Reference Design Solution

Software User's Guide

Document Number: MSBG
Rev 0.1.1
09/2010

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 chosen in such a way 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 PowerPC Referenced Design Board software. However, this guide can also be used for P2020RDB and other QorIQ boards. It contains information on how to connect and configure the PowerPC Referenced Design Board.

Audience

This software manual is intended for the user who wants to become familiar with this device and who is trying to connect and configure this PowerPC Referenced Design Board. It is assumed that the 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
DDNS	Dynamic Domain Name System
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MSBG	Multi-Service Business Gateway
NAS	Network Attached Storage
NVR	Network Video Recorder
POE	Power over Ethernet
PPPOE	Point to Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PSK	Pre-Shared Key
RAID	Redundant Array of Inexpensive Disks
RDS	Reference Design Solution
SSID	Service Set Identifier

SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol-Internet Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDS	Wireless Distribution System
WEP	Wired Equipment Privacy
WPA	Wi-Fi Protected Access

1 Package Contents

The package should contain all the items listed in Table 1-1. This PowerPC Referenced Design Board 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
PowerPC Referenced Design Board 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

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 4 Connecting and Configuring this PowerPC Referenced Design Board.

2.1 Reference Design Solution

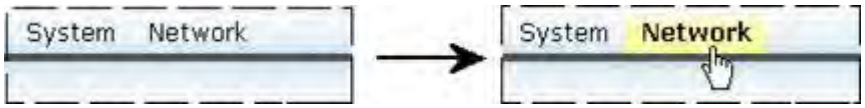
RDS commonly known as Reference Design Solution for this manual can also be used for P2020RDB, MPC8377EWLAN and other QorIQ boards. This RDS supports features like Wireless AP/WLAN, Security Router, Network Attached Storage (NAS), Network Video Recorder, etc. In future, this Reference Design Solution will also support features like IP/PBX and VoIP.

2.2 Introduction to Navigation

2.2.1 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 2-1 shows an example of an option (Network) being highlighted when a cursor is placed on it.

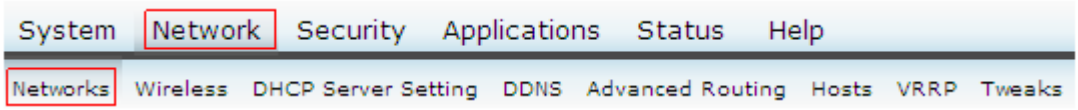
Figure 2-1: Option Cursor Hover



2.2.2 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



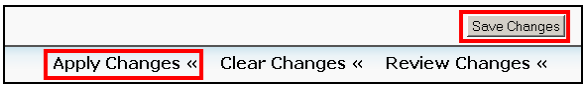
2.2.3 Saving and Applying Changes to Settings

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 Configuration Modes

This device now comes with two functioning modes: **Basic** and **Advanced**. Depending upon the option selected in the Function drop down, the application is customized and more tabs are added to the application. Basic mode is designed for beginners while Advanced mode focuses on advanced users who are quite familiar with the application.

Figure 3-1 shows the Basic mode of this PowerPC Referenced Design Board application.

Figure 3-1: Basic Mode

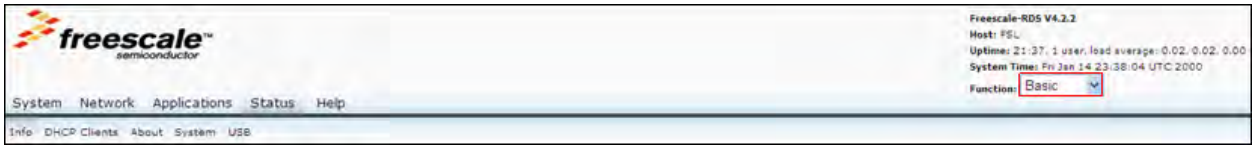


Figure 3-2 shows the Advanced mode of this PowerPC Referenced Design Board application.

Figure 3-2: Advanced Mode

4 Connecting and Configuring this PowerPC Referenced Design Board

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

Before using this device, please ensure that the basic settings to guarantee that it will work in your environment. You can configure this device 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 this device

Step 3. Configure the router, and then

Step 4. Power off/on the unit.

You can configure this device through a web browser. You need a PC connected to this device (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 this device.

NOTE

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

4.1 Connecting this PowerPC Referenced Design Board (Wired Computing)

This section explains the wiring setup for the computer connected to the Internet. This device has the capability to support usage of power adapter (12V power supply) and POE (Power over Ethernet).

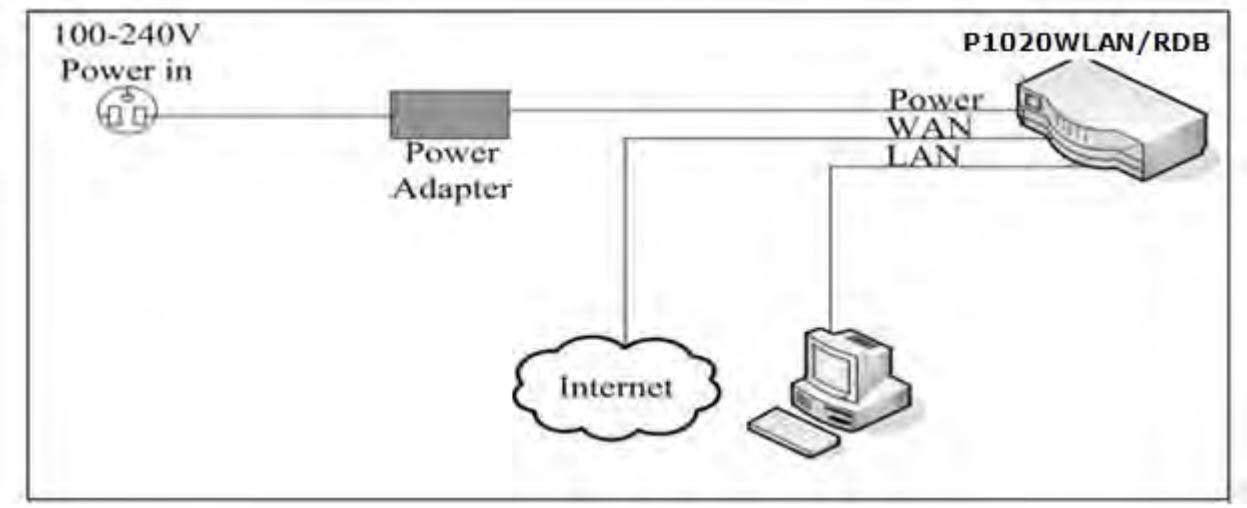
4.1.1 Using the Power Adapter

There must be at least two RJ-45 cables in this PowerPC Referenced Design Board wiring connection while using a power adapter. Table 4-1 lists the cable connections, and Figure 4-1 depicts them below.

Table 4-1: 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 4-1: Cable Connection Layout, Power Adapter



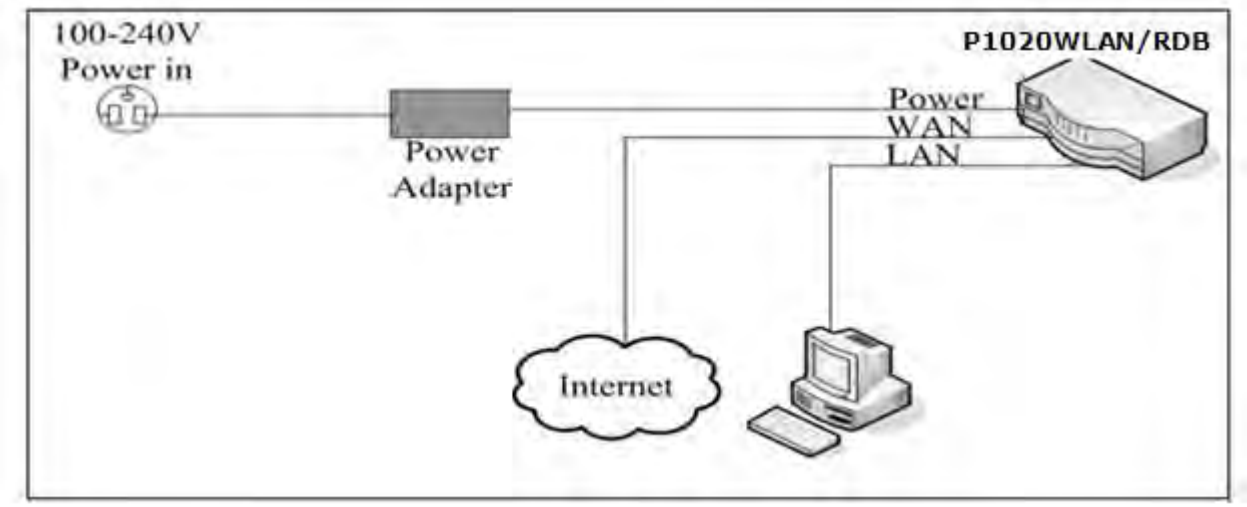
4.1.2 Using the Power over Ethernet (POE)

There must be at least three RJ-45 cables in this PowerPC Referenced Design Board wiring connection while using POE. Table 4-2 lists the cable connections, and Figure 4-2 depicts them.

Table 4-2: 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 4-2: Cable Connection Layout, Power Over Ethernet



4.2 Connecting this PowerPC Referenced Design Board (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 4.1 titled Connecting this PowerPC Referenced Design Board (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 4.5 Wireless Configuration explains the wireless interface setup, with Figure 4-16 showing SSID setting as FSL_AP1.

4.3 Setting Up the IP Address

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

4.3.1 Setting up the IP Address Automatically

This device 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 4-3). (Or you can open **Windows Explorer** window, then right click **My Network Places**.)

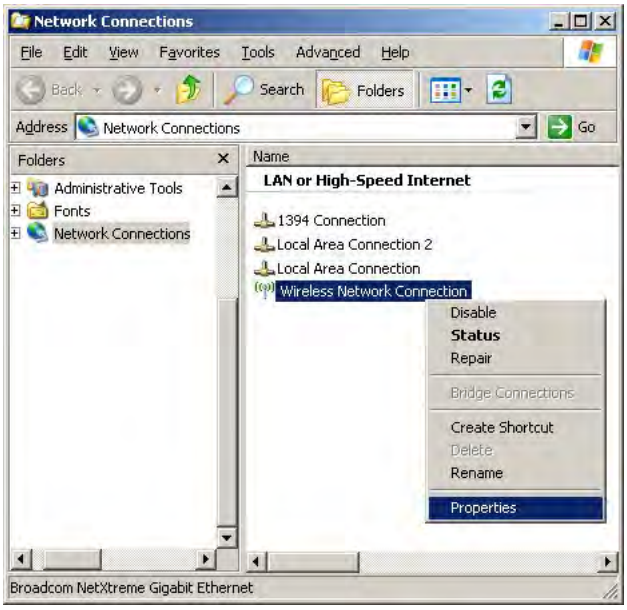
Figure 4-3: My Network Places > Properties

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 4-4).

Figure 4-4: Network Connections, Wired

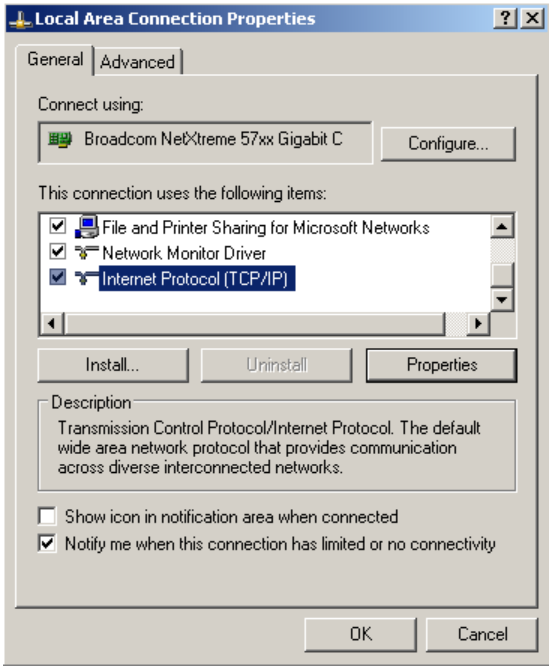
   — If you are using a wireless connection, right click **Wireless Network Connection > Properties** (Figure 4-5).

Figure 4-5: 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 4-6) then double click it to open the **Internet Protocol (TCP/IP) Properties** window (Figure 4-7).

Figure 4-6: Local Area Connection Properties

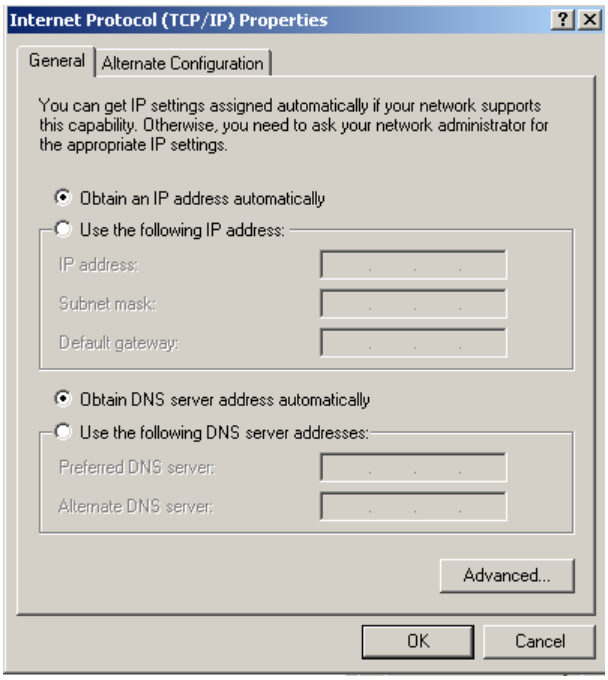


   b. In the **General** tab (Figure 4-7), perform the following steps:
      1.) Click **Obtain an IP** address automatically.

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

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

Figure 4-7: Setting Up the IP Address Automatically



a. In the **Local Area Connection Properties** window, click **OK** to close it.

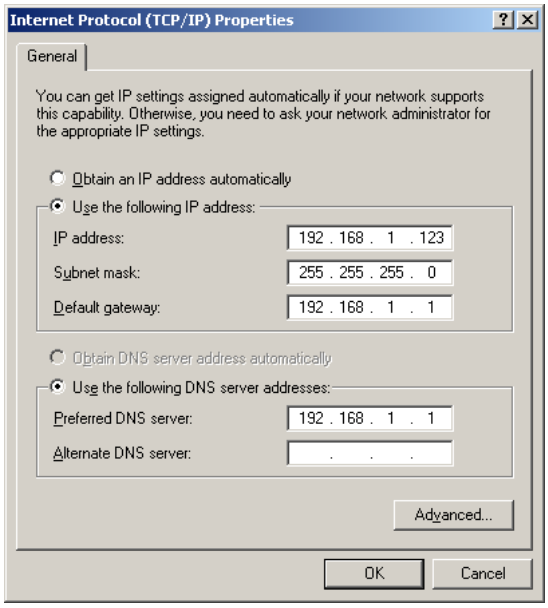
4. For wireless connection, perform step 3 similar to those of wired connection. (The window titles are different.)

4.3.2 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 4.3.1 Setting up the IP Address Automatically until you reach the **Internet Protocol (TCP/IP) Properties** window. Figure 4-8 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 device IP address.
2. Click **Use the following DNS server addresses**.
   a. In the **Preferred DNS server**, type **192.168.1.1**, this is the device IP address or your own.
   b. In the **Alternate DNS server**, leave blank. (See Figure 4-8)
3. Click **OK**.

Figure 4-8: Setting Up the IP Address Manually



4.4 Configuring this PowerPC board

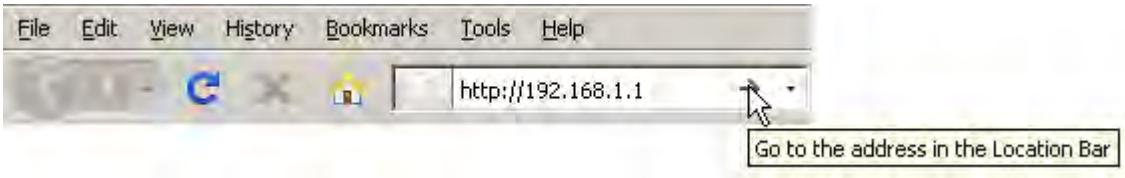
This section explains how to configure your router. The steps consist of opening a browser, going to a website, logging in, and then configuring the router for user equipment. This has been tested with IE7.0 and Firefox 3.0.6 web browser.

4.4.1 Logging In to the Router Home Page

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

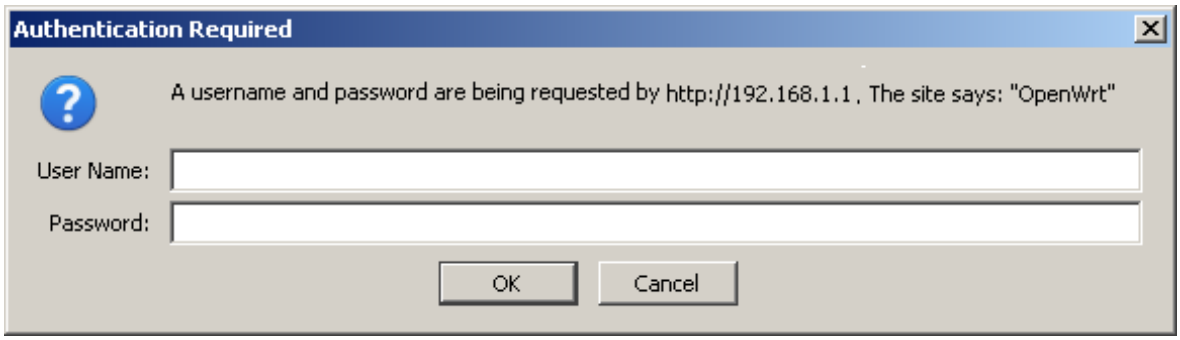
4. Open an Internet browser.
5. Type http://192.168.1.1 in the address bar, then press **Enter** or click the go-to link (Figure 4-9).

Figure 4-9: IP Address in Web Browser



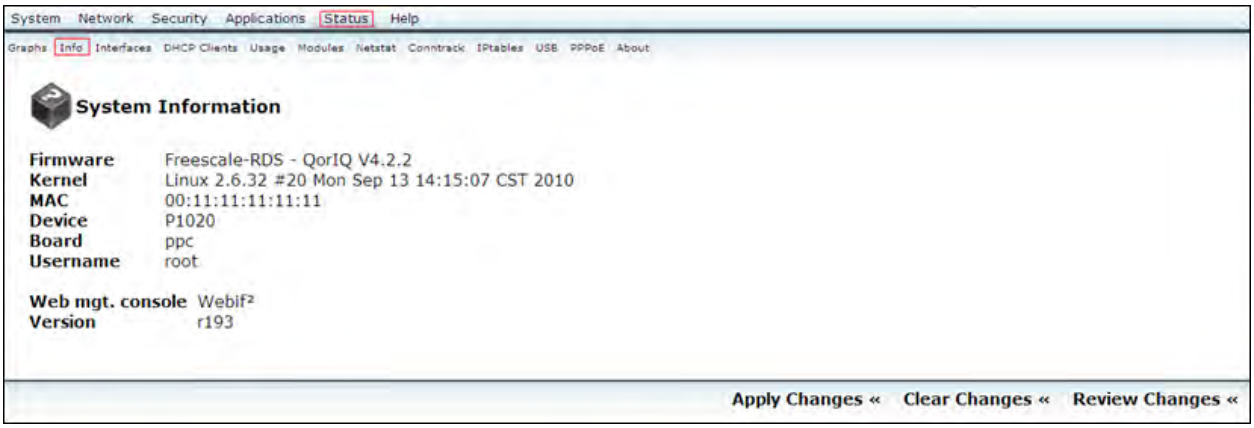
6. In the login window, type `root` for both **User name** and **Password**, then click **OK** (Figure 4-10).

Figure 4-10: Login



The device home page appears (Figure 4-11), with default page **Status > Info**. (For information about the interface, refer to Section 2 titled Introduction to the Interface.)

Figure 4-11: PowerPC Referenced Design Board Home Page



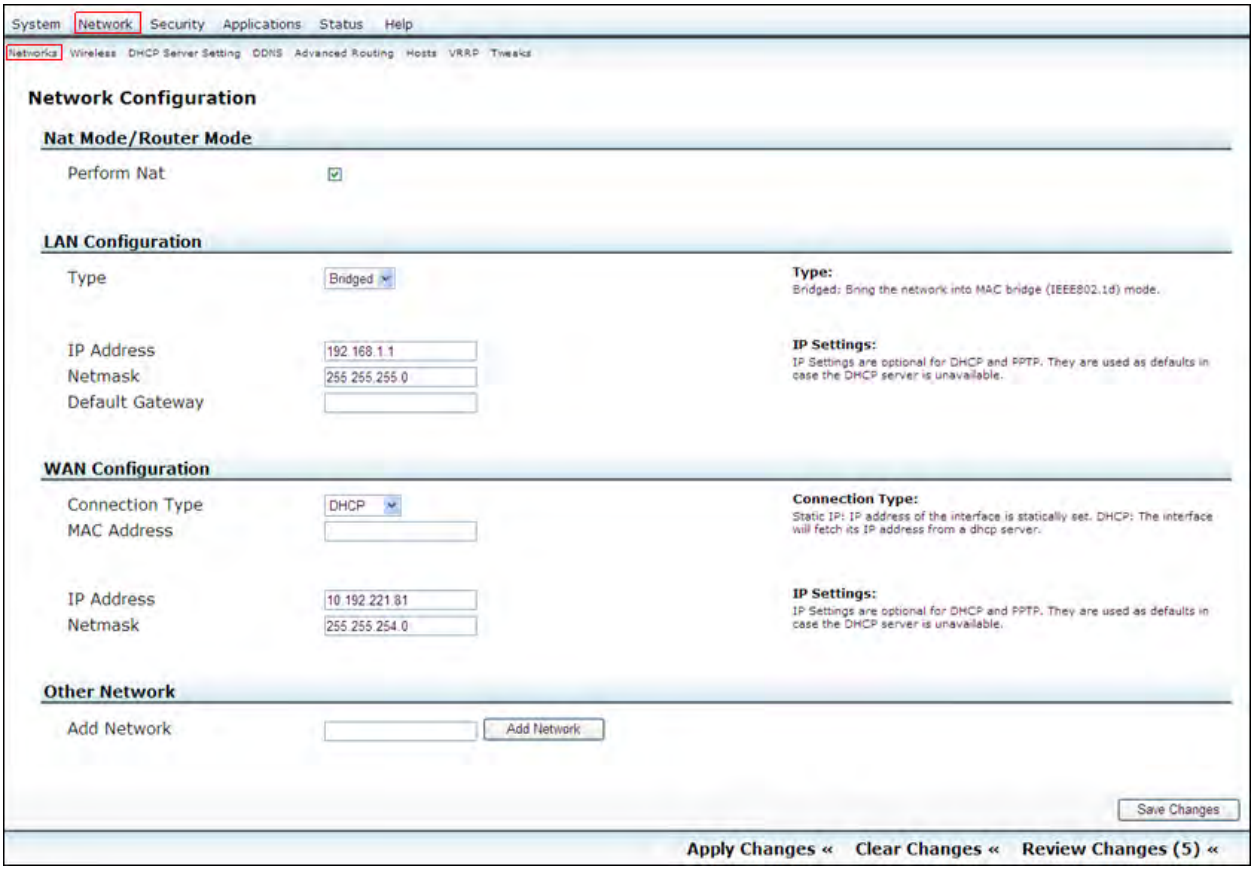
5 Setting up the Network

5.1 Network Configuration

This PowerPC Referenced Design Board supports four types of ISP services—static IP address, PPPOE, PPTP and DHCP. Since each service has its own protocols and standards, during the setup process, there are different identity settings demanded by this device.

At the home page of this PowerPC Referenced Design Board wireless router, click **Network**, select the correct connection type, and then follow instructions for the individual sections.

Figure 5-1: Network Configuration

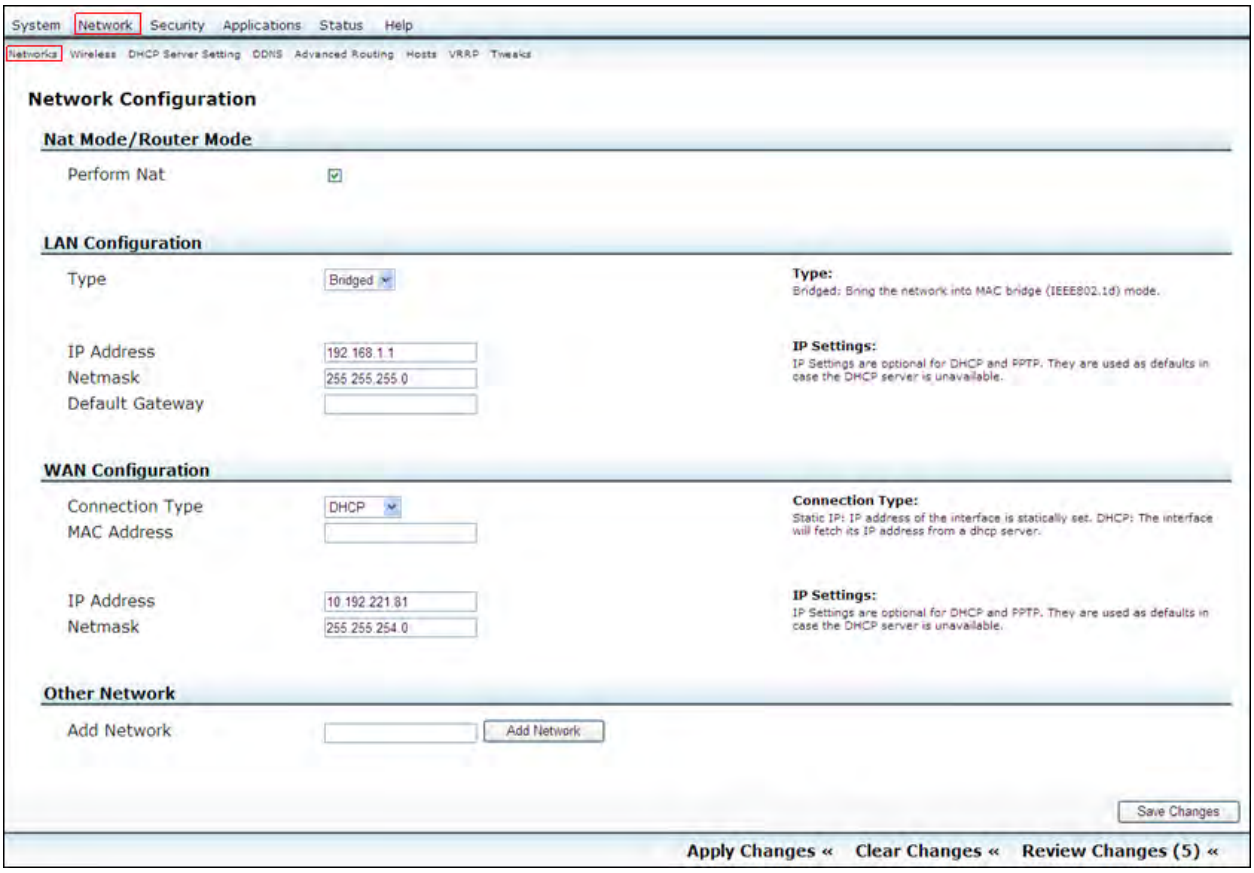


5.1.1 Cable User (Static IP)

If you are receiving services from cable or other ISP assigning IP address automatically, select one of the following (Figure 5-2), for which you can type the static IP address:

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

Figure 5-2: Network Setup—Static IP Address (WAN)



Options include the following:

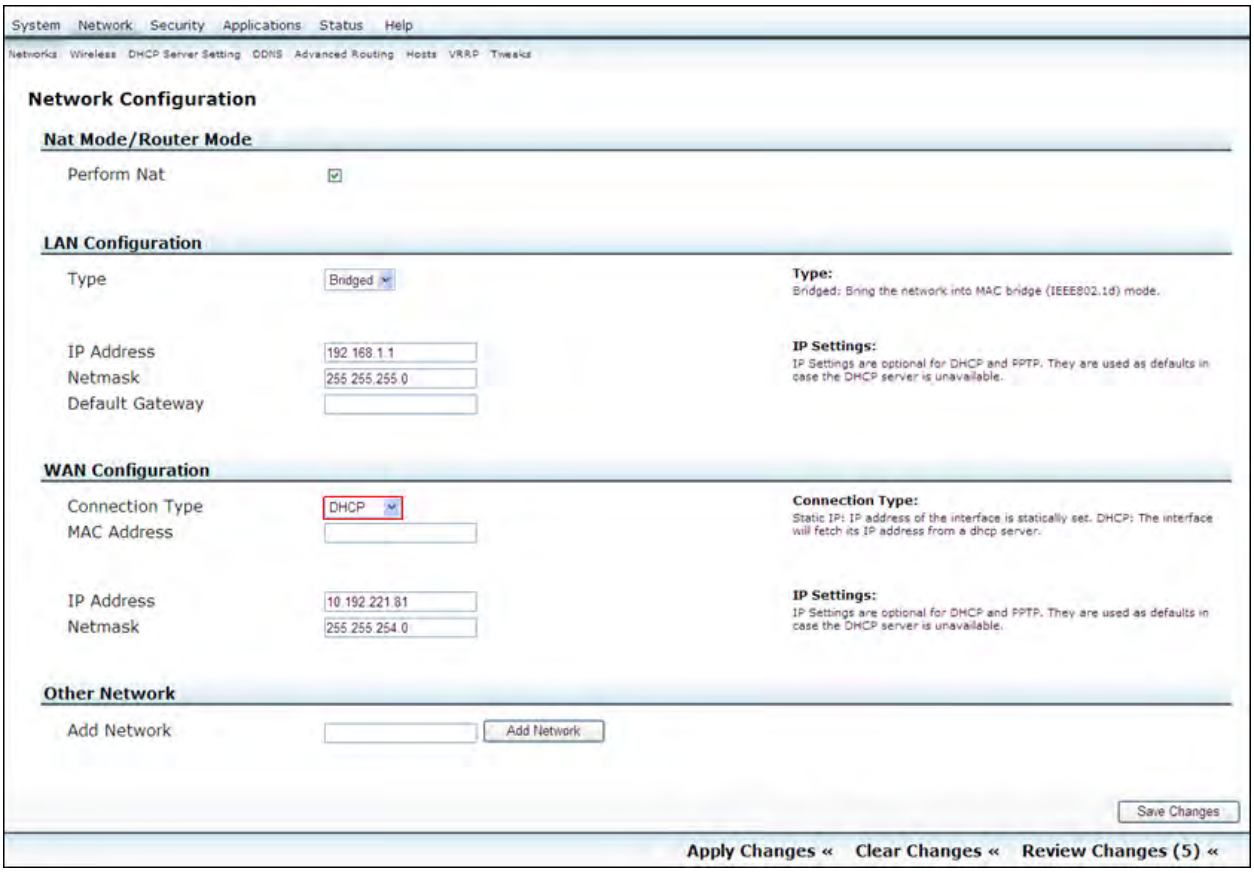
- **WAN DNS Servers** (field and **Add** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.
- **Other Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

5.1.2 DHCP User

If you are a DHCP service user, select one of the following (Figure 5-3):

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

Figure 5-3: Network Setup—DHCP (LAN or WAN)



Options include the following:

- **Other Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

NOTE

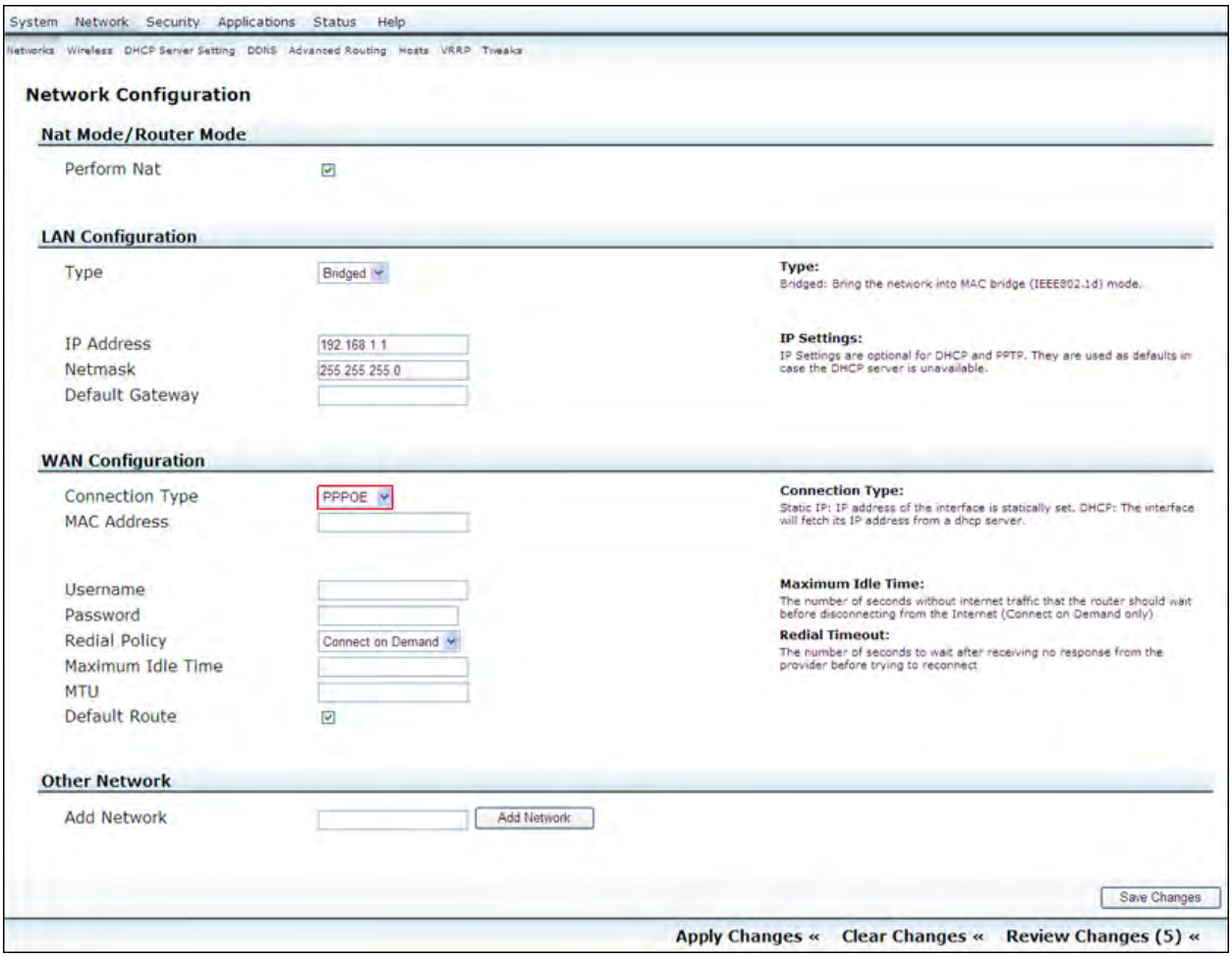
Make sure DHCP server is available on WAN side if you configure its 'Connection Type' to 'DHCP'

5.1.3 PPPOE User

If you are a PPPOE service user, select one of the following (Figure 5-4), for which you must type the **Username** and **Password** provided by your ISP:

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

Figure 5-4: Network Setup—PPPOE (LAN or WAN)



Options include the following:

- **Other Network** (field and **Add Network** button). Also, for any WAN server IP shown (if existing), there is a **Remove** link option.

NOTE

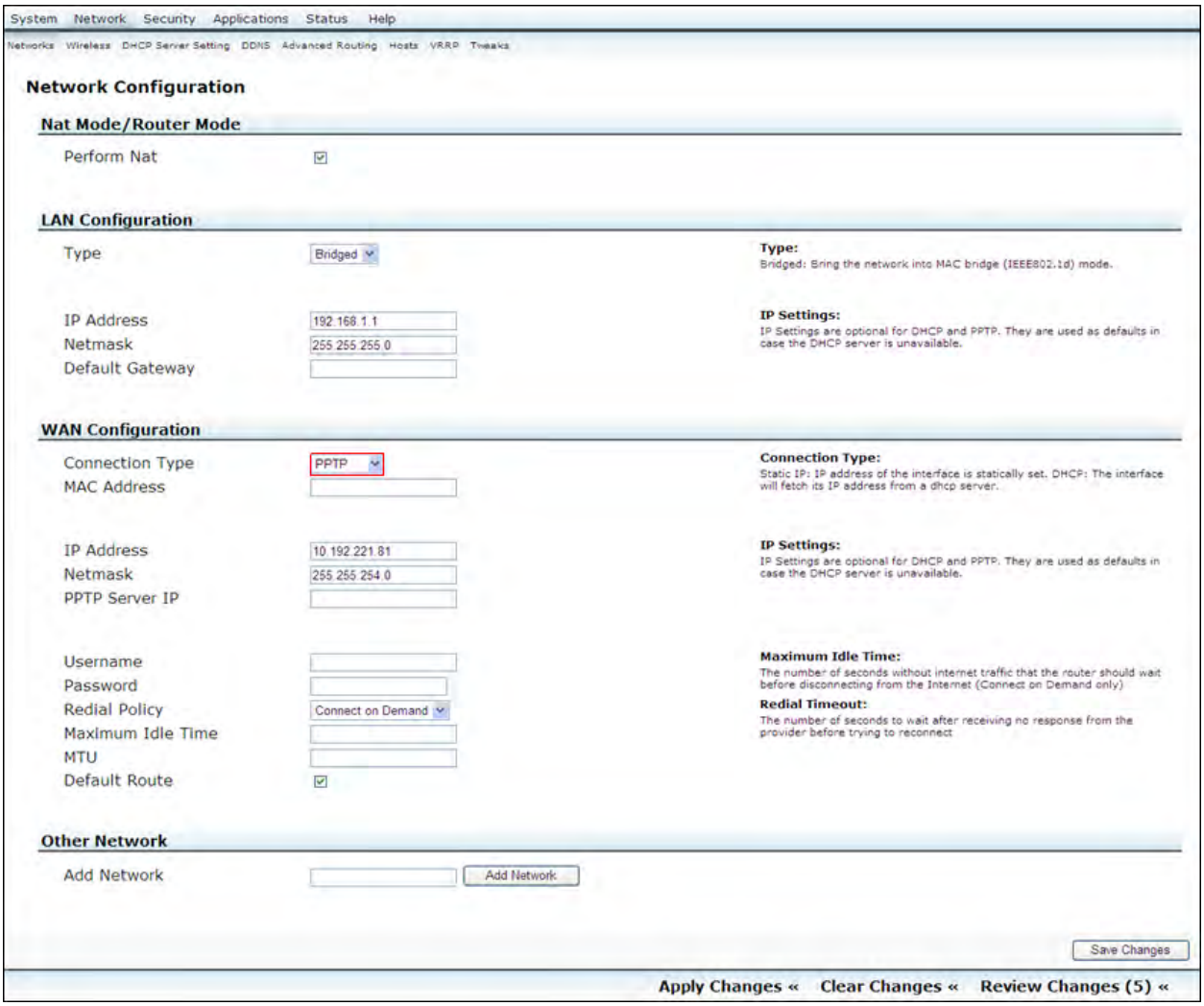
Make sure that PPPOE server is available on WAN side if you configure its 'Connection Type' to 'PPPOE'

5.1.4 PPTP User

If you are a PPTP service user, select one of the following (Figure 5-5), for which you must type the **Username** and **Password** provided by your ISP:

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

Figure 5-5: Network Setup—PPTP (LAN or WAN)



Options include the following:

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

NOTE

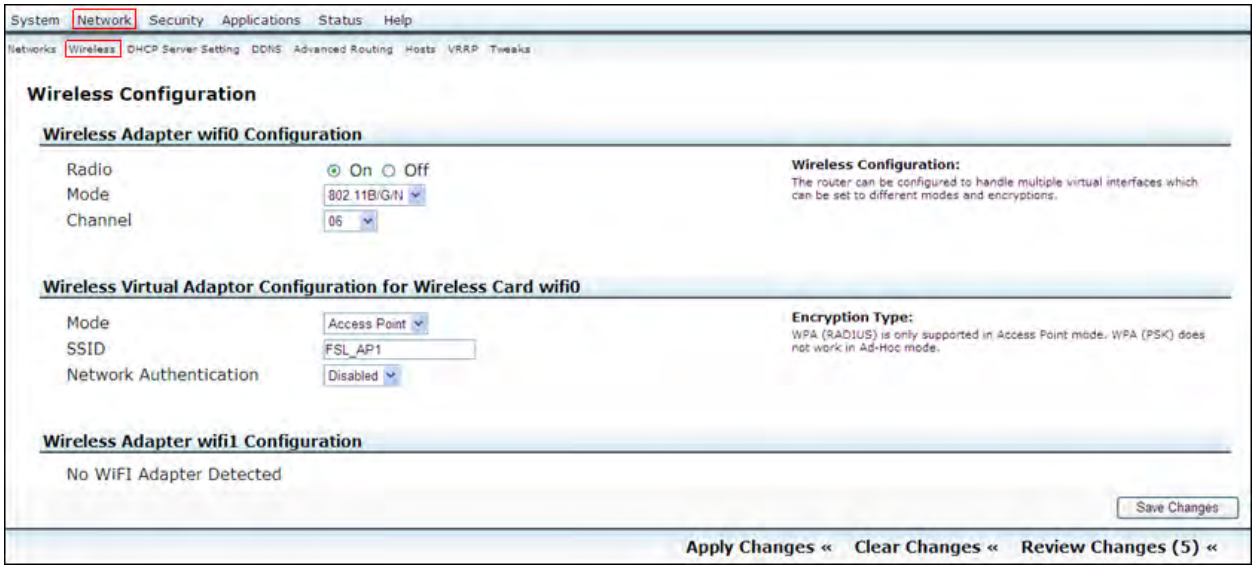
Make sure that PPTP server is available on WAN side if you configure its 'Connection Type' to 'PPTP'.

5.2 Wireless Configuration

The QorIQ board supports two WiFi Modes:802.11B/G/N and 802.11A/N. You can choose the right criteria suitable for your wireless connection. The router supports two wireless cards at the same time. However, the configuration steps for both the wireless cards are same. After configuring 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 open the Wireless configuration page.

Figure 5-6: Network > Wireless Configuration



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.

5.3 DHCP Configuration

The router can be used as network's DHCP (Dynamic Host Configuration Protocol) server, which automatically assigns an IP address to each PC on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.

Click **Network** > **DHCP** to open the DHCP configuration page (Figure 5-7).

Figure 5-7: DHCP Configuration

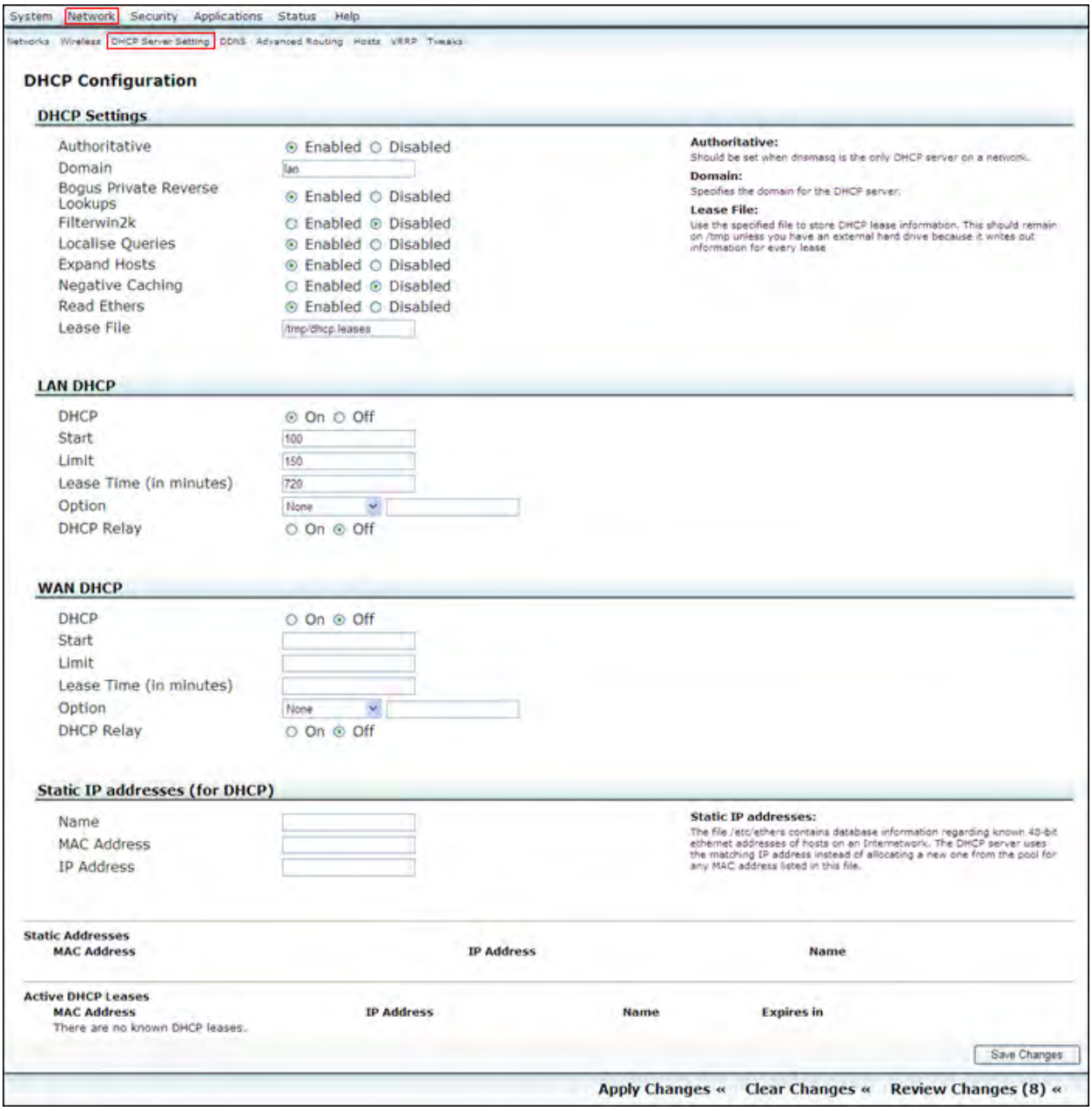


Table 5-1 describes DHCP Configuration page options.

Table 5-1 DHCP Configuration

Options		Description
DHCP Settings	Authorative	Should be set when dnsmasq is the only DHCP server on a network.
	Domain	Specifies the domain for the DHCP server.

	Bogus Private Reverse Lookups	When enabled, it fake reverse lookups for RFC1918 private address ranges.
	Filterwin2K	When disabled, it does not forward spurious DNS requests from Windows hosts.
	Localise Hosts	When enabled, it answers DNS queries based on the interface a query was sent to.
	Expand Hosts	When enabled, it expands simple names in `/etc/hosts` with domain-suffix.
	Negative Caching	When disabled, it does NOT cache failed search results.
	Read Ethers	Read DHCP static host information from /etc/ethers.
	Lease File	Use the specified file to store DHCP lease information. This should remain on `/tmp` unless you have an external hard drive because it writes out information for every lease.
LAN DHCP	DHCP	Specify options to be sent to DHCP clients.
	Start	Enable DHCP assigned IP in the range.
	Limit	Specify maximum number of DHCP leases (defaults to 150).
	Lease Time (in minutes)	Specify maximum time of DHCP leases.
	Option	DHCP option sent even if the client does not request it.
	DHCP Relay	Forwarding client-originated DHCP packets to a DHCP server.
WAN DHCP	DHCP	Specify options to be sent to DHCP clients.
	Start	Enable DHCP assigned IP in the range.
	Limit	Specify maximum number of DHCP leases (defaults to 150).
	Lease Time (in minutes)	Specify maximum time of DHCP leases.
	Options	DHCP option sent even if the client does not request it.
	DHCP Relay	Forwarding client-originated DHCP packets to a DHCP server.
Static IP addresses (for DHCP)	Name	Enter the name
	MAC Address	Enter the MAC address.
	IP Address	Enter the IP address.
Static Addresses		The file `/etc/ethers` contains database information

	regarding known 48-bit Ethernet addresses of hosts on an Inter-network. The DHCP server uses the matching IP address instead of allocating a new one from the pool for any MAC address listed in this file.
Active DHCP Leases	Displays the active DHCP leases.

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

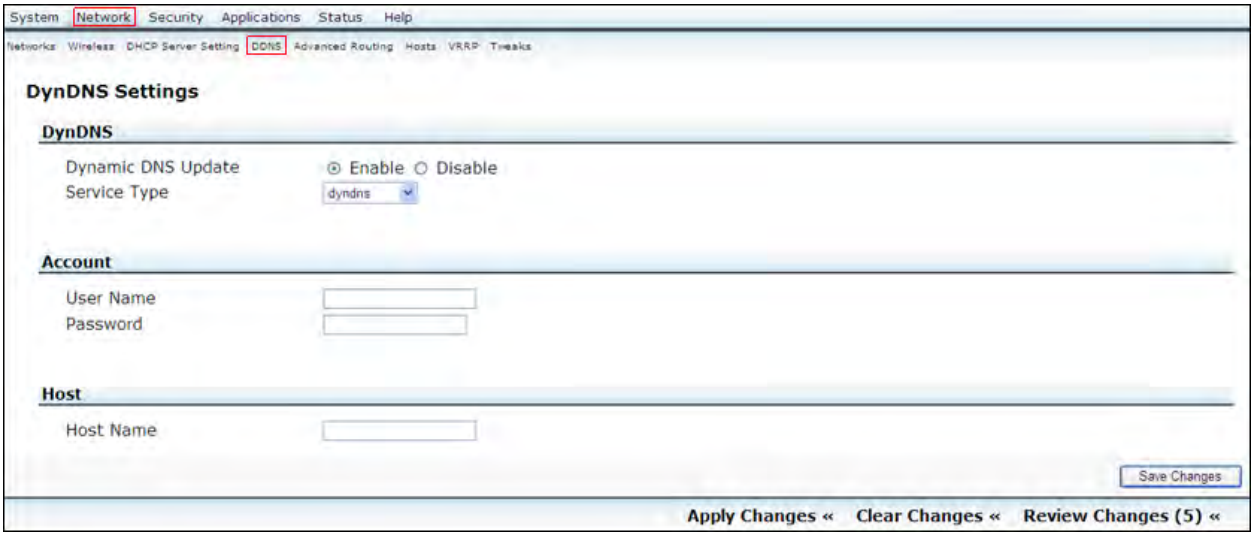
5.4 DDNS

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 this device 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 **DDNS** to open the **DynDNS Settings** page (Figure 5-8), 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 5-8: DynDNS Settings



5.5 Advanced Routing

Static routes while manually intensive to keep up, are a very quick and effective way to route data from one subnet to different subnet.

Some ISPs require static routes to build your routing table instead of using dynamic routing protocols. Static routes do not require CPU resources to exchange routing information with a peer router. You can also use static routes to reach peer routers that do not support dynamic routing protocols. Static routes can be used together with dynamic routes.

Caution!

Do not introduce routing loops in your network.

Click **Network** > **Advanced Routing** to configure static routes. The Static Routes configuration page appears (Figure 5-9).

Figure 5-9: Static Routes Page

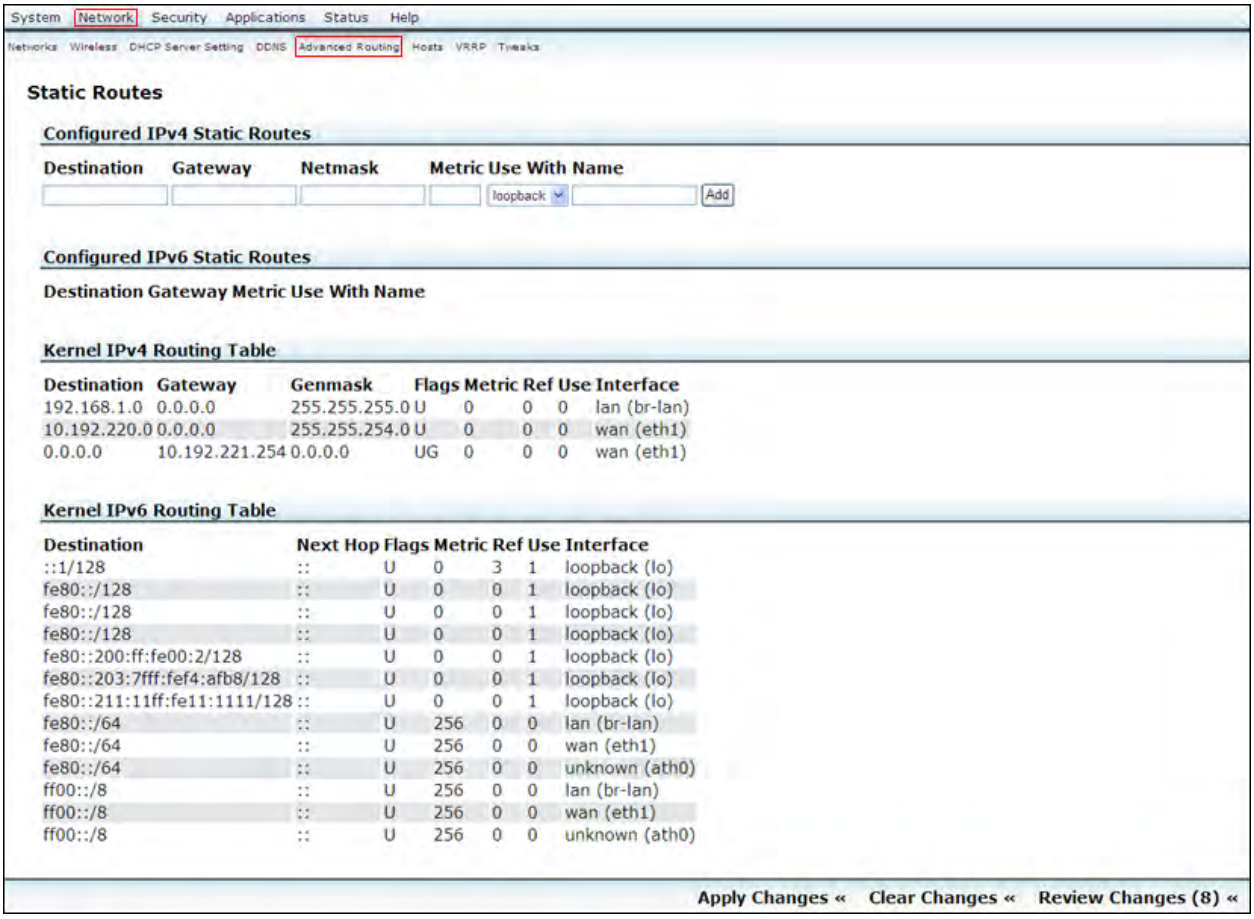


Table 5-2 describes the statics routes options.

Table 5-2: Static Configuration

Options		Description
Configured IPv4 Static Routes	Destination	Enter the network address of the remote LAN segment.
	Gateway	If this Router is used to connect your network to the Internet, then your gateway IP is the Router's IP Address. If you have another router handling your

		network's Internet connection, enter the IP Address of that router instead.
	Netmask	Enter the Netmask used on the destination LAN IP domain.
	Metric Use With	Gives the number of routers that a data packet passes through before reaching its destination.
Configured IPv6 Static Routes	Name	Enter Name.
	Destination	Enter the network address of the remote LAN segment.
	Gateway	If this Router is used to connect your network to the Internet, then your gateway IP is the Router's IP Address. If you have another router handling your network's Internet connection, enter the IP Address of that router instead.
	Netmask	Enter the Netmask used on the destination LAN IP domain.
	Metric Use With	Gives the number of routers that a data packet passes through before reaching its destination.
	Name	Enter Name.
Kernel IPv4 Routing Table	Destination	Network address of the remote LAN segment.
	Gateway	Router's IP Address you are connected to.
	Genmask	Netmask used on the destination LAN IP domain.
	Flags	Displays connection status.
	Metric	Number of routers that a data packet passes through before reaching its destination.
	Ref	Number of reference to this router.
	Use	Count of lookups for the router.
	Interface	Displays connection interface name.

5.6 Hosts

The file /etc/hosts is used to look up the IP address of a device connected to a computer network. The hosts file describes a many-to-one mapping of device names to IP addresses. When accessing a device by name, the networking system attempts to locate the name within the hosts file before accessing the Internet domain name system.

Click **Network** > **Hosts** to configure hosts. The Host Configuration page appears (Figure 5-10).

Figure 5-10: Host Configuration

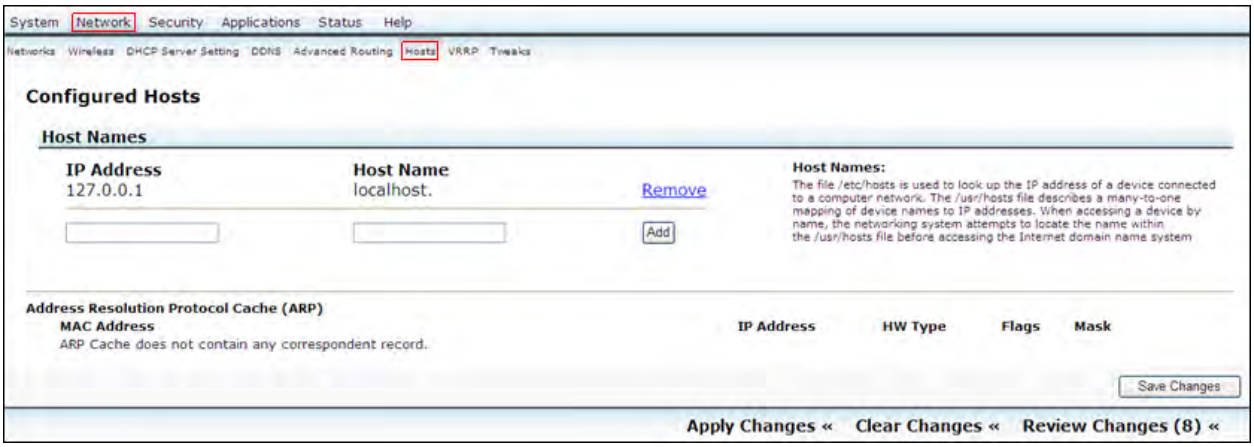


Table 5-3 describes Host Configuration page options.

Table 5-3 Host Configuration

Options		Description
Host Names	IP Address	Displays the host IP address.
	Host Name	Displays the host name.
	Remove Link	Click to remove IP address and host name.
	Add Button	Click to add IP address and host name to the list.
Address Resolution Protocol Cache (ARP)	MAC Address	Displays the MAC address.
	IP Address	Displays the IP address.
	HW Type	Displays the hardware address type.
	Flags	Displays the connection status.
	Mask	Displays the mask.

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

5.7 VRRP

VRRP (Virtual Router Redundancy Protocol) is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts.

Click **Network** > **VRRP**. The VRRP Settings page appears (Figure 5-11).

Figure 5-11: VRRP Settings Page

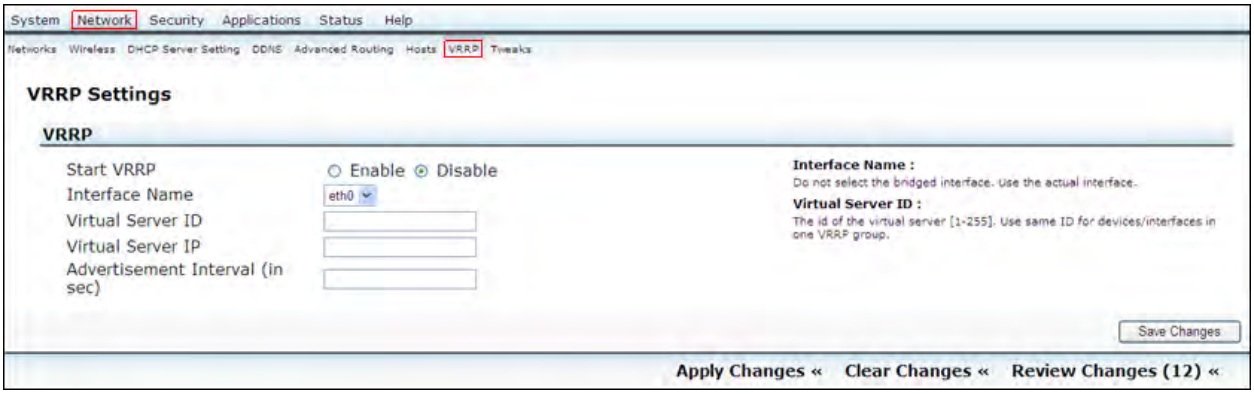


Table 5-4 describes the VRRP settings page.

Table 5-4 VRRP Settings

Options		Description
VRRP	Start VRRP	Enable the VRRP function.
	Interface Name	Select the name of a backup group virtual router interface.
	Virtual Server ID	Identifies the virtual router this packet is reporting status for.
	Virtual Server IP	Enter the Virtual Server IP address. The number of IP addresses contained in this VRRP advertisement.
	Advertisement Interval (in sec)	Indicates the time interval in seconds between advertisements. This field is used for troubleshooting misconfigured routers.

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

5.8 Tweaks

Router Tweaks is a specialized terminal shell that control the configuration of routers easily.

Click **Network** > **Tweaks** to open the network tweaks settings page (Figure 5-12).

Figure 5-12: Networking Tweaks Page

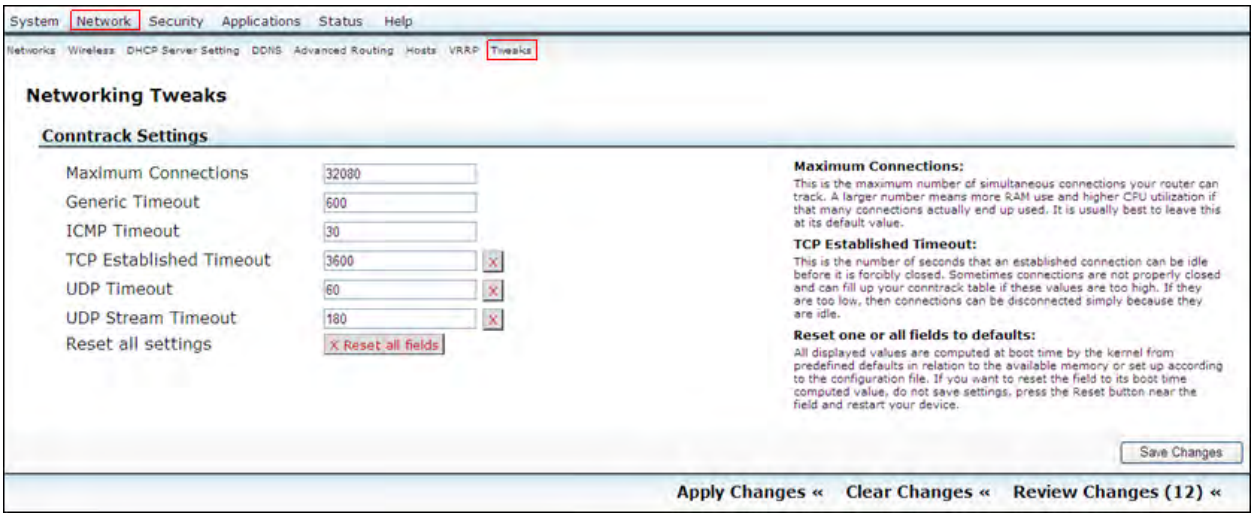


Table 5-5 describes the networking tweaks options.

Table 5-5 Networking Tweaks

Options		Description
Conntrack Settings	Maximum Connections	This is the maximum number of simultaneous connections your router can track. A larger number means more RAM use and higher CPU utilization if that many connections actually end up used. It is usually best to leave this at its default value.
	Generic Timeout	This is the number of seconds that a generic connection is forcibly closed.
	ICMP Timeout	This is the number of seconds that Internet Control Message Protocol for the host, transmission of control messages between routers is closed.
	TCP Established Timeout	This is the number of seconds that an established connection can be idle before it is forcibly closed. Sometimes connections are not properly closed and can fill up your conntrack table if these values are too high. If they are too low, then connections can be disconnected simply because they are idle.
	UDP Stream Timeout	This is the number of seconds that UDP streams should not prevent the screen-saver from starting when they are terminated.

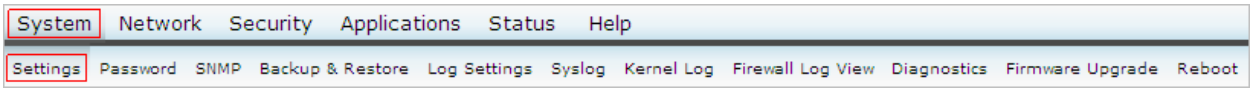
	Reset all settings	All displayed values are computed at boot time by the kernel from predefined defaults in relation to the available memory or set up according to the configuration file. If you want to reset the field to its boot time computed value, do not save settings, press the Reset button near the field and restart your device.

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

6 System

This section explains selecting or changing system items. It has various options like Settings, Password, Firmware Upgrade, SNMP, Reboot etc. Click **System** (Figure 6-1), then proceed with the respective sections.

Figure 6-1: System



6.1 Settings

Configure the system settings for wireless router.

Click **Settings**. Figure 6-2 depicts the **System > Settings** window. Type the host name and select your time zone or closest region.

Figure 6-2: System Settings

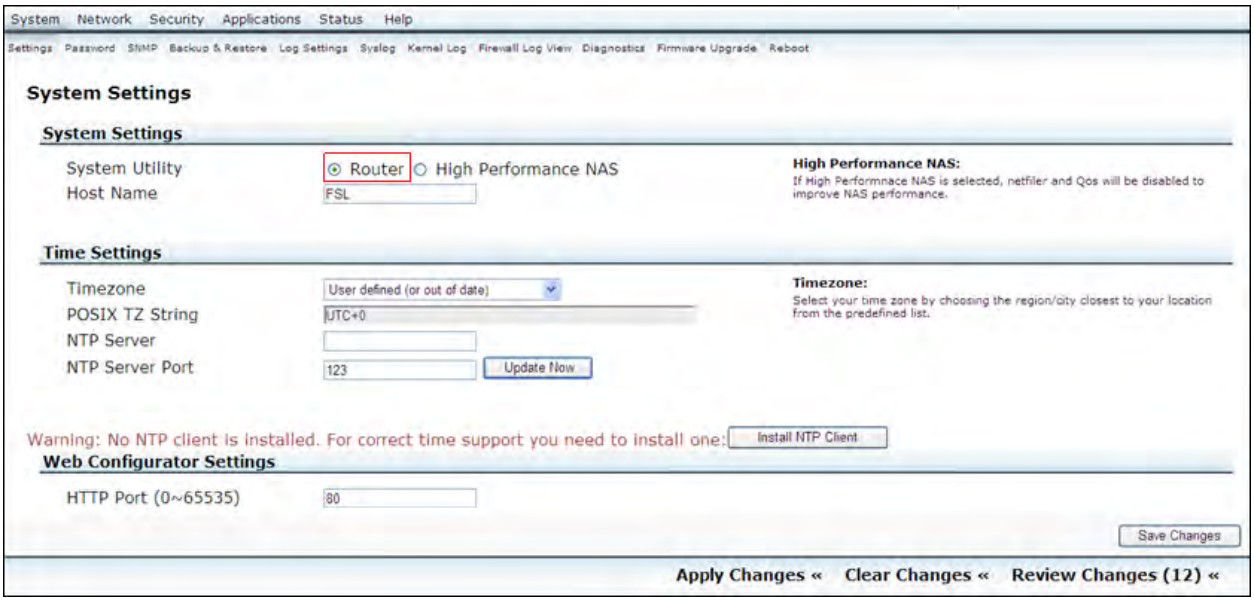


Table 6-1 describes the system settings.

Table 6-1: System Settings Page

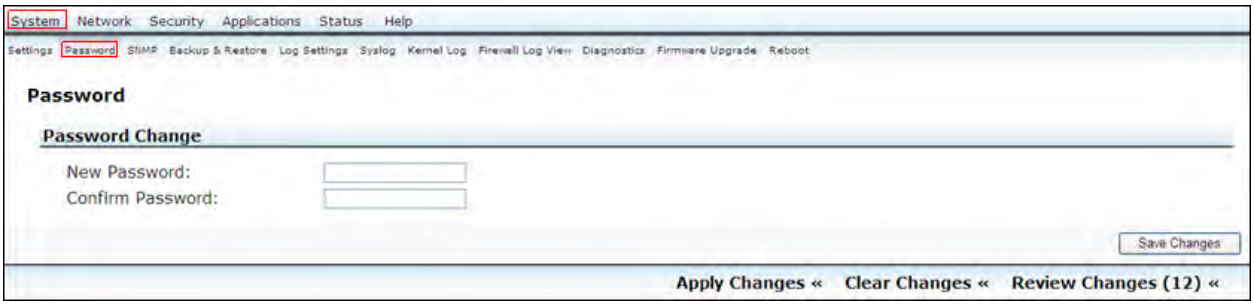
Options			Description
System Settings	System Utility	Router	Select this option for setting the wireless router.
		High Performance NAS	Select this option for disabling the netfilter and QOS to.
	Host Name		Enter the host name.
Time Settings	Timezone		Select the timezone from the drop-down list. Set up your time zone according to the nearest city of your region from the predefined list.
	POSIX TZ String		Provide accuracy for at least one transition into and out of daylight saving time (DST) and possibly for more transitions.
	NTP Server		Enter the IP address of your own NTP server.
	NTP Server Port		Enter the Port of your own NTP server.
Web Configurator Settings	HTTP Port (0~65535)		Enter the Port of your own HTTP server.

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

6.2 Password

Click **System** > **Password** to open the 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 6-3: Password



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

6.3 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 6-4 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 6-4: SNMP Settings

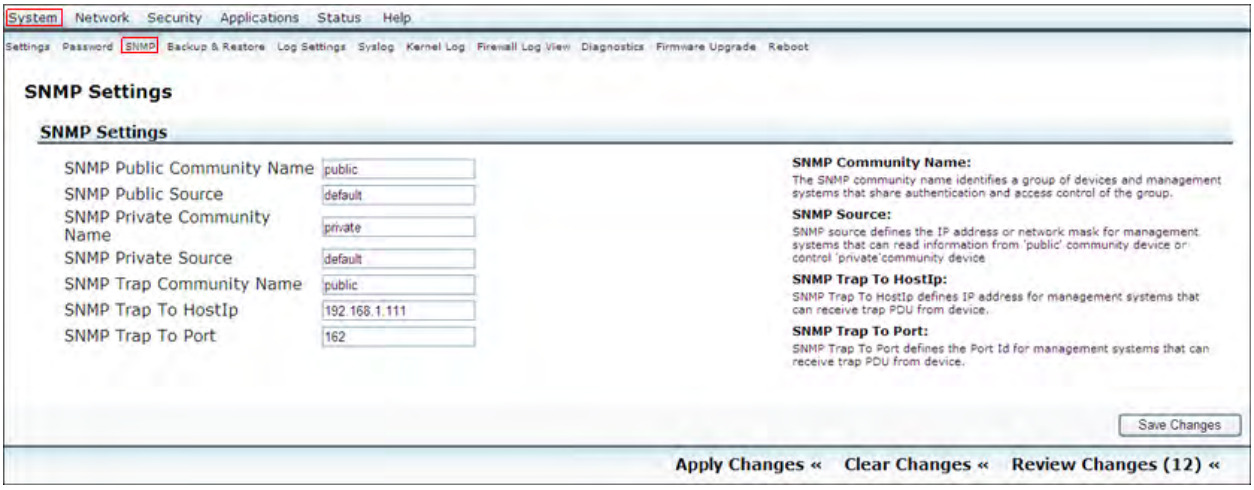


Table 6-2 describes each SNMP setting options in detail.

Table 6-2 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.

6.4 Backup & Restore

Click **System** > **Backup & Restore** to open Backup and Restore configuration page (Figure 6-5).

Figure 6-5: Backup and Restore Page

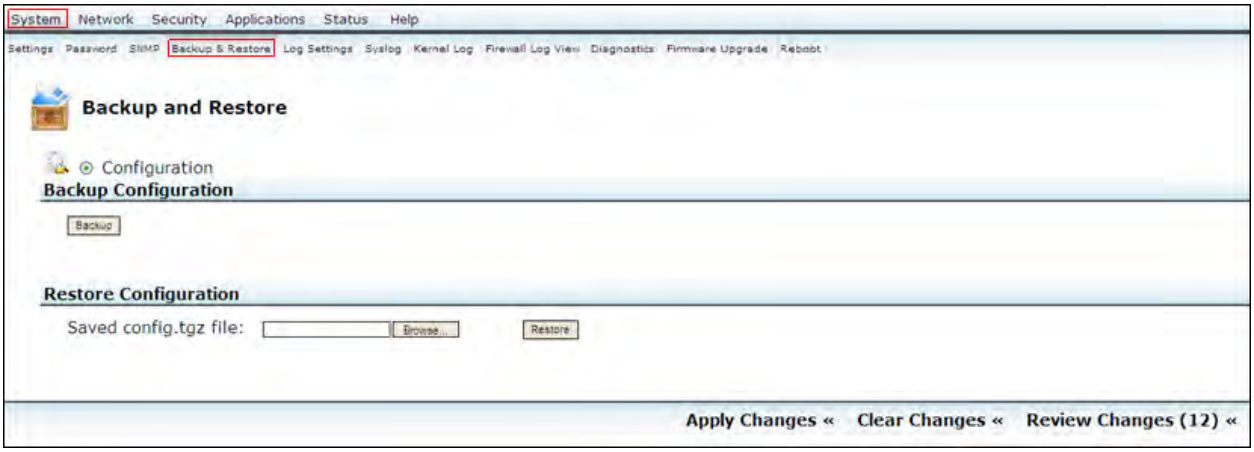


Table 6-3 describes backup and restore configuration.

Table 6-3: Backup and Restore Configuration

Options		Description
Backup Configuration	Backup	To download a copy of the current configuration and store the file (config.tgz) on your PC.
Restore Configuration	Saved config.tgz file	To select a file from the Windows file

		system (previous saved config.tgz file)
	Restore	To start the restoration process.

6.5 Log Settings

This settings work when routers are on the same network, but you can edit the hosts. It allows file to enter the IP of the router. If you want to check the log you can find some information in the log settings and the startup configuration log.

Click **System** > **Log Settings** to open Log Settings page.

Figure 6-6: Log Settings Page

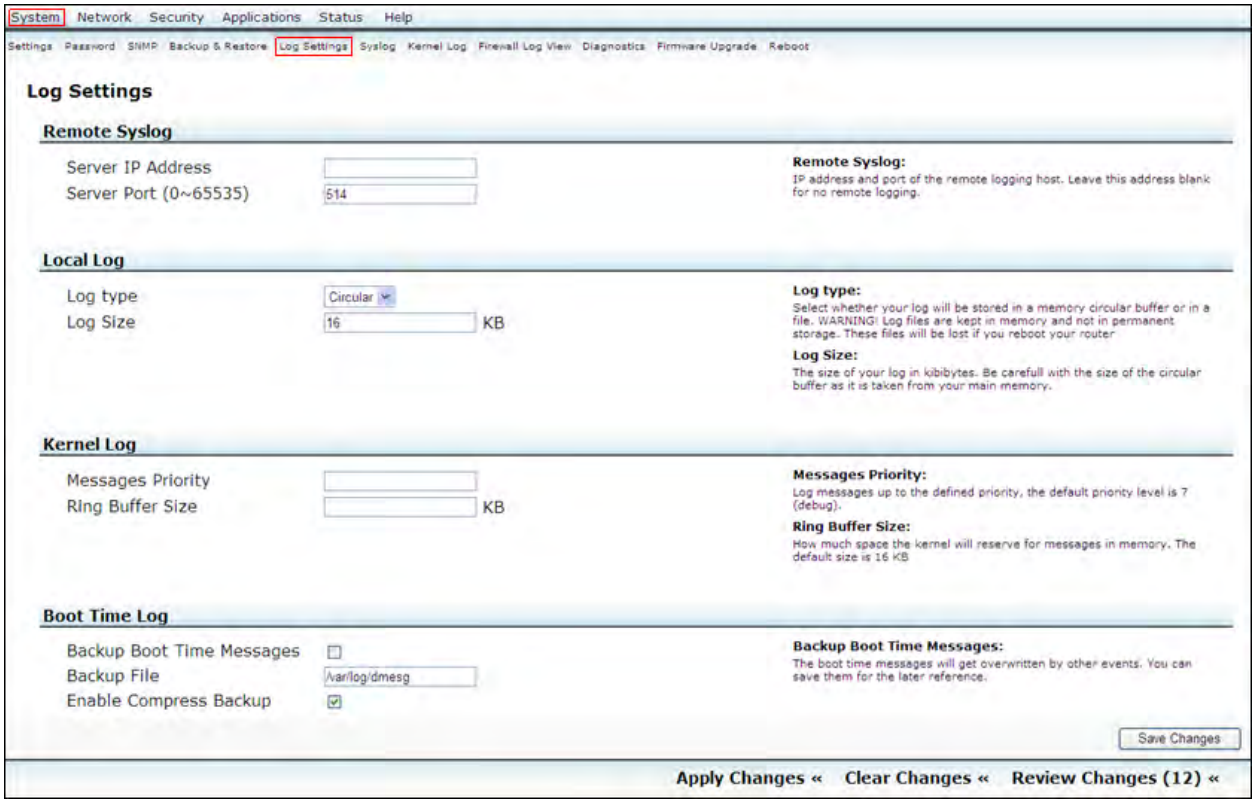


Table 6-4 describes Log setting options.

Table 6-4: Log Settings

Option		Description
Remote Syslog	Server IP Address	This is the IP address of the remote logging host. Leave this address blank for no remote logging.
	Server Port (0~65535)	This is the port of the remote logging host. Leave this address blank for no

		remote logging.
Local Log	Log Type	Whether your log will be stored in a memory circular buffer or in a file. Beware that files are stored in a memory filesystem which will be lost if you reboot your router.
	Log Size	The size of your log in kibibytes. Be carefull with the size of the circular buffer as it is taken from your main memory.
Kernel Log	Message Priority	Log messages up to the defined priority, the default priority level is 7 (debug).
	Ring Buffer Size	How much space will kernel reserve for messages in memory. The default size is 16 KB.
Boot Time Log	Backup Boot Time Messages	The boot time messages will get overwritten by other events. You can save them for the later reference.
	Backup File	Log info saved in defined file.
	Enable Compress Backup	When selected, the log file is saved as compressed.

6.6 Syslog

The Syslog describes a number of related service options. It generates a log message that is distributed by the system logger to propagating event messages.

Click **System** > **Syslog** to open Syslog view page (Figure 6-7).

Figure 6-7: Syslog View

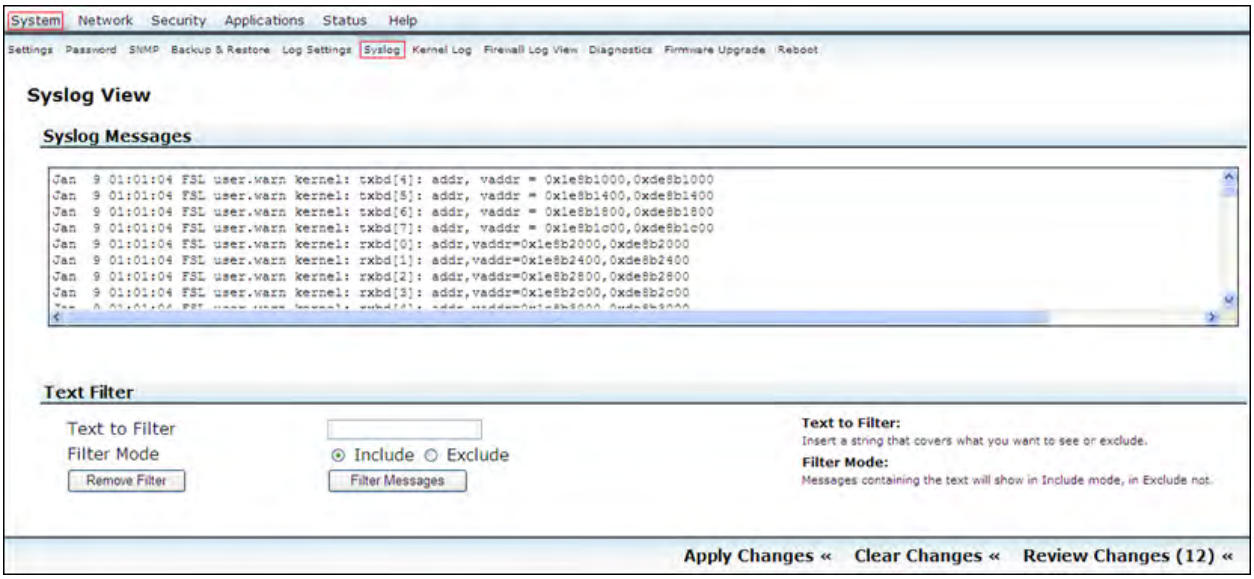


Table 6-5 describes the Syslog page.

Table 6-5: Syslog View

Option		Description
Syslog Messages		Displays syslog messages
Text Filter	Text to Filter	Insert a string that covers what you want to see or exclude.
	Filter Mode	Messages containing the text will show in Include mode. Messages will not display in Exclude mode.
	Remove Filter	Click to remove filter.
	Filter Messages	Click to filter messages.

6.7 Kernel Log

You can check the kernel ring buffer to see what it found during boot up and current operation and message. You can also insert a string that covers what you want to include or exclude.

Click **System** > **Kernel Log** to open Kernel Ring Buffer page (Figure 6-8).

Figure 6-8: Kernel Ring Buffer

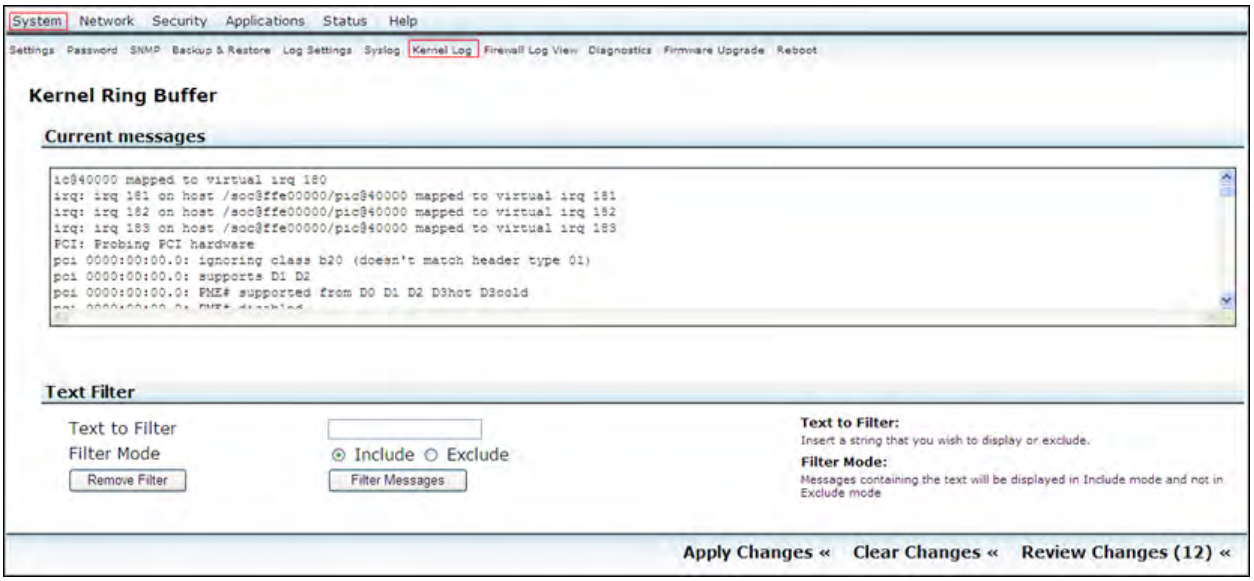


Table 6-6 describes the Kernel Ring Buffer page.

Table 6-6: Kernel Ring Buffer

Option		Description
Current Messages		Displays current messages.
Text Filter	Text to Filter	Insert a string that covers what you want to see or exclude.
	Filter Mode	Messages containing the text will show in Include mode. Messages will not display in Exclude mode.
	Remove Filter	Click to remove filter.
	Filter Messages	Click to filter messages.

6.8 Firewall Log View

Displaying log information about firewall filters. Use this when you want to view the data that has been written to the Firewall log. This is useful if you are troubleshooting Firewall problems or you are temporarily monitoring Firewall behavior.

Click **System** > **Firewall Log View** to open Netfilter log page (Figure 6-9).

Figure 6-9: Firewall Log View

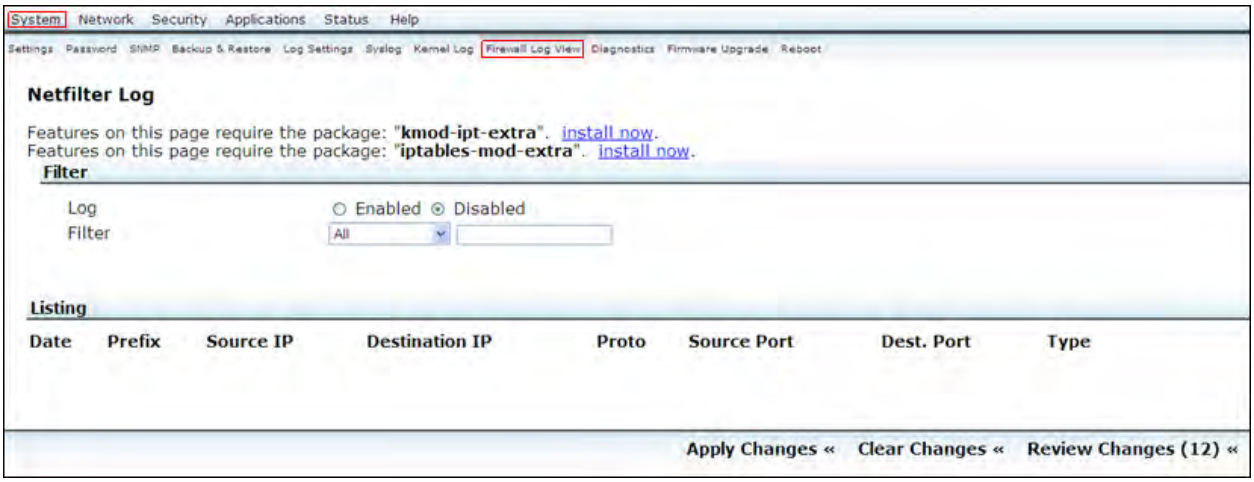


Table 6-7 describes the Netfilter Log page.

Table 6-7: Netfilter Log

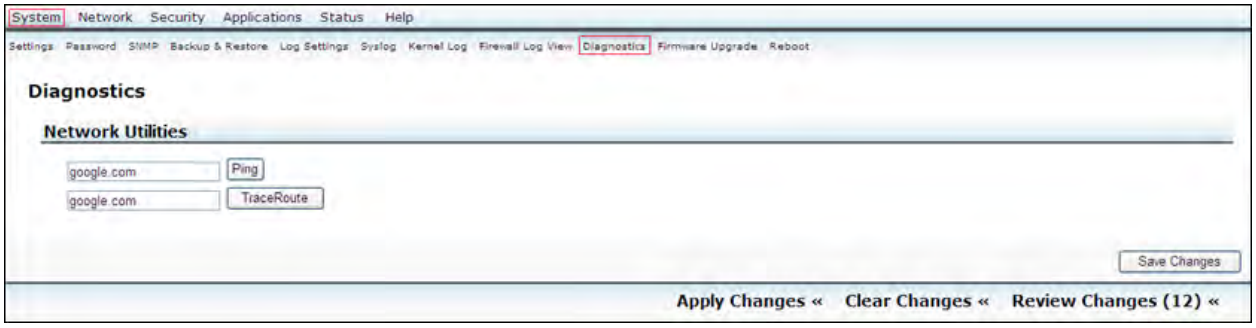
Option		Description
Filter	Log	Click Enabled to enable the Firewall Netfilter Log.
	Filter	Select the Filter type to display log information about configured firewall filters that have been configured with the filter statement at the hierarchy level.
Listing	Date	Display the Netfilter creating date.
	Prefix	Display prefix action statistics about configured firewall filters.
	Source IP	Packet's source IP address.
	Destination IP	Packet's destination IP address.
	Proto	Packet's protocol name.
	Source Port	Packet's source port.
	Dest. Port	Packet's destination port.
	Type	Display the netfilter type.

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

6.9 Diagnostics

Click **Diagnostics**. Use this to verify whether a particular web address or IP address exists or not. In High Performance mode, you can only ping an IP address while in Router mode, you can ping the web address. Also, clicking TraceRoute traces the route of the website or IP address. Figure 6-10 displays the network utilities options to ping and trace route.

Figure 6-10: Diagnostics



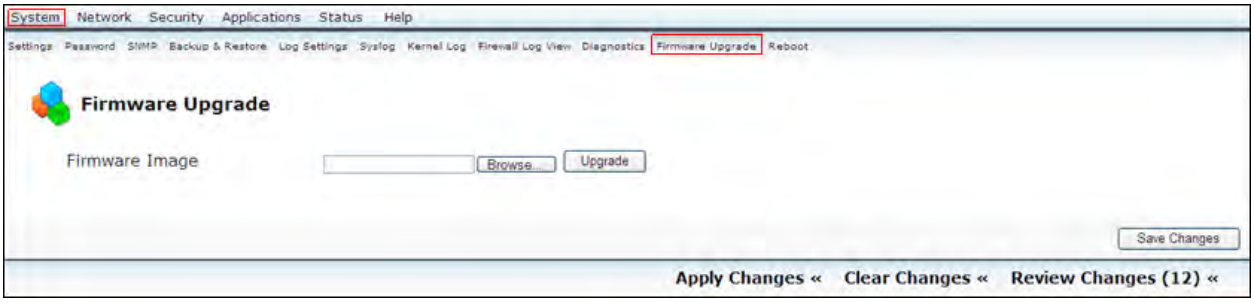
6.10 Firmware Upgrade

Click **Upgrade**. Figure 6-11 depicts the **System > Firmware Upgrade** window. Click **Browse** to locate the new firmware, and 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 6-11: Firmware Upgrade

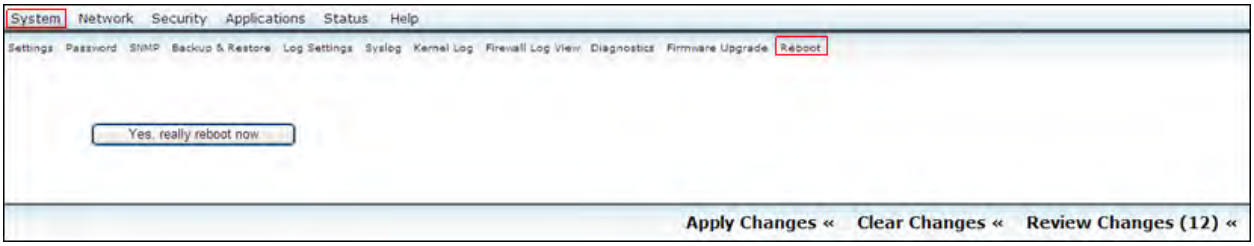


Click **Save Changes**, if certain.

6.11 Reboot

Click **Reboot**. Figure 6-12 depicts the **System > Reboot** window. Click **Yes, really reboot now** button to reboot the router.

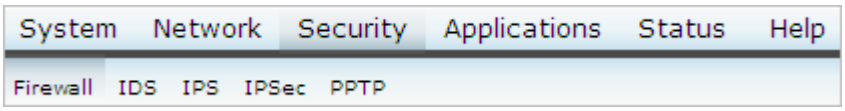
Figure 6-12: Reboot



7 Security

This section explains the various security settings for the device. Click **Security** (Figure 7-1), then proceed with the respective sections.

Figure 7-1: Security

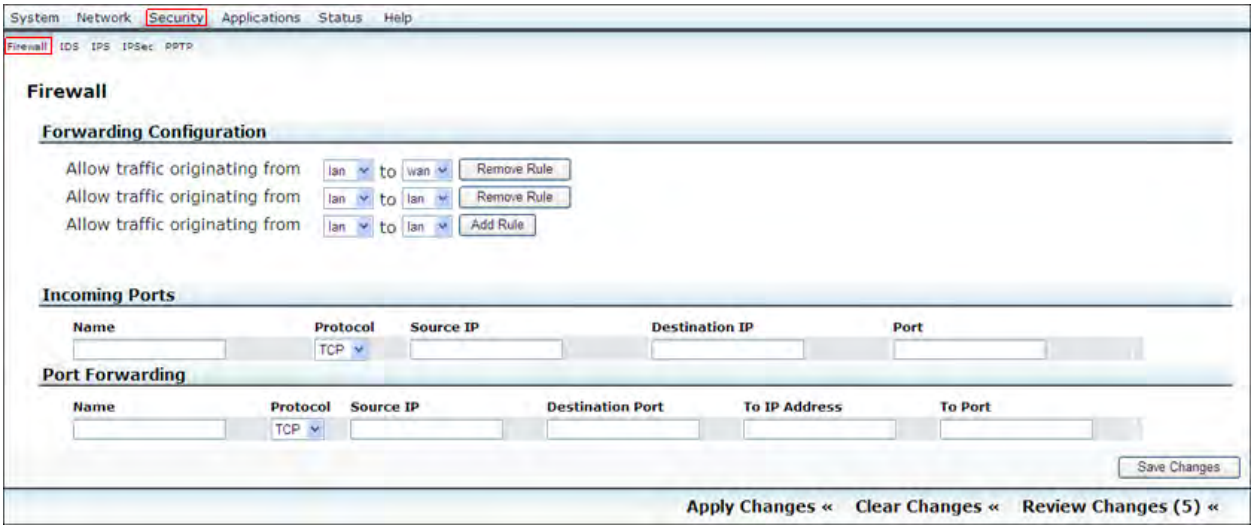


7.1 Firewall

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

Click **Security** > **Firewall** to open the Firewall configuration page (Figure 7-2).

Figure 7-2: Firewall Configuration



7.1.1 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 7-2) 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 server on PC2 and a tftp client on PC1(fill PC2's IP address in the Host IP column). Both of their ports of tftp are set as 69.

4. Use the tftp software; PC1 can transfer any file to PC2 successfully.

7.1.2 Incoming Ports

The Incoming Port screen allows you to customize incoming ports. (Figure 7-3) 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 7-3: Incoming Ports

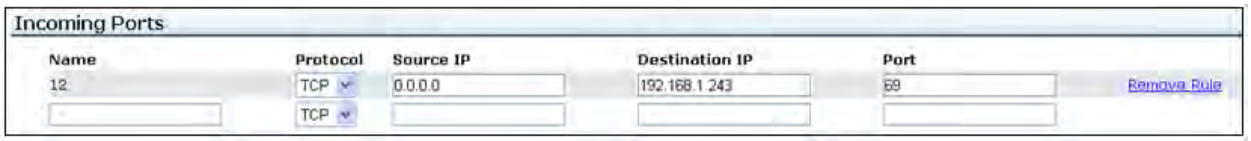


Table 7-1 describes each of the Incoming ports option.

Table 7-1 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.

7.1.3 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 7-4: Port Forwarding

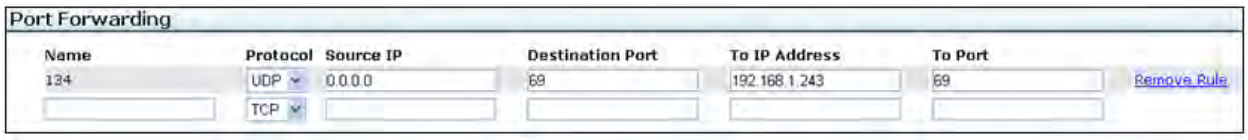


Table 7-2 describes each of the Incoming ports option.

Table 7-2 Port Forwarding

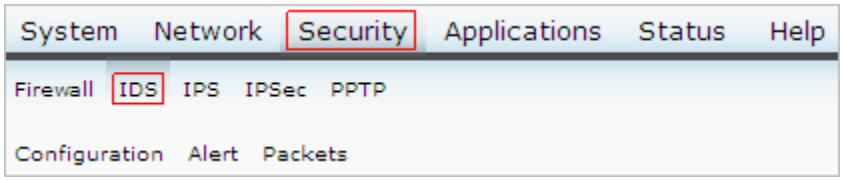
Options	Description
Name	Enter the name of the port.
Protocol	Select the protocol used for this application from the drop-down list. You can select TCP, UDP or Both as a protocol.
Source IP	Enter the source IP.
Destination IP	Enter the destination IP.
To IP Address	Enter the IP address.
Port	Enter the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

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

7.2 Intrusion Detection Systems

This section explains detection of electronic intrusion attempts. Click **IDS** (Figure 7-5), then proceed with the respective sections.

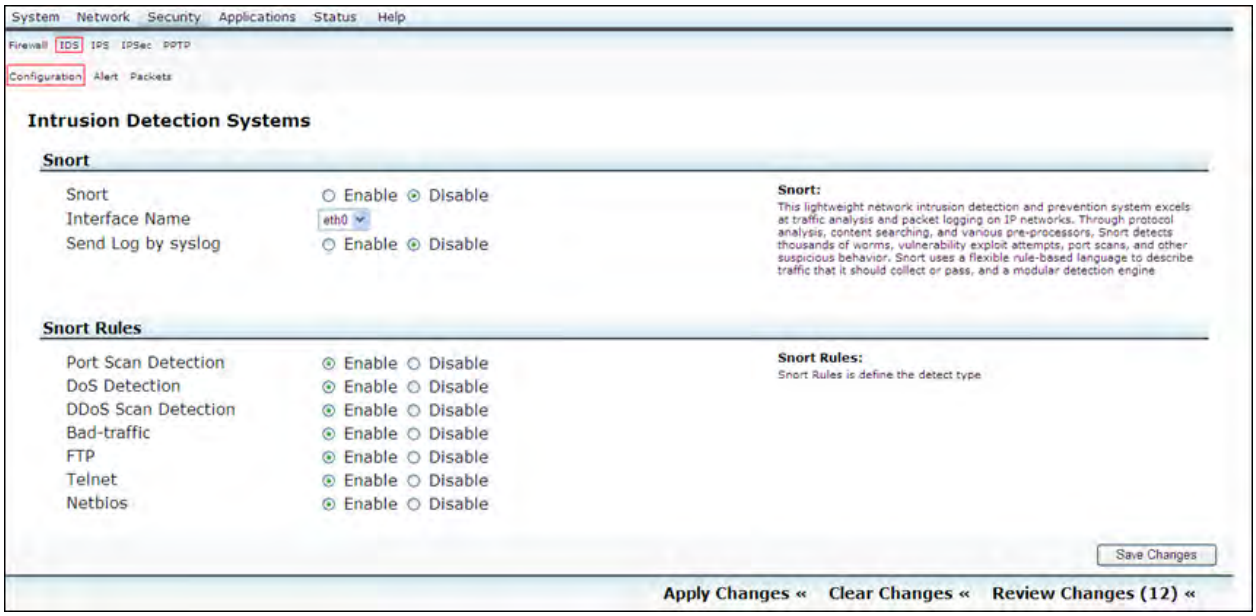
Figure 7-5: IDS



7.2.1 Configuration

Click **IDS**. Figure 7-6 depicts the **IDS > Configuration** window.

Figure 7-6: IDS Configuration



7.2.1.1 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 7-6:

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**.

7.2.1.2 Snort Rules

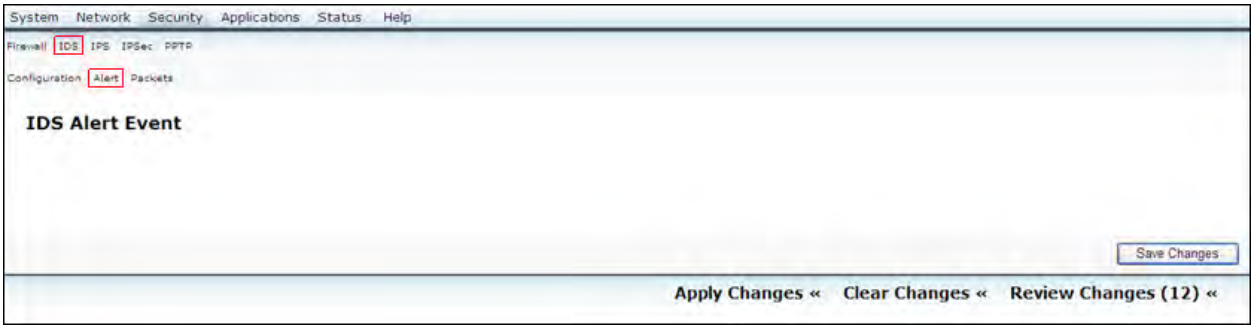
The snort rules define the detect type. Perform the following steps to set snort rules.

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**.

7.2.2 Alert

Click **Alert**. Figure 7-7 shows a log of intrusion alerts.

Figure 7-7: IDS Alert



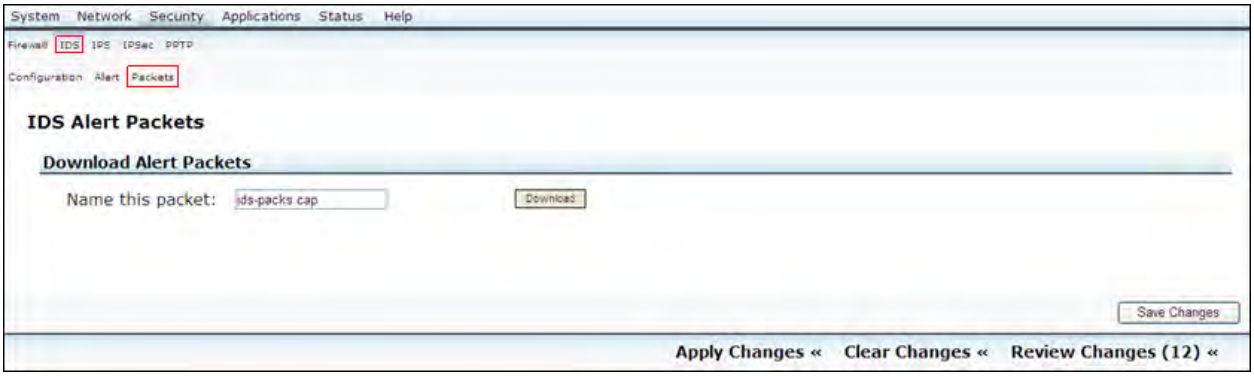
7.2.3 Packets

Click **Packets**. When intrusion occurs, you can save the packet from EWLAN to your PC by clicking **Download** (Figure 7-8).

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 7-8: IDS Packets



7.3 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 7-9), then proceed with the respective sections.

Figure 7-9: IPS

7.3.1 Configuration (IPS Configuration)

Click **Configuration**. Figure 7-10 shows IPS Configuration.

Figure 7-10: IPS Configuration

7.3.1.1 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 7-10.

1. Enable/disable **IPS Function**.

2. Click **Save Changes** button to save the changes.

7.3.2 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 7-11.

Figure 7-11: IPS P2P/IM

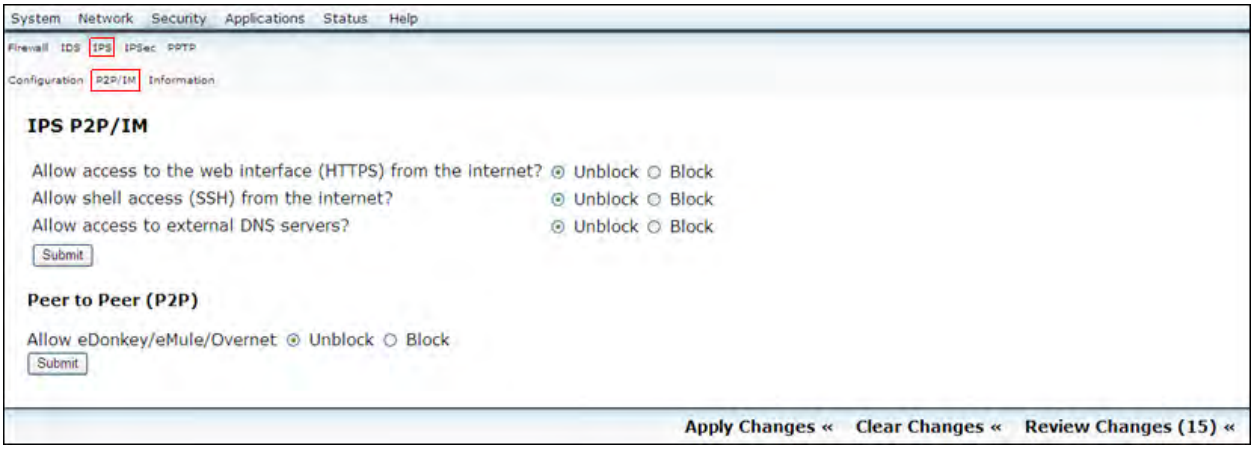


Table 7-3 explains each option given in the **IPS > P2P/IM** page.

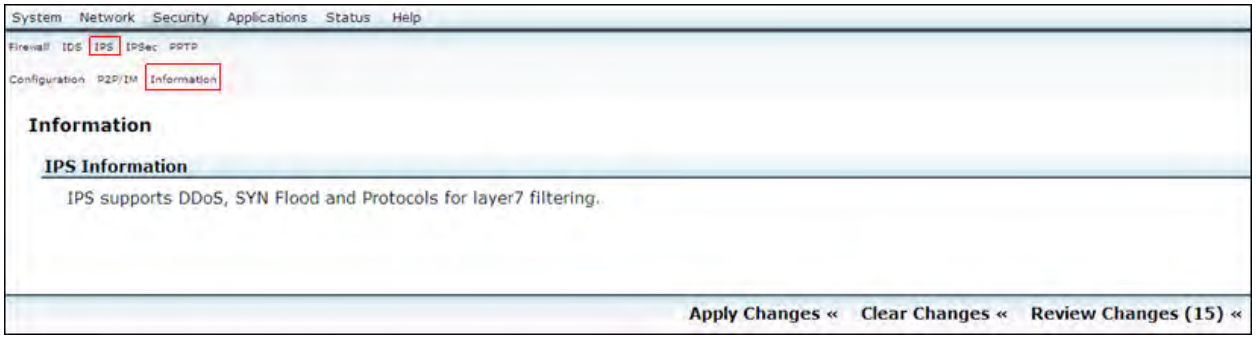
Table 7-3 IPS > P2P/IM Options

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.

7.3.3 Information

Click **Information** to read about IPS support (Figure 7-12).

Figure 7-12: IPS Information



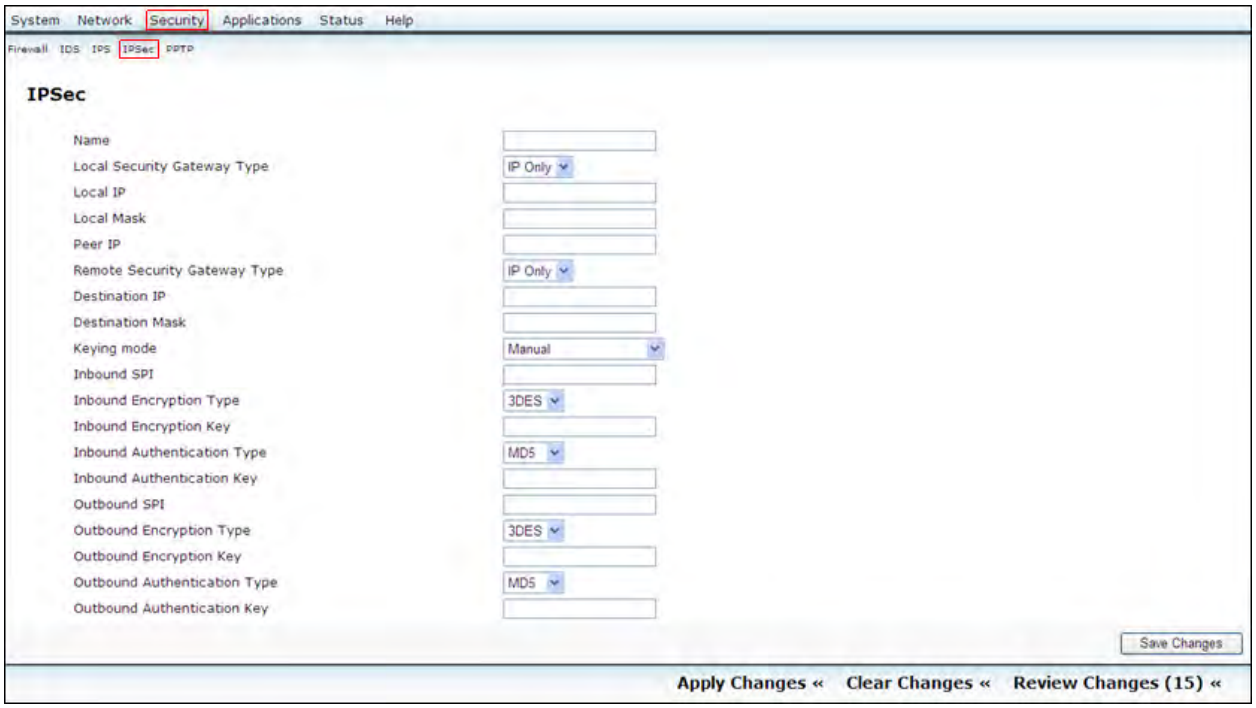
7.4 IPSec

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 **Security > IPSec** to open the IPSec page (Figure 7-13).

Figure 7-13: IPSec



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. In case, 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. In case, 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 5.4.1.1 for details.

7.4.1 Keying Mode

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.

7.4.1.1 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 7-14 below:

Figure 7-14: IKE with preshared Key

Table 7-4 describes the IKE with preshared key options for phase 1 and phase 2.

Table 7-4 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.

7.4.1.2 Manual

Select **Manual** from **Keying mode** drop-down list. The options changes in the application page as shown in Figure 7-15 below:

Figure 7-15: Manual Keying Mode

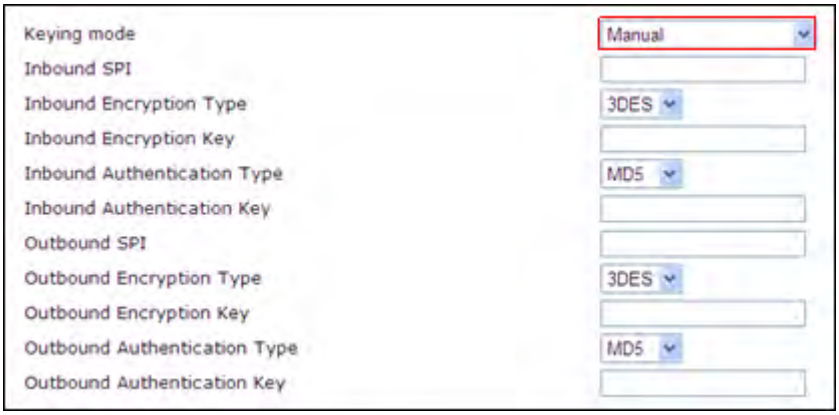


Table 7-5 describes the Manual keying mode.

Table 7-5 Manual Keying Mode

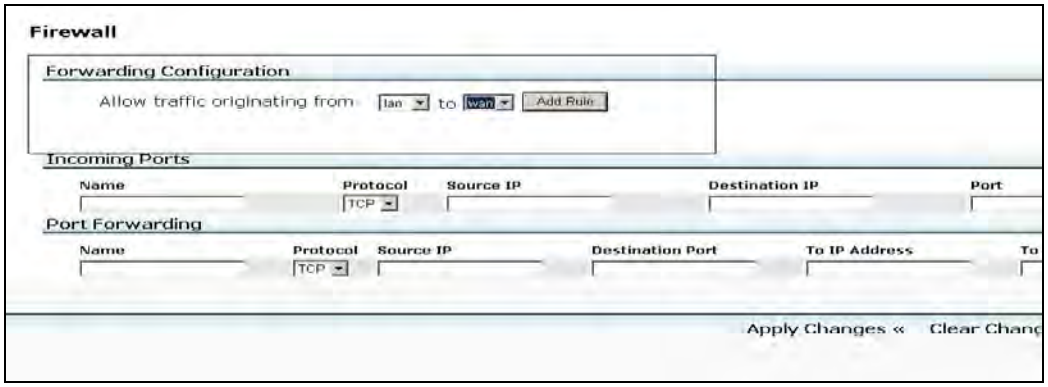
Function	Description
Inbound/Outbound SPI	The SPI (Security Parameter Index) is carried in the ESP header. Its range is 256 -65535. Each tunnel must have an unique Inbound SPI and Outbound SPI. Notice that Inbound SPI must match the other router's Outbound SPI.

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 7-16 below:

Figure 7-16: Firewall tab



7.5 PPTP

Click **Security** > **PPTP** to open the PPTP page (Figure 7-17).

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

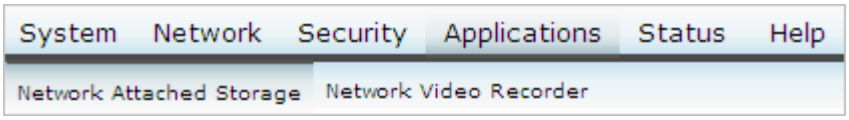
5. Click **Save Changes** to save the configuration data.

Figure 7-17: VPN > PPTP VPN Users page

8 Applications

This section explains the unit's various applications. Click **Applications** (Figure 8-1), then proceed with the two respective sections.

Figure 8-1: Applications

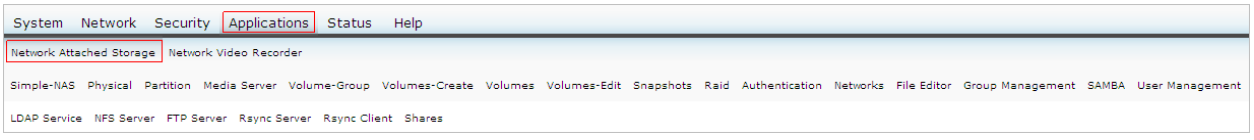


8.1 Network Attached Storage

Network Attached Storage (NAS) is file-level computer data storage connected to a computer network that provides data access to heterogeneous network clients. NAS is essentially a self-contained computer connected to a network, with the sole purpose of supplying file-based data storage services to other devices on the network. The operating system and other software on the NAS unit provide the functionality of data storage, file systems, and access to files, and the management of these functionalities.

Click **Network Attached Storage** (Figure 8-2), then proceed with the respective sections.

Figure 8-2: Network Attached Storage

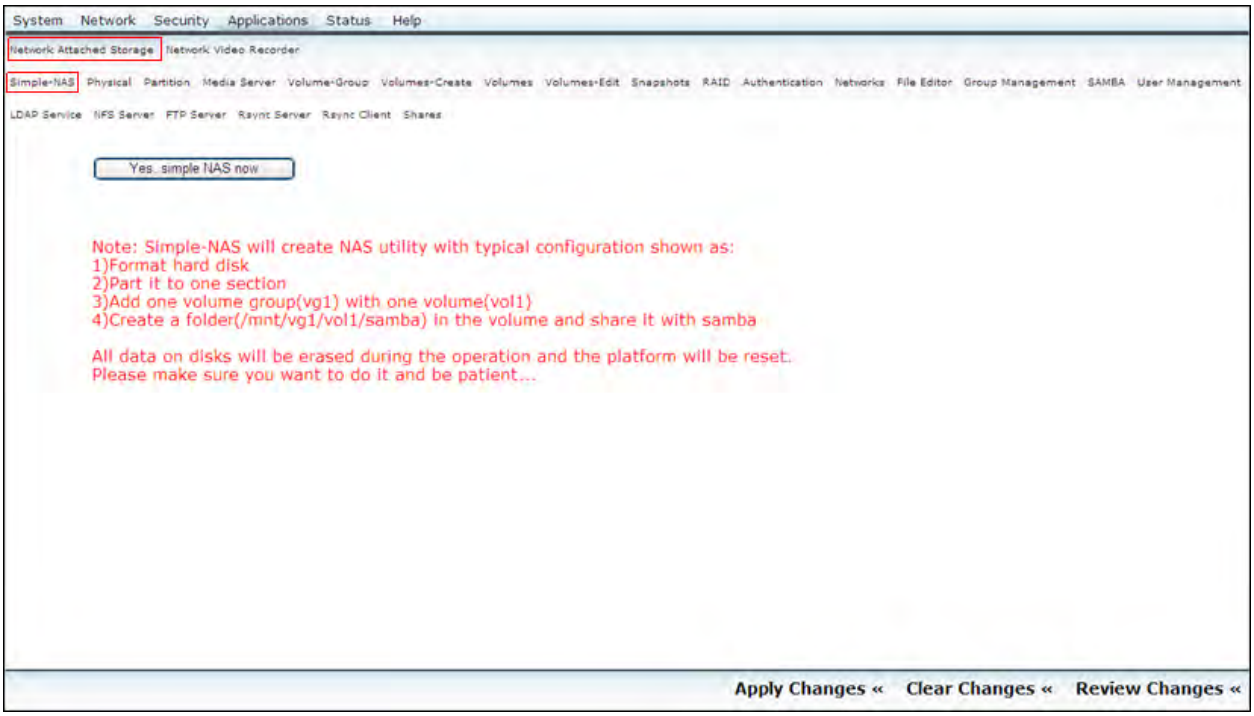


8.1.1 Simple-NAS

The Simple NAS tab allows you to configure NAS. It creates NAS utility with typical configuration. During the operation all data on disk is erased and the platform is reset.

Click **Yes, simple NAS now**. Figure 8-3 displays the **Simple-NAS** window.

Figure 8-3: Simple-NAS Page



Click **Apply Changes** to apply the changes.

8.1.2 Physical

The Physical page allows you to view disk and scsi status.

Click **Physical**. Figure 8-4 depicts the **Disk Management** window.

Figure 8-4: Disk Management

Table 8-1 describes the Disk Management window.

Table 8-1: Disk Management Window

Function	Description
Devices	Displays the path name.
Type	Display the hard disk interface type.
Description	Display the hard disk product information.
Size	Display the disk size.
Label Type	Display the disk label type.
Partitions	Display the disk partition number.
Action	Click **Edit** to move to partition tab.

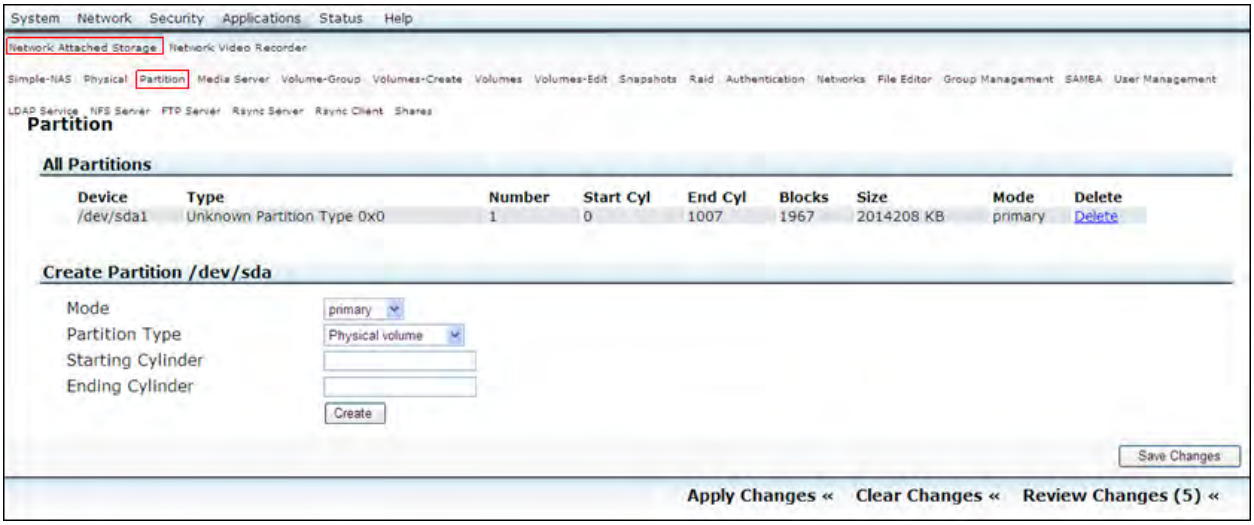
Click **Save Changes** button to save the changes.

8.1.3 Disk Partition Management

You can add/delete a primary/extended/logical partition with physical/raid type from Volume Edit Partition tab.

Click **Edit** on the **Applications** >**Network Attached Storage** >**Physical** tab to open **Partition** page. (Figure 8-5)

Figure 8-5: Partition Page



CAUTION!

If you select Edit, the disk will be parted.

Table 8-2 describes options in partition window.

Table 8-2: Partition Window

Options		Description
All Partition	Device	Displays the path name of the partition disk.
	Type	Displays the disk partition type.
	Number	Displays the disk partition order.
	Start Cyl	Displays the one disk partition starting cylinder.
	End Cyl	Displays the one disk partition ending cylinder.
	Blocks	Displays the disk partition blocks size.
	Size	Displays the total capacity of the partition disk.
Create Partition dev/sda	Mode	A maximum of four primary partitions can be placed on any hard disk. One of the four partitions may be designated as an extended partition. This partition may then be subdivided into multiple logical partitions
	Partition Type	Add the physical volume/RAID array member flag on partitions.
	Starting Cylinder	Enter the disk partition starting cylinder.
	Ending Cylinder	Enter the disk partition ending cylinder.

Click **Save Changes** button to save changes.

8.1.4 UPnP Configuration

The UPnP configuration page allows you to set WAN speeds in kilobits. This is for reporting to UPnP clients that request it only.

Click **Applications** >**Network Attached Storage** >**Media Server**. The UPnP configuration page appears (Figure 8-6).

Figure 8-6: UPnP Configuration Page

Table 8-3 describes UPnP configuration options.

Table 8-3 UPnP Configuration

Options		Description
UPNP	UPNP Daemon	For the background process to send and receive here.
	WAN Upload (bits/sec)	Displays the WAN upload speeds in kilobits.
	WAN Download (bits/sec)	Displays the WAN download speeds in kilobits
	Log Debug Output	Use the Log Debug Output command to redirect protocol debug output to the current log.

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

8.1.5 Volume Group Management

The Volume Group management page allows you to create or delete a volume group. It also allows you to add a PV (Physical Volume) to an existing volume group. You can also get detailed information of volume group through Volume Group Management table.

NOTE

You cannot delete Volume group, if it contains volumes.

Figure 8-7 displays the Volume Group Management page.

Figure 8-7: Volume Group Management Page

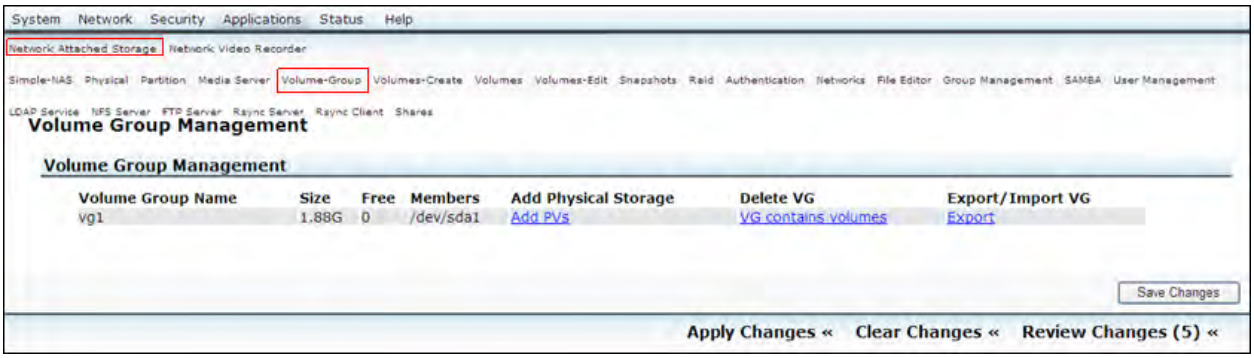


Table 8-4 describes options in volume group management page.

Table 8-4: Volume Group Management Page

Options	Description
Volume Group Name	Enter the name for volume group that you want to create.
Size	Display the capacity of the volume group that you choose.
Free	Display the volume group remaining capacity.
Members	Display the path name of the disk partition you choose.
Add Physical Storage	Add the disk partition that you have created in the volume group.
Delete VG	Delete the volume group that you have created.
Export/Import VG	Export VG deletes VG information from local odm library while keep all data unchanged. Import VG imports VG to a new system with all saved information For example, To use this function follow the steps given below: 1. Create a partition at a disk. 2. Create a volume group(vg1). 3. Create a volume(vol1). 4. Create a file and input some information to created file by this command at volume

	path:echo "1111111111111111" > /mnt/vg1/vol1/test.txt 5. Export volume group which volume group includes created volume at volume group page 6. Restart you ewlan board and shutdown your board when u-boot load 7. Remove disk and input the disk at new ewlan board 8. Start new ewlan board 9. Import volume group at volume group page at new board 10. Check test.txt information by this command at shell(cat /mnt/vg1/vol1/test.txt)

Click **Save Changes** button to save changes.

8.1.6 Volume-Create

The Volume create page allows you to create a logical volume with ext3/xfs file system on an existing volume group. You can also get the detail of storage statistics for the volume groups.

Click **Volumes-Create**. Figure 8-8 displays the **Applications** >**Network Attached Storage** > **Volumes-Create** page.

Figure 8-8: Volume-Create Page

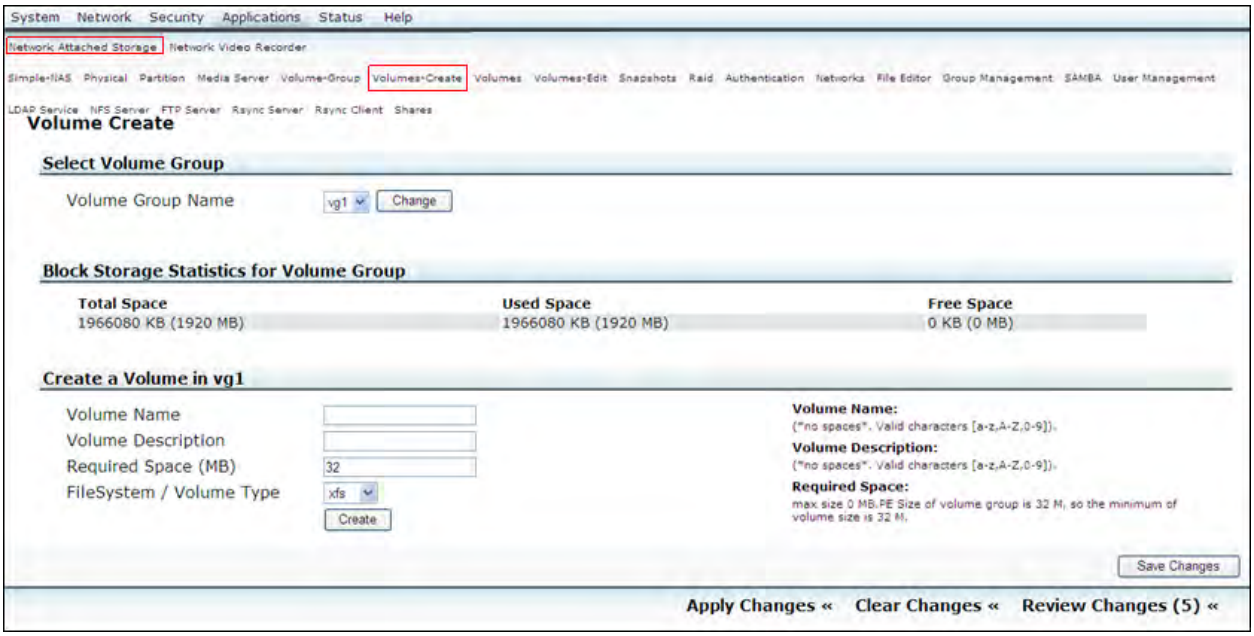


Table 8-5 describes the volume-create page in detail.

Table 8-5: Volume Create

Options		Descriptions
Select Volume Group	Volume Group Name	Select the name from the volume group drop-down list.
	Change Button	Click to change the next volume group that you have created.
Block Storage Statistics for Volume Group	Total Space	Display the total space of block storage in the volume group that you choose.
	Used Space	Display the space that the volumes have used.
	Free Space	Display the space that the volumes group remaining.
Create a Volume in test2	Volume Name	Enter volume name.
	Volume Description	Enter the volume description.
	Required Space (MB)	Enter the required space (MB).
	File System/Volume Type	Select the file system or volume type from the volume group drop-down list.
	Create button	Click to create volume.

Click **Save Changes** button to save changes.

8.1.7 Volumes

Users can get detail information for an existing volume group, or delete it through “Volumes in volume group” table. Note that if it has a snapshot, the snapshot should be deleted first.

Click **Volumes**. Figure 8-9 displays the **Applications** >**Network Attached Storage** > **Volumes** page.

Figure 8-9: Volumes Page

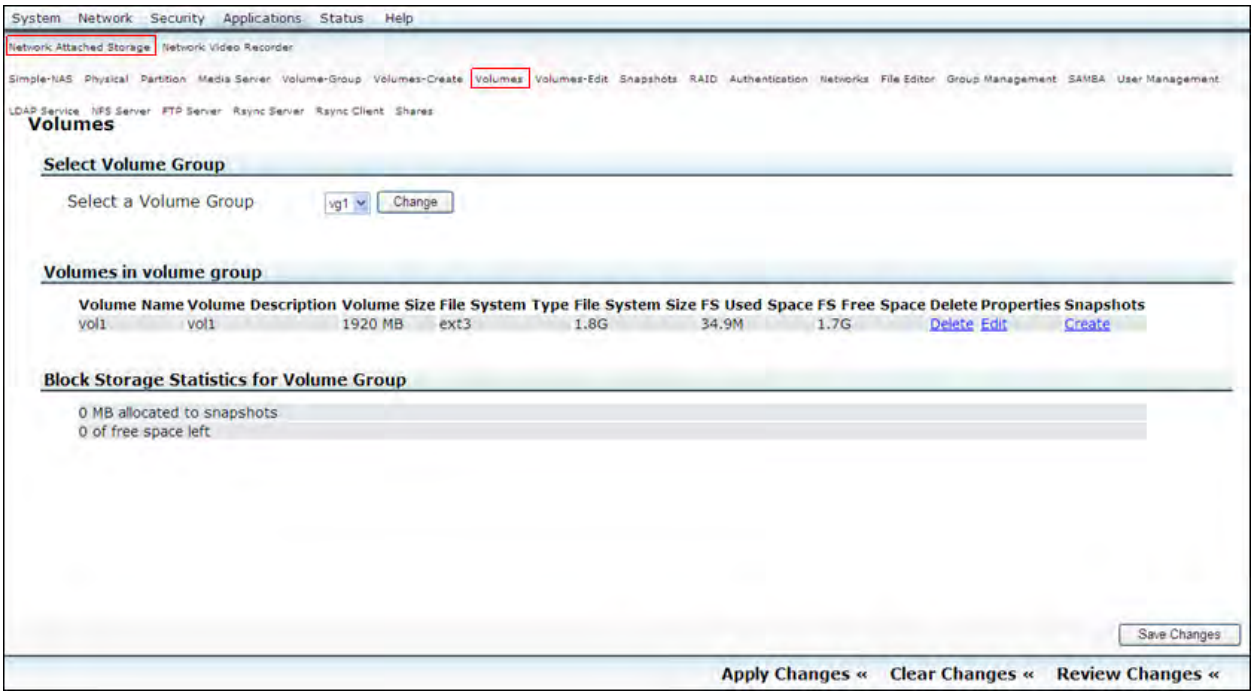


Table 8-6 describes the options available in Volumes page.

Table 8-6: Volumes Information Page

Options		Description
Select Volume Group	Select a Volume Group	Select the name from the volume group drop-down list.
	Change	Click to change the next volume group that you have created.
Volumes in volume group	Volume Name	Displays volume name
	Volume Description	Displays volume description
	Volume Size	Displays volume size
	File System Size	Displays file system size.
	FS Used Space	Displays file system used space.
	FS Free Space	Displays file system free space.
	Delete	Click to delete
	Properties	Click to edit volume properties.
	Snapshot	Click to create snapshot.
Block Storage Statistics for Volume Group		Display the specific information of the

	block storage statistics for volume group.

8.1.8 Volume Edit

The Volume Edit page allows you to expand volume size online if it has enough space in this volume group. You can also modify the description of this volume and its size.

Click **Edit**. Figure 8-10 displays the **Applications** >**Network Attached Storage** > **Volumes Edit** page.

Figure 8-10: Volume Edit Page

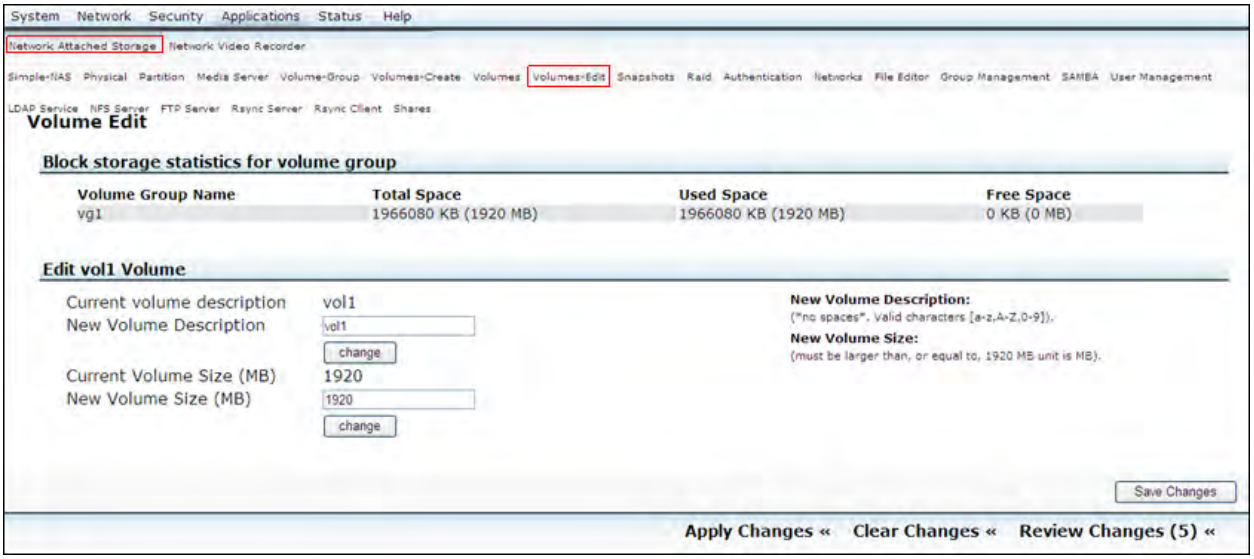


Table 8-7 describes options available in volume edit page.

Table 8-7: Volume Edit Page

Options		Description
Block Storage Statistics for Volume Group	Volume Group Name	Displays the volume group name
	Total Space	Displays the total space (MB) in the volume group
	Used Space	Displays the space that the volumes have used
	Free Space	Displays the space that the volumes group remaining
Edit vol1 Volume	Current volume description	Displays the name of the volume that you edit
	New Volume Description	Enter the new volume name to replace the old one

	Current Volume Size (MB)	Displays the current volume space (MB)
	New Volume Size (MB)	Enter the new volume space (MB) to replace the old one
	Change button	Click to the change button to update the volume

Click **Save Changes** button to save changes.

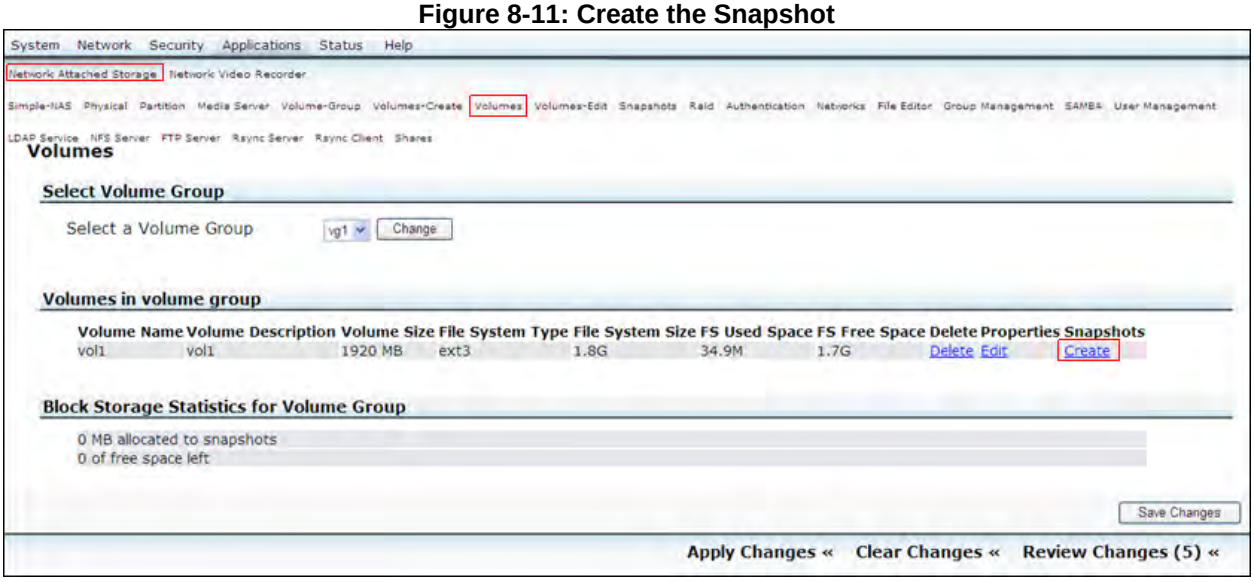
8.1.9 Snapshots

You can create or delete a snapshot manual on a **Volumes** page.

Click the **Create** link to create a snapshot manual on a volume.

Figure 8-11 displays the **Applications** >**Network Attached Storage** >**Volumes** >**Create page**.

Figure 8-11: Create the Snapshot



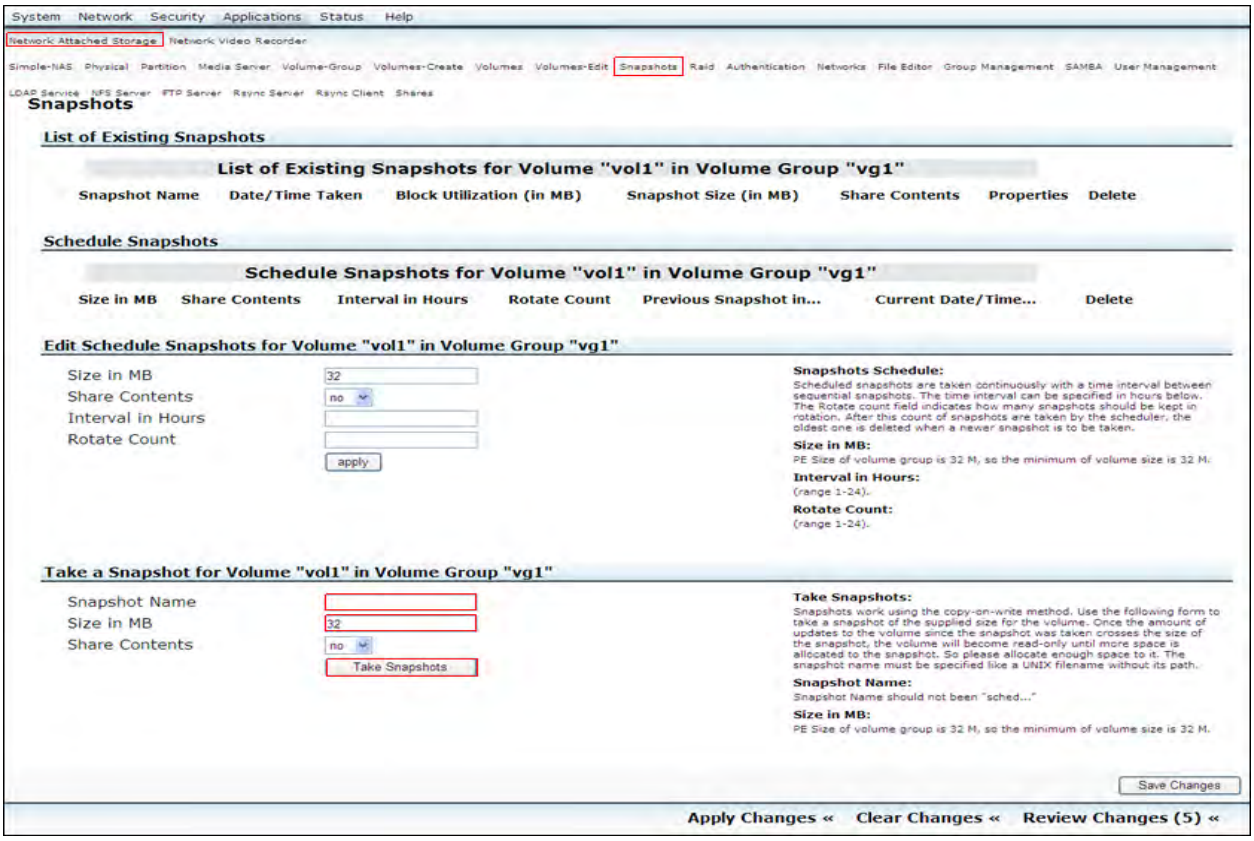
Edit the size/share-contents through “List of existing snapshots” table. You can also get information through “List of existing snapshots” table. You can create or delete a schedule snapshot for this volume.

8.1.10 Create a Snapshot

Click **Create** link in Volumes page takes you to Snapshot Management page.

Figure 8-12 displays the snapshot page.

Figure 8-12: Snapshot Management



Perform the following steps to create a Snapshot.

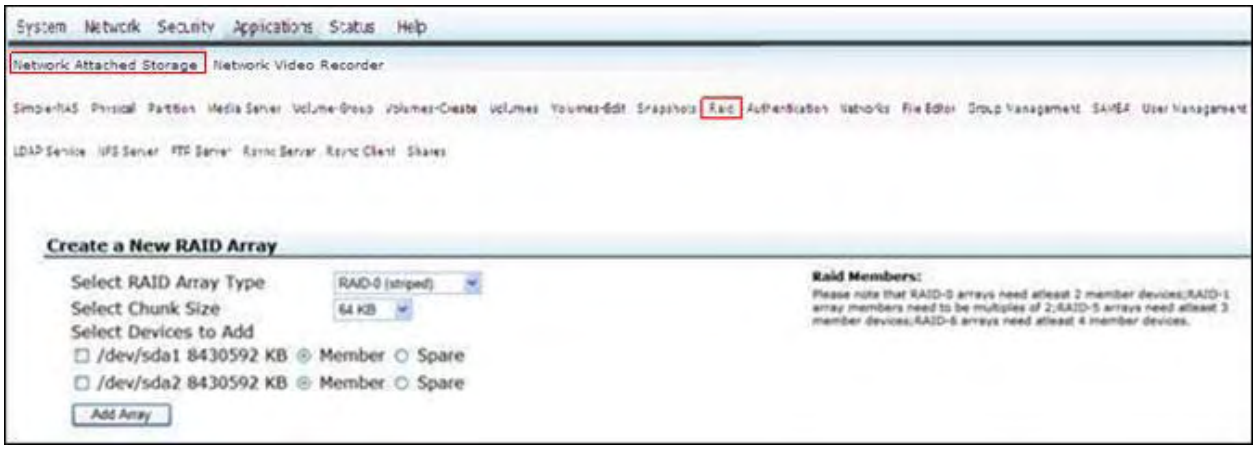
1. Enter the **Snapshot Name.**
2. Enter the **Size in MB.**
3. From the **Share Contents**, select **No**.
4. Click the **Take Snapshots.**

8.1.11 Raid Management

You can create or delete a raid array with raid0/raid1/raid5/raid6 type, and can add a disk partition to a raid array by “Add PVs (Physical Volumes)” through “Software RAID Management” menu. You can also get detail information through “Software RAID Management” table, as well as the details of raid array members.

The Chunk Size is the size of bytes for 'chunks' and is only relevant to raid levels that involve striping (1, 4, 5, 6, and 10). The address space of the array is divided into chunks and consecutive chunks are striped onto neighboring devices. The size should be at least PAGE_SIZE (4k) and should be a power of two.

Figure 8-13: Raid Management



8.1.12 Authentication

You can choose authentication type and configure it through Authentication Configuration page. In Phase 3-1, LDAP is supported.

Click **Applications** >**Network Attached Storage** > **Authentication**. Figure 8-14 displays the Authentication Configuration page.

Figure 8-14: Authentication Configuration Page

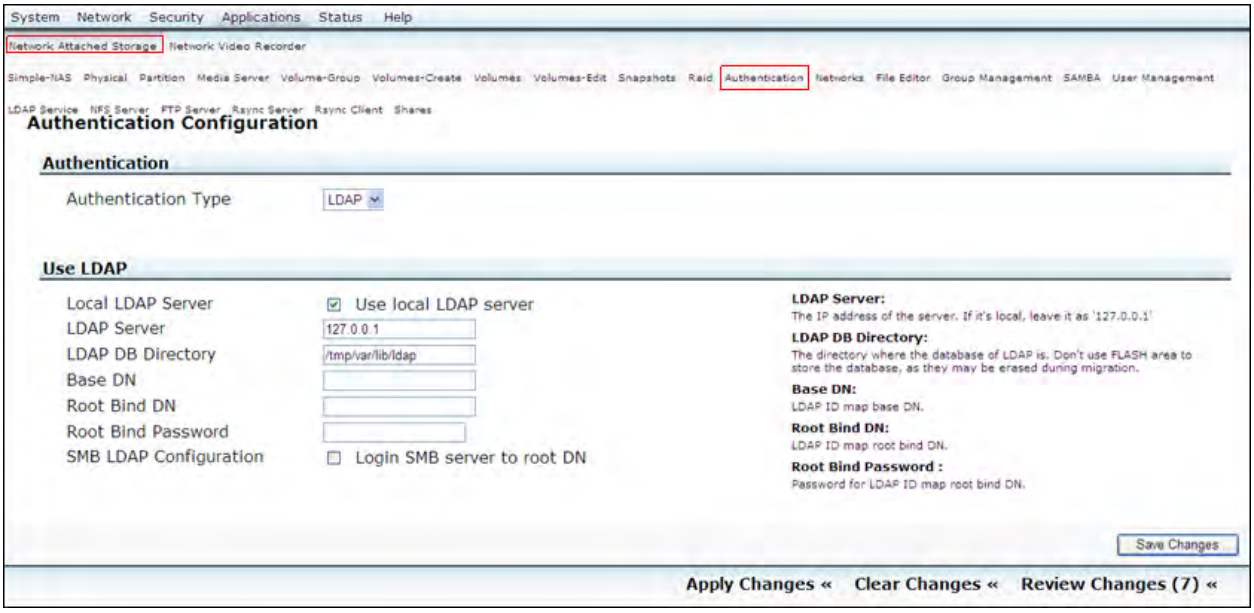


Table 8-8 describes the Authentication Configuration options.

Table 8-8: Authentication Configuration options

Options		Description
Authentication	Authentication Type	Select None or LDAP.
Use LDAP	Local LDAP Server	Click to use Local LDAP Sever.
	LDAP Server	The IP address of the server. If it's local, leave it as '127.0.0.1'.
	LDAP DB Directory	The directory where the database of LDAP is. Don't use FLASH area to store the database, as they may be erased during migration.
	Base DN	LDAP ID map base DN. Set Base DN as “dc=example,dc=com”.
	Root Bind DN	LDAP ID map root bind DN. Set Root Bind DN as “dc=manager,dc=example,dc=com”.
	Root Bind Password	Enter password for LDAP ID map root bind DN.
	SMB LDAP Configuration	Select to login SMB server to root DN and allow user to change password.

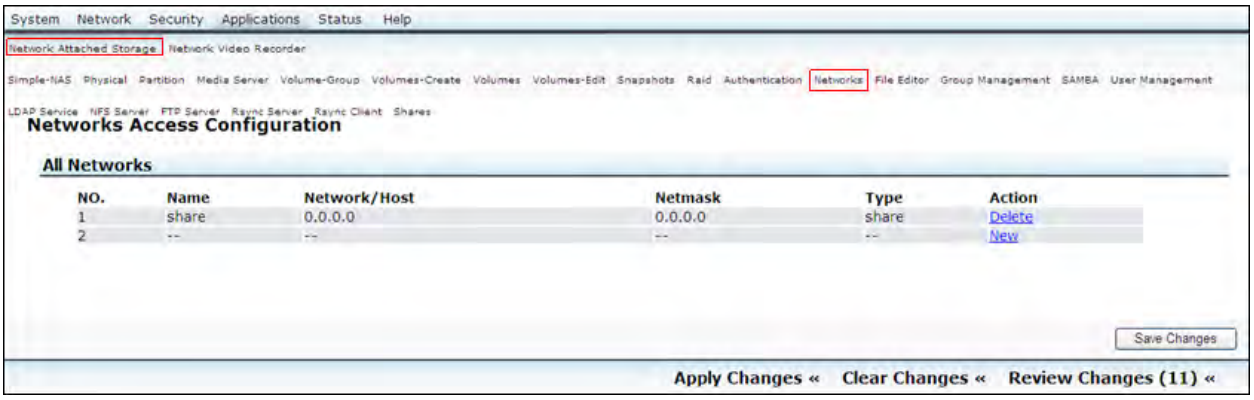
Click **Save Changes** button to save changes.

8.1.13 Networks

The Networks tab allows you to create the new network and configure the network access. The alternative to NAS storage on a network is to use a computer as a file server.

Snapshot is a copy of a set of files and directories. Snapshots are sometimes called branching snapshots, they implicitly create diverging versions of their data. Apart from backups and data recovery, snapshots are used frequently in virtualization, sandboxing and virtual hosting setups because of their usefulness in managing changes to large sets of files.

Figure 8-15: Networks Access Configuration Page

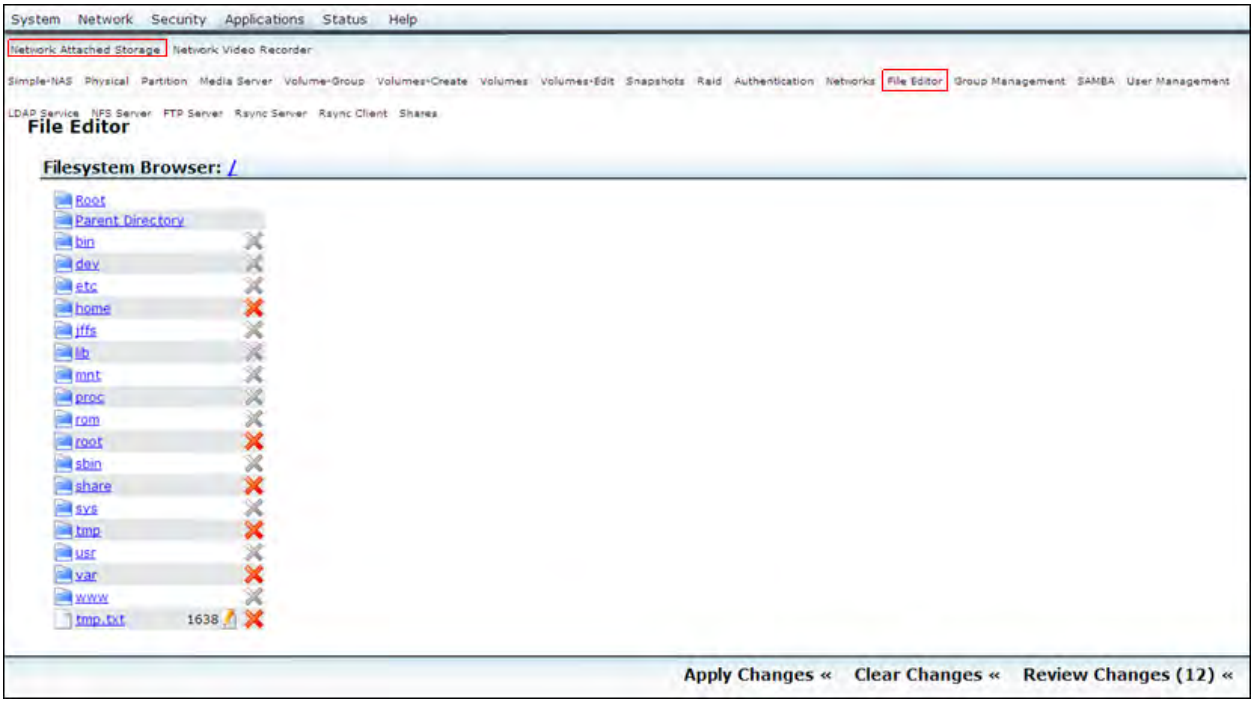


8.1.14 File Editor

The file system browser is a computer program that provides a user interface to work with file systems. The most common operations used are create, open, edit, view, print, play, rename, move, copy, delete and permissions. The files are displayed in a hierarchy.

Click **File Editor**. Figure 8-16 displays the **Applications** >**Network Attached Storage** > **File Editor** page.

Figure 8-16: File Editor Page



8.1.15 Groups

The Groups tab allows you to manage the all groups. The most common operations used are create, open, edit, view, play, rename, delete and permissions.

Click **Applications** >**Network Attached Storage** > **Groups**. Figure 8-17 displays the Groups Management page.

Figure 8-17: Groups Management Page

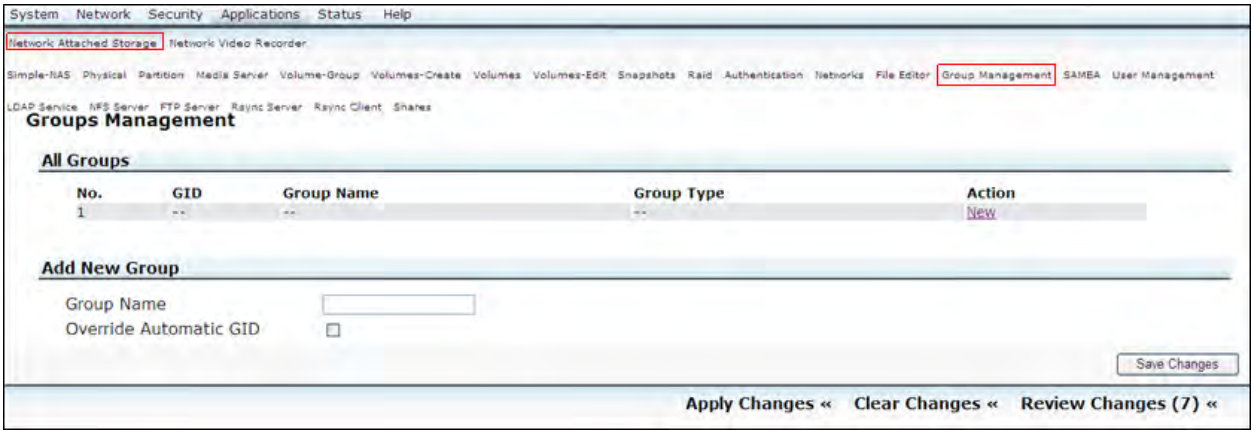


Table 8-9 describes the Group Management options.

Table 8-9: Group Management Options

Options		Description
All Groups	No.	Display order of the group you have added.
	GID	Display the Group Identification(GID).
	Group Name	Display the group name.
	Group Type	Display the group type.
	Action	Click to add a new group that you want to create.
Add New Group	Group Name	Enter the group name that you want to add.
	Override Automatic GID	Choose to override automatic GID.

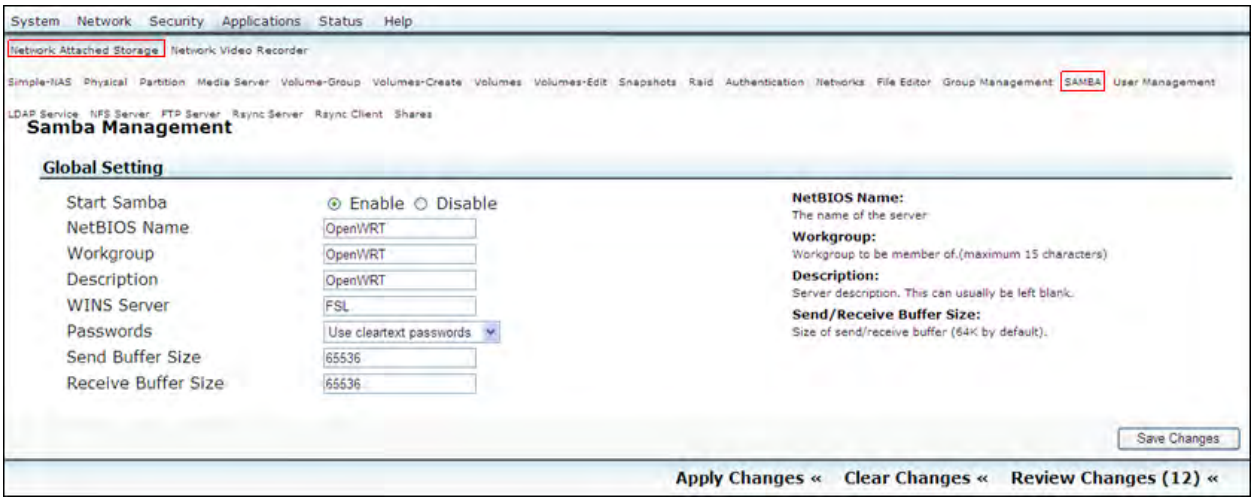
Click **Save Changes** button to save changes.

8.1.16 SAMBA

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 8-18 depicts the **Applications** >**Network Attached Storage** >**SAMBA** window.

Figure 8-18: Samba Management



NOTE

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

Table 8-10 describes options available in Samba management window.

Table 8-10: Samba Management

Options		Description
Global Settings	Start Samba	Enable or disable the samba service.
	NetBIOS Name	The name of the server.
	Workgroup	Workgroup to be member of.(maximum 15 characters)
	Description	Server description.(optional)
	WINS Server	Enter the name of the WINS server.
	Password	Select the password type from the drop-down list.
	LDAP User Suffix	Enter the user suffix for the Lightweight Directory Access Protocol (LDAP) servers.
	LDAP Group Suffix	Enter the group suffix for the Lightweight Directory Access Protocol (LDAP) servers.

	Send Buffer Size	Size of send buffer (64K by default).
	Receive Buffer Size	Size of receive buffer (64K by default).

8.1.17 Users

You can add/edit/delete user through Users Management page. You can also change password of the user.

Click **Accounts** > **Users**. Figure 8-19 displays the User Management page.

Figure 8-19: Users Management page

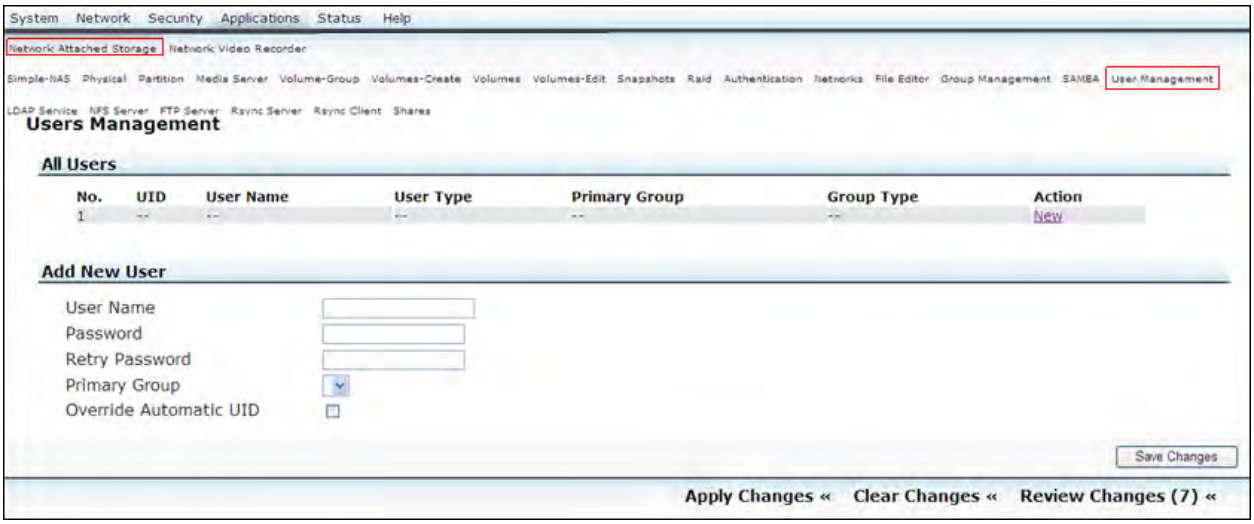


Table 8-11 describes the Users Management options.

Table 8-11: Users Management Options

Options		Description
All Users	No.	Display order of the user you have added.
	UID	Display the user identification.
	User Name	Display the user name.
	User Type	Display the user type.
	Primary Group	Display the primary group.
	Group Type	Display the group type.

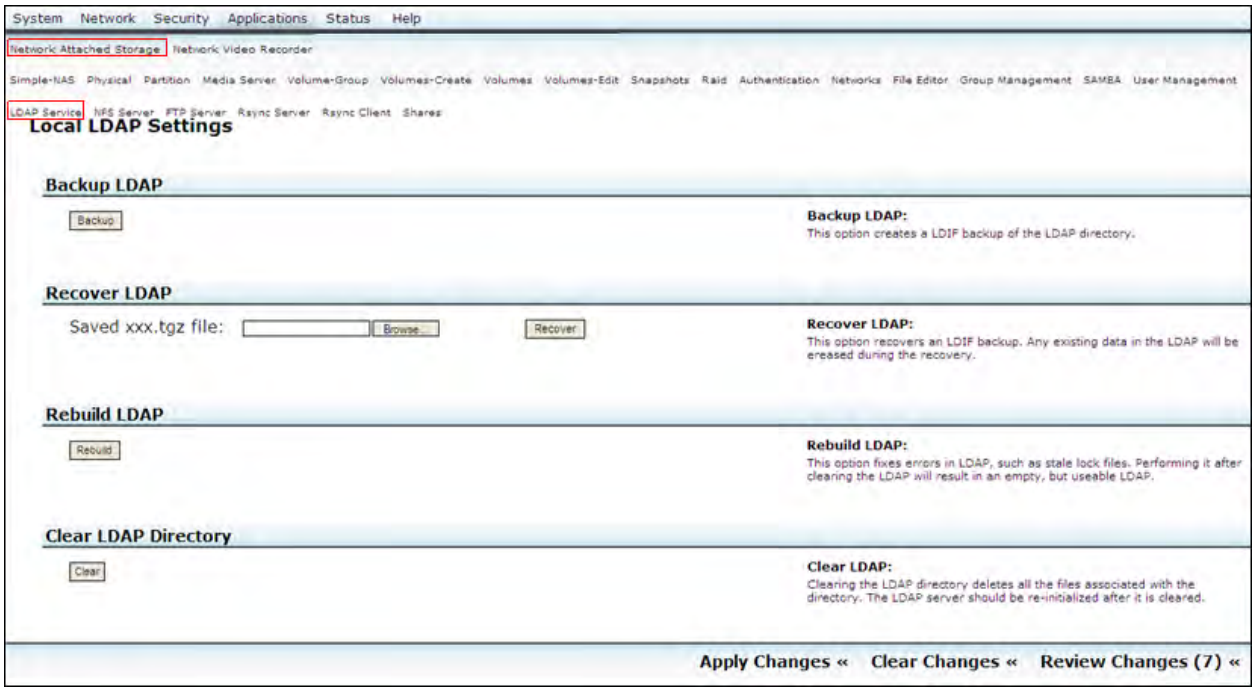
	Action	Click to add a new user that you want to create.
Add New Group	User Name	Enter the name of user that you want to add.
	Password	Enter the user password.
	Retry Password	Enter the retry password.
	Primary Group	Choose the primary group from the group drop-down list.
	Override Automatic UID	Choose to override automatic UID.

Click **Save Changes** button to save changes.

8.1.18 LDAP Service

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP. A directory is a set of objects with attributes organized in a logical and hierarchical manner. LDAP Account Manager is a web frontend for managing various account types in an LDAP directory.

Figure 8-20: Local LDAP Settings



8.1.19 NFS Server

The NFS service enables computers of different architectures that run different operating systems to share file systems across a network.

Click **Applications** >**Network Attached Storage** >**NFS Server**. Figure 8-21 displays NFS Service Management page.

Figure 8-21: NFS Service Management Page

Table 8-12 describes NFS Service Management options.

Table 8-12: NFS Service Management – Global Settings

Options		Description
Start nfsd	Enable	When enabled, the NFS process can be found.
	Disable	When disabled the NFS process is killed.

8.1.20 FTP Server

File Transfer Protocol (**FTP**) is a standard network protocol used to exchange and manipulate files over an Internet Protocol computer network. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications. The FTP service enables computers to upload and download files for data sharing.

Click **Applications** >**Network Attached Storage** > **FTP Server**. Figure 8-22 displays the FTP Service Management page.

Figure 8-22: FTP Service Management Page

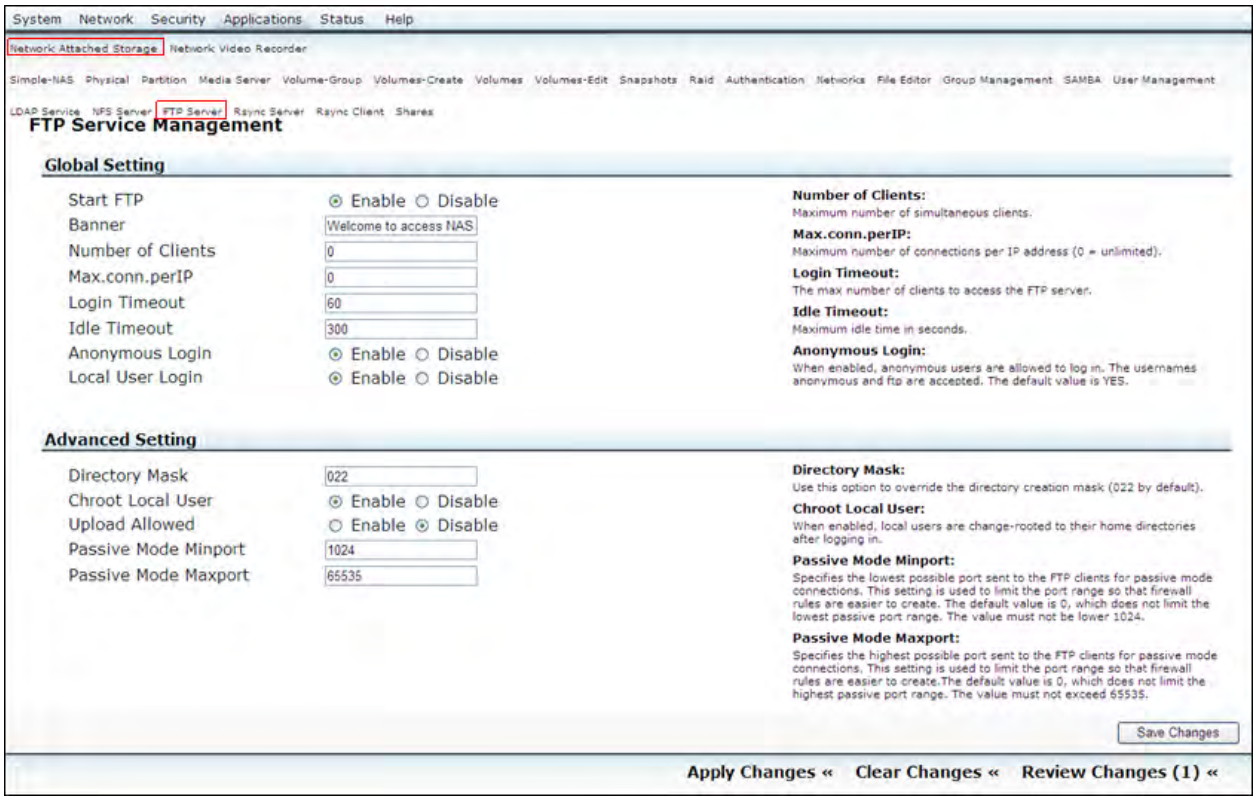


Table 8-13 describes FTP Service Management options.

Table 8-13: FTP Service Management

Options		Description
Global Settings	Start FTP	Enable to start the FTP Service.
	Banner	Enter the banner.
	Number of Clients	Maximum number of simultaneous clients
	Max. conn. perIP	Maximum number of connections per IP address (0 = unlimited).
	Login Timeout	The max number of clients to access the FTP server
	Idle Timeout	Maximum idle time in seconds
	Anonymous Login	When enabled, anonymous users are allowed to log in. The usernames anonymous and ftp are accepted. The default value is YES

	Local User Login	Enable to login the local user
Advanced Settings	Directory Mask	Use this option to override the directory creation mask (022 by default)
	Chroot Local User	When enabled, local users are change-rooted to their home directories after logging in
	Upload Allowed	Enable to allow upload
	Passive Mode Minport	Specifies the lowest possible port sent to the FTP clients for passive mode connections. This setting is used to limit the port range so that firewall rules are easier to create. The default value is 0, which does not limit the lowest passive port range. The value must not be lower 1024.
	Passive Mode Maxport	Specifies the highest possible port sent to the FTP clients for passive mode connections. This setting is used to limit the port range so that firewall rules are easier to create. The default value is 0, which does not limit the highest passive port range. The value must not exceed 65535.

Click **Save Changes** button to save changes.

8.1.21 Rsync Server

Rsync is a program, used for taking the backups on regular interval. It can be configured to upload large portals and other data on the remote servers. Rsync can copy or display directory contents and copy files, optionally using compression and recursion.

You can manage Rsync Server through Rsync Server Management page. It includes Global Settings and Module settings for access control (sharing).

Click **Applications** >**Network Attached Storage** > **Rsync Server**. Figure 8-23 displays Rsync Server Management Page.

Figure 8-23: Rsync Server Management Page

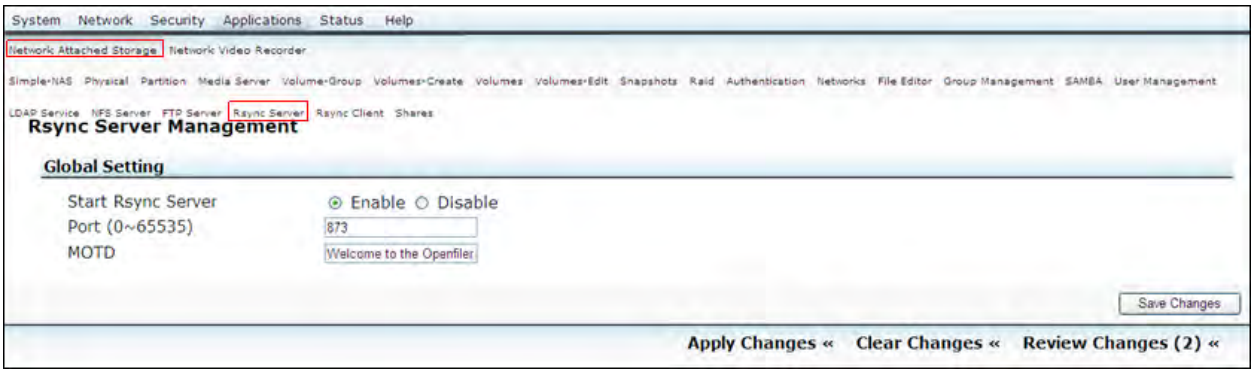


Table 8-14 describes Rsync Server Management options.

Table 8-14: Rsync Server Management Options

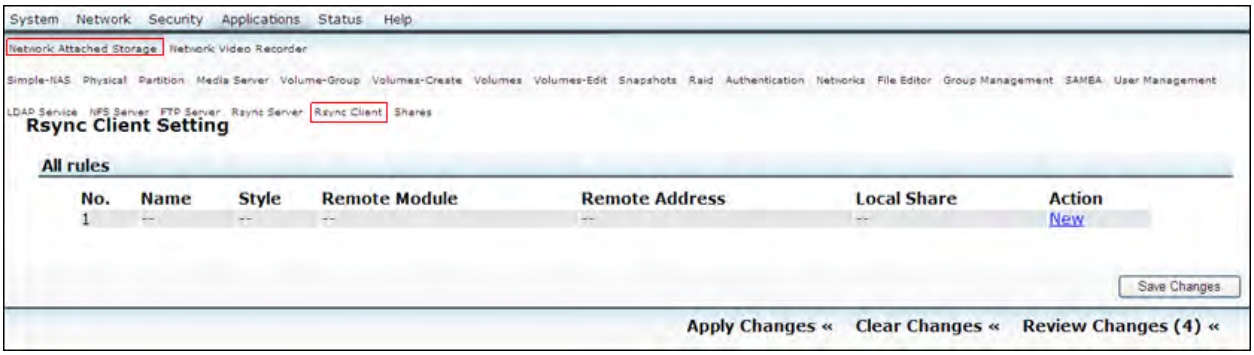
Options		Description
Global Settings	Start Rsync Server	Enable to start the Rsync Service.
	Port (0~65535)	Enter the Rsync service port.
	MOTD	Enter the Rsync service MOTD. In config file `rsyncd.motd` records rsync service welcome message. You can enter any text .

Click **Save Changes** button to save the changes.

8.1.22 Rsync Client

You can list/add/edit/delete a rule through Rsync Client Setting page. Figure 8-24 displays the **Applications** >**Network Attached Storage > Rsync Client** page.

Figure 8-24: Rsync Client Settings Page



When a new rule is added, you can define the synchronization time, depicts the **Applications** >**Network Attached Storage > Rsync Client > Edit** page.

Figure 8-25: Add a new Rsync Client rule

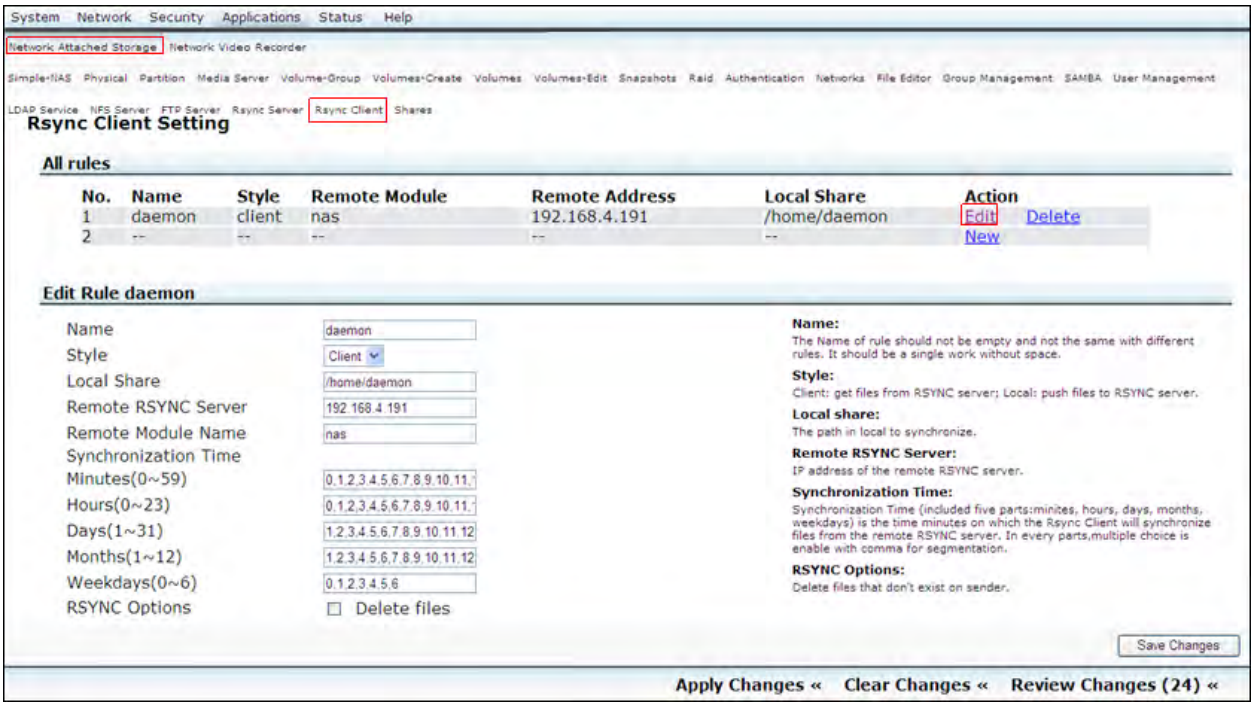


Table 8-15 describes each Rule setting options in detail.

Table 8-15: Rule Settings

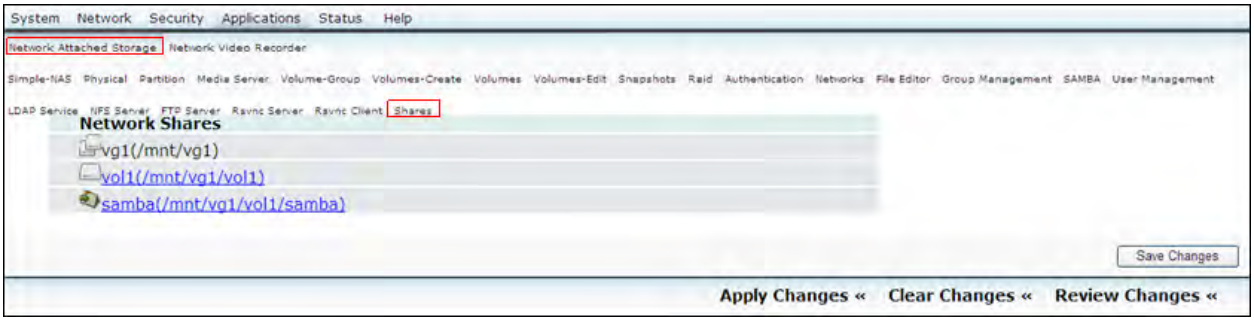
Options	Description
Name	Enter the Name of rule. It should not be empty and not the same with different rules. It should be a single word without space.
Local Share	Enter the path to synchronize.
Remote RSYNC Server	Enter the IP address of the remote RSYNC server.
Synchronization Time	Synchronization Time (included five parts: minutes, hours, days, months, weekdays) is the time minutes on which the Rsync Client will synchronize files from the remote RSYNC server. In every part, multiple choices are enabled with comma for segmentation.
RSYNC Options	Delete files that don't exist on sender.

8.1.23 Shares

A **shared file system** is an enterprise storage file system which can be shared (concurrently accessed for reading and writing), by multiple computers. Such devices are usually clustered servers, which connect to the underlying block device over an external storage device.

Click **Applications** >**Network Attached Storage** > **Shares**. Figure 8-26 displays the network shares page.

Figure 8-26: Network Shares Page



NOTE

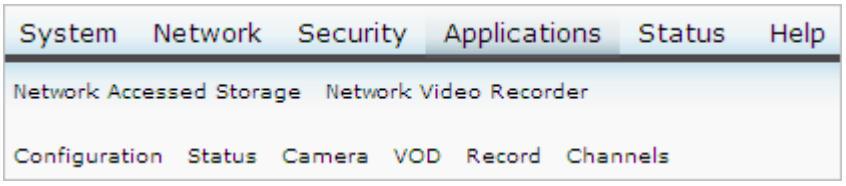
Make sure while setting up NVR system, the Override SMB/Rsync share name must be disk.

8.2 Network Video Recorder (NVR)

NVR stands for Network Video Recorder. It connects to the network camera through the router. The client terminal displays a webcam image as HTML webpage. It can also do image processing.

Click **NVR** (Figure 8-27), then proceed with the respective sections.

Figure 8-27: NVR



8.2.1 Configuration

The NVR configuration page

Click **Applications** >**Network Video Recorder** > **Configuration,** to view the configuration page (Figure 8-28).

Figure 8-28: Configuration Page

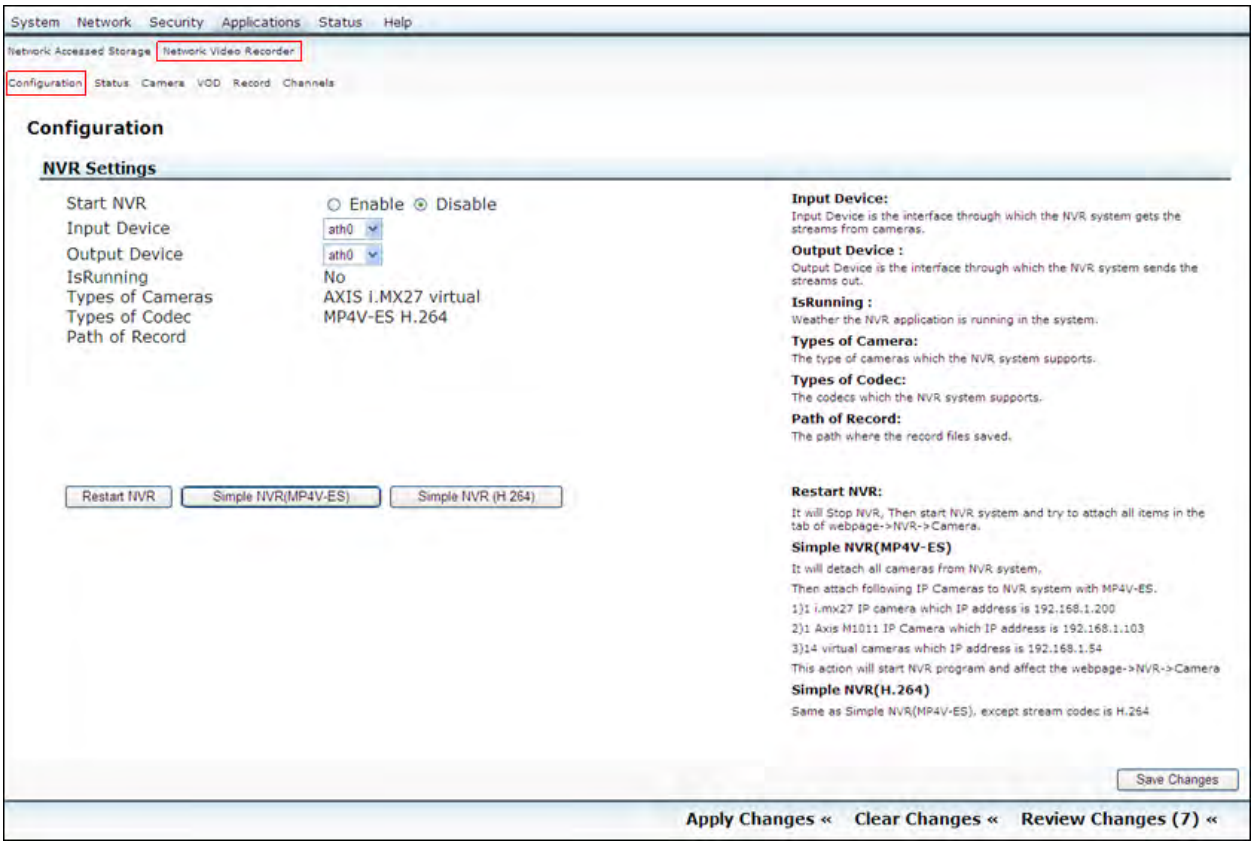


Table 8-16 describes the NVR configuration page in detail.

Table 8-16: NVR Configuration

Options	Description
Start NVR	Enable or Disable NVR.
Input Device	It is an interface, through which the NVR system gets the streams from camera.
Output Device	It is the interface, through which the NVR system sends the streams out.
Is Running	Displays weather the NVR application is running in the system.
Type of Cameras	Displays the type of camera
Type of Codec	Displays type of codec. Codec is a device or computer program capable of encoding and/or decoding a digital data stream or signal.
Path of Record	Displays the path where the recorded file is saved

	that was created in NAS.
Reset NVR	Resets NVR configuration
Simple NVR (MP4V-ES)	It will detach all cameras from NVR system, and then attach following IP Cameras to NVR system with MP4V-ES. 1) 1 i.mx27 IP camera whose IP address is 192.168.1.200 2) 1 Axis M1011 IP Camera whose IP address is 192.168.1.103 3) 14 virtual cameras whose IP address is 192.168.1.54 This action will start NVR program and affect the webpage- NVR-> Camera
Simple NVR (H.264)	It works similar to Simple NVR(MP4V-ES), except stream codec is H.264

WARNING

If the Simple NVR button is pressed, the NVR system will start with default configurations, and all saved configurations will be deleted.

8.2.2 Status

The Status page displays all the cameras, virtual and non-virtual cameras and VOD used by NVR.

Click **Applications >Network Video Recorder** > **Status** to view the status of the camera. If you have clicked Simple NVR button in NVR Configuration page then following webpage appears.

Figure 8-29: Status Page

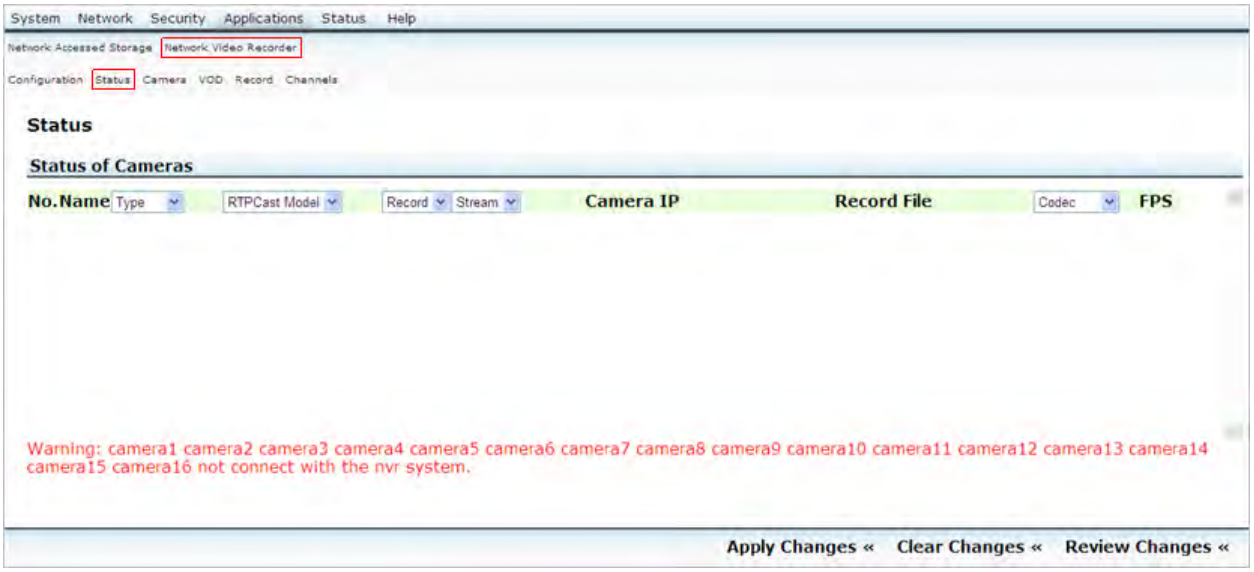


Table 8-17 below describes the status page options in detail.

Table 8-17: Status of Camera

Options	Description
Type	Displays the camera type(camera/vod)
RTPCast Model	Displays the RTPCast Model (multicast / unicast)
Record	Displays the status of camera recording (Yes/No)
Stream	Displays the status of camera streaming (Yes/No)
Camera IP	Displays the Camera IP
Record File	Displays the record file name
Codec	Displays the codec type
FPS	Displays the FPS (Frames per second) of camera

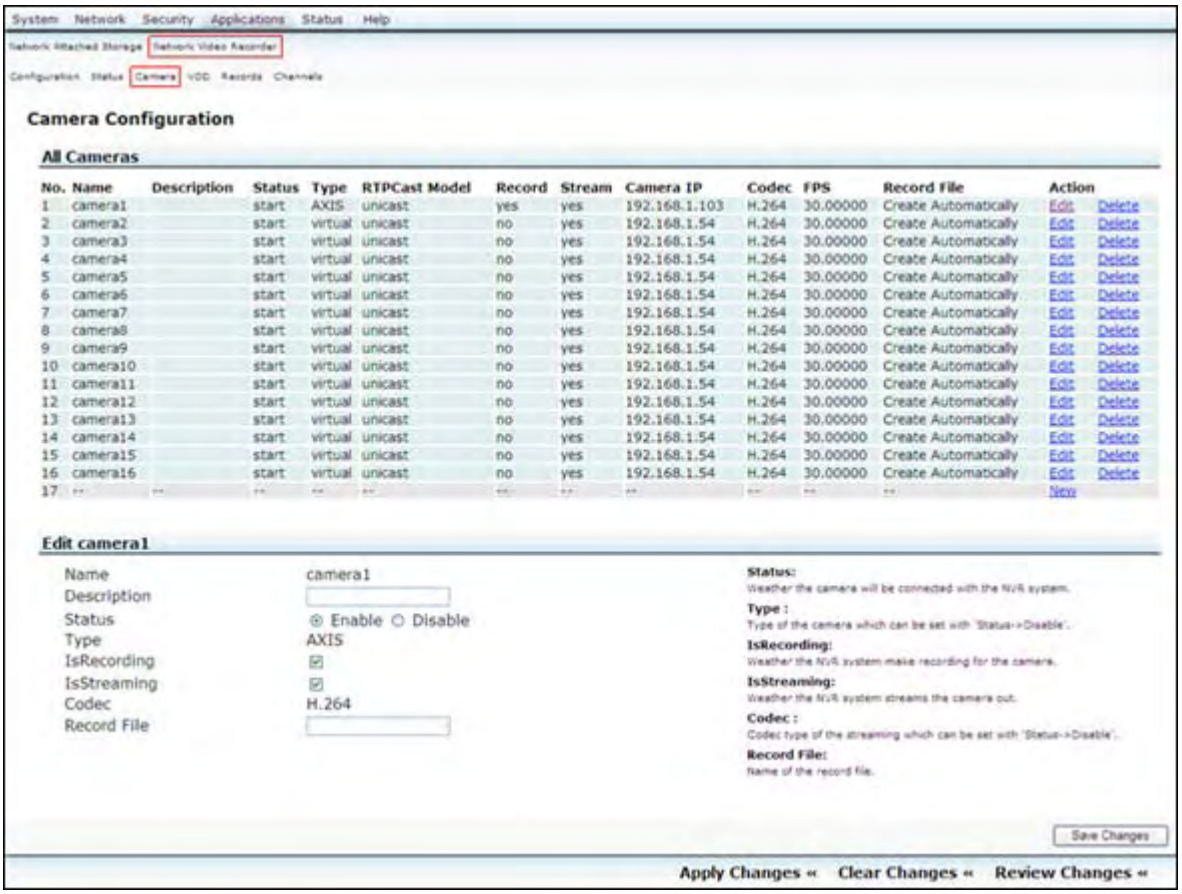
8.2.3 Camera

Click **Applications** >**Network Video Recorder** > **Camera** to open the Camera Configuration page.

8.2.3.1 Edit Camera

Click “Edit”, and then change “Status” to “Disable”. Then “Save changes” and “Apply changes”.

Figure 8-30: Edit Camera



Click “Edit” again, in this page, tester can edit camera configuration.

Figure 8-31: Edit Camera1

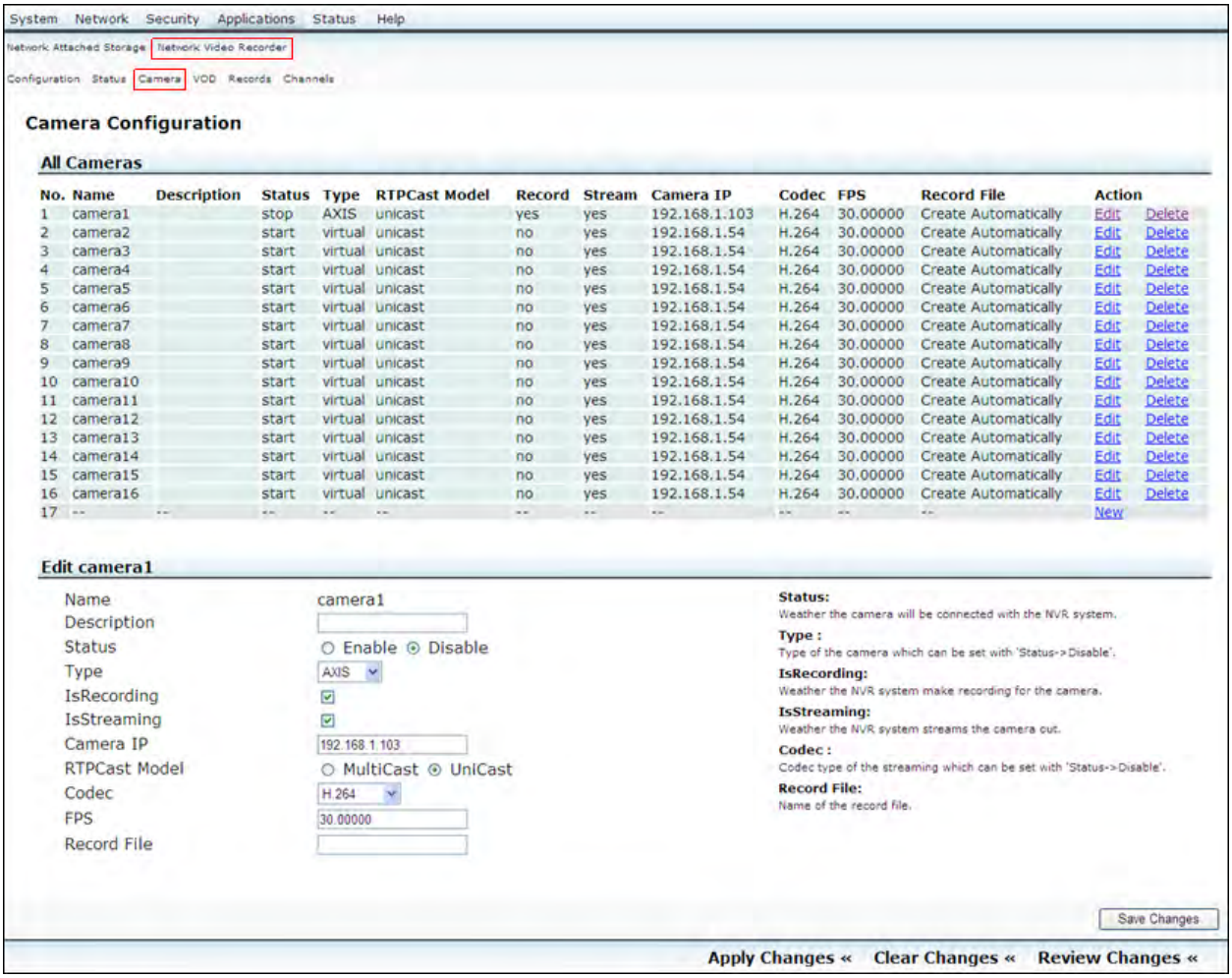


Table 8-18 describes the Edit camera configuration in detail.

Table 8-18: Virtual Camera Configuration

Options	Description
Name	Displays name of the camera
Description	Displays the description of the camera
Status	Select start or stop
Type	Select camera type
IsRecording	Selecting isRecording records the video
IsStreaming	Selecting isStreaming streams the video
Camera IP	Set the IP address of the camera
No. of Virtual Stream	Displays the number of virtual camera

RTPCast Model	Select either multicast or unicast
Codec	Codec Supported – MP4V-ES
FPS	Frames per second (Set at 30.000)
Record File	Assigned automatically, leave blank

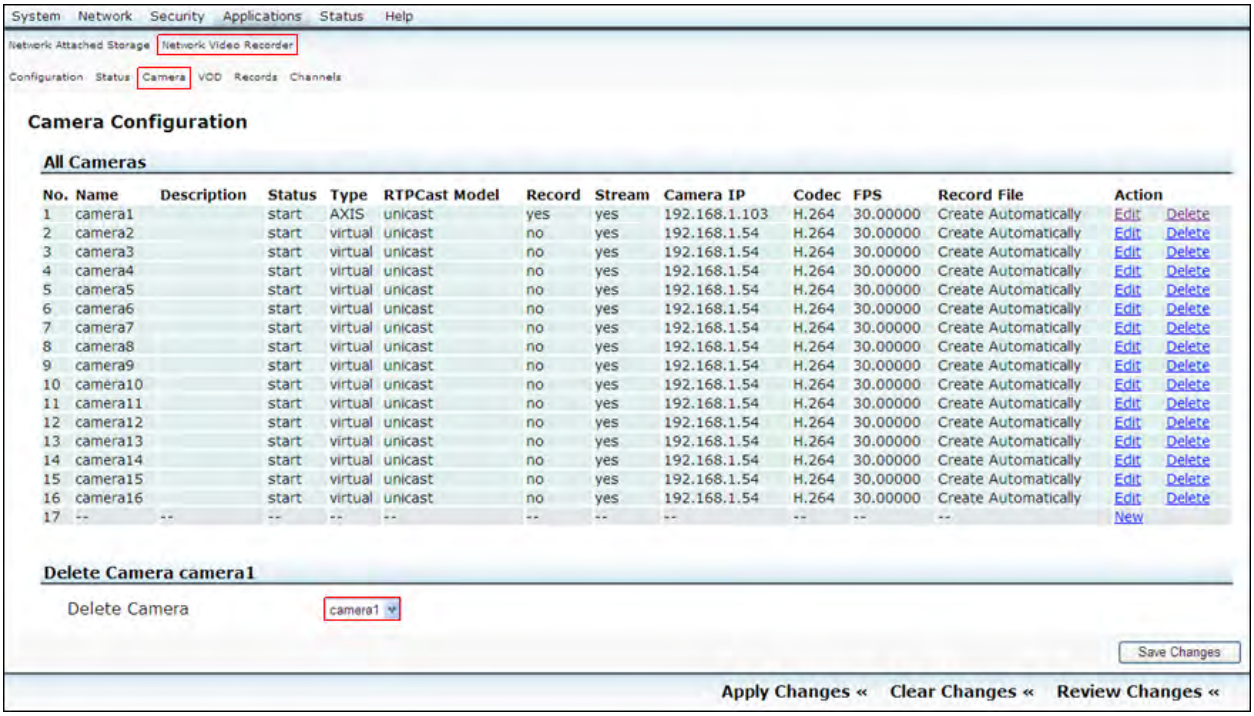
Click Save Changes to apply your changes.

8.2.3.2 Delete Camera

Click **Applications** >**Network Video Recorder** > **Camera** to open the Camera Configuration page.

Click **Delete**. Then **Save changes** and **Apply changes**.

Figure 8-32: Delete Camera



8.2.4 VOD

VOD (Video on Demand) is system, which allows users to select and watch the video content on demand.

Click **Applications** >**Network Video Recorder** > **VOD** and click on new to create a **VOD**.

Figure 8-33: VOD

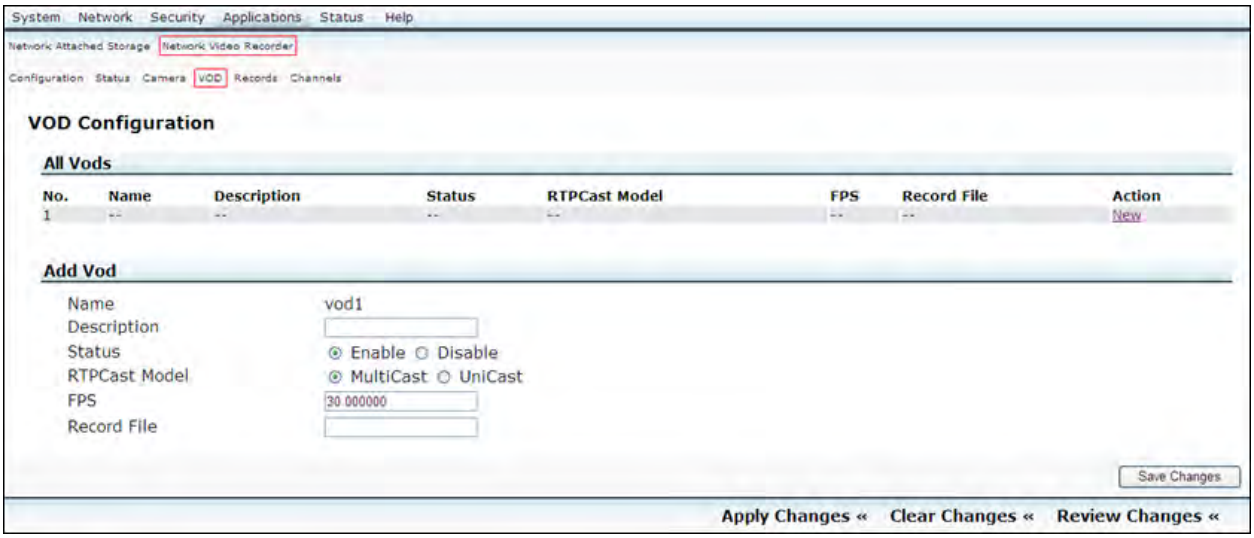


Table 8-19 describes the VOD configuration in detail.

Table 8-19: VOD Configuration

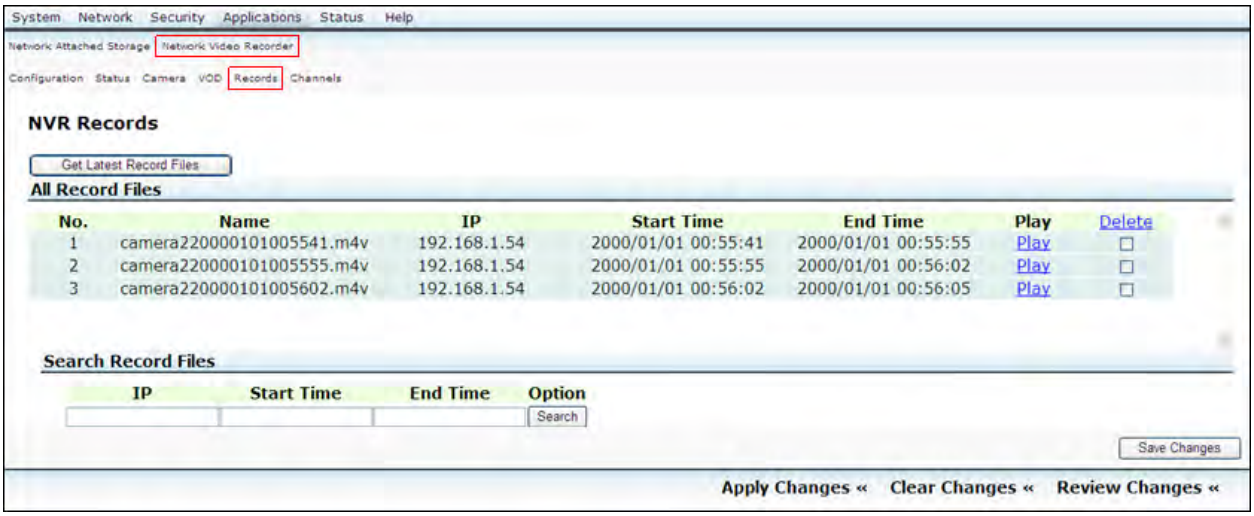
Options	Description
Name	Displays name of the vod
Description	Displays the description of the vod
Status	Select start or stop
RTPCast Model	Select the Real-time Transport Protocol cast model. You may select MultiCast or Unicast
FPS	Enter the frames per second (Set at 30.000)
Record File	Must enter an existing root file

8.2.5 Record

You can view the recorded video.

Click **Applications** >**Network Video Recorder** > **Record** to view the recorded video. Several records appear on the screen.

Figure 8-34: NVR Records



NOTE

If you checked isRecording while creating a new camera, then you should be able to view the recorded video.

Select **Applications** >**Network Video Recorder** > **Camera** and click on **Edit**.

Uncheck the **isRecording** option.

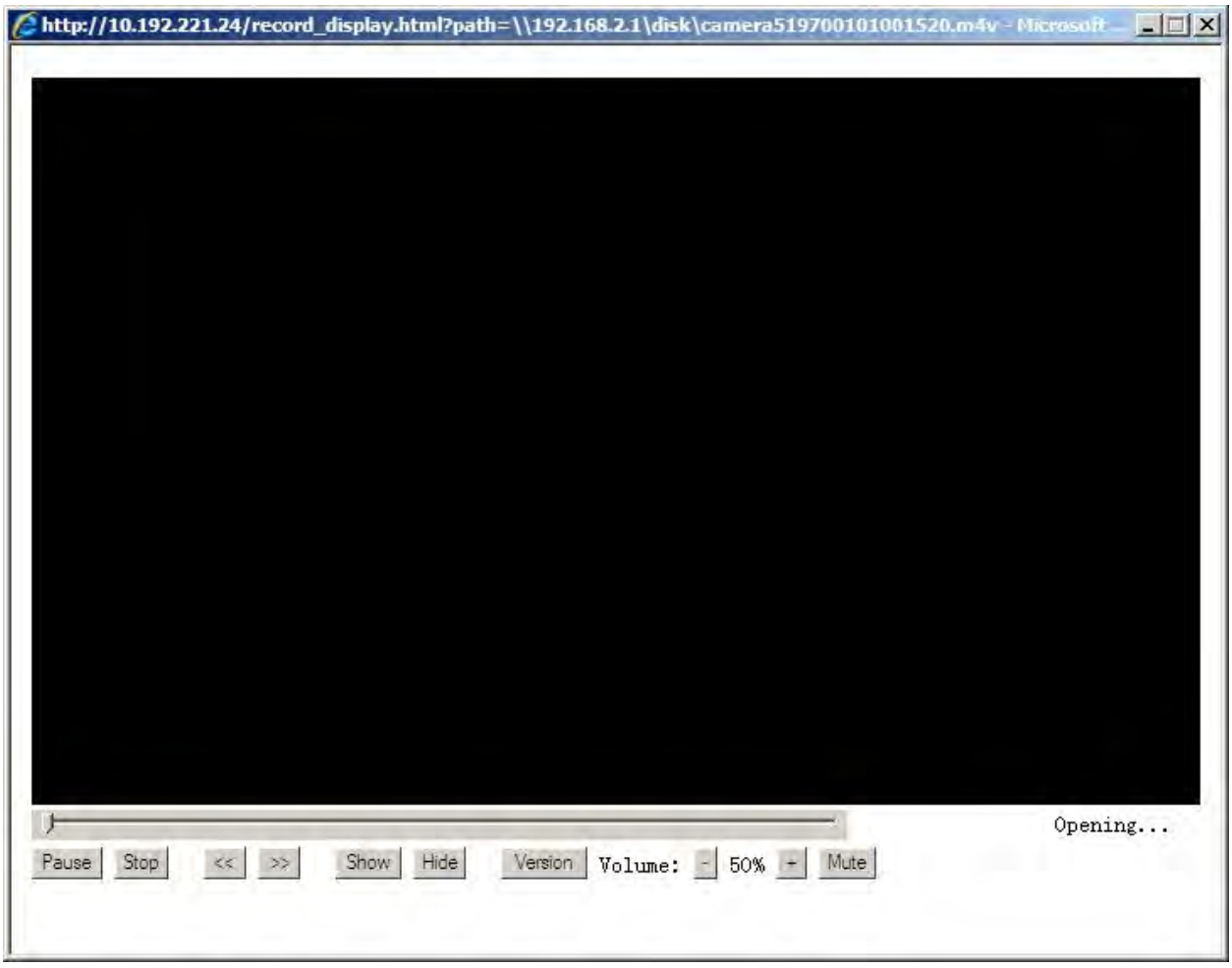
Click **Save** and **Apply changes**.

The isRecording option is unchecked in order to view the recorded file because this flushes out all the recorded files till that point and stops the recording. To restart the recording, just check **isRecording** option again and save the changes.

Click **Applications** >**Network Video Recorder** > **Record**. Many records will appear on the right.

Click **Play**.

Figure 8-35: NVR Records



Note

You can search your records by IP address, start time or end time.

8.2.6 Search Record Files

There are three ways to search record files, by IP, by Start Time or by End Time. It can work each way. Enter record filenames in the IP, Start time or End time text boxes and click “search” to start.

Note

Time format is accurate to seconds.

8.2.7 Channels

The channels can transmit data and control information between different channels. Different channels represent various camera, when you input the channel IP address, you can view the video captured by the camera.

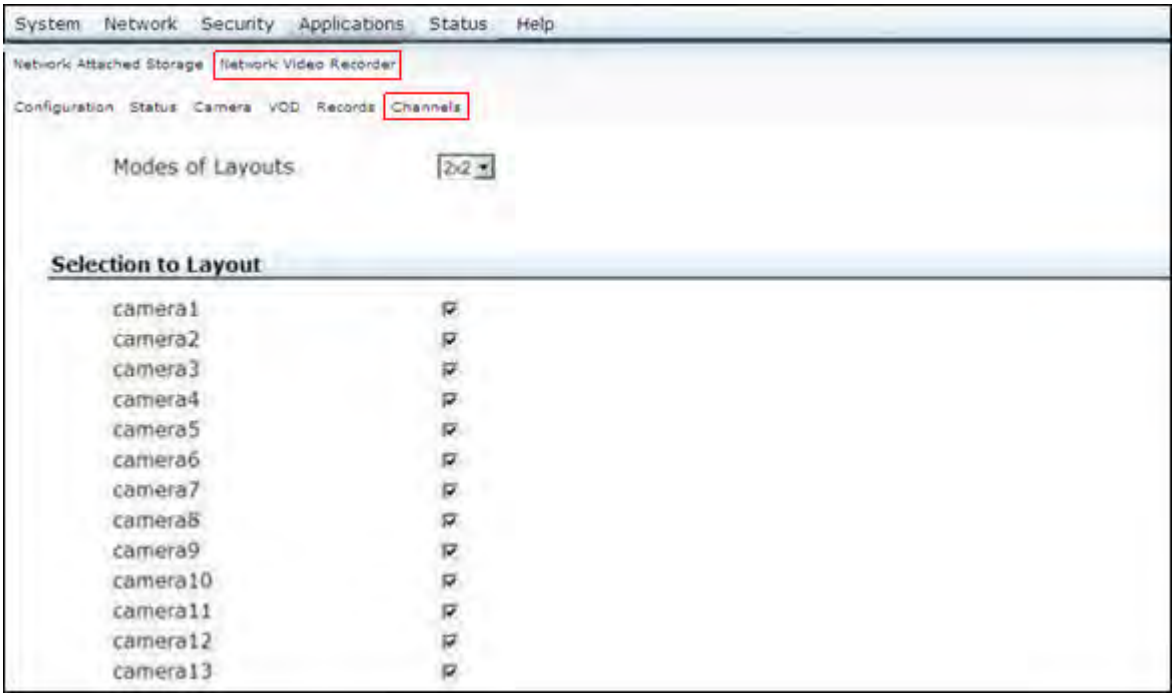
Click **Applications** >**Network Video Recorder** > **Channels**. You can choose the layout to display the number of the menu.

Perform the following steps, as depicted in (Figure 8-36):

1. From the **Layout** drop-down list, select the number of the camera.
2. In the **Channel IP** text box, type the scream URL of the camera, which you want to view live.

   You can change the layout to display the number of the menu.

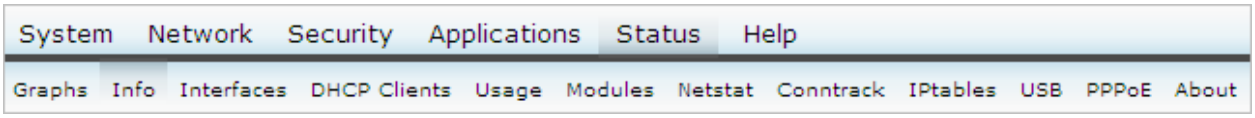
Figure 8-36: Channels Live View Page



9 Status

This section explains viewing the unit's status. Click **Status** (Figure 9-1), then proceed with the respective sections.

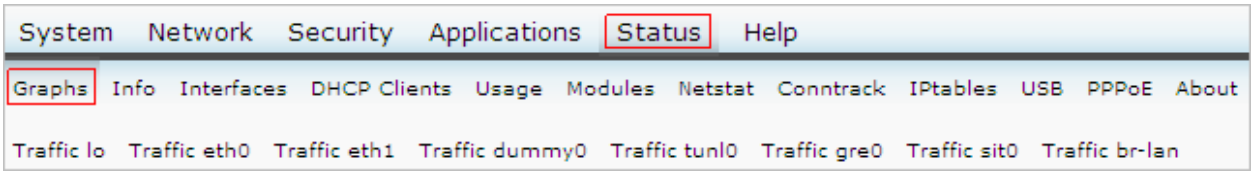
Figure 9-1: Status



9.1 Graphs

This section displays various graphs. Click **Graphs** (Figure 9-2), then proceed with the respective sections.

Figure 9-2: Graphs



9.1.1 Traffic lo

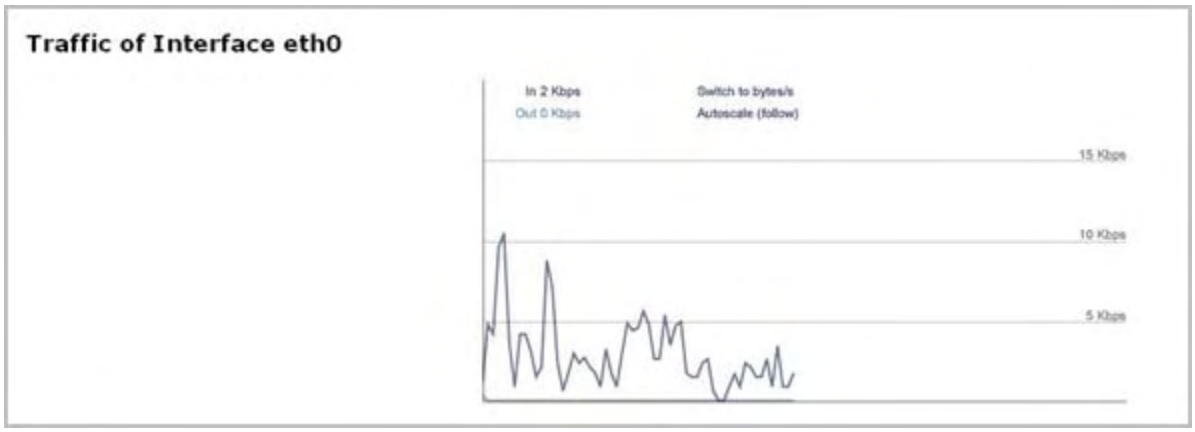
Click **Status** >**Graphs** > **Traffic lo** to display traffic interface lo (lo for loopback), including Incoming Traffic and Outgoing Traffic. (Figure 9-3)

Figure 9-3: Traffic lo

9.1.2 Traffic eth0

Click **Status** >**Graphs** > **Traffic eth0** to display traffic interface eth0 (eth0 for first IEEE 802.3 Ethernet), including Incoming Traffic and Outgoing Traffic. (Figure 9-4)

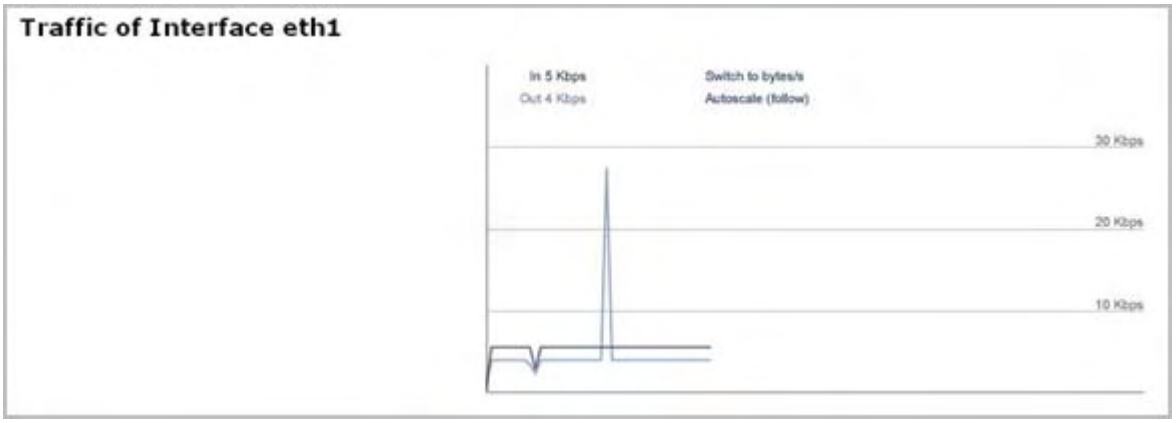
Figure 9-4: Traffic eth0



9.1.3 Traffic eth1

Click **Status** >**Graphs** > **Traffic eth1** to display traffic interface eth1 (eth1 for second IEEE 802.3 Ethernet), including Incoming Traffic and Outgoing Traffic. (Figure 9-5)

Figure 9-5: Traffic eth1



9.1.4 Traffic dummy0

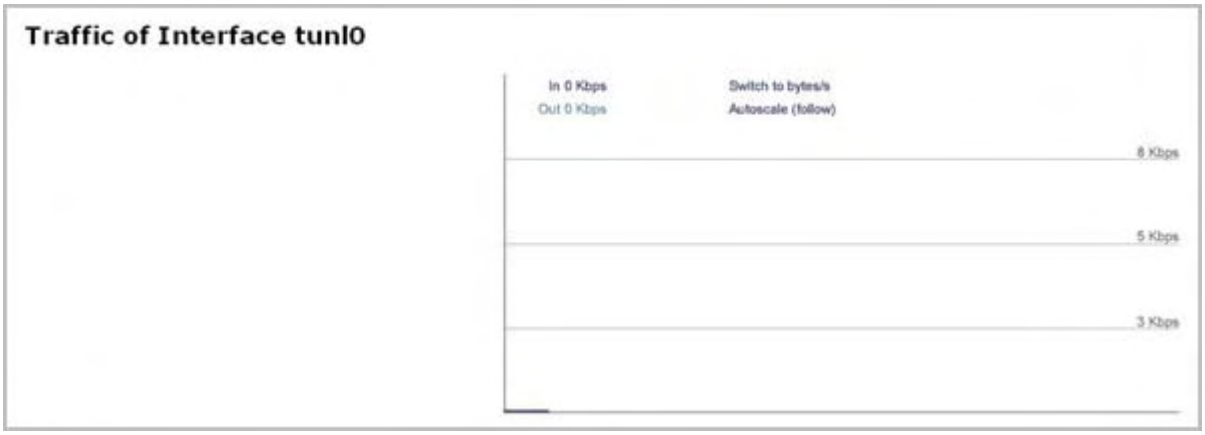
Click **Status** >**Graphs** > **Traffic dummy0** to display traffic interface dummy0 (dummy0 for dialup link interface), including Incoming Traffic and Outgoing Traffic. (Figure 9-6)

Figure 9-6: Traffic dummy0

9.1.5 Traffic tunl0

Click **Status** >**Graphs** > **Traffic tunl0** to display traffic interface tunl0 (tunl0 for first VPN tunnel), including Incoming Traffic and Outgoing Traffic. (Figure 9-7)

Figure 9-7: Traffic tunl0



9.1.6 Traffic gre0

Click **Status** >**Graphs** > **Traffic gre0** to display traffic interface gre0 (gre0 for Generic Routing Encapsulation tunnel pseudo-interface), including Incoming Traffic and Outgoing Traffic. (Figure 9-8)

Figure 9-8: Traffic gre0

9.1.7 Traffic sit0

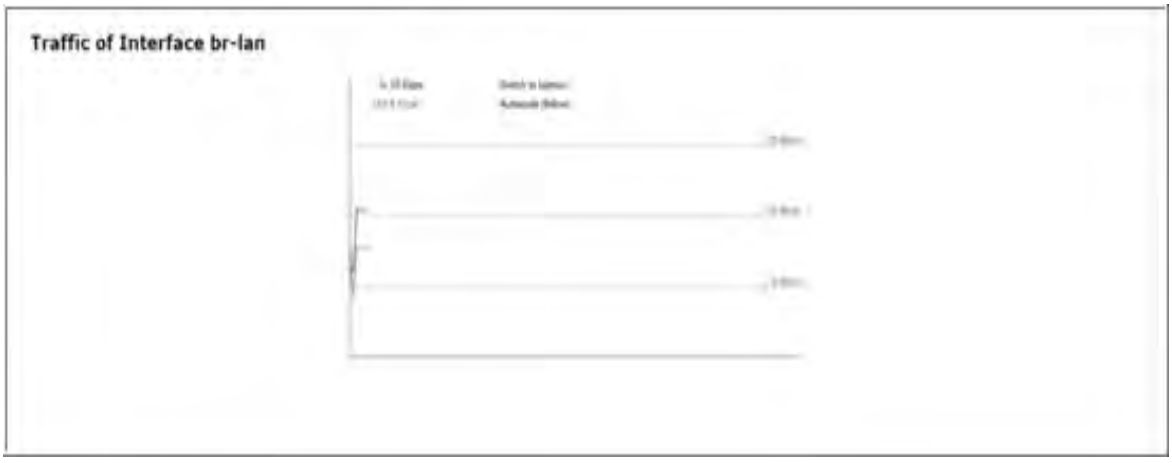
Click **Status** >**Graphs** > **Traffic sit0** to display traffic interface sit0 (sit0 for Link encapsulation: IPv6-in-IPv4), including Incoming Traffic and Outgoing Traffic. (Figure 9-9)

Figure 9-9: Traffic sit0

9.1.8 Traffic br-lan

Click **Status** >**Graphs** > **Traffic br-lan** to display traffic interface br-lan (br-lan for bridge-lan interface), including Incoming Traffic and Outgoing Traffic. (Figure 9-10)

Figure 9-10: Traffic br-lan



9.1.9 Traffic wifi0

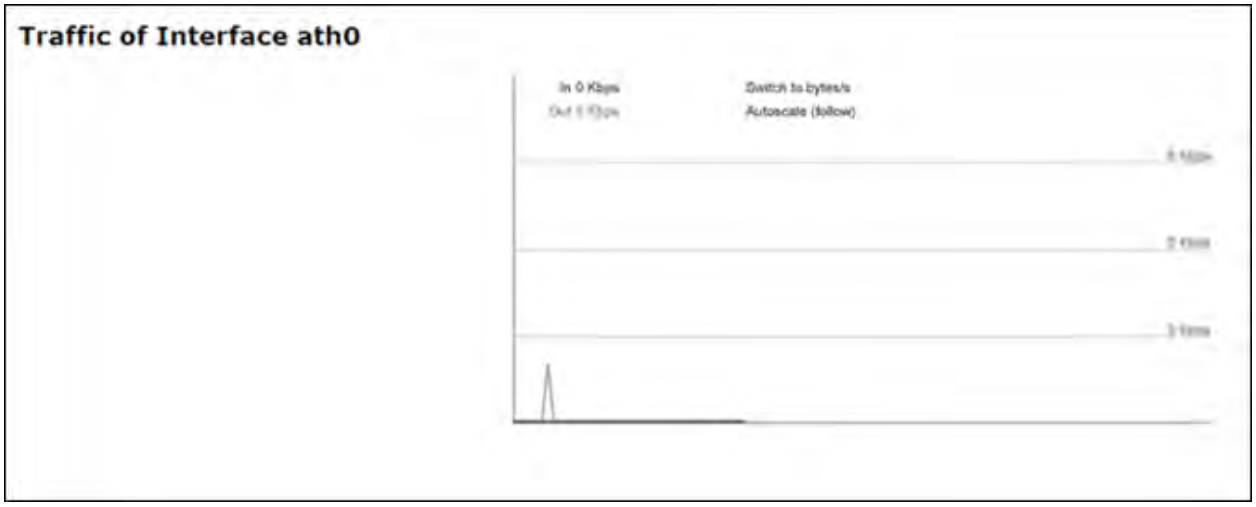
Click **Status** >**Graphs** > **Traffic wifi0** to display traffic interface wifi0 (wifi0 for wifi network interface), including Incoming Traffic and Outgoing Traffic. (Figure 9-11)

Figure 9-11: Traffic wifi0

9.1.10 Traffic ath0

Click **Status** >**Graphs** > **Traffic ath0** to display traffic interface ath0 (ath0 for atheros wifi card), including Incoming Traffic and Outgoing Traffic. (Figure 9-12)

Figure 9-12: Traffic ath0



9.2 Interfaces

Click **Interfaces**. Figure 9-13 depicts the **Status > Interfaces** window and various interface settings.

Figure 9-13: Interfaces

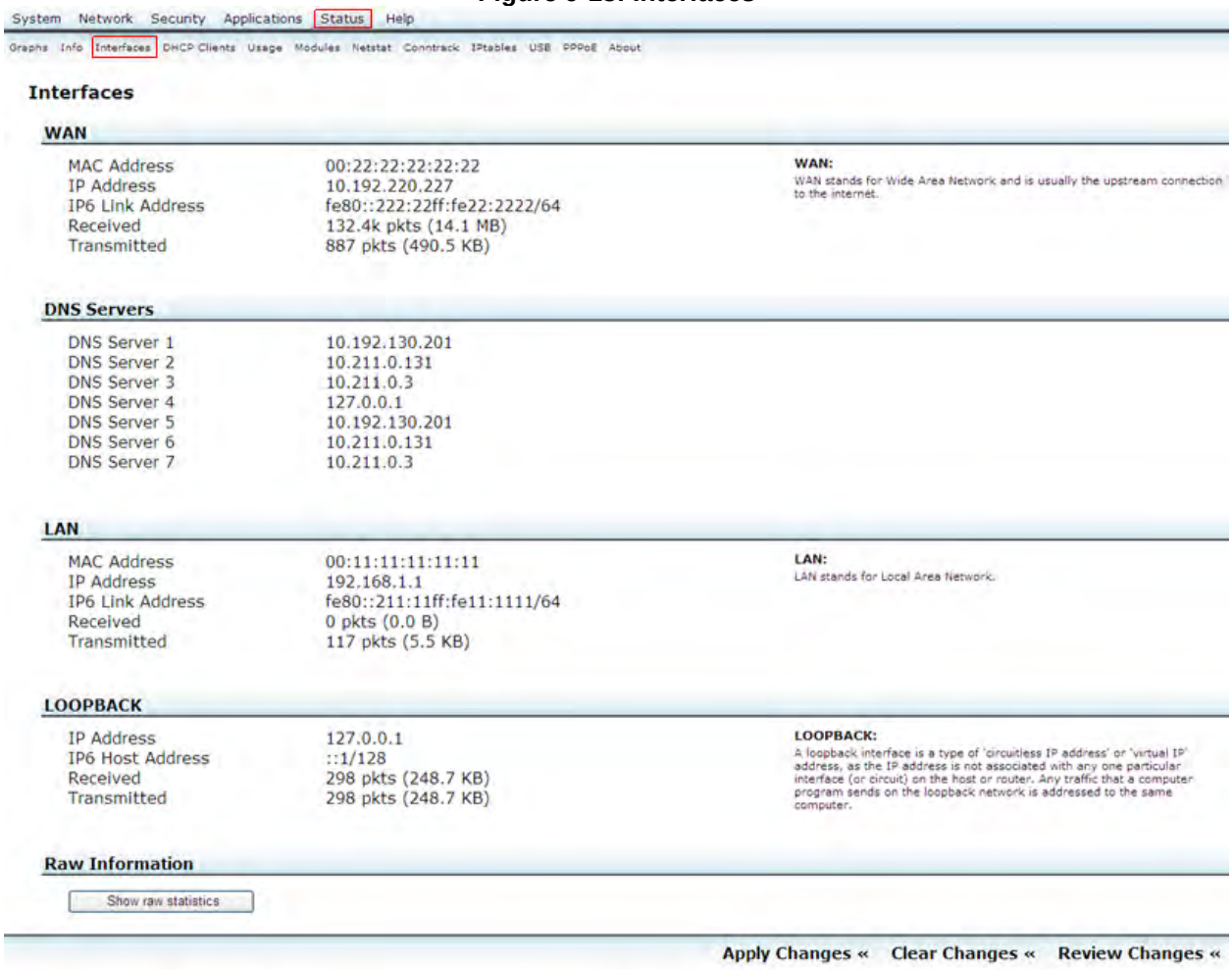


Table 9-1 describes each of the section of Interfaces page.

Table 9-1 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.
LAN	LAN stands for Local Area Network. It displays LAN 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 9-14)

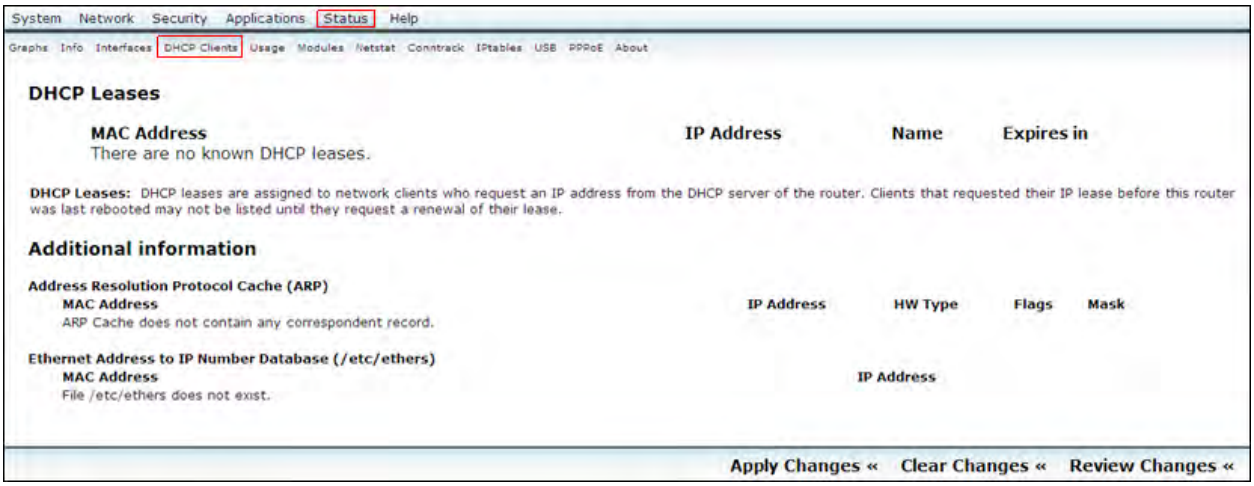
Click the **Show raw statistics** button, to view the **Raw Information** page at the bottom of the page. (Figure 9-14)

Figure 9-14: Raw Information

9.3 DHCP Clients

Click **Status** >**DHCP Clients**. Figure 9-15 displays the DHCP leases.

Figure 9-15: DHCP Clients

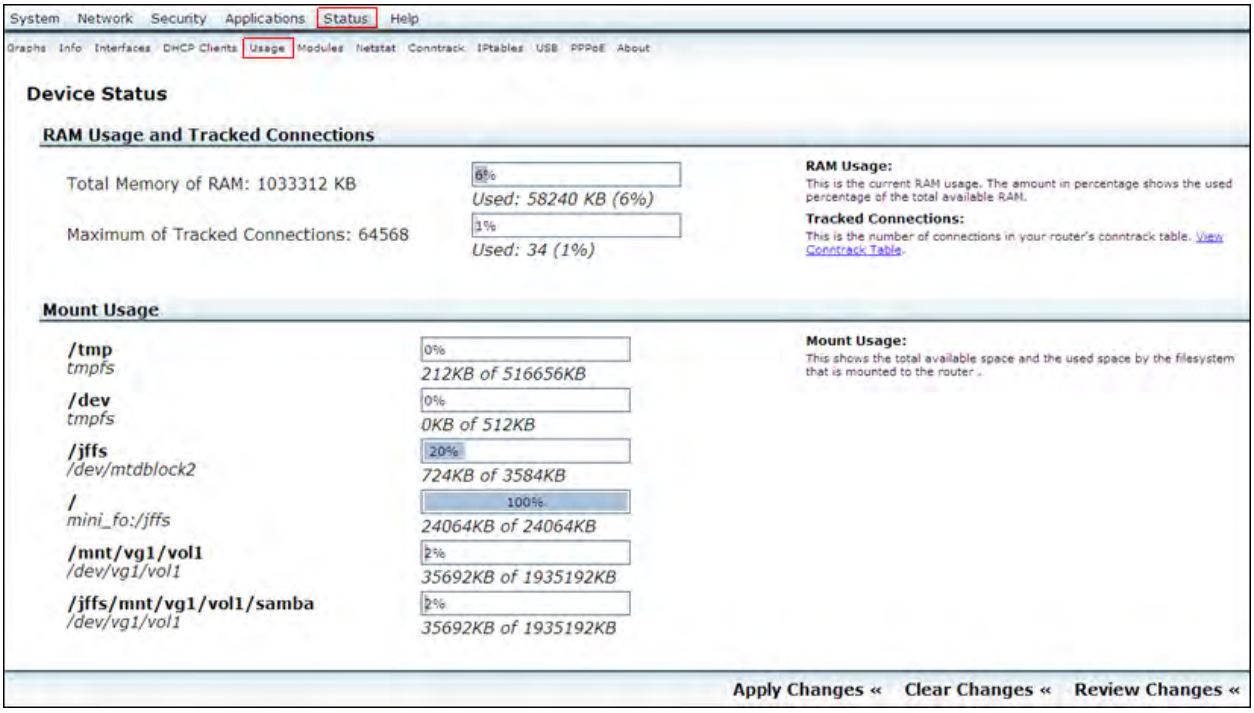


DHCP leases are assigned to network clients that request an IP address from the DHCP server of the router. Clients, who have requested their IP lease before this router, are rebooted and may not be listed until they request a renewal of their lease.

9.4 Usage

This section describes the status of device. (Figure 9-16)

Figure 9-16: Device Status



9.4.1 RAM Usage

This section displays the current RAM usage. It also tells the total available RAM and percentage of used RAM. (Figure 9-16)

9.4.2 Tracked Connections

This section displays the number of connections in your router's conntrack table (Figure 9-16). You can click the **View Conntrack Table** link to jump to Conntrack Table page.

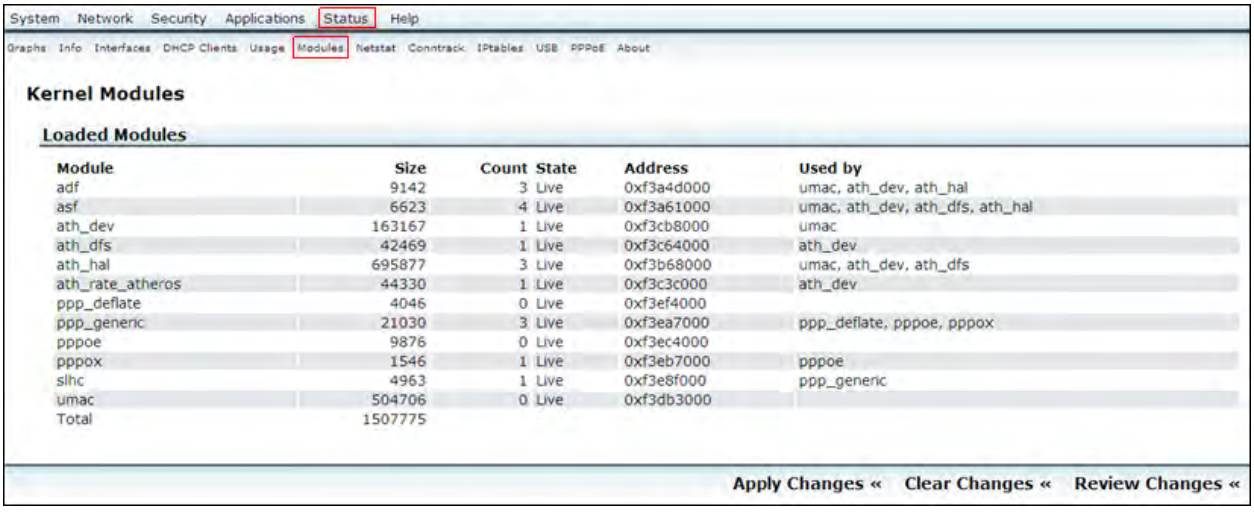
9.4.3 Mount Usage

This section displays the total amount of space and used on the file systems mounted to your router (Figure 9-16).

9.5 Modules

Click **Modules**. Figure 9-17 displays information about kernel modules. It displays all the loaded modules and provide information about module name, size, count, state, address and used by.

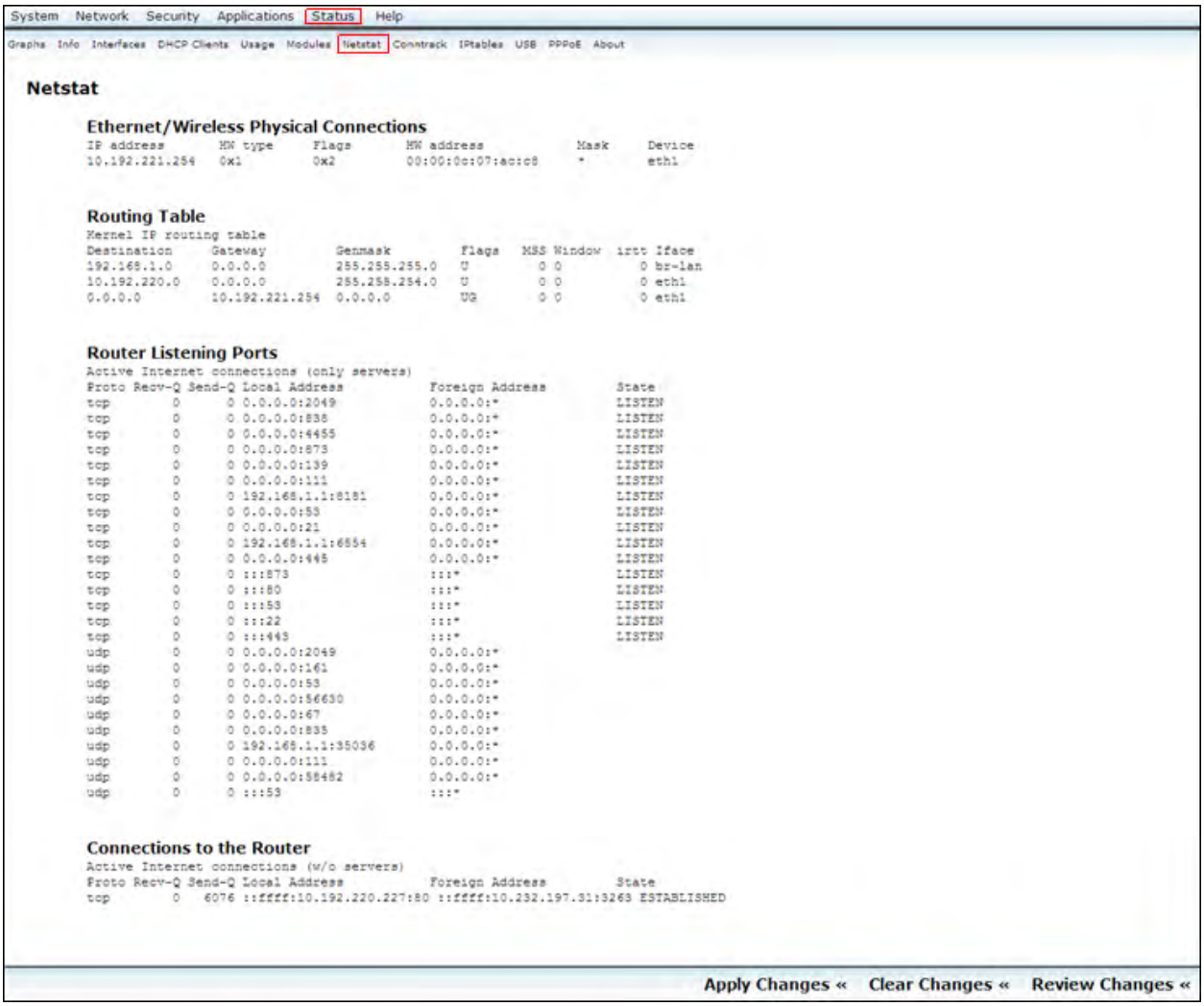
Figure 9-17: Kernel Modules



9.6 Netstat

Click **Netstat**. Figure 9-18 displays the detailed information about Ethernet/Wireless physical connections, routing table, router listening ports and connections to the routers.

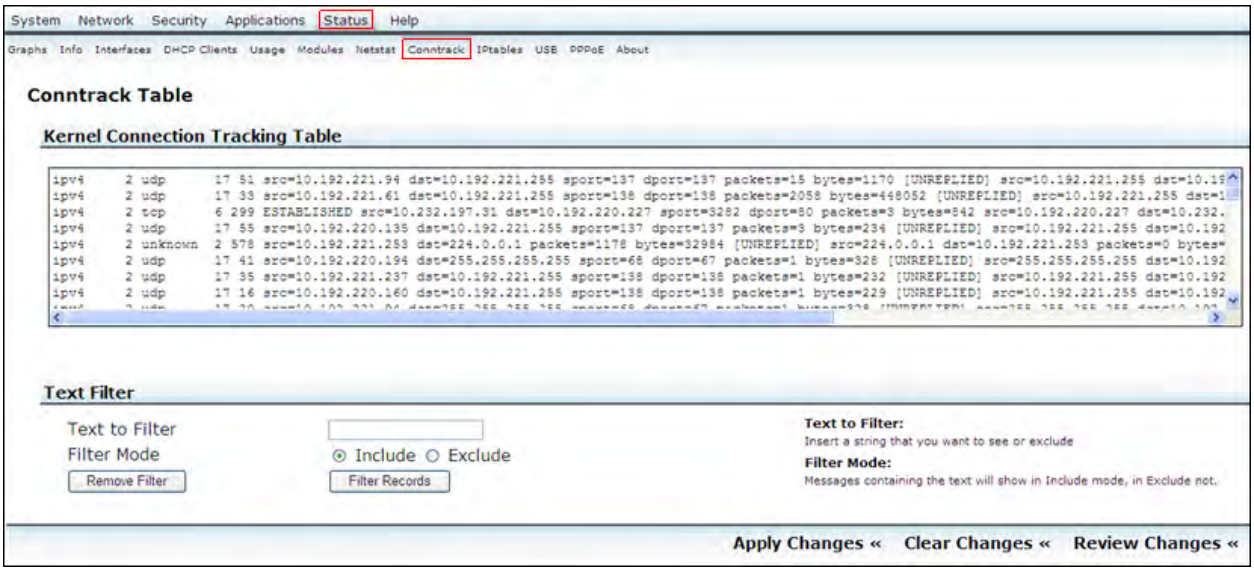
Figure 9-18: Netstat



9.7 Conntrack

Click **Conntrack**. Figure 9-19 displays conntrack table.

Figure 9-19: Conntrack

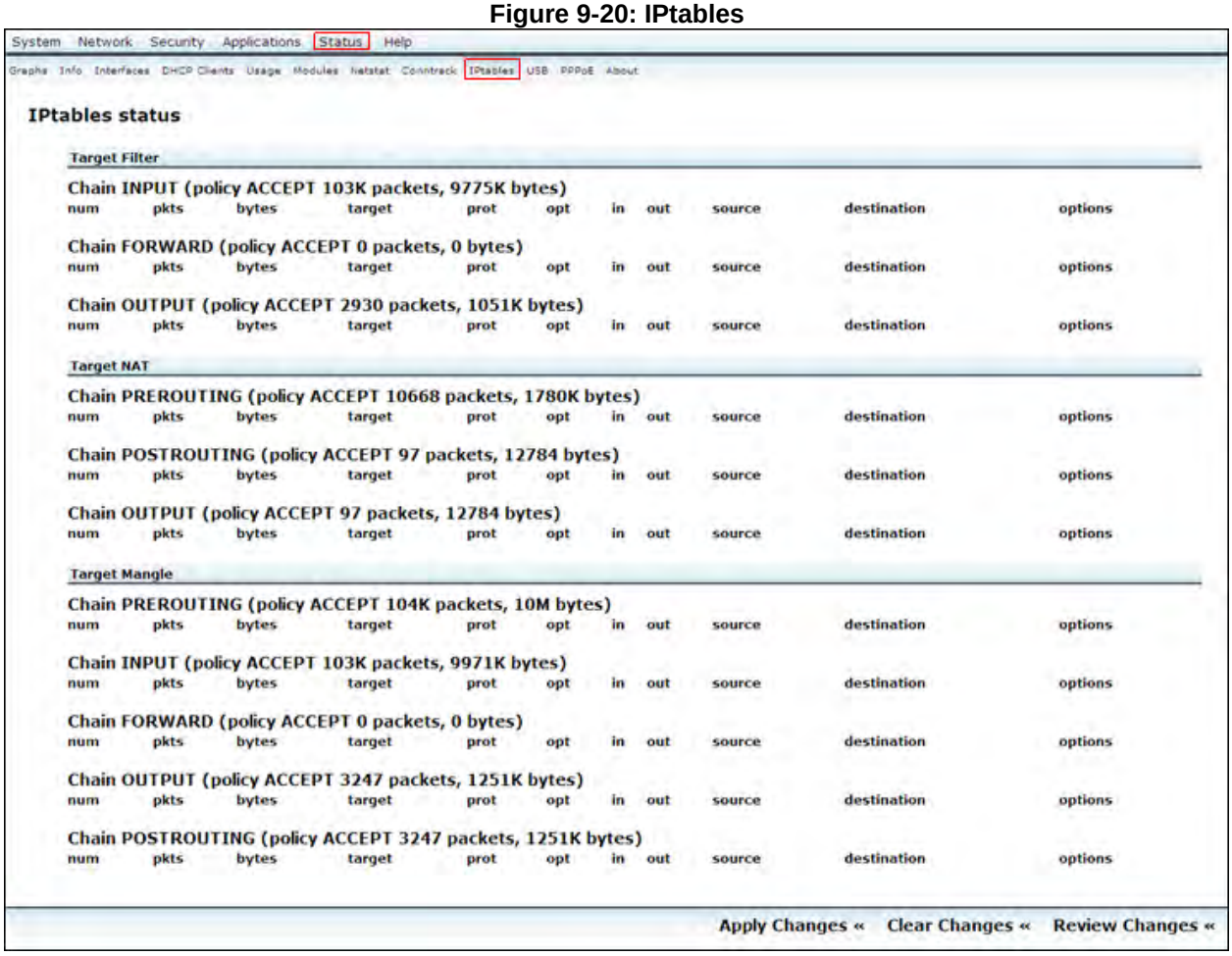


1. Insert a string to include or exclude in the **Text to Filter** text box. You can also type the regular expression constants like: 00:[[:digit:]]{2}:[[:digit:]]{2} or debug|.err
2. From the **Filter Mode** drop-down list, select **Include** or **Exclude** option.
3. Click **Remove Filter** button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

9.8 IPtables

Click **IPtables**. Figure 9-20 displays IPtables status.

Figure 9-20: IPtables



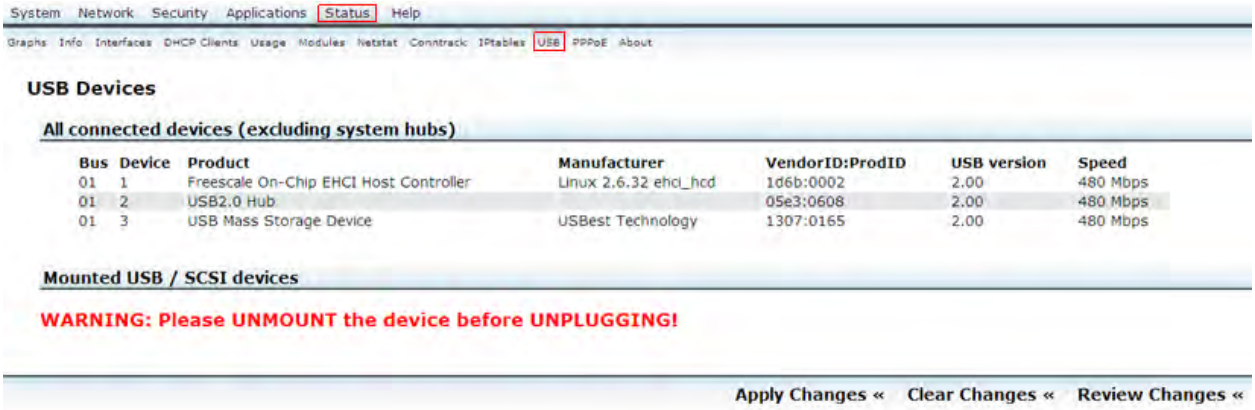
9.9 USB

Click **USB**. Figure 9-21 displays the information about all the connected devices (excluding system hubs) and mounted USB/SCSI devices.

NOTE

Do ‘umount’ before plug out the USB Flash.

Figure 9-21: USB



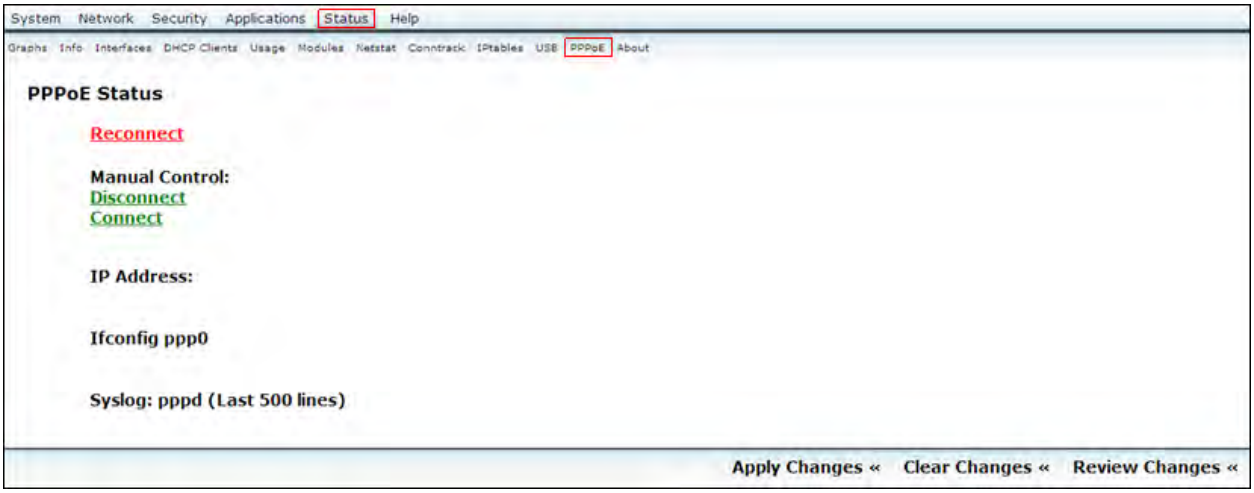
Warning!

You must umount the device before unplug.

9.10 PPPoE

Click **PPPoE**. Figure 9-22 displays the PPPoE status.

Figure 9-22: PPPoE



Note

If the manual differs from the real device, please follow Web GUI on the real device, or contact FAE for the latest document.