 Managing Storage, Samba, and File Editing in NAS

This section explains managing storage and other related items in Network-Attached Storage (NAS): Disk, RAID (Redundant Array of Independent Disks), Samba, File Editor. Click **NAS** (Figure 7-1), then proceed with the respective sections.

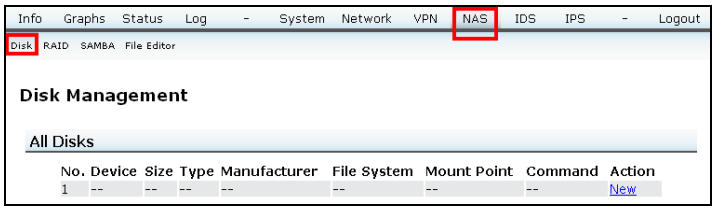
Figure 7-1. NAS



7.1 Disk Management

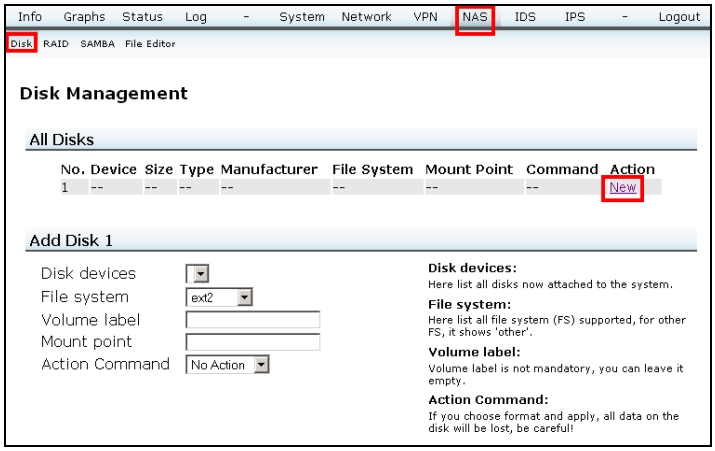
Click **Disk**. Figure 7-2 depicts the **NAS** > **Disk Management** window.

Figure 7-2. Disk Management



To add a new disk, click **New**. Figure 7-3 depicts the **NAS** > **Disk Management** > **New** window. Type in fields or select from drop-down lists as appropriate.

Figure 7-3. Add New Disk



The **Action Command** drop-down list includes the following possible actions besides **No Action**: **Format**, **Mount**, and **Umount**.

7.2 Format Disk

CAUTION

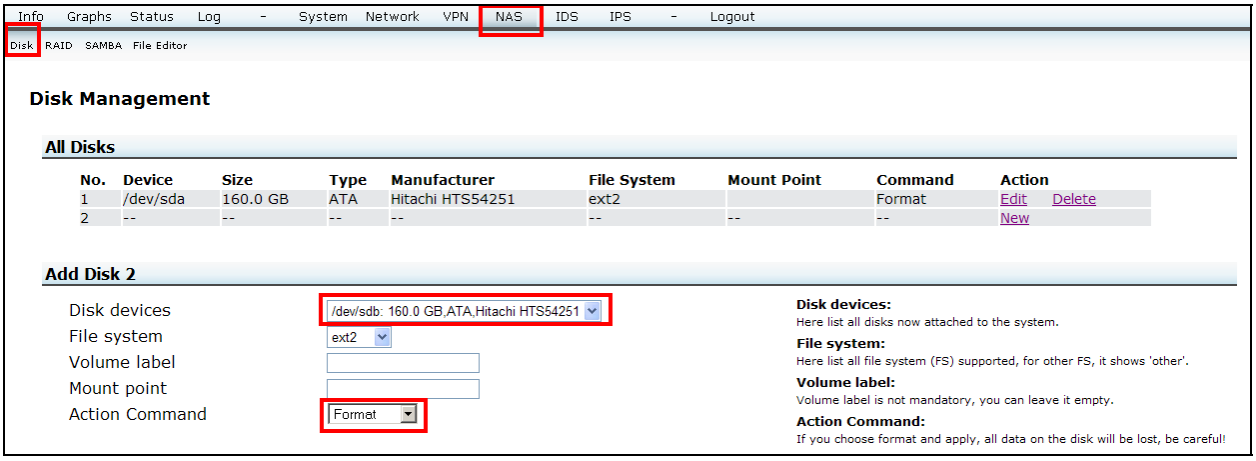
If you select **Format**, all data on the disk will be lost.

Perform the following steps, as depicted in Figure 7-4:

1. From the **Disk devices** drop-down list, select the device.

2. From the **Action Command** drop-down list, select **Format**.

Figure 7-4. Format Disk

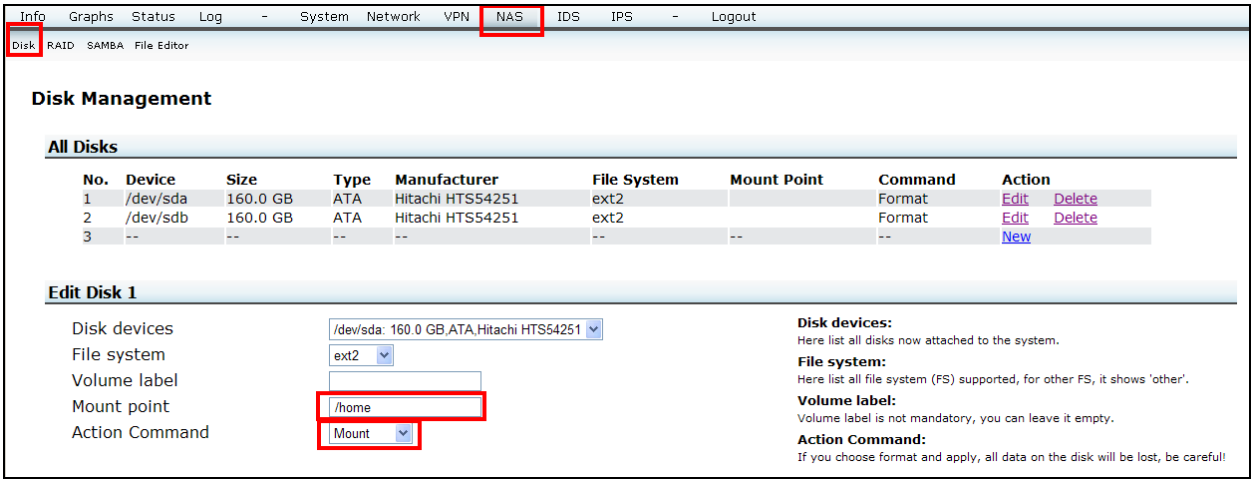


7.2.1 Mount Disk

Perform the following steps, as depicted in Figure 7-5.

1. In the **Mount point** field, type the address you want to mount. For example, **/home**.
2. From the **Action Command** drop-down list, select **Mount**.

Figure 7-5. Mount Disk

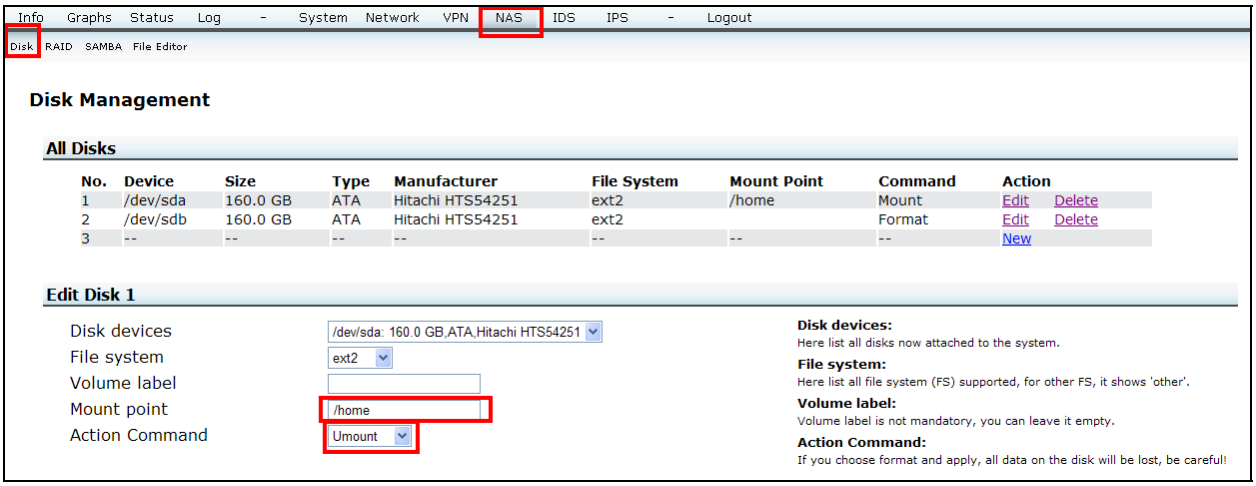


7.2.2 Unmount Disk

Perform the following steps, as depicted in Figure 7-6.

1. In the **Mount point** field, type the address where your disk is mounted.
2. From the **Action Command** drop-down list, select **Umount**.

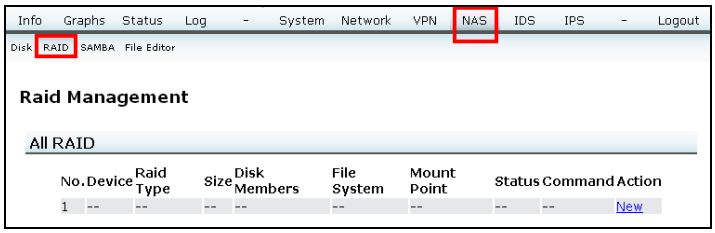
Figure 7-6. Unmount Disk



7.3 RAID Management

Click **RAID**. Figure 7-7 depicts the **NAS > RAID Management** window.

Figure 7-7. RAID Management



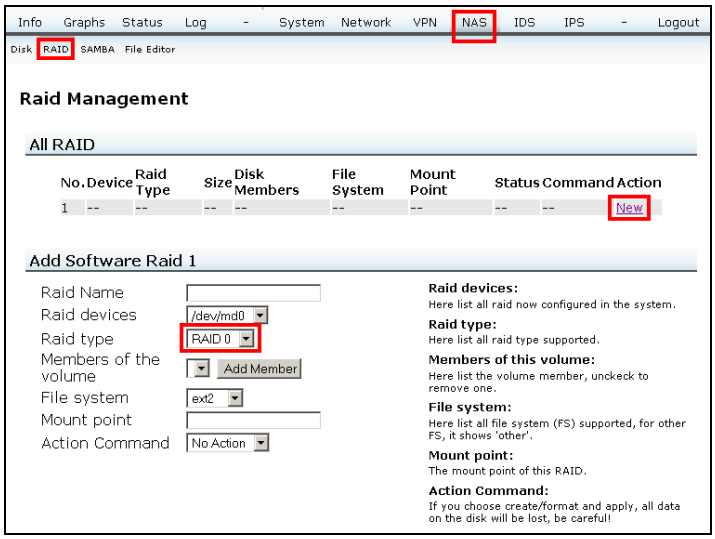
To add a new disk, click **New**. Figure 7-8 depicts the **NAS > RAID Management > New** window. Type in fields or select from drop-down lists as appropriate. The (Table 7-1) below explains each of the option present in RAID management window in detail.

Table 7-1 RAID Management

Option	Description
Raid Name	Enter the RAID name.
RAID devices	These are all the RAID devices attached to the system.
RAID type	These are all the RAID devices supported.
Members of this volume	These are all the members of the volume. Uncheck to remove.

File system	These are the entire file systems (FS) supported. “Other” represents other file systems
Mount point	This is the mount point of this RAID device.
Action Command	Caution: If you choose Create/Format, then all data is deleted from the disk.

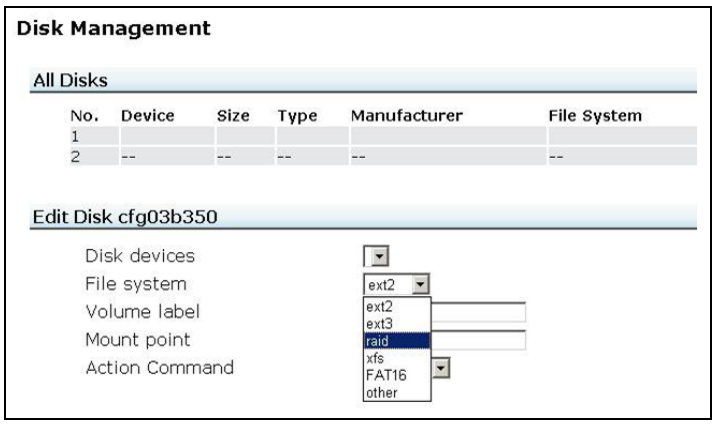
Figure 7-8. Add New RAID



NOTE

Before using RAID management, make sure that you have selected **RAID** in the **File system** drop-down list (Figure 7-9).

Figure 7-9. RAID File System Selection

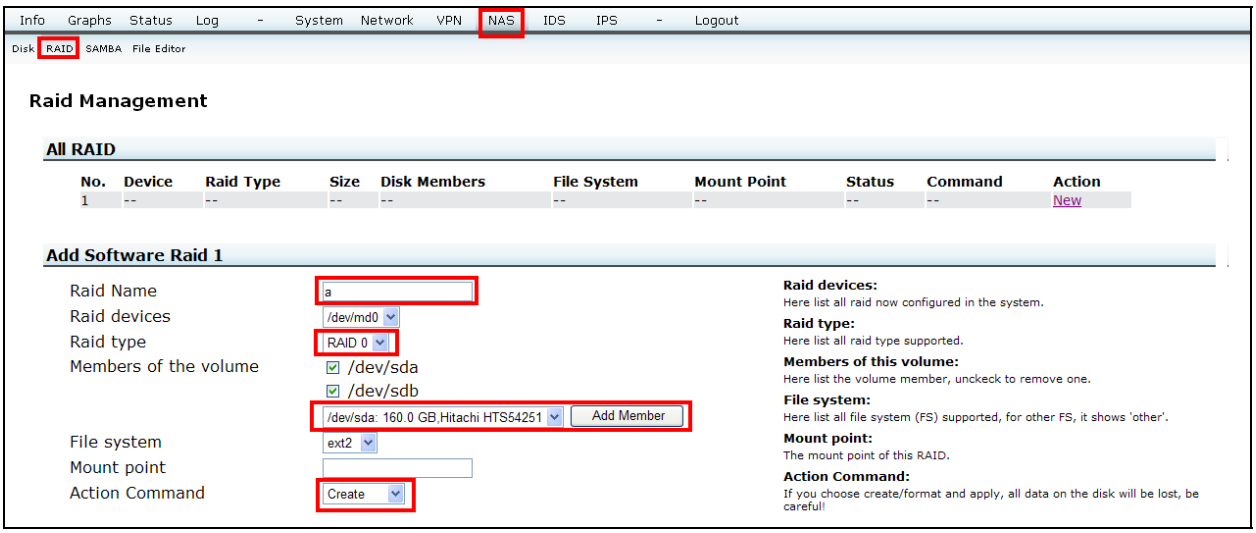


7.3.1 Create RAID0

This procedure creates the software RAID0. Perform the following steps, as depicted in Figure 7-10:

1. In the **Raid Name** text box, type the name.
2. From the **Raid type** drop-down list, select **RAID 0**.
3. Click **Add Member**. (You must have two disks on the 8377.)
4. From the **Action Command** drop-down list, select **Create**.

Figure 7-10. Create RAID0

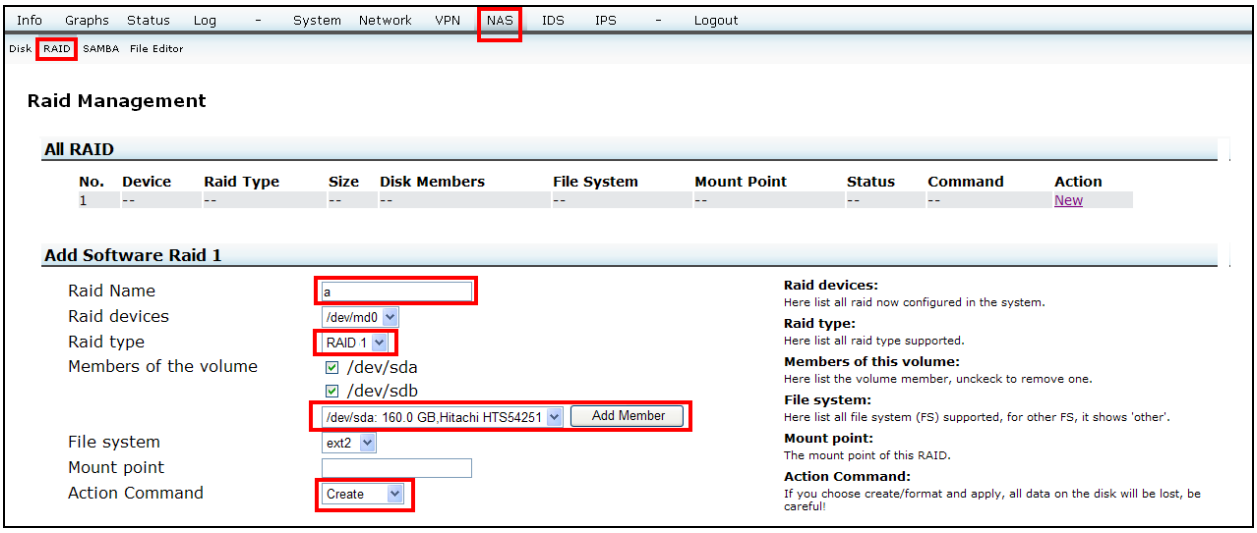


7.3.2 Create RAID1

This procedure creates the software RAID1. Perform the following steps, as depicted in Figure 7-11:

1. In the **Raid Name** text box, type the name.
2. From the **Raid type** drop-down list, select **RAID 1**.
3. Click **Add Member**. (You must have two disks on the 8377.)
4. From the **Action Command** drop-down list, select **Create**.

Figure 7-11. Create RAID1

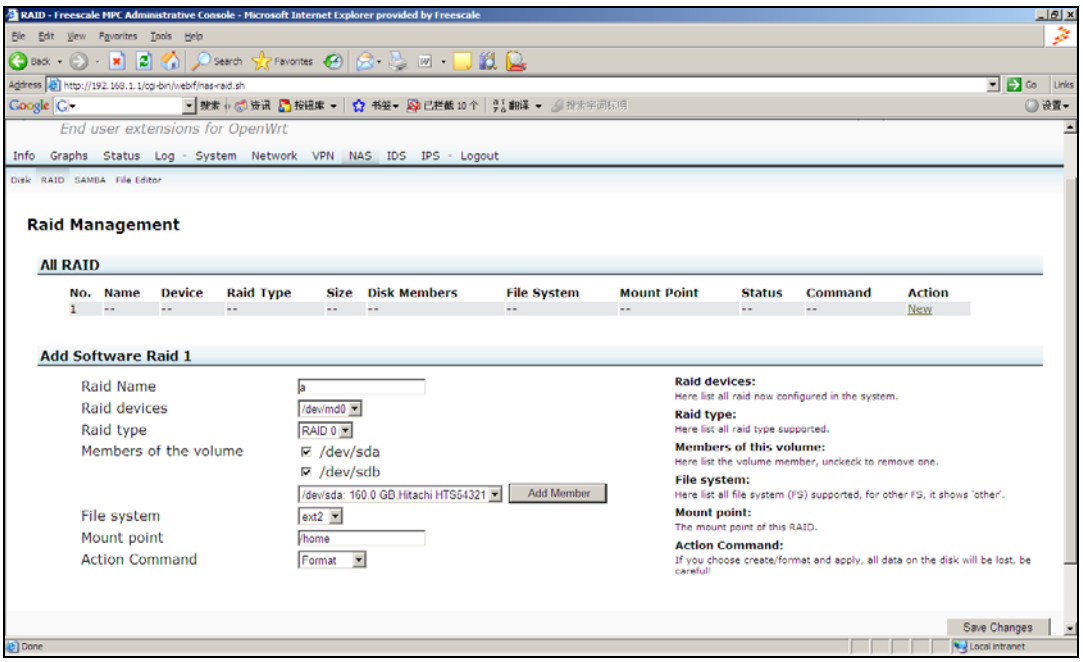


7.3.3 Format RAID

After creating software RAID0/1, format the RAID to one file system of your choosing. Perform the following steps as depicted in Figure 7-12:

1. From the **Raid devices** drop-down list, select the device.
2. From the **Action Command** drop-down list, select **Format**.

Figure 7-12. Format RAID

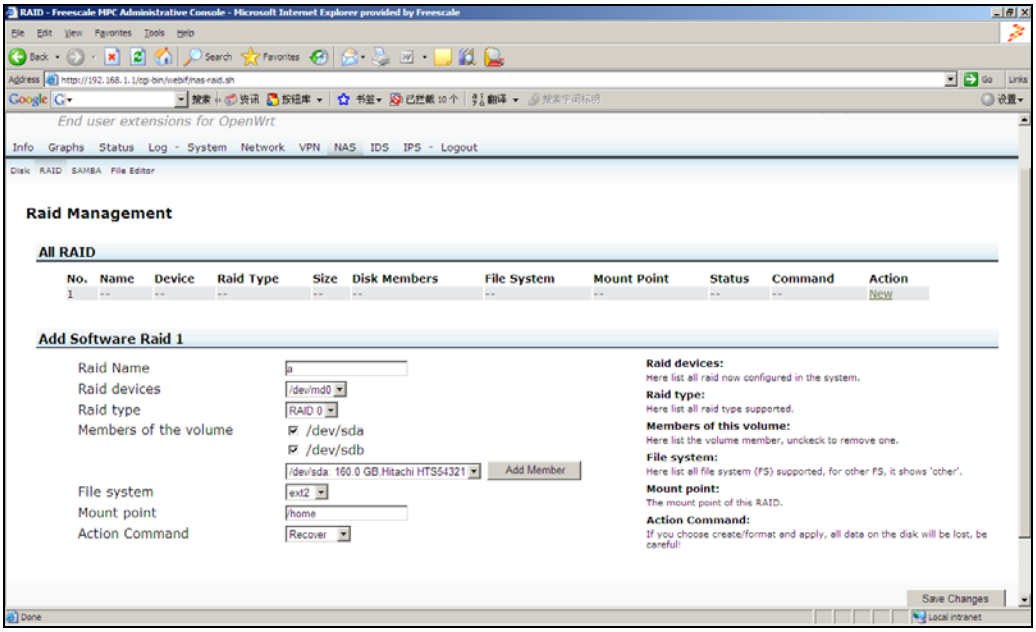


7.3.4 Recovery

If one disk is out of service, and a new disk is added or any other reason that makes the state of RAID abnormal, you can choose this command to recover the RAID. Perform the following steps as depicted in Figure 7-13:

1. From the **Raid devices** drop-down list, select the device.
2. From the **Action Command** drop-down list, select **Recover**.

Figure 7-13. RAID Recovery

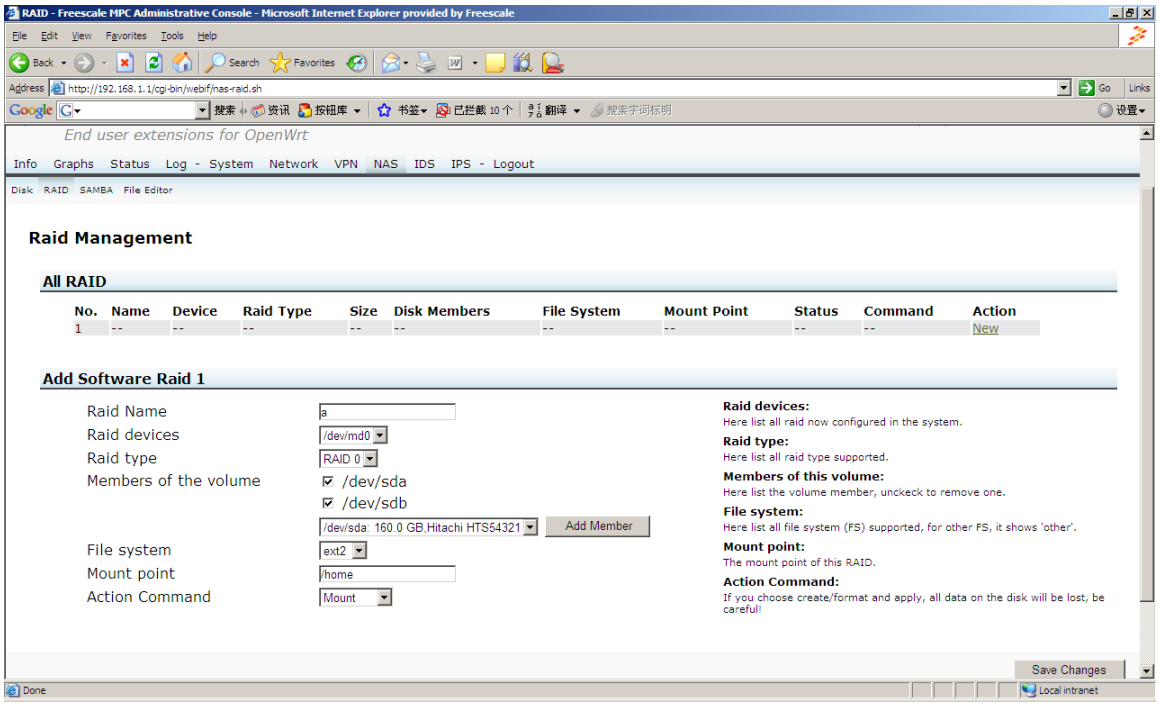


7.3.5 Mount

To mount the RAID to one folder, such as /home, perform the following steps as shown in Figure 7-14:

1. In the **Mount point** field, type the address you want to mount. For example, /home.
2. From the **Action Command** drop-down list, select **Mount**.

Figure 7-14. Mount RAID

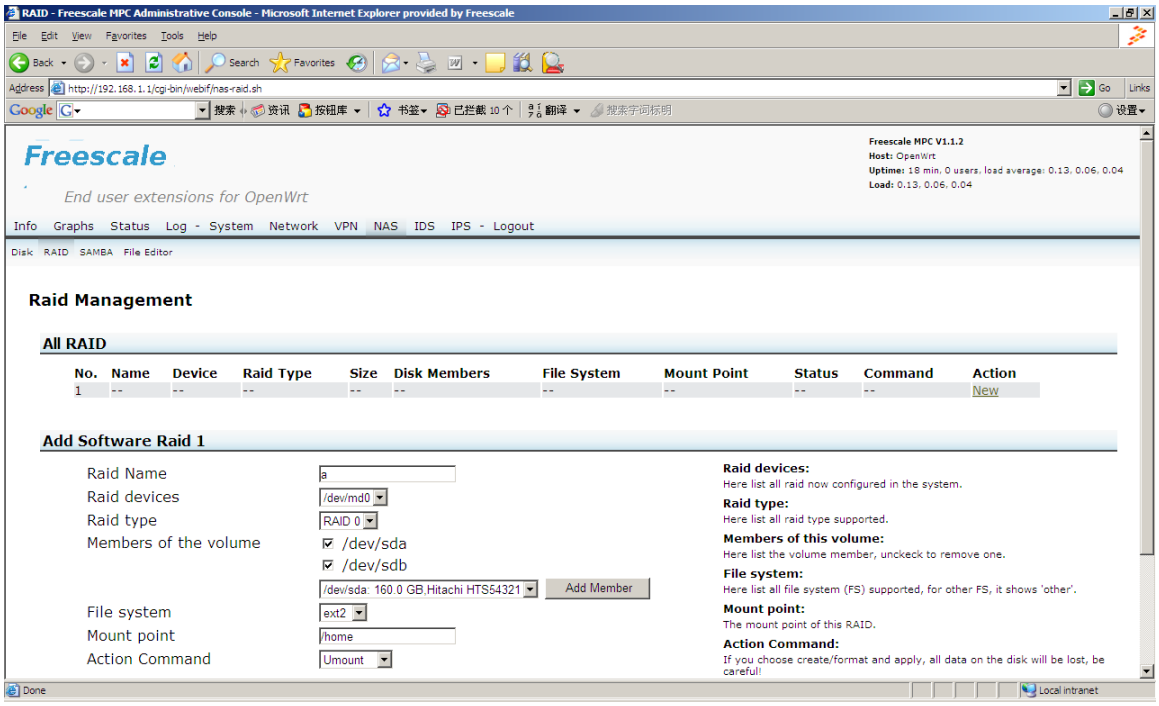


7.3.6 Unmount

To unmount RAID, perform the following steps as shown in Figure 7-15:

1. In the **Mount point** field, type the address where your disk is mounted.
2. From the **Action Command** drop-down list, select **Umount**.

Figure 7-15. Unmount RAID

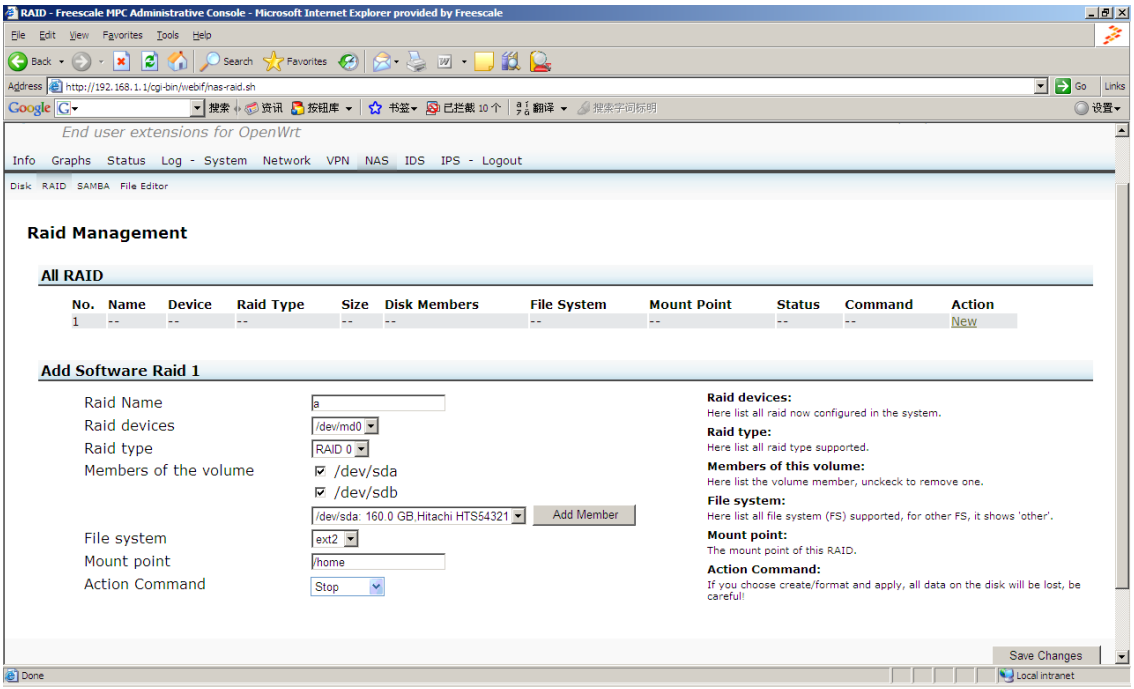


7.3.7 Stop

Make sure your disk is not operational at this time and un-mounted already before you stop RAID management. Perform the following steps as depicted in Figure 7-16.

1. From the **Action Command** drop-down list, select **Stop**.

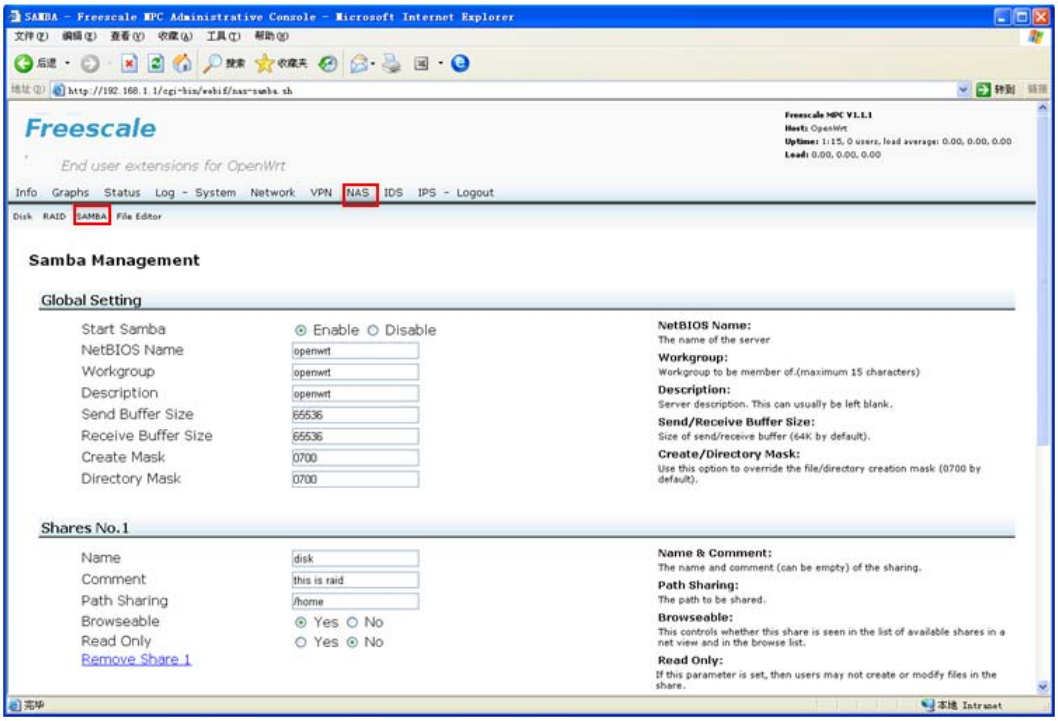
Figure 7-16 Stop



7.4 Samba Management

Samba is free, open source software that allows a UNIX server to act as a file server to Windows clients. It runs under Linux, FreeBSD, and other UNIX variants. Click **Samba**. Figure 7-17 depicts the **NAS > Samba Management** window.

Figure 7-17. Samba Management, Shares No. 1 Section Shown



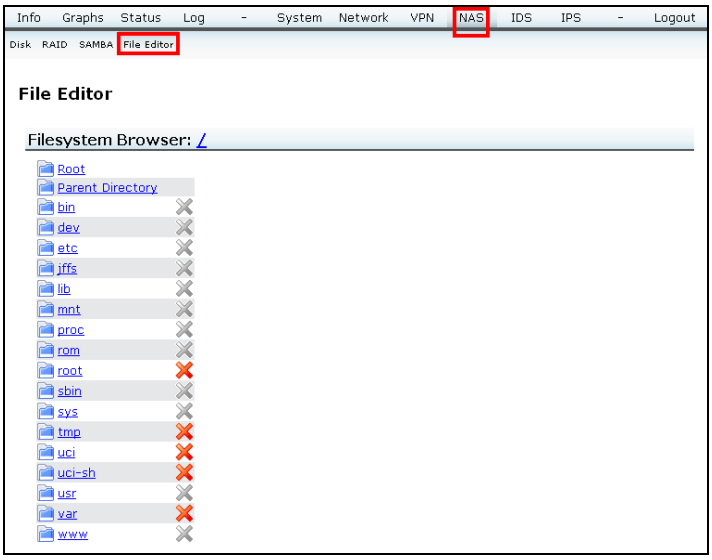
NOTE

You can access all the shares by using the Samba service. You can edit, remove, or add one share.

7.5 File Editor

The file editor makes it possible to browse, and operate files through the web (Http/Https). Click **File Editor**. (Figure 7-18) depicts the **NAS > File Editor** window.

Figure 7-18. File Editor



8 Intrusion Detection Systems

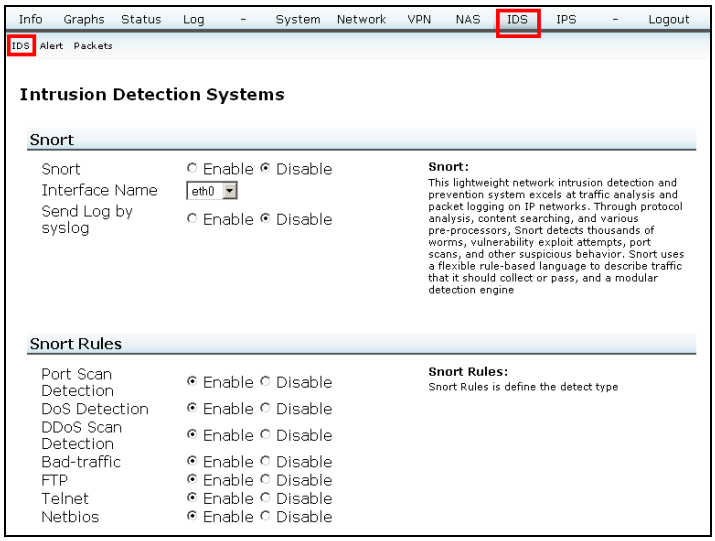
This section explains detection of electronic intrusion attempts. Click **IDS** (Figure 8-1), then proceed with the respective sections.

Figure 8-1. IDS

8.1 IDS (Intrusion Detection Systems)

Click **IDS**. Figure 8-2 depicts the **IDS** > **Intrusion Detection Systems** window.

Figure 8-2. IDS, Snort



8.1.1 Snort

Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior through protocol analysis, content searching, and various pre-processors. Snort uses a flexible rule-based language to describe traffic that it should collect or pass a modular detection engine. Perform the following steps as shown in Figure 8-2:

1. Under **Snort** section, in the **Snort**, click **Enable** to turn on the IDS function.
2. From the **Interface Name** drop-down list, select **eth0** (WAN port).
3. In the **Send Log by syslog**, click **Enable**.

8.1.2 Snort Rules

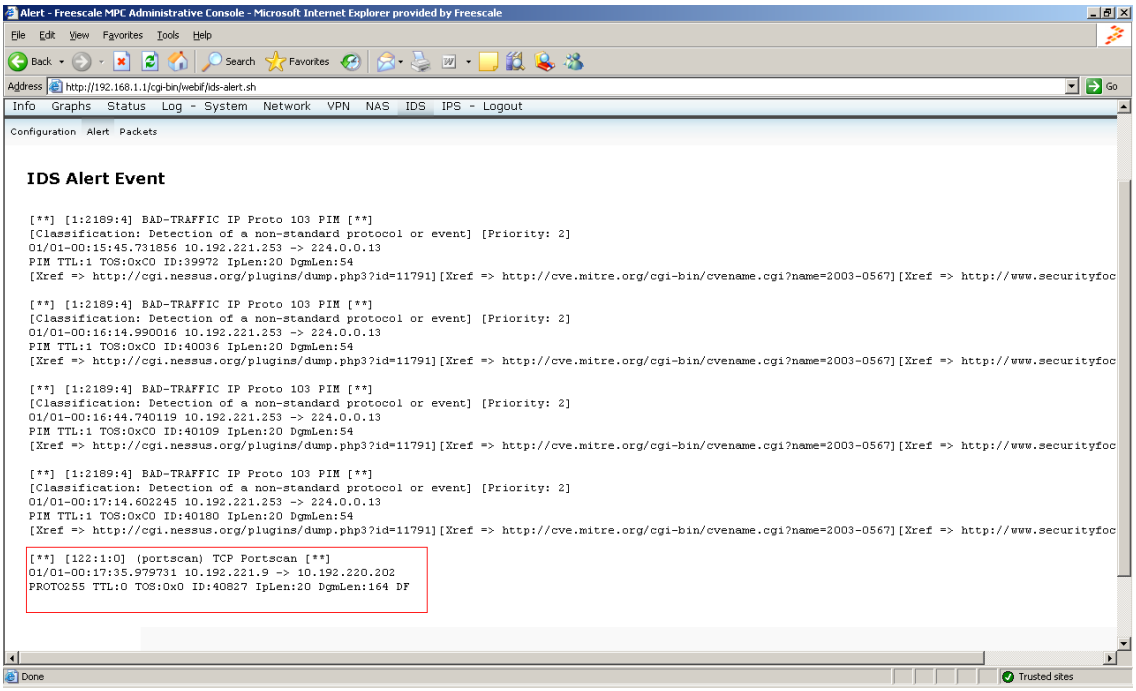
The snort rules define the detect type. Perform the following steps to set snort rules.

1. Under **Snort Rules** section in the **Port Scan Detection**, click **Enable**.
2. In the **DoS Detection**, click **Enable**.
3. In the **DDos Scan**, click **Enable**.
4. In the **Bad-traffic**, click **Enable**.
5. In the **FTP**, click **Enable**.
6. In the **Telnet**, click **Enable**.
7. In the **Netbios**, click **Enable**.

8.2 Alert (IDS Alert Event)

Click **Alert**. Figure 8-3 shows a log of intrusion alerts.

Figure 8-3. Alert



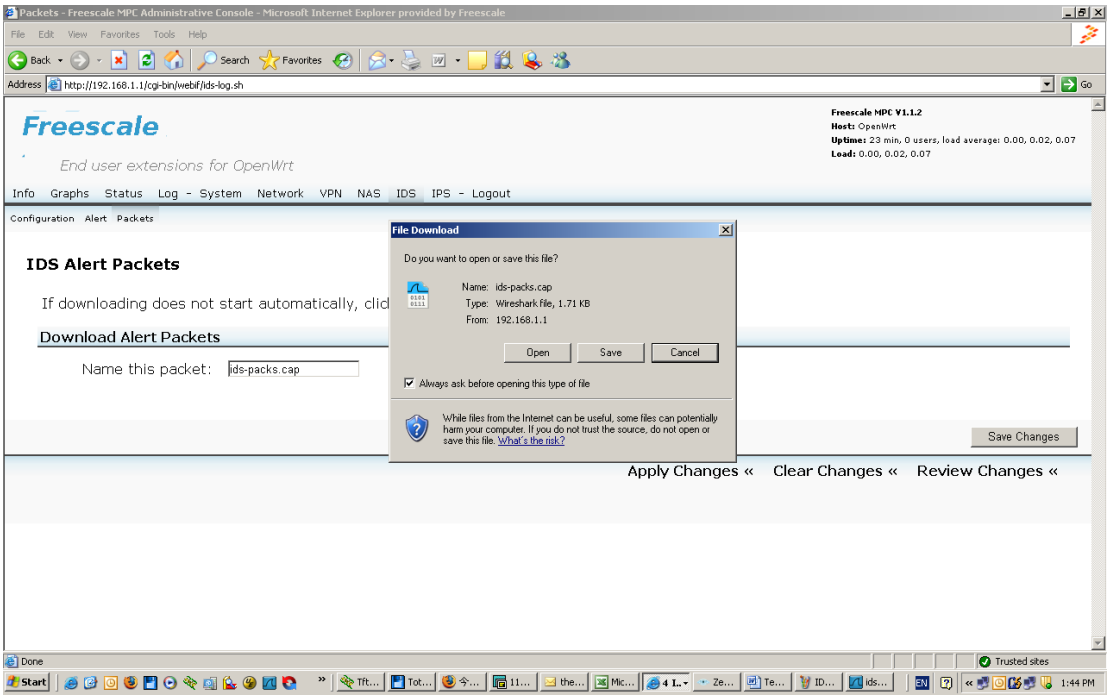
8.3 Packets (Download Alert Packets)

Click **Packets**. When intrusion occurs, you can save the packet from EWLAN to your PC by clicking **Download** (Figure 8-4).

To download alert packet, follow the steps given below:

1. Enter the file name in the **Name this packet** text box. For example, “xx.cap”.
2. Click **Download** and save the file to the local PC.

Figure 8-4. IDS Alert Packets



9 Intrusion Prevention Systems

This section explains configuring the unit to detect electronic intrusion attempts. IPS is an advanced technology to protect your network from malicious attacks. IPS works together with your SPI Firewall, IP Based Access List (IP ACL), Network Address Port Translation (NAPT), and Virtual Private Network (VPN) to achieve the highest amount of securities.

IPS works by providing real-time detection and prevention as an in-line module in a router. The Wireless-N Security Router has hardware-based acceleration for real-time pattern matching for malicious attacks. It actively filters and drops malicious TCP/UDP/ICMP/IGMP packets and can reset TCP connections. This protects your client PCs and servers running various operating systems including Windows, Linux, and Solaris from network worm attacks. However, this system does not prevent viruses attached emails.

The P2P (peer to peer) and IM (instant messaging) control allows the system administrator to prevent network users from using those protocols to communicate with people over the Internet. This helps the administrators to set up company policies on how to use their Internet bandwidth wisely.

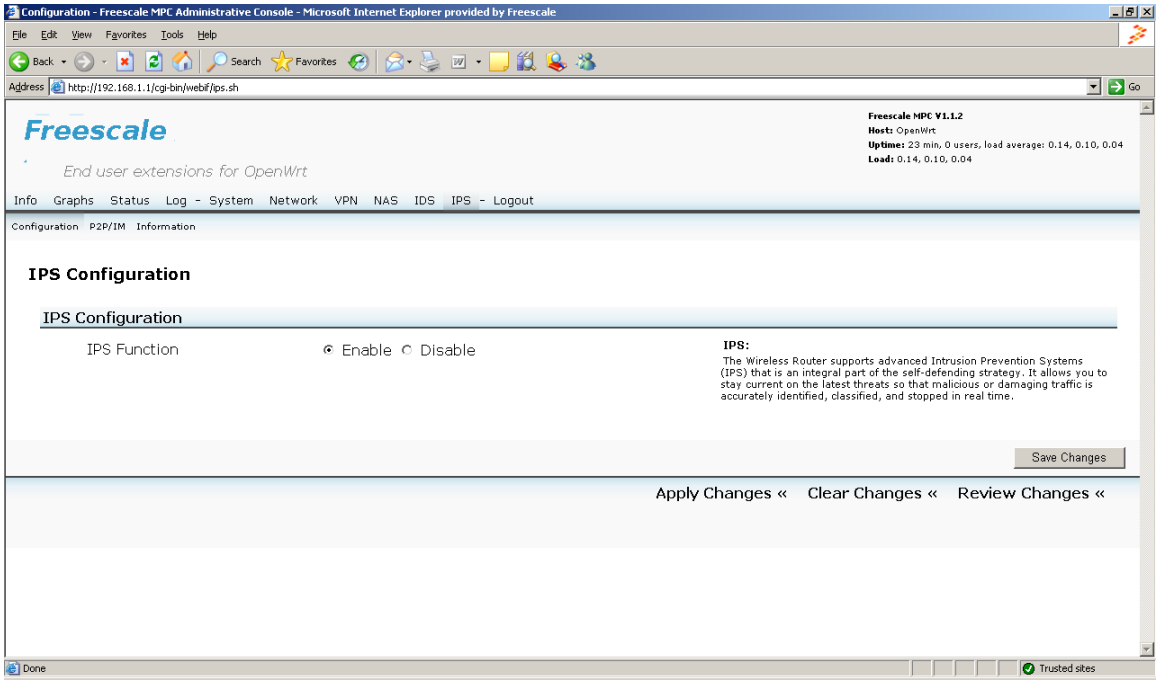
Click **IPS** (Figure 9-1), then proceed with the respective sections.

Figure 9-1. IPS

9.1 Configuration (IPS Configuration)

Click **Configuration**. Figure 9-2 shows IPS Configuration.

Figure 9-2. IPS Configuration



9.1.1 IPS Configuration

The Wireless Router support advanced Intrusion Prevention System (IPS) is an integral part of the self-defending strategy. It allows you to stay current on the latest threats to identify, classify, and stop malicious and damaging traffic in real-time.

Perform the following steps as depicted in Figure 9-2.

1. Enable/disable **IPS Function**.
2. Click **Save Changes** button to save the changes.

9.2 IPS P2P/IM (Peer to Peer, Instant Messaging)

Click **P2P/IM**. Block/unblock various categories of peer-to-peer, instant-messaging connections, and remote logins. Click **Submit** in the appropriate categories. See Figure 9-3.

Figure 9-3. IPS P2P/IM

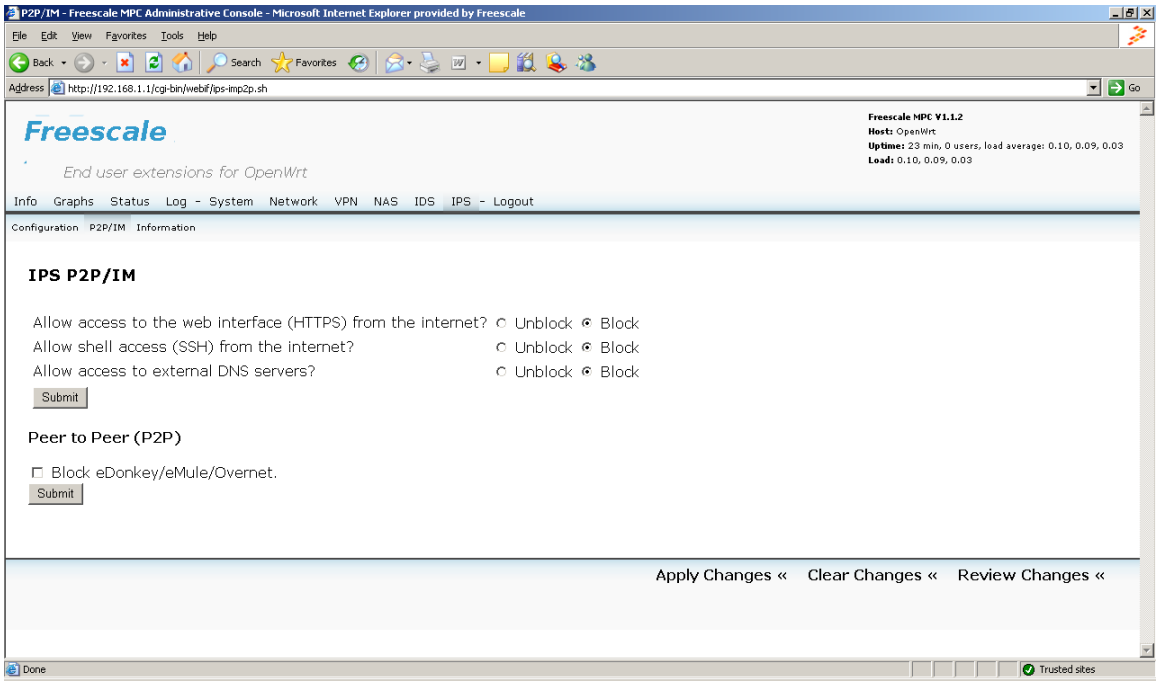


Table 9-1 explains each option given in the **IPS > P2P/IM** page.

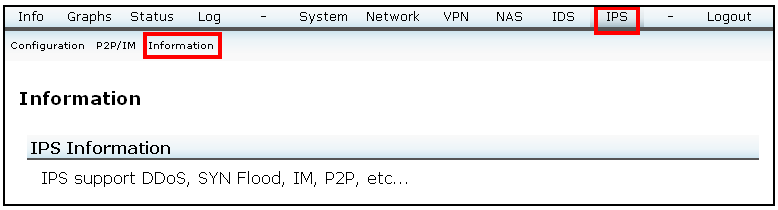
Table 9-1 IPS > P2P/IM Options

Option	Description
IPS P2P/IM	
Allow access to web interface (HTTPS) from the Internet	You can block or unblock access to web interface (HTTPS) from the Internet.
Allow shell access (SSH) from the Internet	You can block or unblock shell access (SSH) from the Internet.
Allow access to external DNS servers	You can block or unblock access to external DNS servers.
Peer to Peer (P2P)	
Block eDonkey/eMule/Overnet	Check this option to block eDonkey/eMule/Overnet.

9.3 Information

Click **Information** to read about IPS support (Figure 9-4).

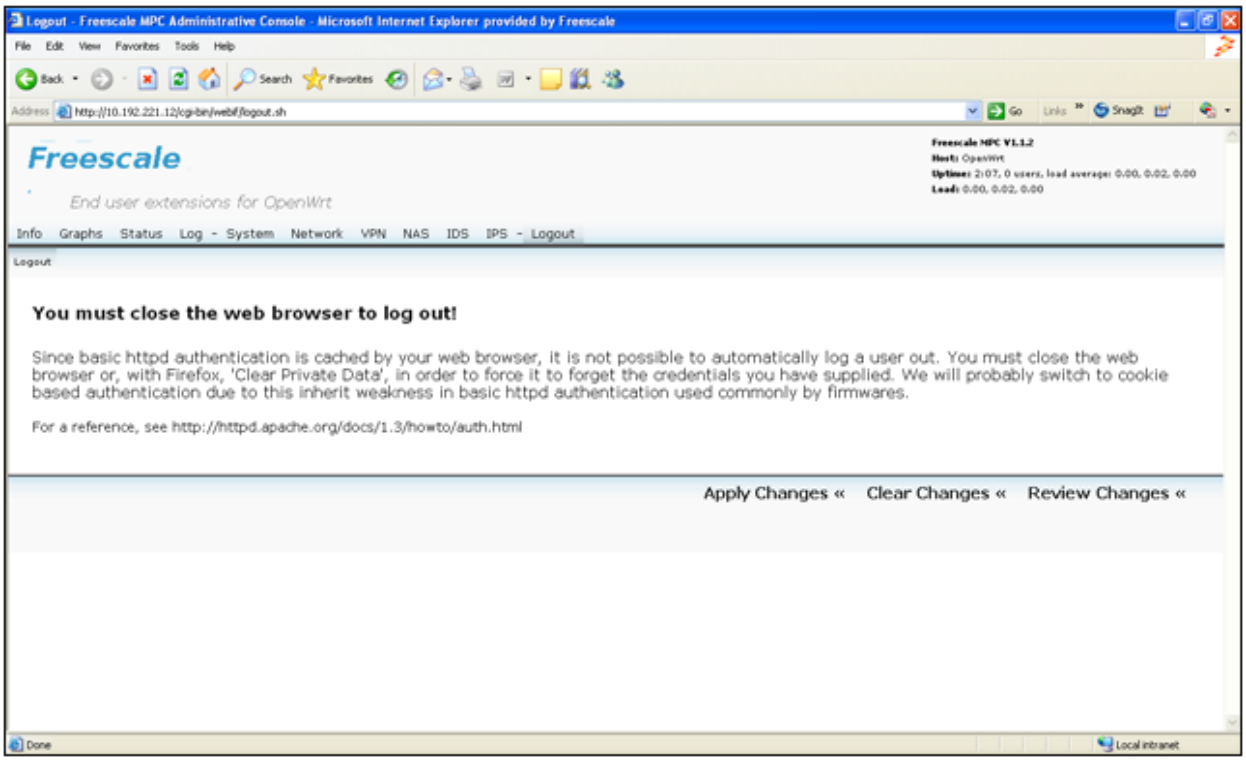
Figure 9-4. IPS Information



10 Logout

Click **Logout** to logout from the web page. (Figure 10-1)

Figure 10-1. IPS Information



NOTE

You must close the web browser to logout.

It is not possible to logout automatically until you close the web browser. Your web browser caches the basic httpd authentication. Therefore, you must close the web browser. With Firefox, clear private data to force it to forget the credentials you have supplied.