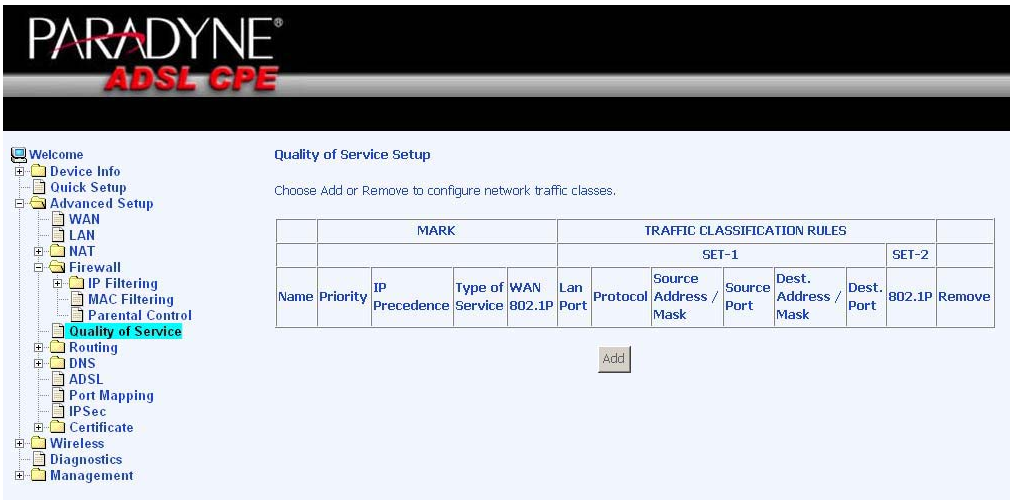
Quality of Service

You can configure the Quality of Service to apply different priorities to traffic on the router. Click on **Add** to view the *Add Network Traffic Class Rule* screen.

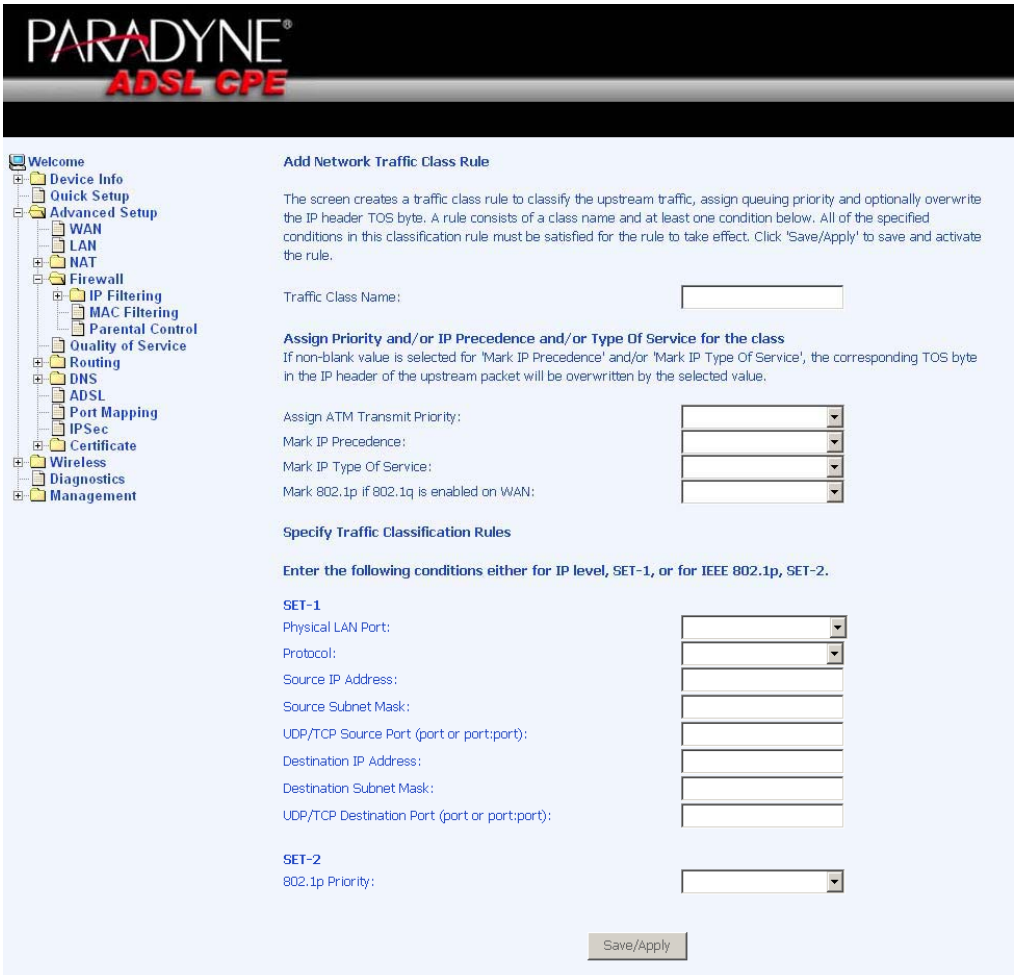


This screen allows you to add a network traffic class rule. Procedures for this setup are as follows—

1. Give a name to this traffic class.
2. Assign a priority level—low, medium, and high—to this traffic class.
3. Select an IP precedence from the 0-7 range.
4. Enter an IP Type of Service from the following selections—

   - Normal Service
   - Minimize Cost
   - Maximize Reliability
   - Maximize Throughput
   - Minimize Delay

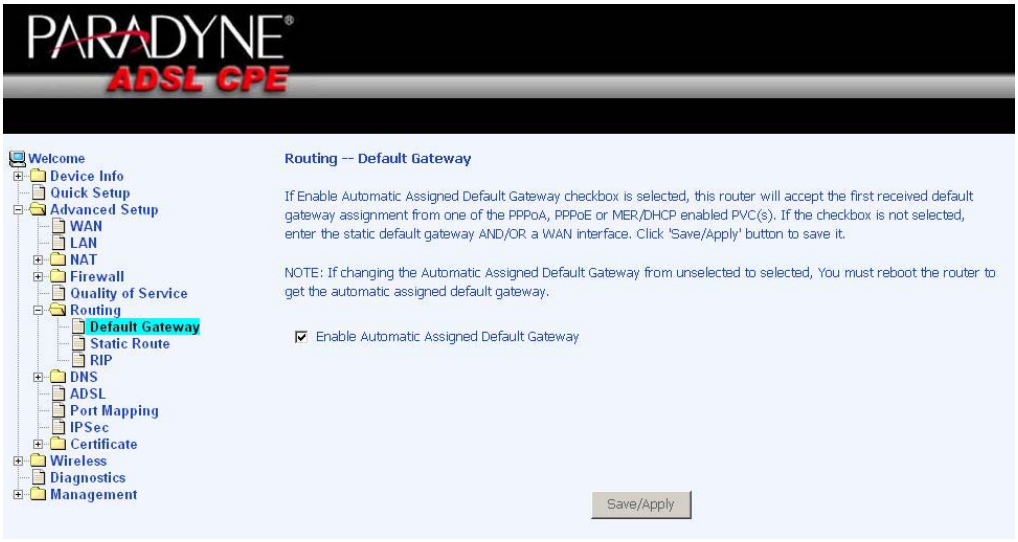
5. Last, enter the traffic conditions for the class such as the protocol (TCP / UDP, TCP, UDP, or ICMP) to be used. Click **Save / Apply** to save the settings.



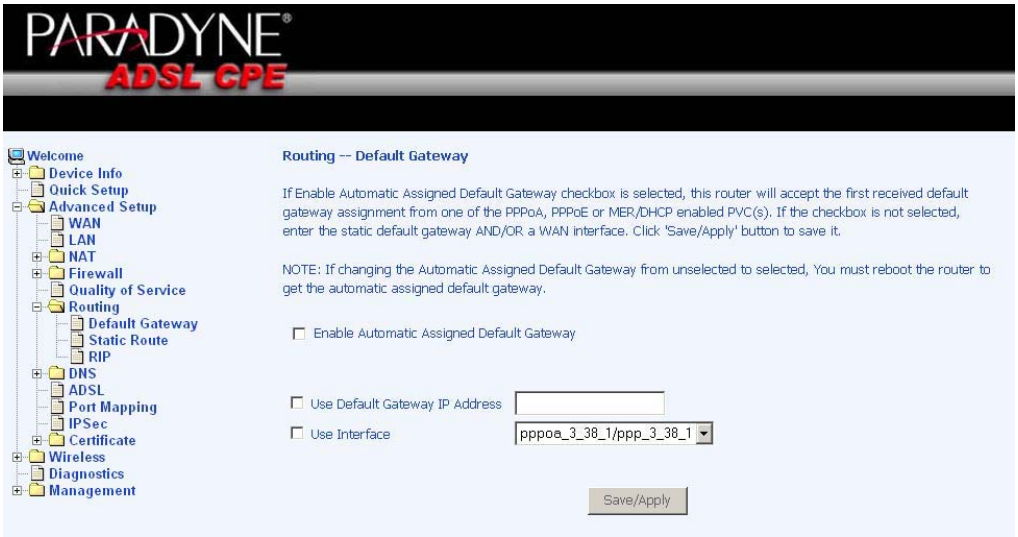
Routing

Default Gateway

You can enable automatic assigned default gateway on the Routing – Default Gateway screen. As default, the box is checked for automatic assigned default gateway to be enabled. Click the **Save / Apply** button to enable or disable this feature.



If you do not want to enable Automatic Assigned Default Gateway, then uncheck the box as seen below. You will be given the choice to use the default gateway IP address. If you decide to change the automatic assigned default gateway address, you must reboot the router to be assigned a new default gateway IP address. Also, select the WAN interface that you will be using. Click on **Save / Apply** to save the settings.



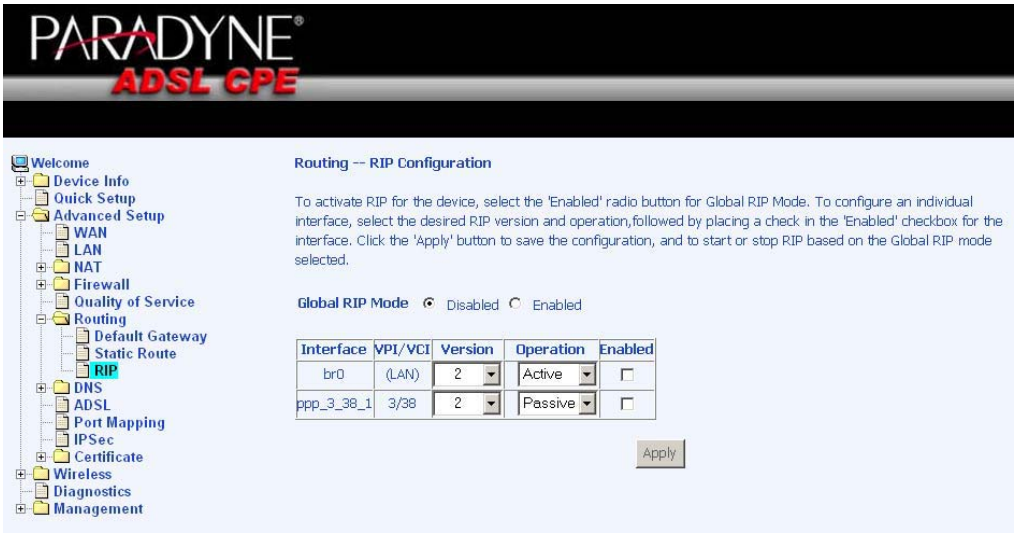
Static Route

The Static Route page can be used to add a routing table (a maximum of 32 entries can be configured). Click on **Next** to add.

Enter the route information and then save and apply your configurations.

RIP

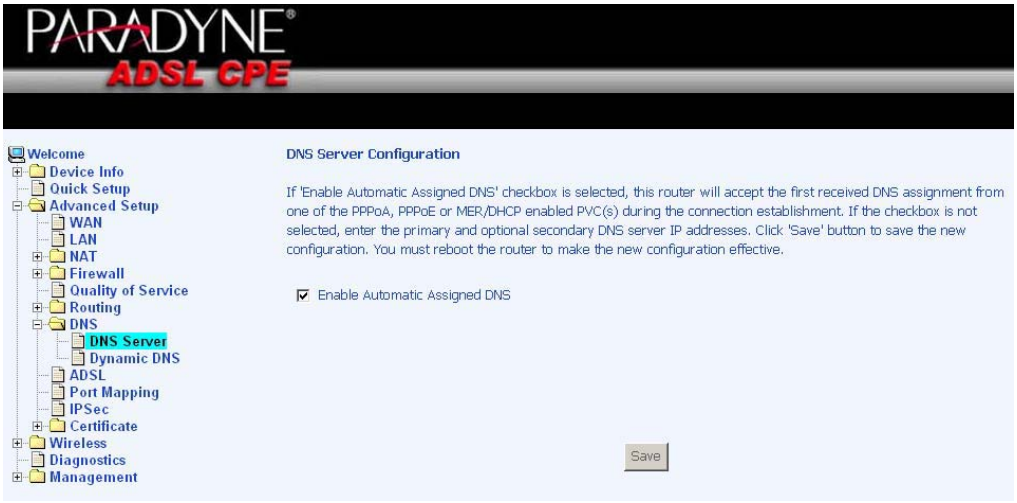
If RIP (Routing Information Protocol) is enabled, the router operation can be configured as active or passive.



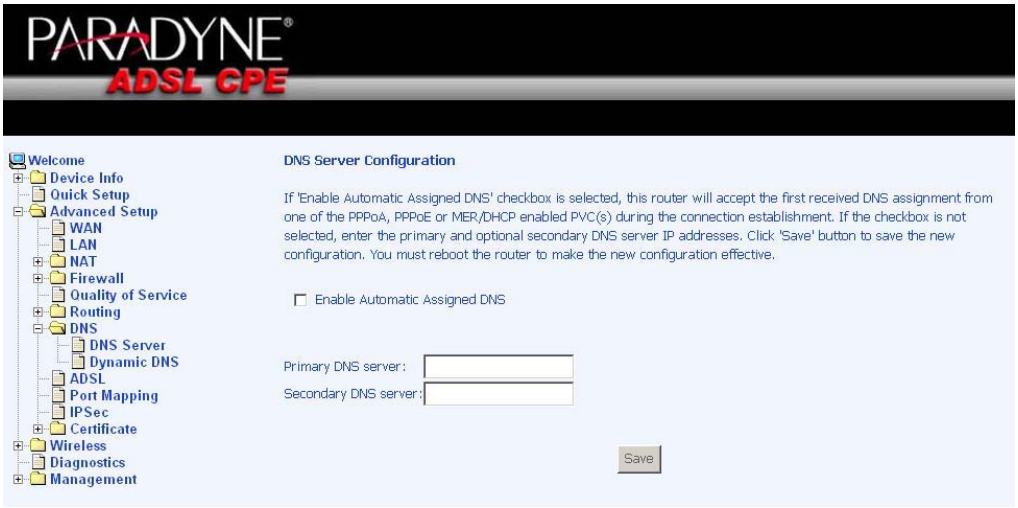
DNS

DNS Server

Use the DNS Server Configuration screen to request automatic assignment of a DNS or to specify a primary and secondary DNS.

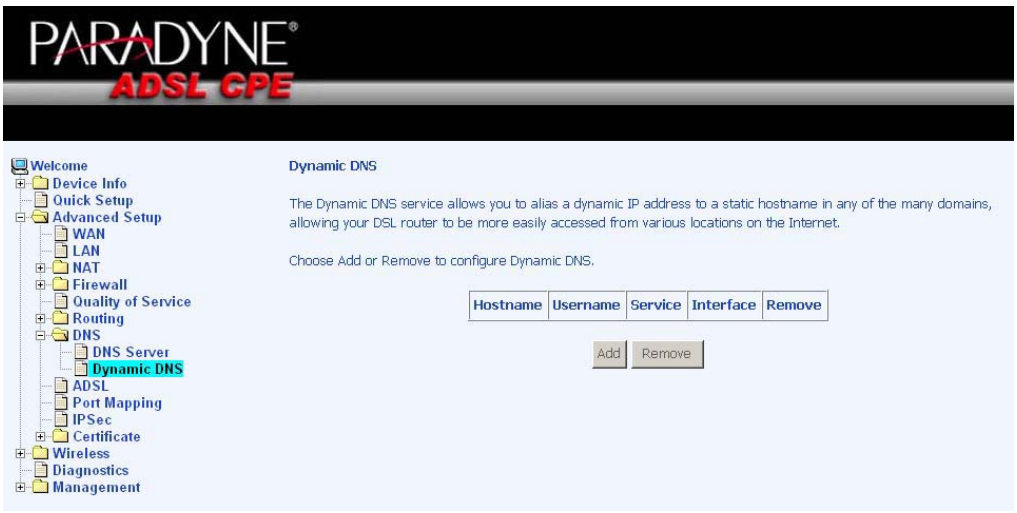


If you uncheck the *Enable Automatic Assigned DNS* checkbox, then there will be two additional fields—primary and secondary DNS server—to enter as seen below.

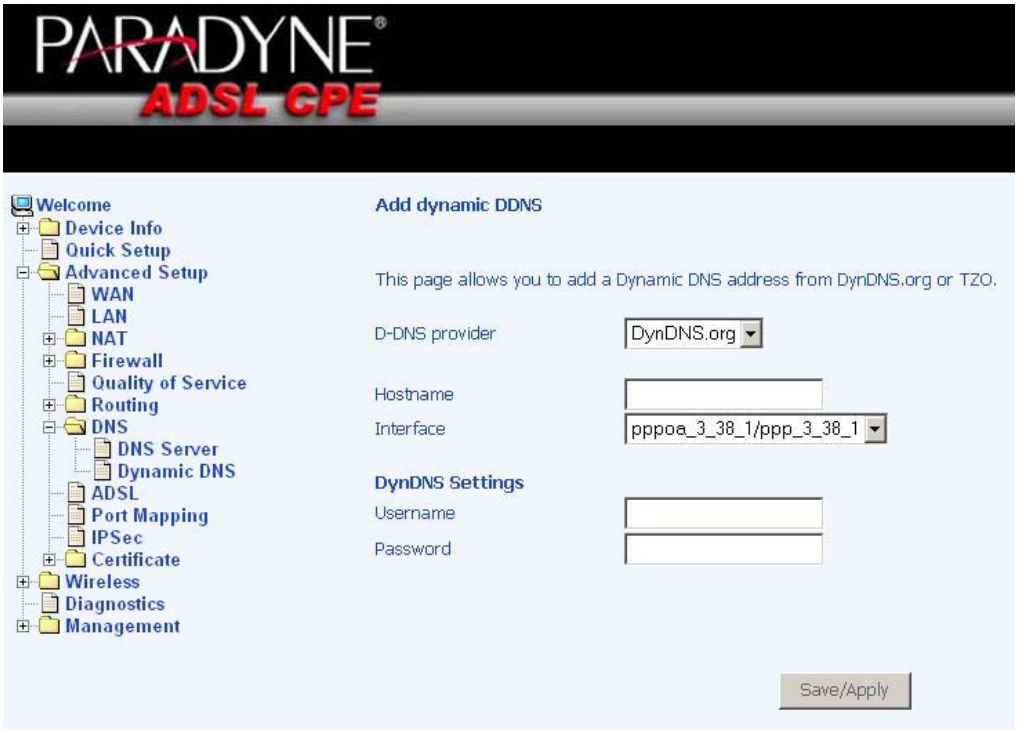


Dynamic DNS

Dynamic DNS is a service for allowing an Internet domain name to be assigned to a varying IP address. This makes it possible for other sites on the Internet to establish connections to your router without needing to track the IP address themselves. Click on **Add** to set up a dynamic DNS configuration.

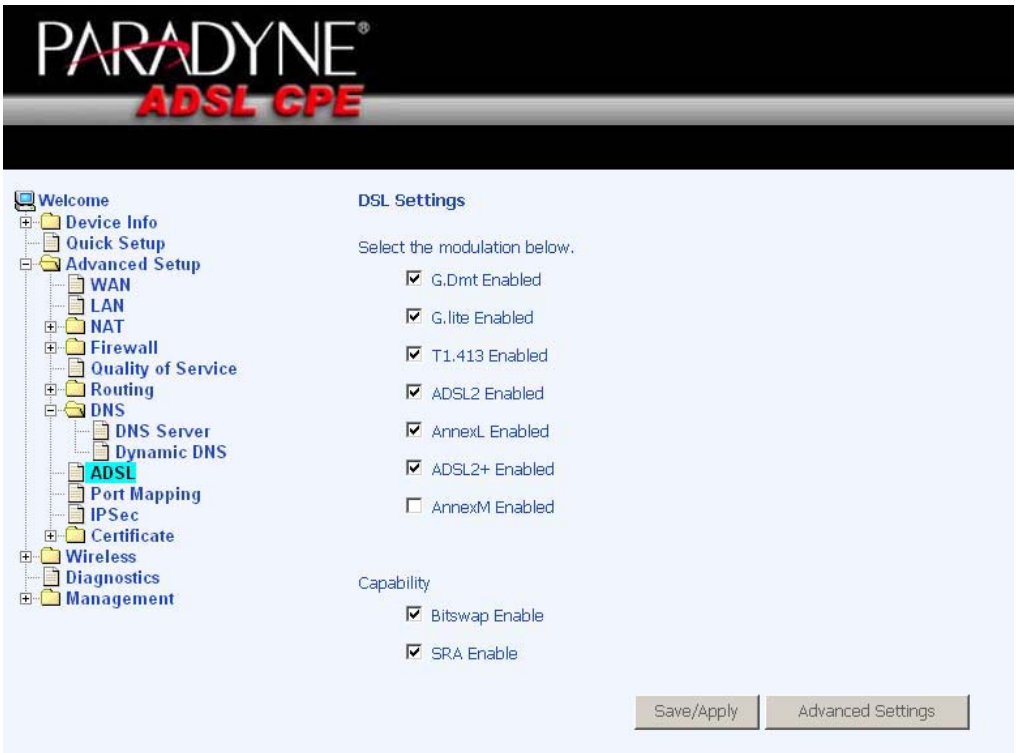


This screen allows you to add a dynamic DNS address from DynDNS.org or TZO. Enter the hostname and the interface that you are using. Also enter the username and password assigned by the DNS service. Click on **Save / Apply** to save these configurations.



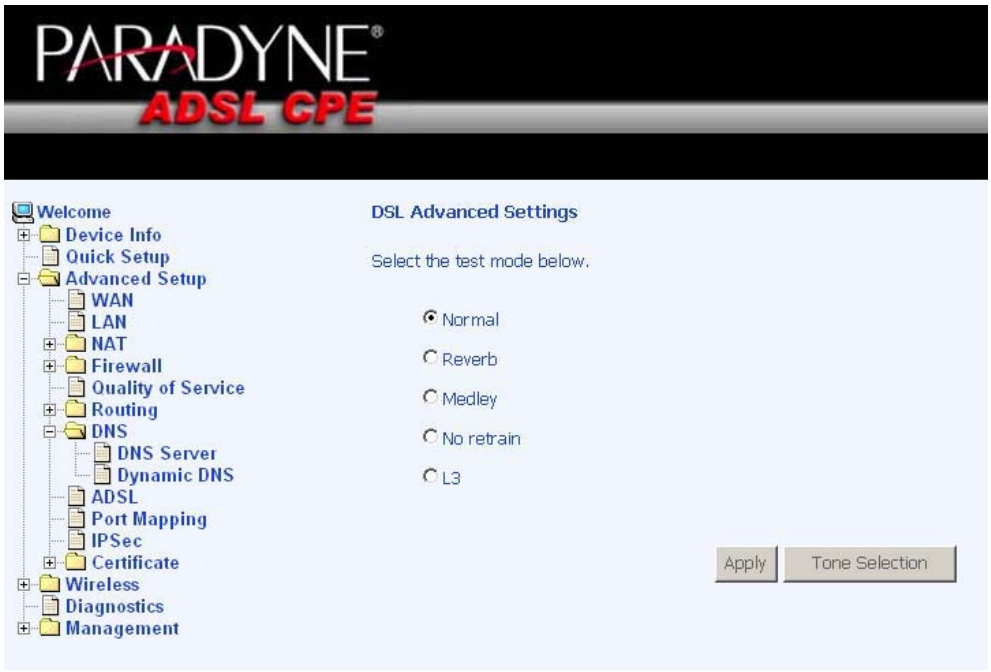
ADSL

The DSL settings page contains three sections—modulation and capability—that should be specified by your ISP. Consult with your ISP to select the correct settings for each. Then click on **Save / Apply** if you are finished or click on **Advanced Settings** if you want to configure more advanced settings.



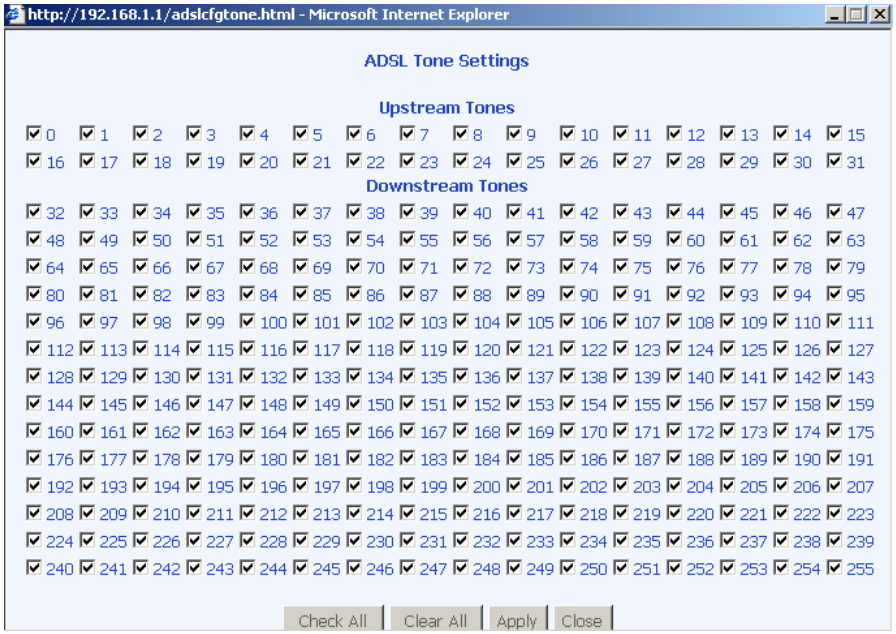
DSL Advanced Settings

The test mode can be selected from the DSL Advanced Settings page. Test modes include—normal, reverb, medley, no retrain, and L3. After you make your selections of the test mode, click on **Apply** to save these settings first before you go to *Tone Selection*.



Tone Settings

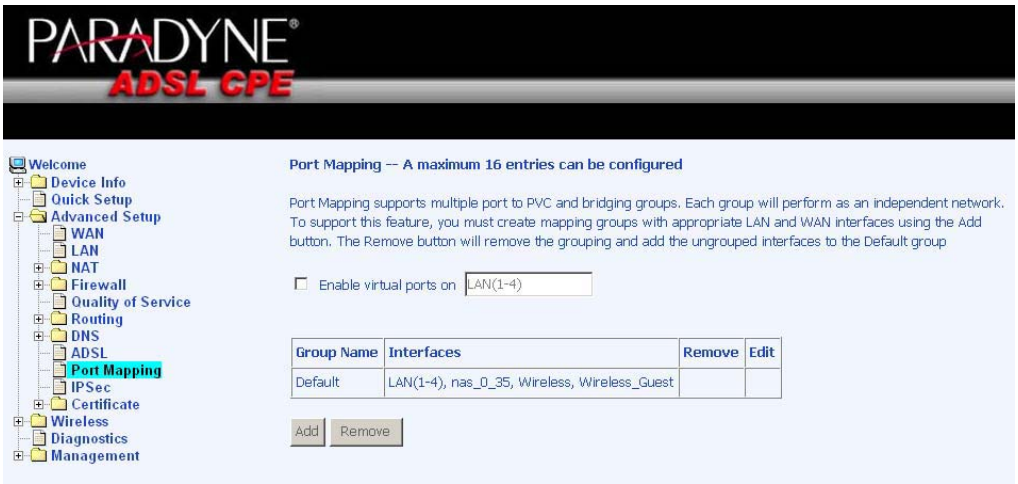
The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart. With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream. Do not change these settings unless directed by your ISP.



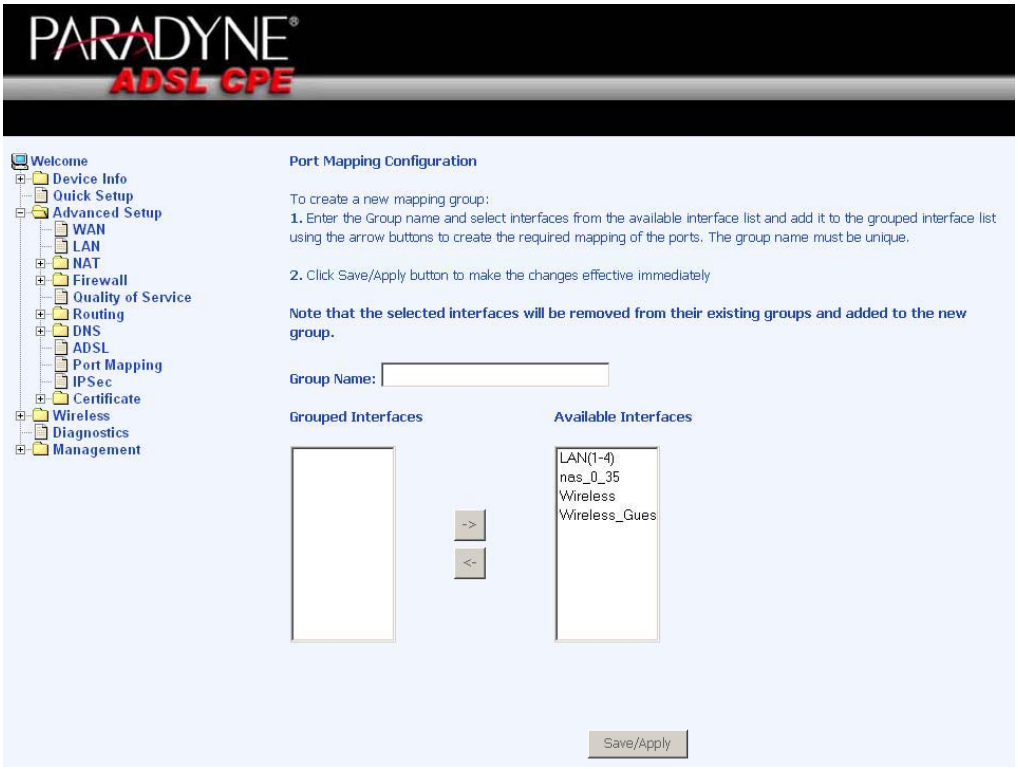
Port Mapping

Port mapping is a feature that allows you to open ports to allow certain Internet applications on the WAN side to pass through the firewall and enter your LAN. To use this feature, mapping groups should be created.

Click on the **Add** button as displayed below. If you need to edit an entry, then click on the **Edit** button.

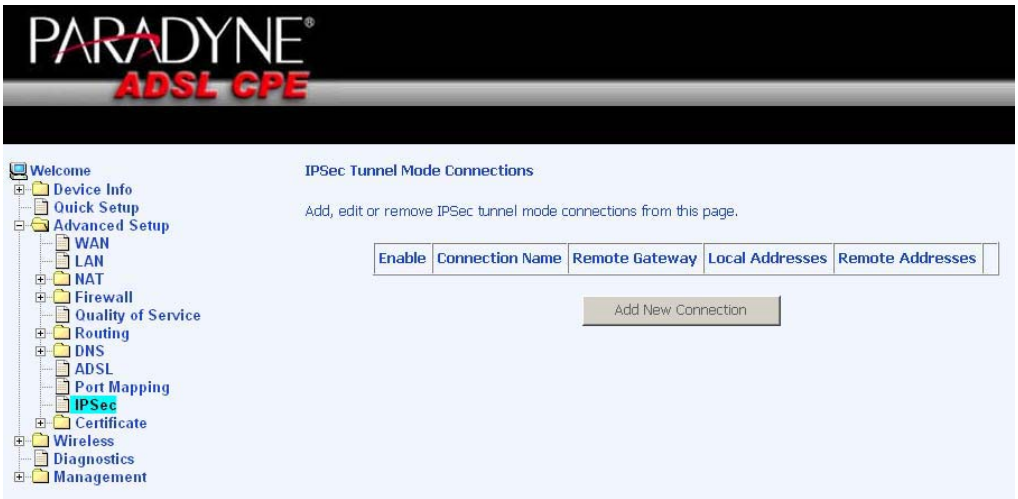


After clicking the **Add** button, the below configuration screen appears, allowing you enter the groups and the interfaces they are associated with.

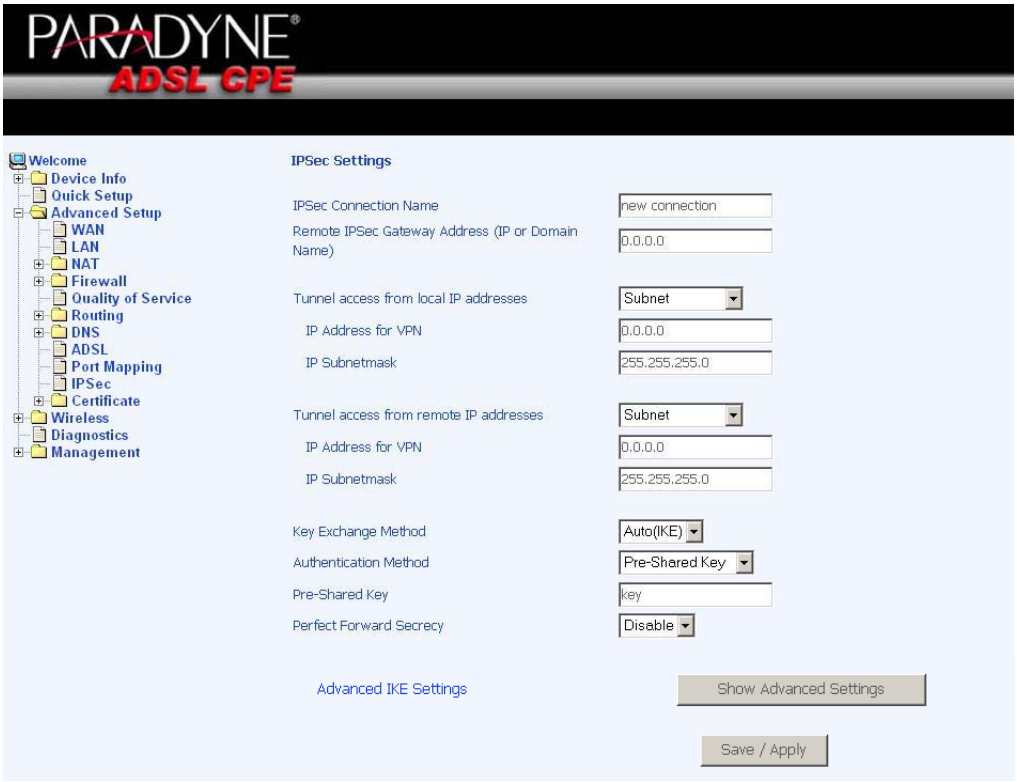


IPSec

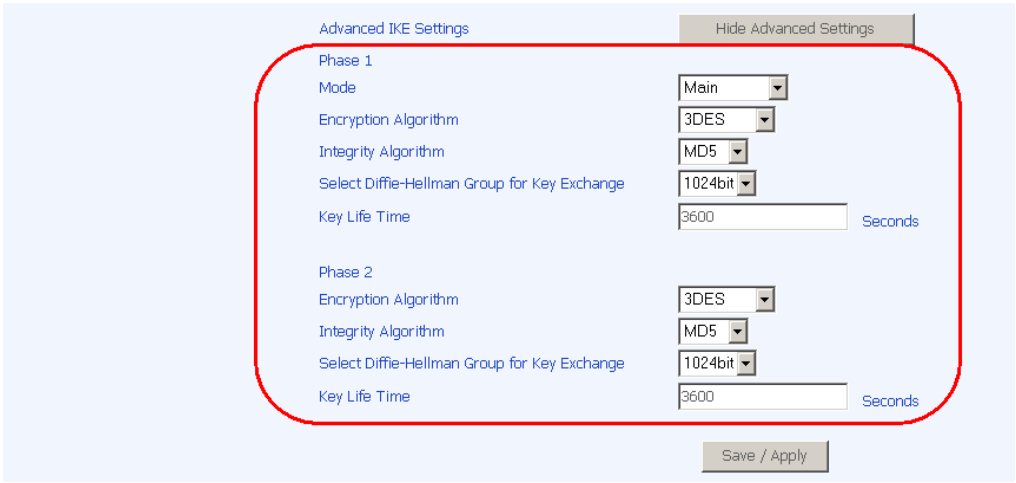
Internet Protocol Security (IPSec) allows you to set up secure tunnel access between two IP addresses. Encryption and key exchange make this a secure way to access remote networks. Contact your ISP for the necessary information to correctly configure this connection.



Click on **Add New Connection** to access the IPSec Settings screen to enter your configurations. Notice the **Show Advanced Settings** button at the bottom of the screen for additional encryption settings.



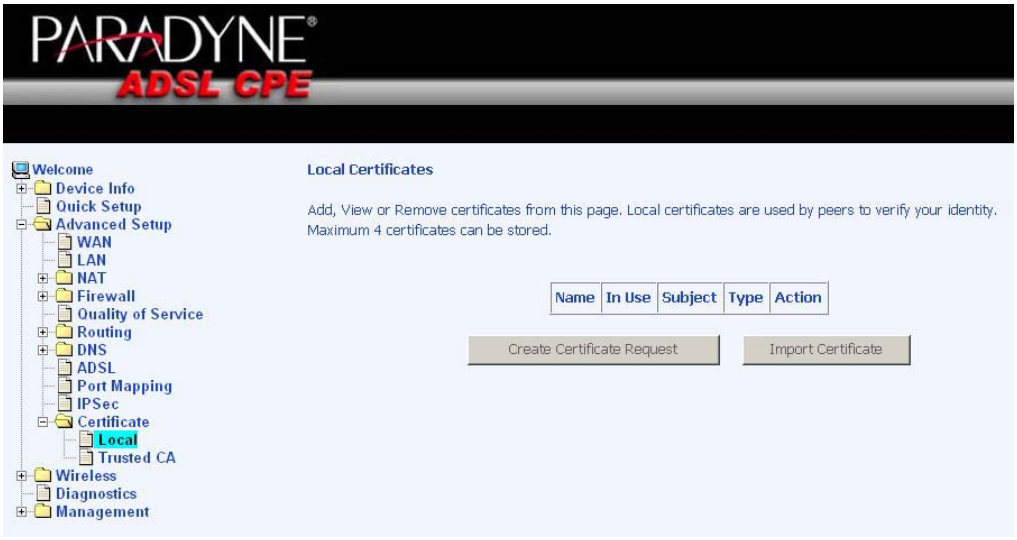
The following portion of the IPSec Settings screen can be seen when you click on the the **Show Advanced Settings** button.



Certificate

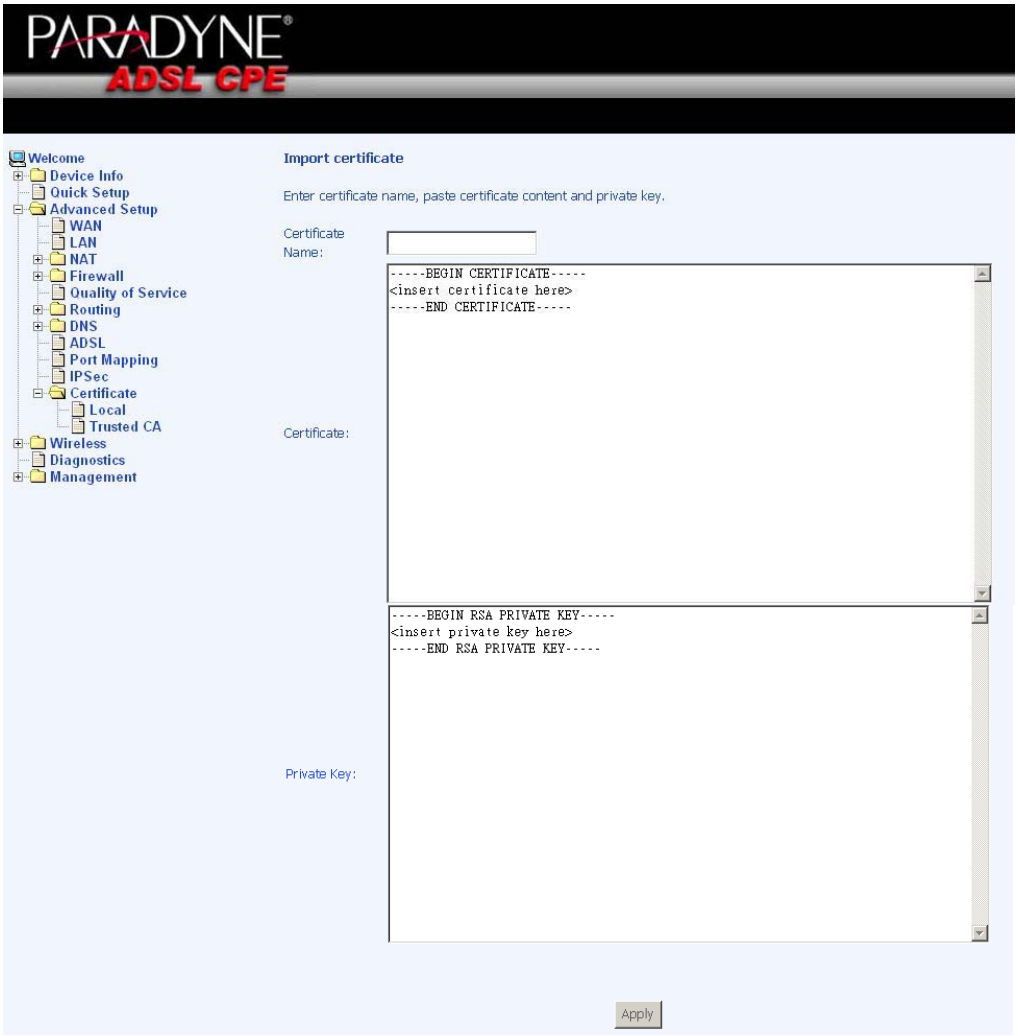
Local

A local certificate identifies yourself over the network. To apply for a certificate, click on **Create Certificate Request** and if you have an existing certificate, click on **Import Certificate** to retrieve it.



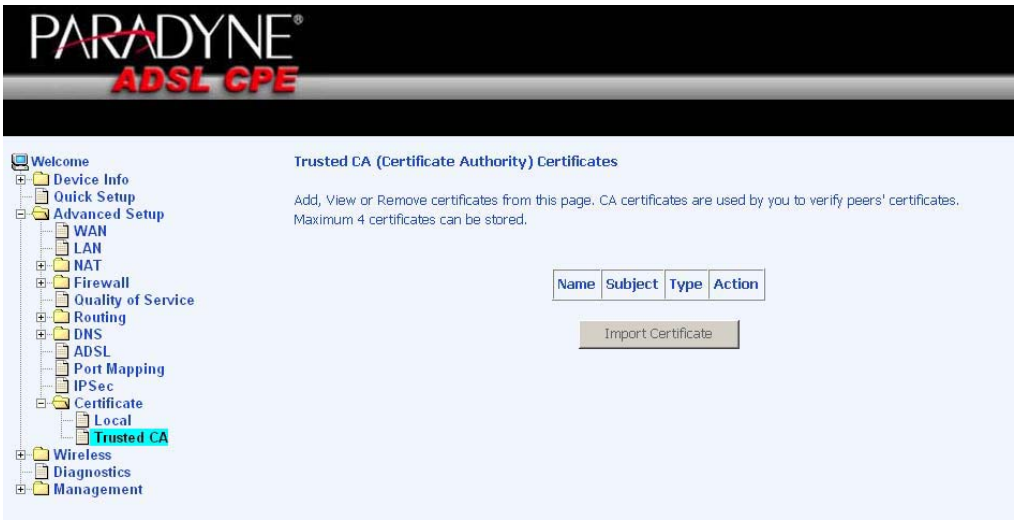
The below screen allows you to request a new certificate request. Enter the required information and click **Apply** to submit the request.

Additionally, if you have a certificate already, you can simply import the certificate by pasting the certificate content and private key into the space provided. Click **Apply** to submit the request to import the certificate.

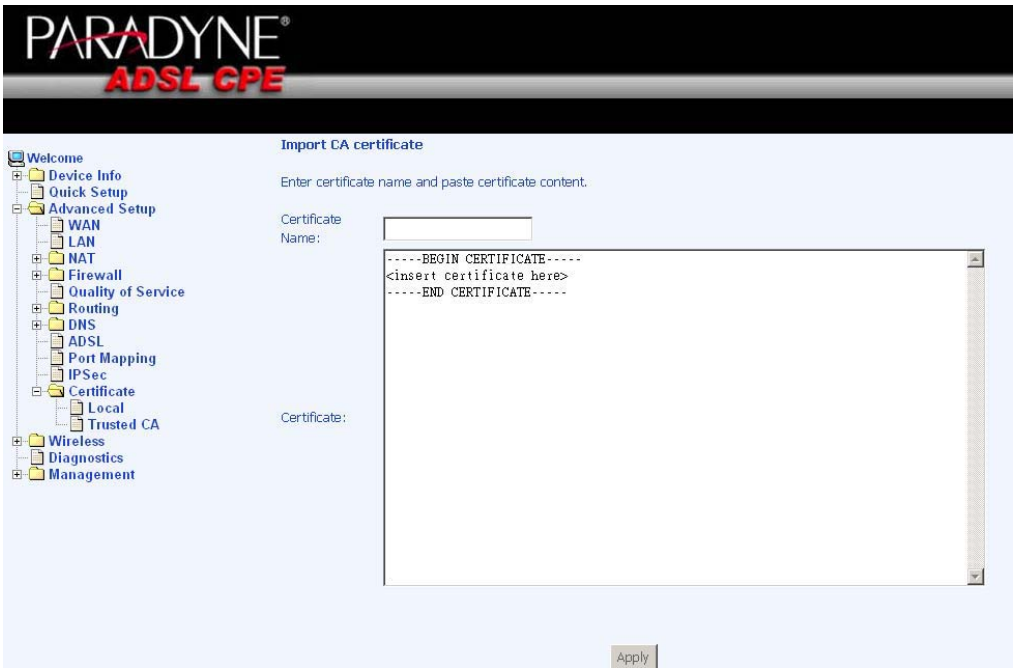

PARADYNE
ADSL CPE
Welcome
Device Info
Quick Setup
Advanced Setup
WAN
LAN
NAT
Firewall
Quality of Service
Routing
DNS
ADSL
Port Mapping
IPSec
Certificate
Local
Trusted CA
Wireless
Diagnostics
Management
Import certificate
Enter certificate name, paste certificate content and private key.
Certificate Name:
Certificate:
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
Private Key:
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
Apply

Trusted CA

The trusted certificate authority (CA) allows you to verify the certificates of your peers. Note that you can store up to 4 certificates. The below screen also allows you to view the CA's that you may have already added and can be removed. Click on **Import Certificate** to continue to the next screen.



Paste the content of the certificate that you wish to add and click **Apply**.

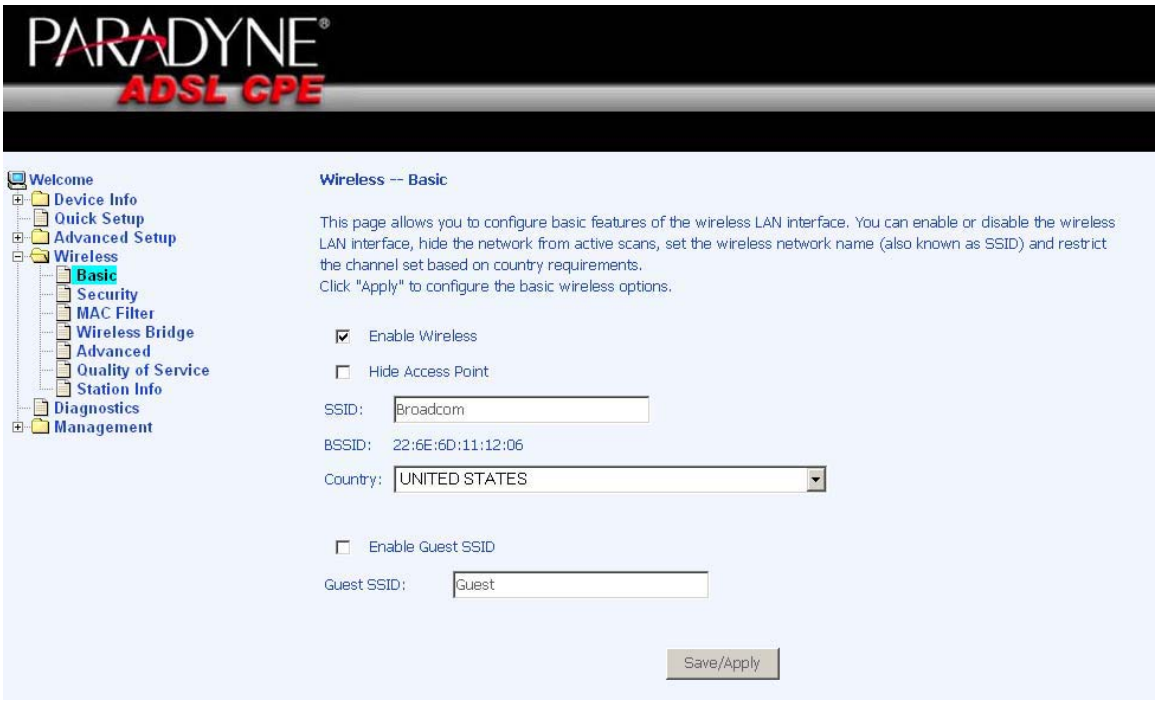


Wireless

The router's wireless feature can be configured to your needs. Sections covered under the wireless section include—basic, security, MAC filter, wireless bridge, advanced, quality of service and station info.

Basic

The below **Wireless - Basic** screen allows you to enable or disable wireless function. You can also hide the access point so others cannot see your ID on the network. If you enable wireless, be sure to enter an SSID, your wireless network name and select the country that you are in.



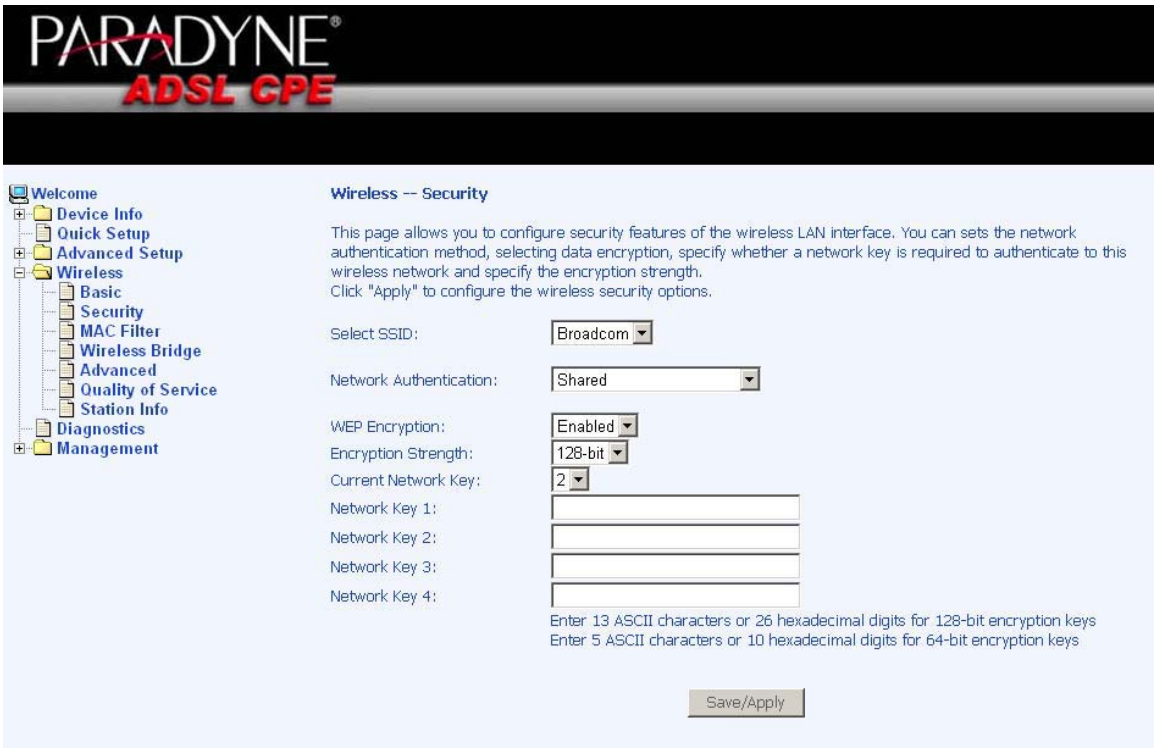
Security

The next screen is the **Wireless - Security** screen which allows you to select the network authentication method and to enable or disable WEP encryption. Note that depending on the network authentication that is selected, the screen will change accordingly so additional fields can be configured for the specific authentication method.

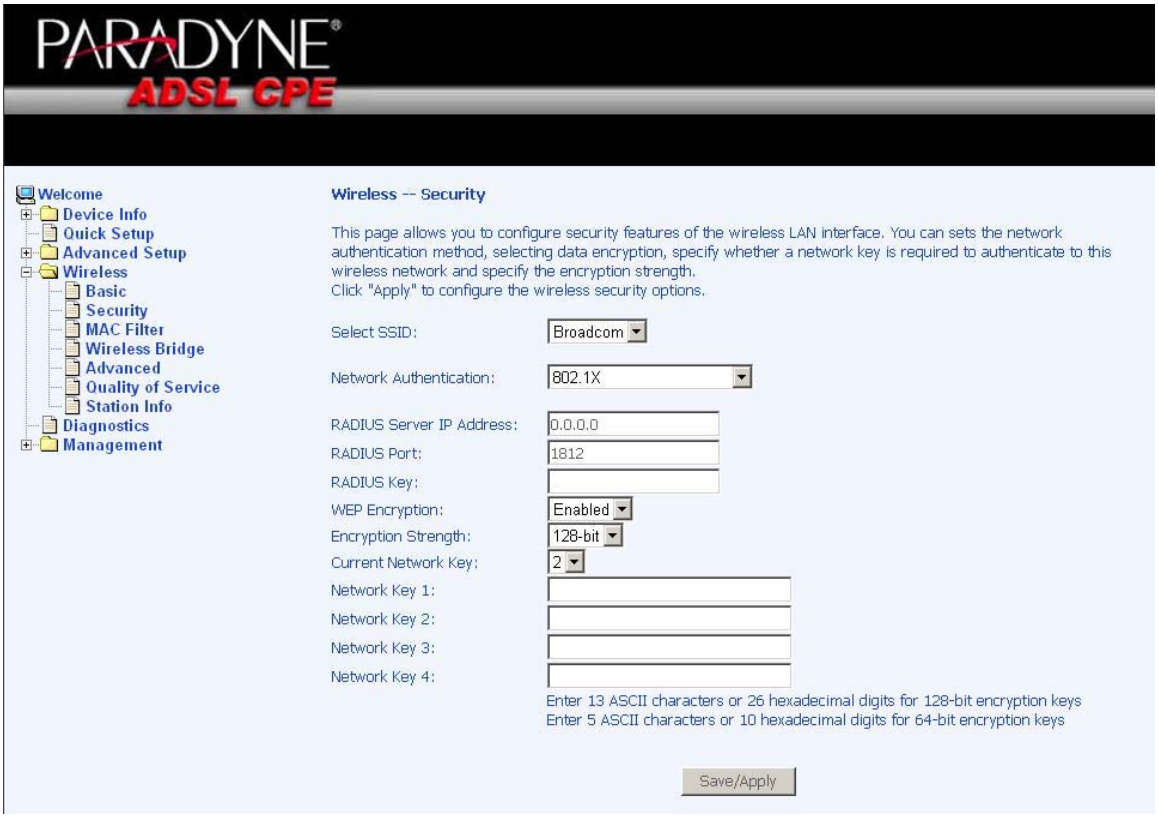
Network authentication methods include the following—

- **Open**—anyone can access the network. The default is a disabled WEP encryption setting.

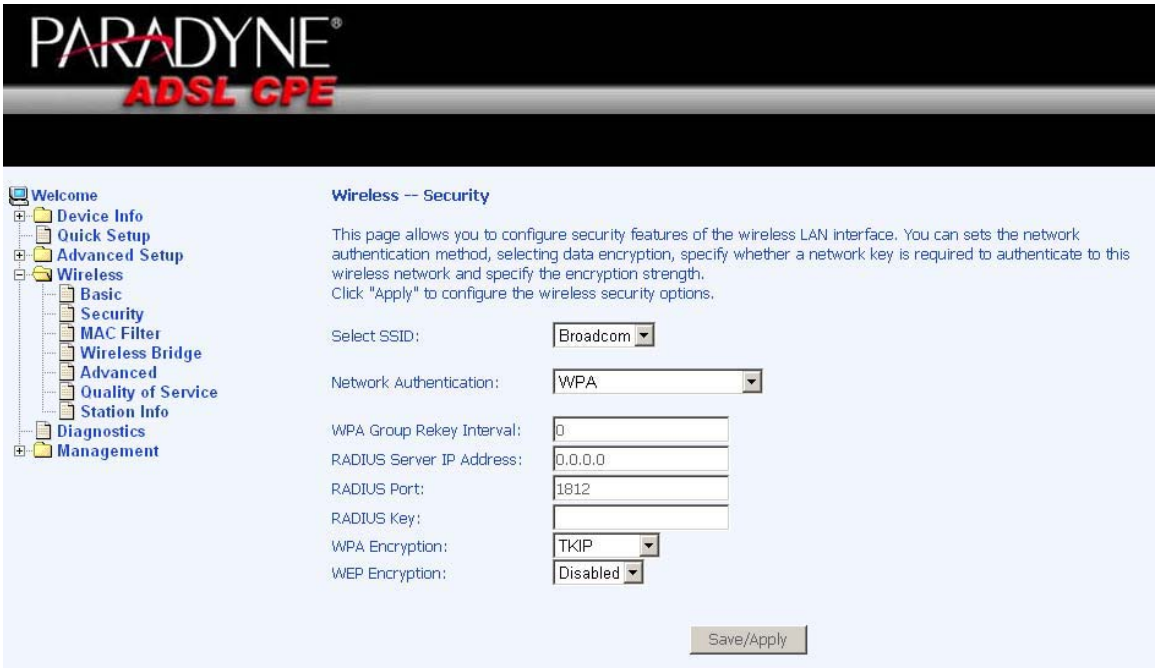
- **Shared**—WEP encryption is enabled and encryption key strength of 64-bit or 128-bit needs to be selected. Click on **Set Encryption Keys** to manually set the network encryption keys. Up to 4 different keys can be set and you can come back to select which one to use at anytime.



- **802.1X**—requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is also enabled and the encryption strength must also be selected.

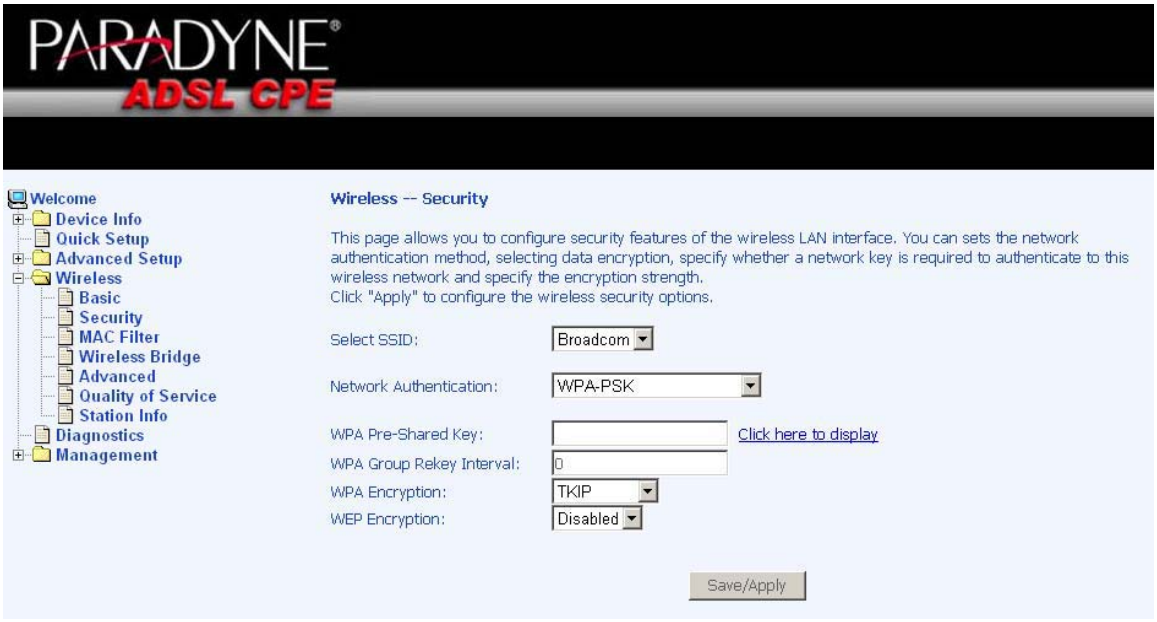


- **WPA—(Wi-Fi Protected Access)**— usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses128-bit dynamic session keys (per user, per session, and per packet keys).

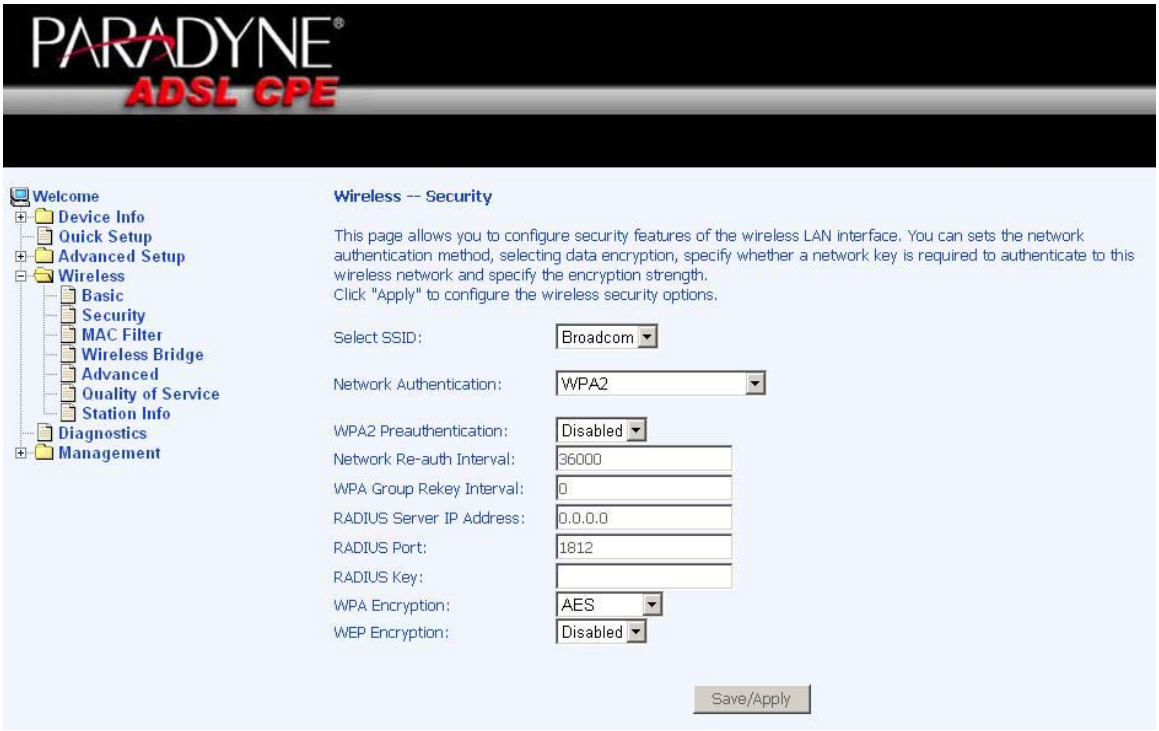


- **WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key)**—WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet

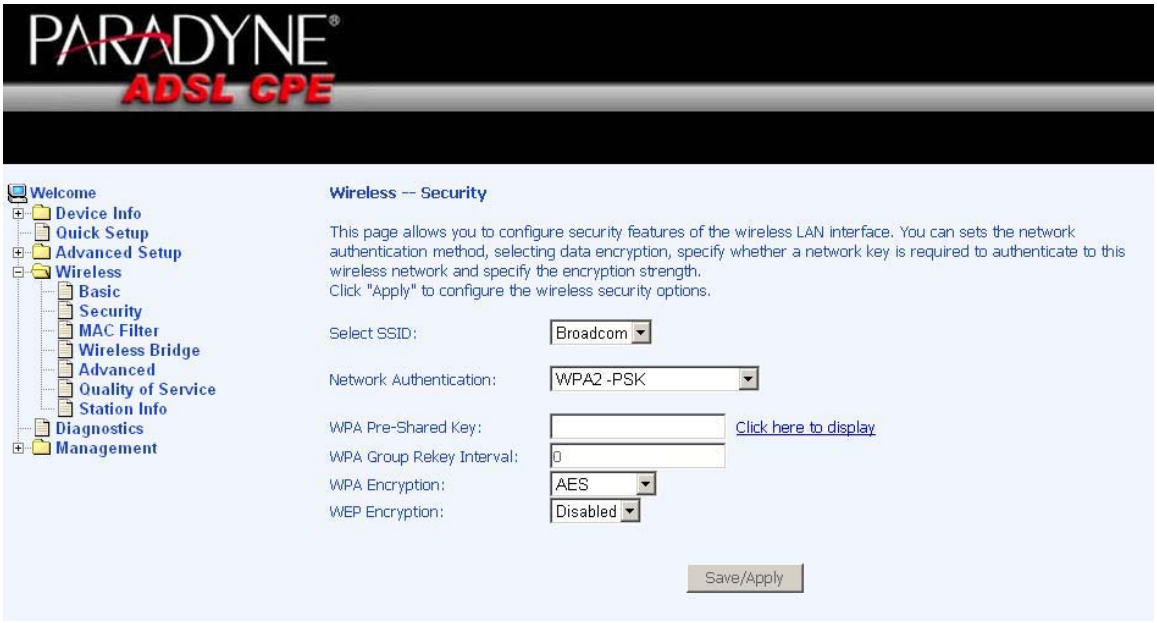
key construction, and key management that WPA provides in the enterprise environment. The main difference is that the password is entered manually. A group re-key interval time is also required.



- **WPA2 (Wi-Fi Protected Access 2)**—second generation of WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method. Network re-auth interval is the time in which another key needs to be dynamically issued.



- **WPA2-PSK (Wi-Fi Protected Access 2 – Pre-Shared Key)**—suitable for home and SOHO environments, it also uses AES encryption and requires you to enter a password and an re-key interval time.



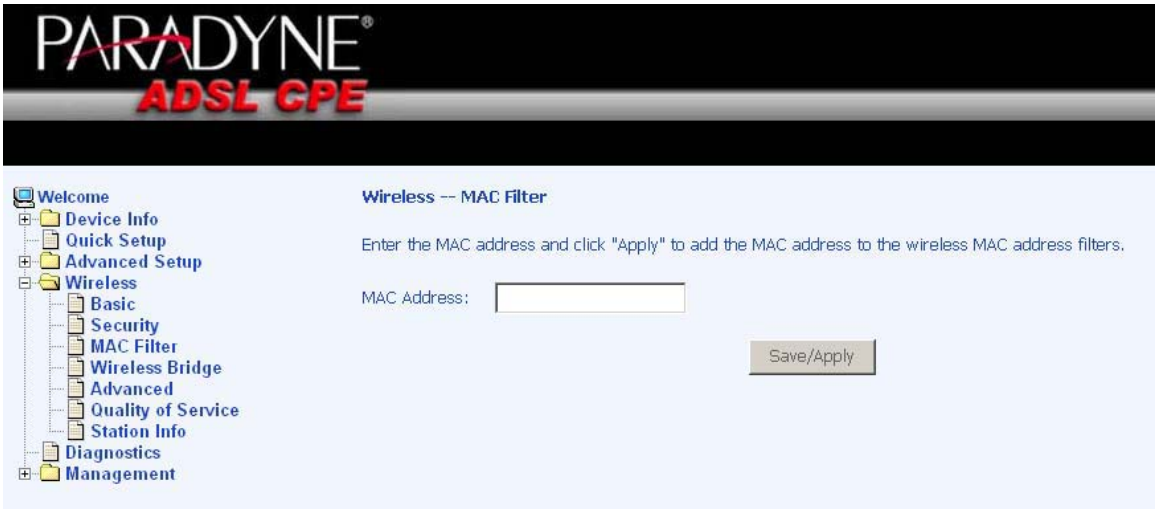
- **Mixed WPA2 / WPA**—during transitional times for upgrades in the enterprise environment, this mixed authentication method allows "upgraded" and users not yet "upgraded" to access the network via the router. RADIUS server information must be entered for WPA and a as well as a group re-key interval time. Both TKIP and AES are used.

- **Mixed WPA2 / WPA-PSK**—useful during transitional times for upgrades in the home or SOHO environment, a pre-shared key must be entered along with the group re-key interval time. Both TKIP and AES are also used.

MAC Filter

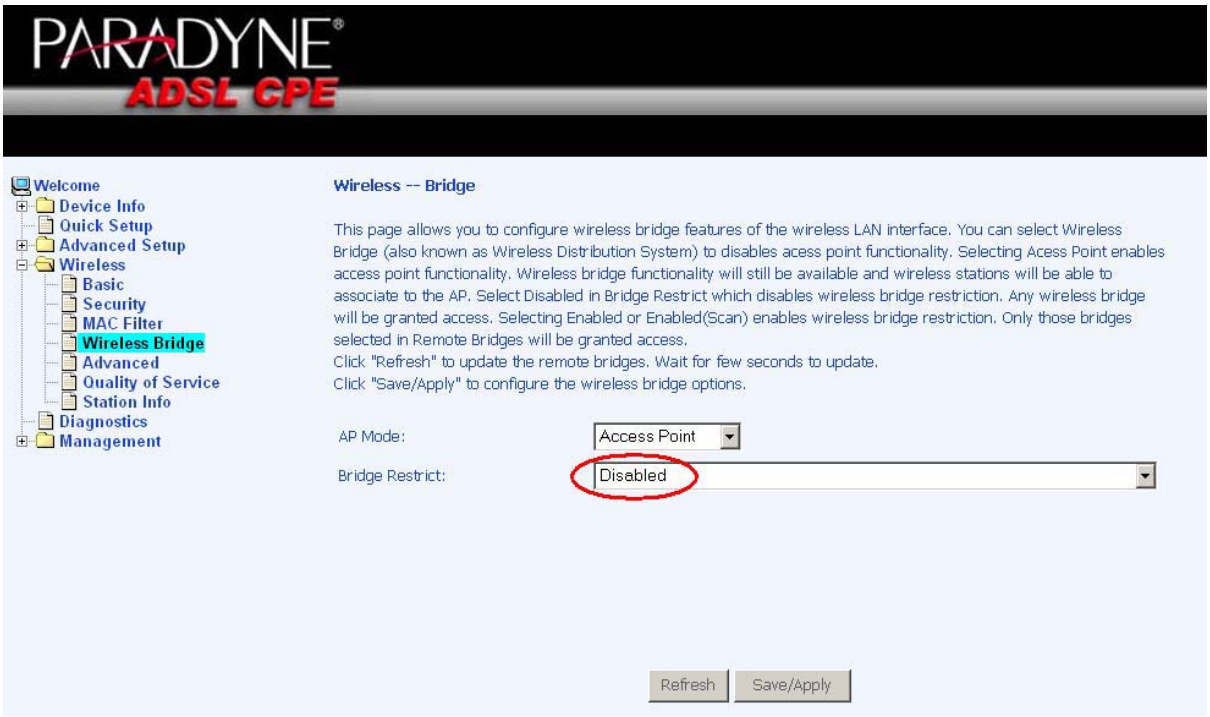
The MAC filter screen allows you to manage MAC address filters. Add the MAC addresses that you want to manage and then select the mode that you want to use to manage them. You can disable this feature or you can allow or deny access to the MAC addresses that you add to the list.

The following screen appears when you want to add a MAC address to the filter. When completed, click on the **Save / Apply** button.

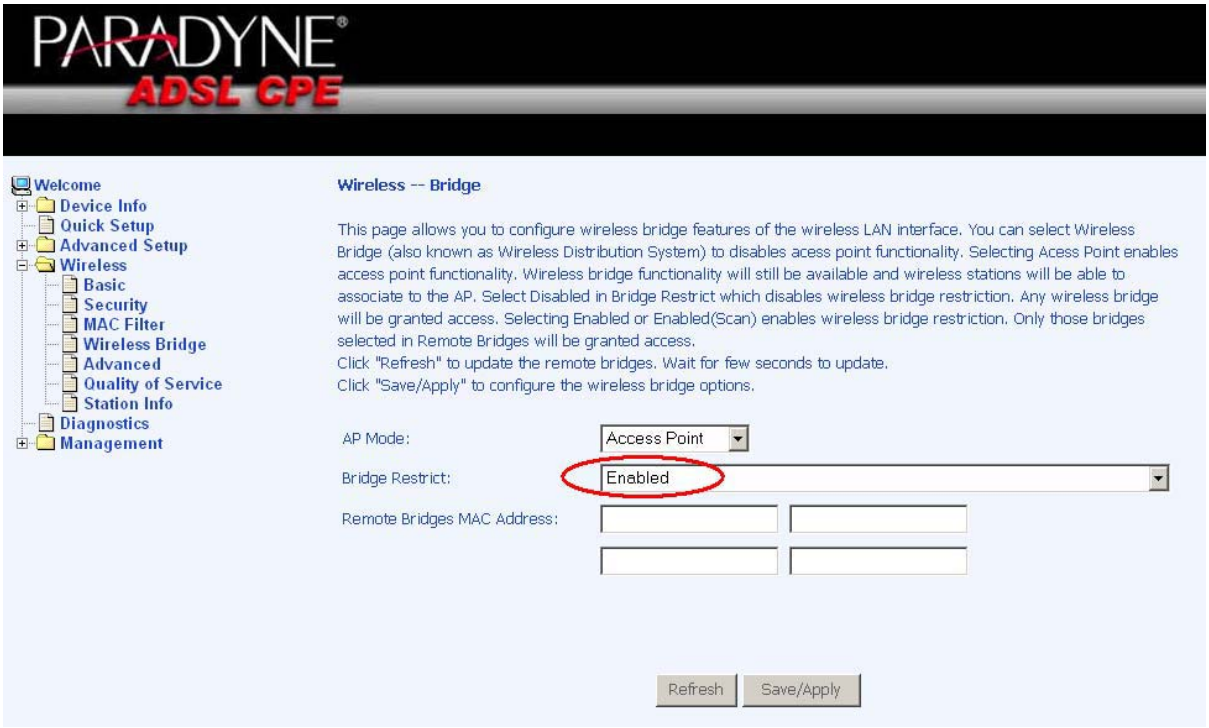


Wireless Bridge

In this next screen, you can select the mode you want the router to be in, either access point or wireless bridge.



If you enable the bridge restrict option, then proceed to enter the MAC addresses of the remote bridges.



Advanced

Advanced features of the wireless LAN interface can be configured in this section.

Settings can be configured for the following—

- **AP Isolation**—if you select enable, then each of your wireless clients will not be able to communicate with each other.
- **Band**—a default setting at 2.4GHz – 802.11g
- **Channel**-- 802.11b and 802.11g use channels to limit interference from other devices. If you are experiencing interference with another 2.4Ghz device such as a baby monitor, security alarm, or cordless phone, then change the channel on your router.
- **Multicast Rate**—the rate at which a message is sent to a specified group of recipients.
- **Basic Rate**—the set of data transfer rates that all the stations will be capable of using to receive frames from a wireless medium.
- **Fragmentation Threshold**—used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.
- **RTS Threshold (Request to Send Threshold)**—determines the packet size of a transmission through the use of the router to help control traffic flow.
- **DTIM Interval**—sets the Wake-up interval for clients in power-saving mode.
- **Beacon Interval**—a packet of information that is sent from a connected device to all other devices where it announces its availability and

readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).

- **Xpress Technology—**a technology that utilizes standards based on framebursting to achieve higher throughput. With Xpress Technology enabled, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by up to 25% in 802.11g only networks and up to 75% in mixed networks comprised of 802.11g and 802.11b equipment.

- **54g Mode—** 54g is a Broadcom Wi-Fi technology.

- **54g Protection**--the 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without "speaking" at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS (Request to Send / Clear to Send) to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.

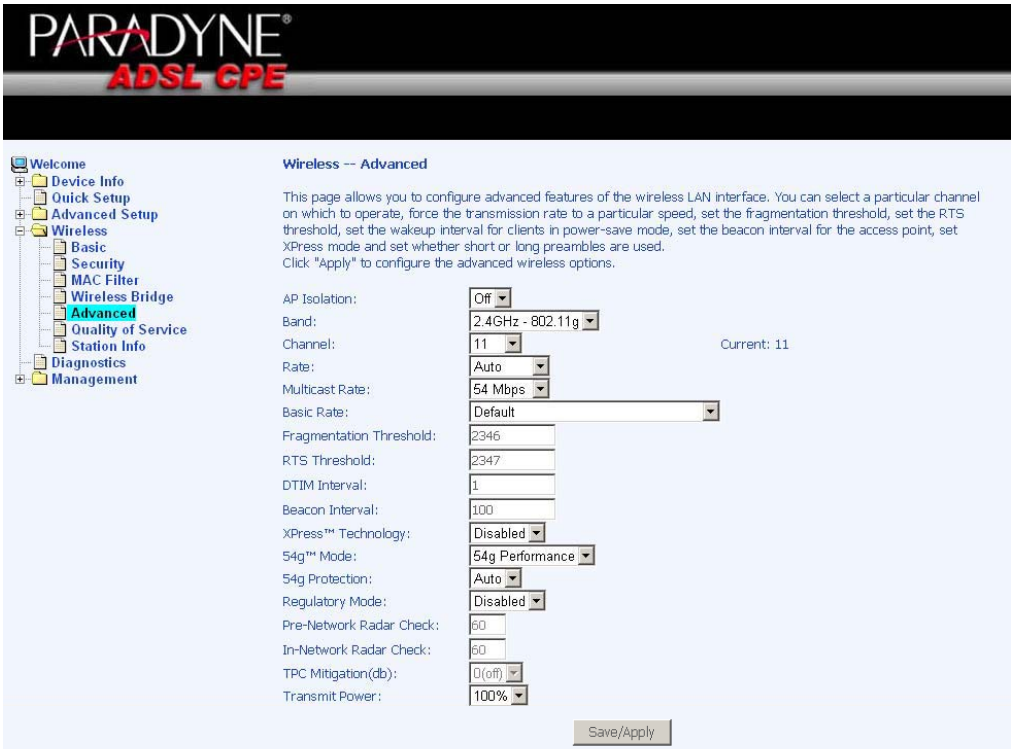
- **Regulatory Mode**—there are two regulatory modes to choose from—802.11h and 802.11d—or you can disable the function.

- **Pre-Network Radar Check**—default value is set at 60 and cannot be changed.

- **In-Network Radar Check**—default value is set at 60 and cannot be changed.

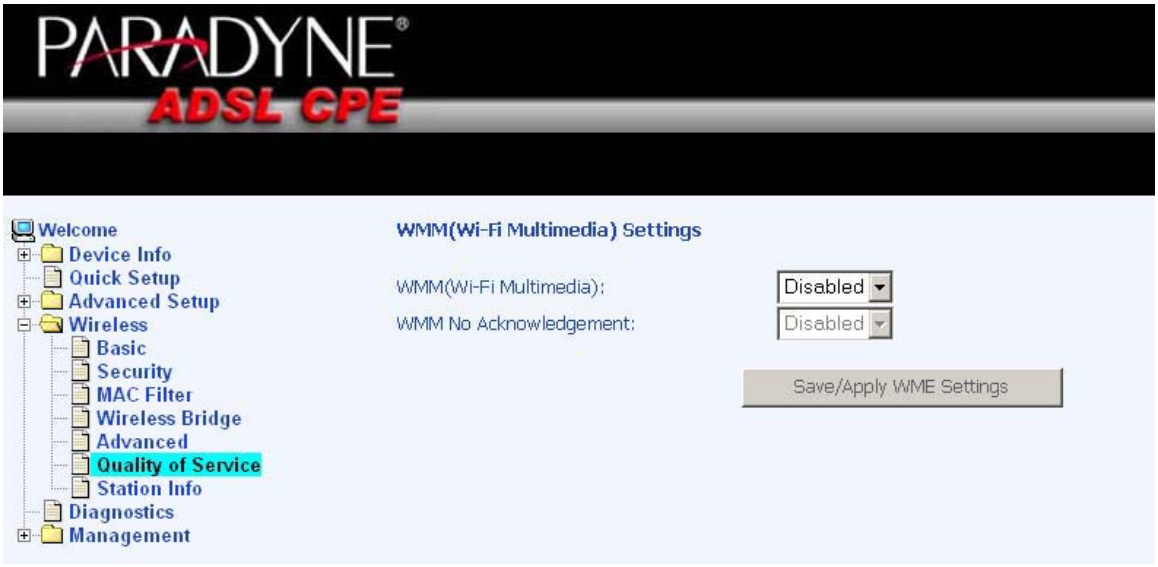
- **TPC Mitigation (db)**—default value is set at 0(off) and cannot be changed.

- **Transmit Power**—select from 20%, 40%, 60%, 80% and 100%. The default value is 100% but can be changed.

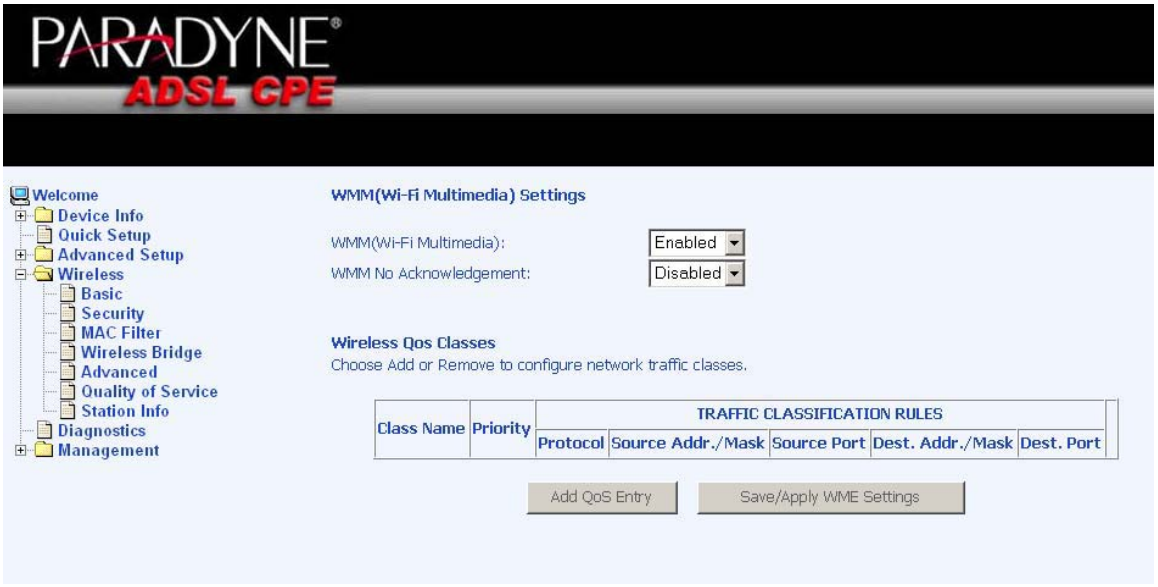

PARADYNE
ADSL CPE
Welcome
Device Info
Quick Setup
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Quality of Service
Station Info
Diagnostics
Management
Wireless -- Advanced
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply" to configure the advanced wireless options.
AP Isolation: Off
Band: 2.4GHz - 802.11g
Channel: 11 Current: 11
Rate: Auto
Multicast Rate: 54 Mbps
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
XPress™ Technology: Disabled
54g™ Mode: 54g Performance
54g Protection: Auto
Regulatory Mode: Disabled
Pre-Network Radar Check: 60
In-Network Radar Check: 60
TPC Mitigation(db): 0(off)
Transmit Power: 100%
Save/Apply

Quality of Service

- **WMM (Wi-Fi Multimedia)**—feature that improves the your experience for audio, video and voice applications over a Wi-Fi network.



If you enable WMM, then you will need to configure the network traffic classes by clicking on the **Add Qos Entry** button.



The below screen allows you to set up your wireless traffic quality of service rule. To set up your traffic rule, start by giving a name to the traffic class. Then set up the conditions that must be satisfied for the rule to take effect.

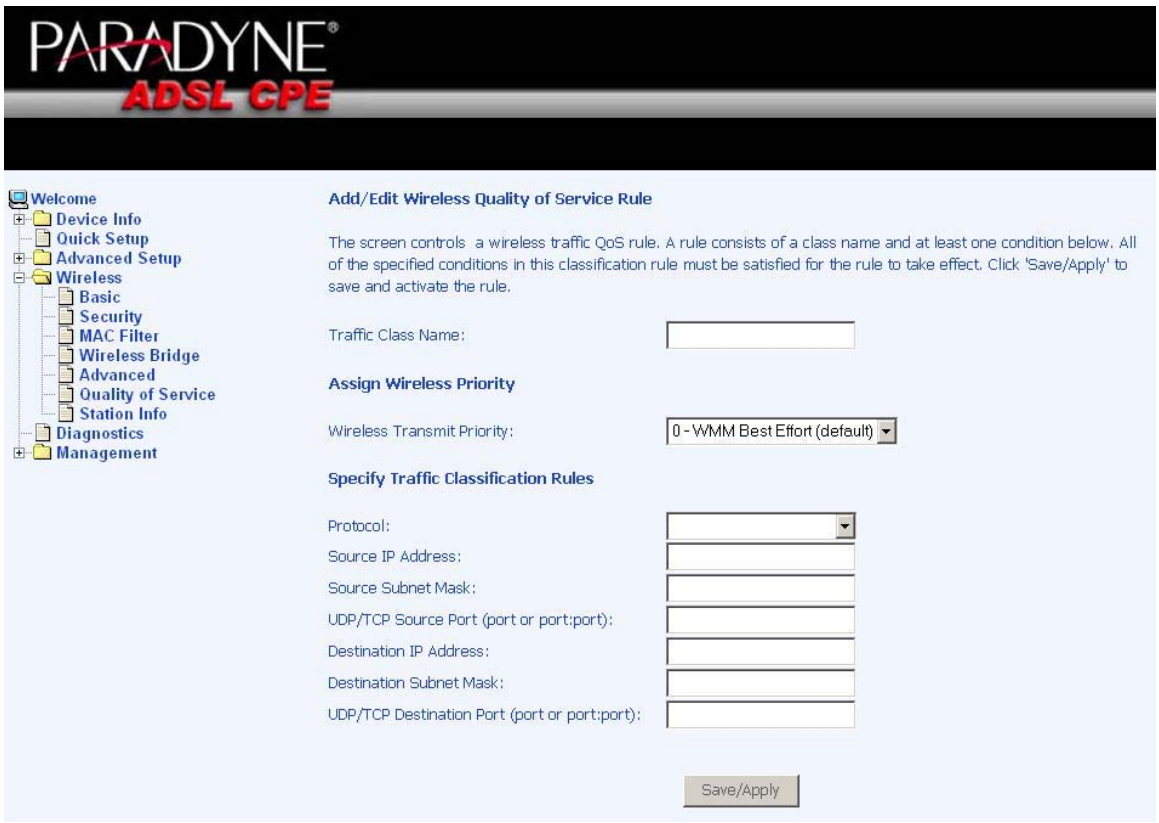
Also, assign a wireless transmit priority from the selection of 0-7. The following are the different priority levels to choose from.

- 0 – WMM Best Effort (default)
- 1 – WMM Background

- 2 – WMM Background
- 3 – WMM Best Effort
- 4 – Video Priority
- 5 - Video Priority
- 6 – Voice Priority
- 7 - Voice Priority

To specify the traffic class rules, enter the information for the following fields—

- **Protocol**—select from the below protocols—
  - TCP/UDP
  - TCP
  - UDP
  - ICMP
- **Source IP Address**
- **Source Subnet Mask**
- **UDP / TCP Source Port (port or port:port)**
- **Destination IP Address**
- **Destination Subnet Mask**
- **UDP / TCP Destination Port (port or port:port)**



Station Info

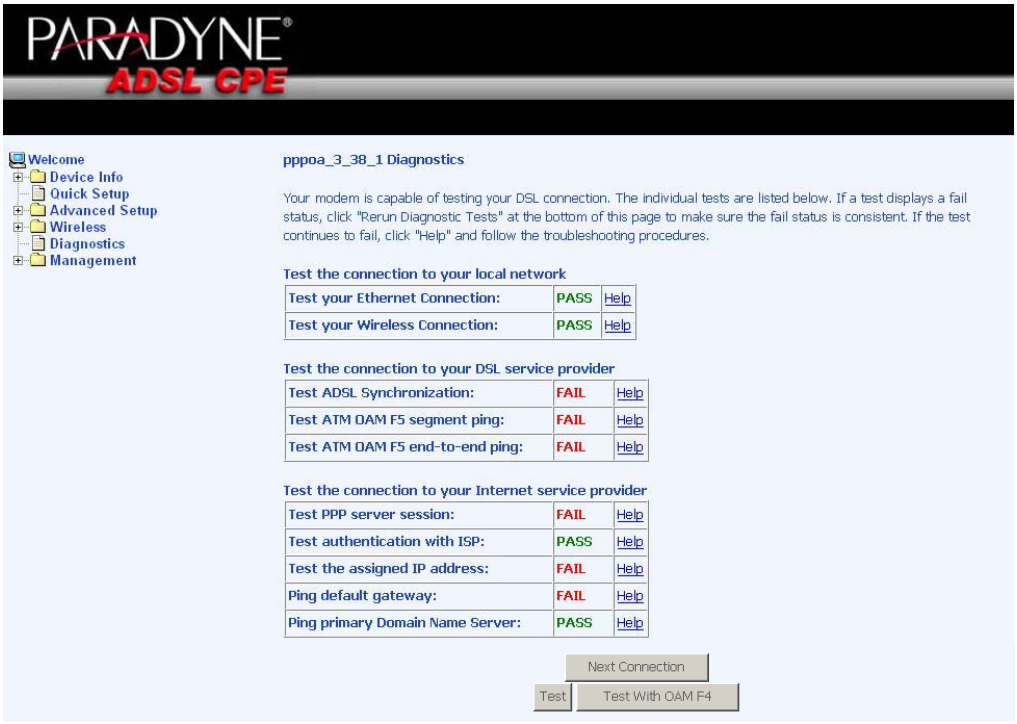
The **Station Info** page shows stations that have been authorized access to the router through its wireless function.

Diagnostics

The diagnostics screen allows you to run diagnostic tests to check your DSL connection. The outcome will show test results of three connections—

- Connection to your local network
- Connection to your DSL service provider
- Connection to your Internet service provider

There are two buttons at the bottom of the page—**Test** and **Test with OAM F4**—which allow you to retest if necessary.



Management

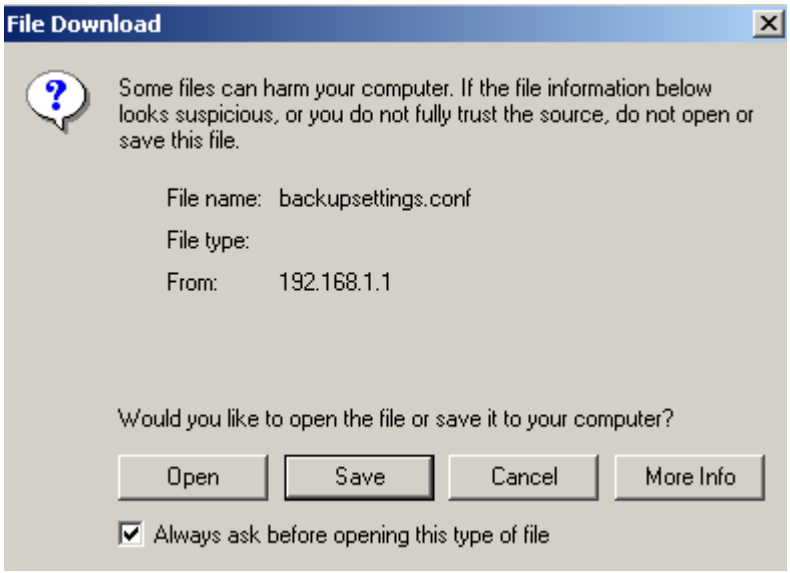
The Management section gives you access to certain setups for the purpose of maintaining the system, including backing up the configurations, viewing system log, maintaining access control, updating software, etc.

Settings

Backup Settings

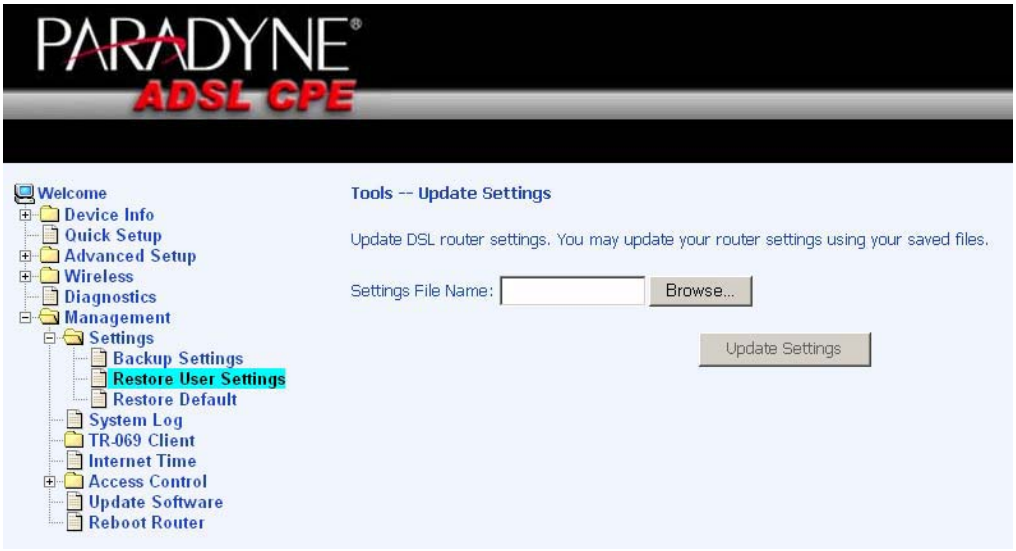
To save a copy of the configurations that you have made on your router, click on the **Backup Settings** button.

The below pop-up screen will appear with a prompt to open or save the file to your computer.



Restore User Settings

To load a previously saved configuration file onto your router, click **Browse** to find the file on your computer and click on **Update Settings**.

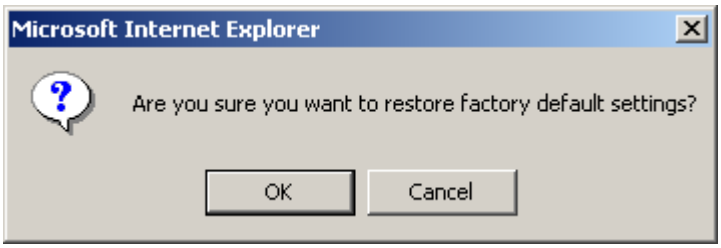


The router will restore settings and reboot to activate the restored settings.

Restore Default

Restore Default will delete all current settings and restore the router to factory default settings.

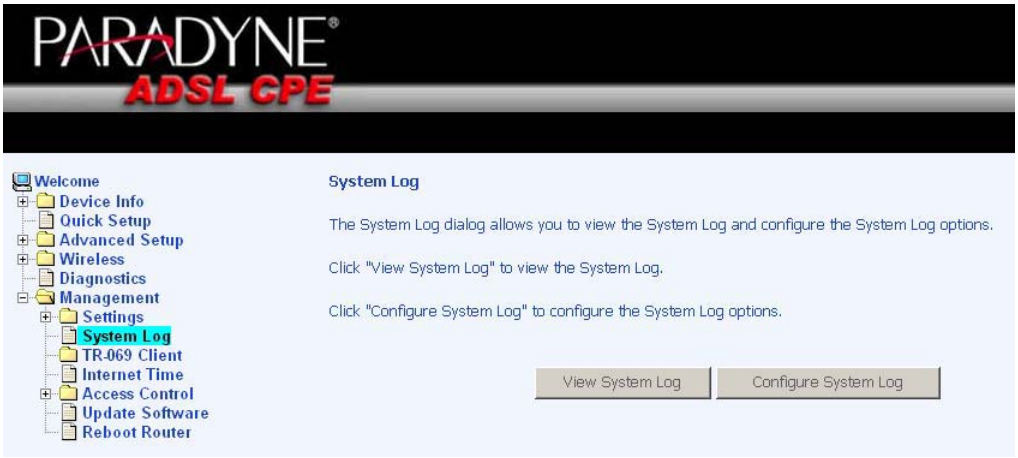
Click on **OK** when the pop-up window appears confirming that you want to restore factory default settings to your router.



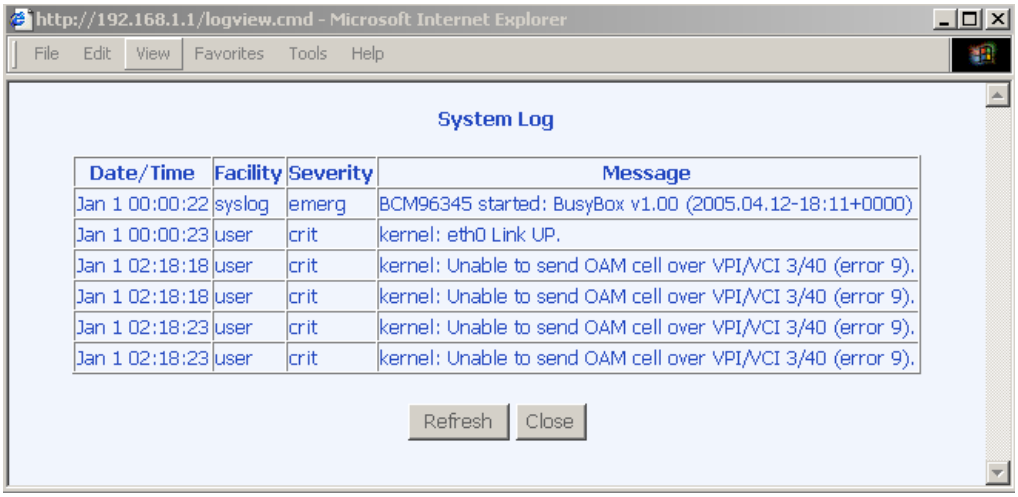
The router will restore the default settings and reboot.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options. To view the System Log click on the **View System Log** button to check the log file.



Below is a view of the **System Log**.



Configure System Log

If the log is enabled, the system will log selected events including *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Informational*, and *Debugging*. All events above or equal to the selected log level will be logged and displayed.

If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of a remote system log server. If the selected mode is "Local" or "Both", events will be recorded in the local memory. Select the desired values and click on the "**Save/Apply**" button to configure the system log options.

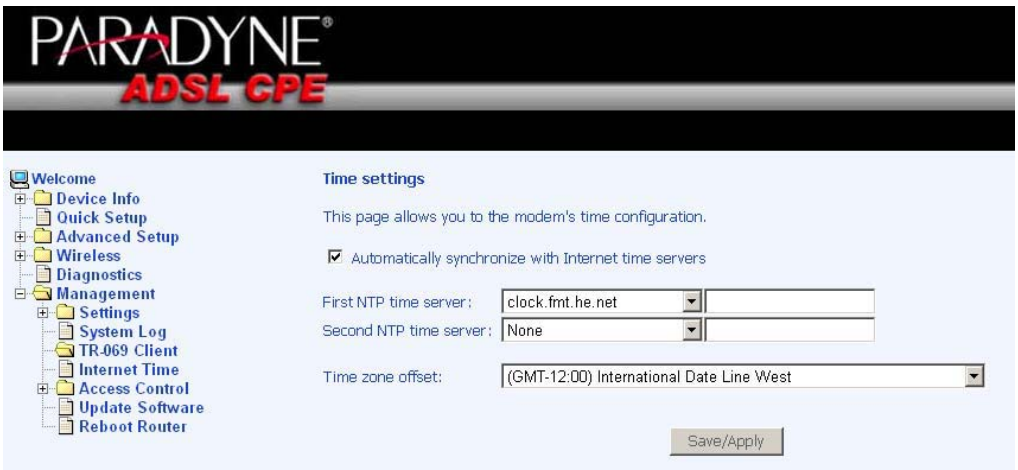
TR-069 Client

The router includes a TR-069 client which is a WAN management protocol. All the values are already filled in. If you wish to enable this protocol, then select *enable*. You must click on the **Save/Reboot** button for the change to take place.

Internet Time

The Time Settings page allows you to automatically synchronize your time with a timeserver on the Internet.

If you choose to automatically synchronize with Internet time servers, then click on the box and the below fields appear. Select from the list of NTP (Network Time Protocol) time servers. Then select the time zone that you are in and click on **Save / Apply** to save and complete your time settings.

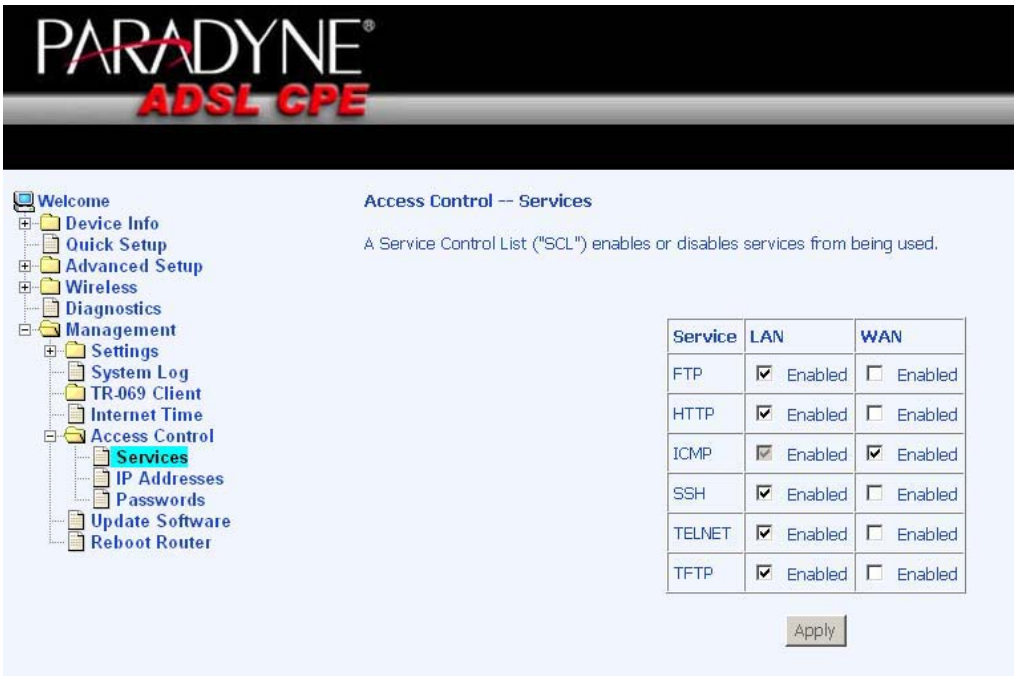


Access Control

You can enable or disable some services of your router by LAN or WAN. If no WAN connection is defined, only the LAN side can be configured.

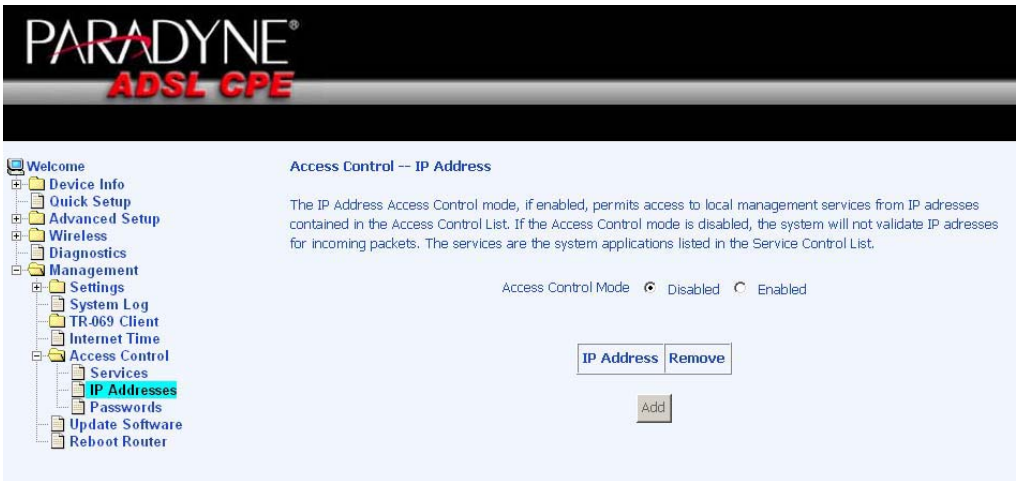
Services

Services that can be enabled / disabled on the LAN / WAN are FTP, HTTP, ICMP, SNMP, SSH, Telnet, and TFTP.

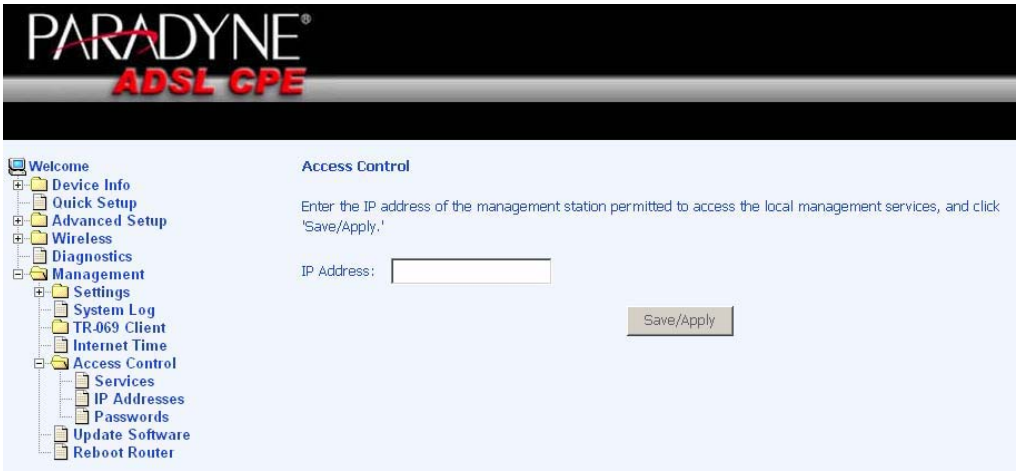


IP Addresses

Web access to the router can be limited when Access Control Mode is enabled. Add the IP address to the IP address list by clicking on the **Add** button, then select "**Enabled**" to enable Access Control Mode.

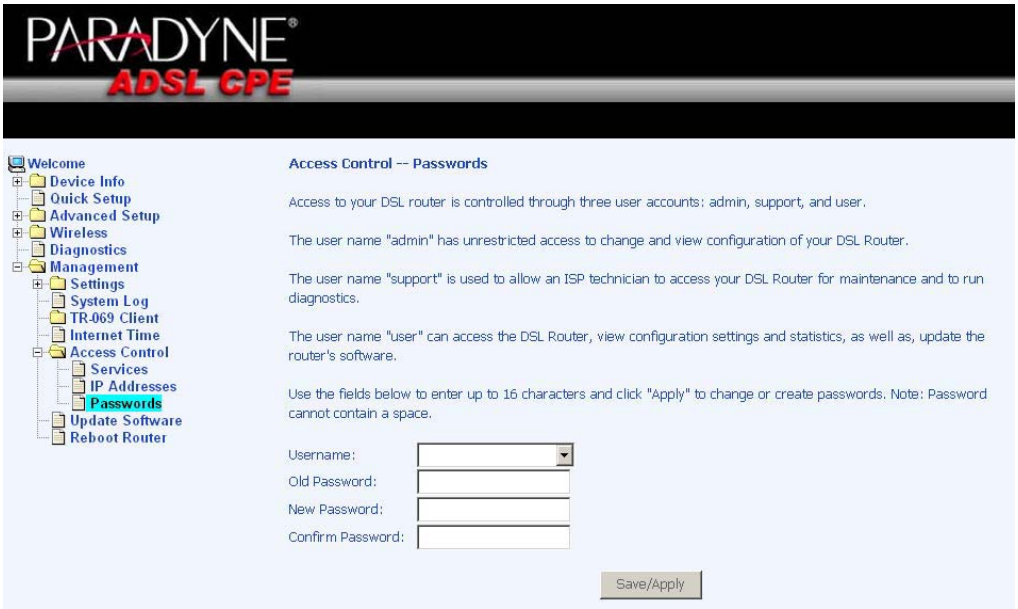


To assign the IP address of the management station that is permitted to access the local management services, enter the IP address in the box and click on the **Save / Apply** button.



Passwords

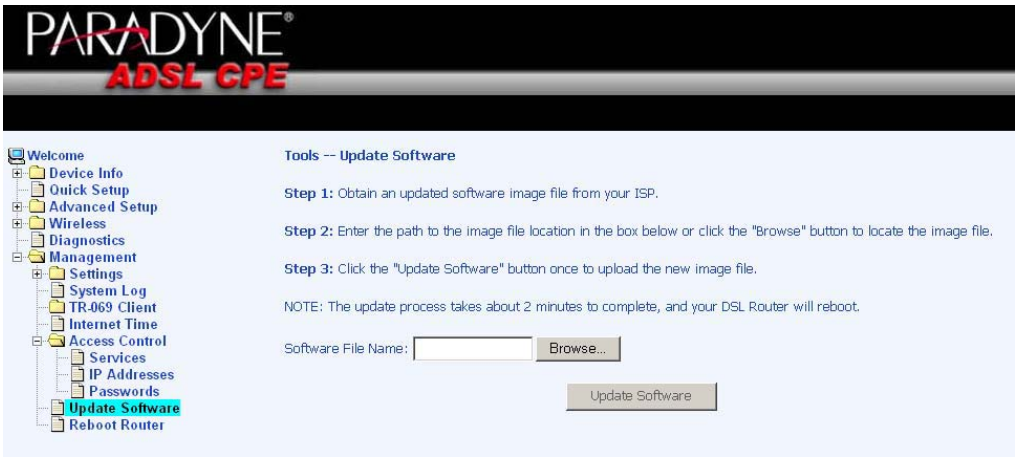
Access the **Passwords** screen under the **Access Control** section to change a password. Select an account and enter the current password and the new password and then click on the **Save / Apply** button.



Update Software

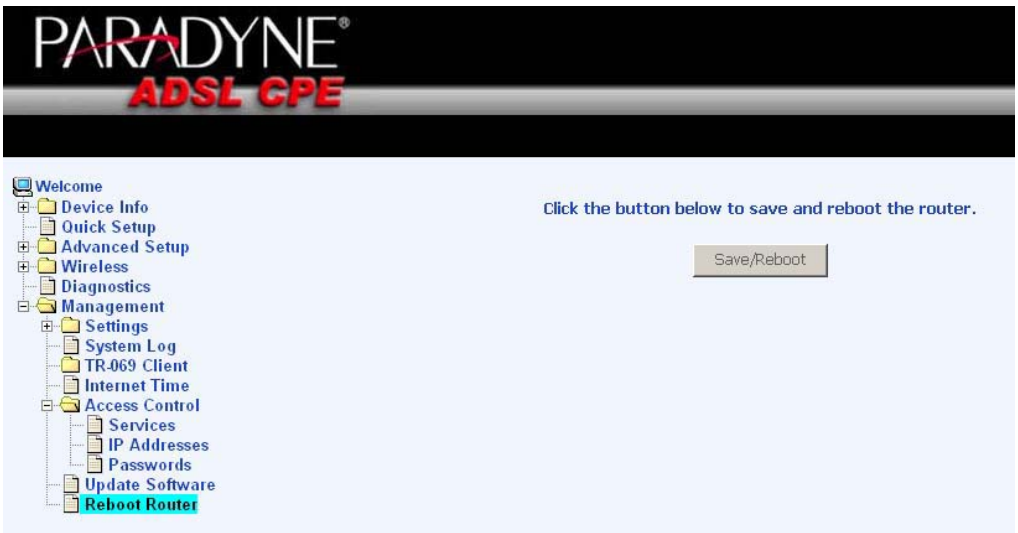
If your ISP releases new software for this router, follow these steps to perform an upgrade.

1. Obtain an updated software image file from your ISP.
2. Enter the path to the image file location or click on the **Browse** button to locate the image file.
3. Click the **Update Software** button once to upload the new image file.



Reboot Router

To save all the configurations you have made, click on the **Save/Reboot** button and the router will reboot itself using the new configurations.



This is the end of the configurations. You have successfully configured your router.

FCC Warning 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 may cause undesired operation.

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter

Safety Information

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.