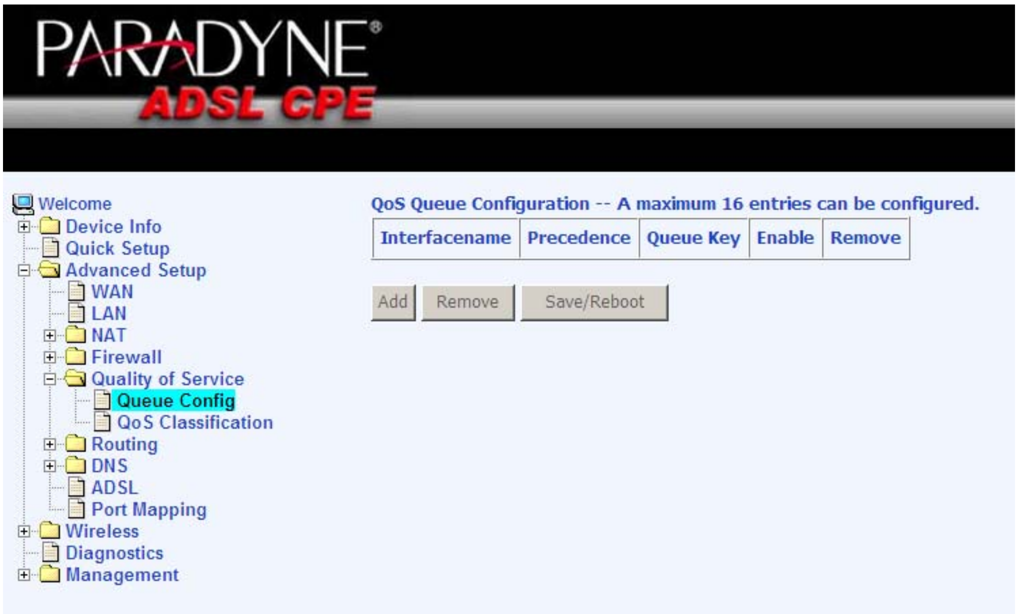
Queue Config

To add or remove a QoS queue, click on the corresponding **Add** or **Remove** button. Click on **Save / Reboot** after removing a selection.

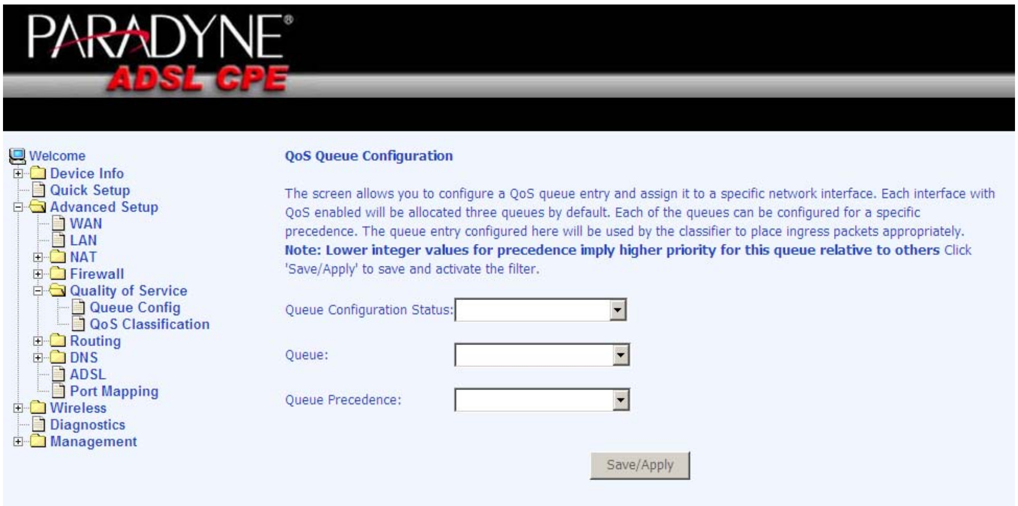


QoS Queue Configuration -- A maximum 16 entries can be configured.

Interfacename	Precedence	Queue Key	Enable	Remove

The QoS queue configured here will apply to incoming IP packets. Items that need to be configured include the following—

- *Queue configuration status*— select disable or enable
- *Queue*— select Null or leave blank
- *Queue precedence*— select integers 1, 2, or 3



QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Save/Apply' to save and activate the filter.

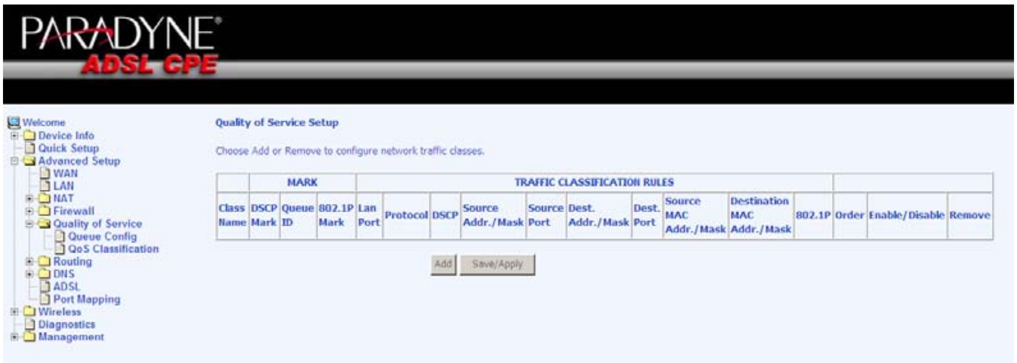
Queue Configuration Status:

Queue:

Queue Precedence:

QoS Classification

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.

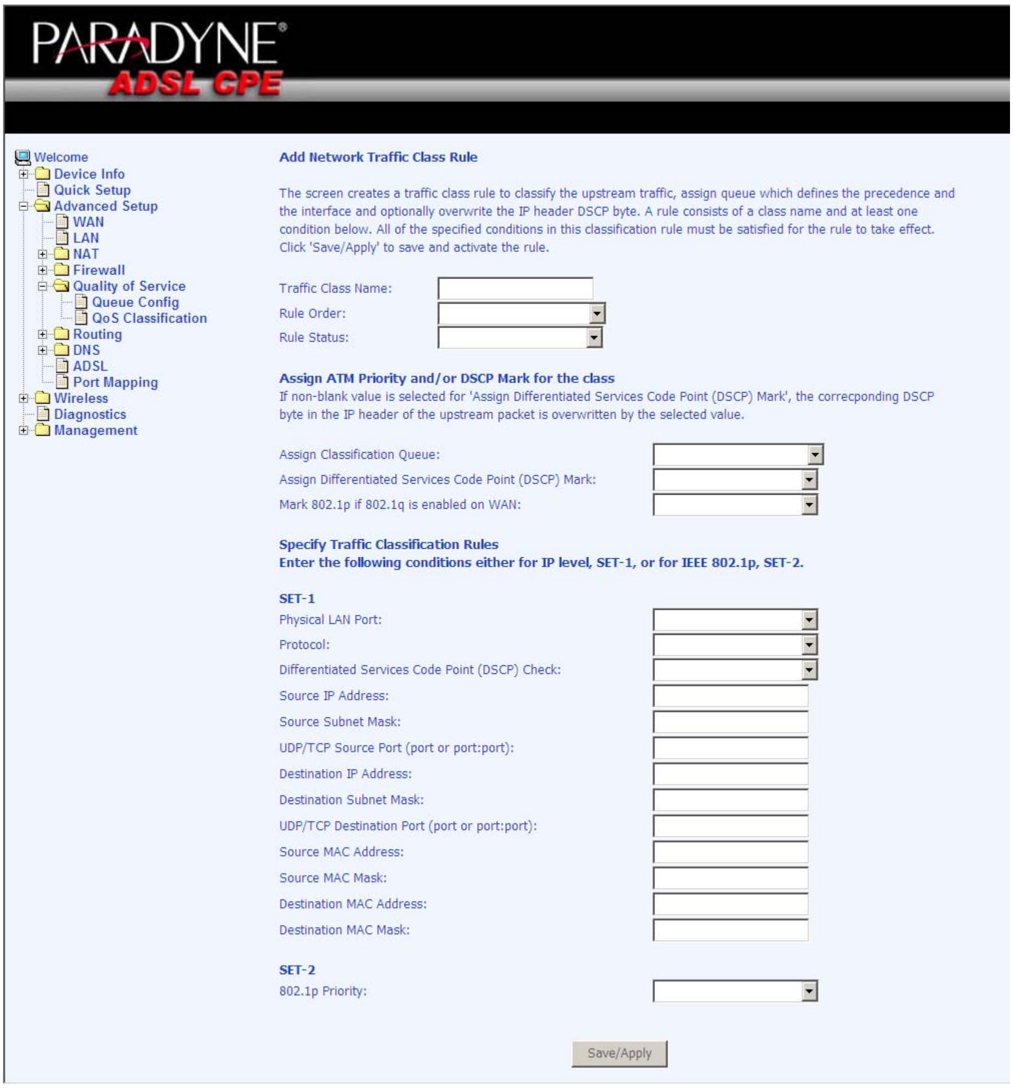


Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

	MARK			TRAFFIC CLASSIFICATION RULES												
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Order	Enable/Disable	Remove

The following screen allows you to add a network traffic class rule.



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Assign ATM Priority and/or DSCP Mark for the class

If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled on WAN:

Specify Traffic Classification Rules

Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

SET-1

Physical LAN Port:

Protocol:

Differentiated Services Code Point (DSCP) Check:

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):

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

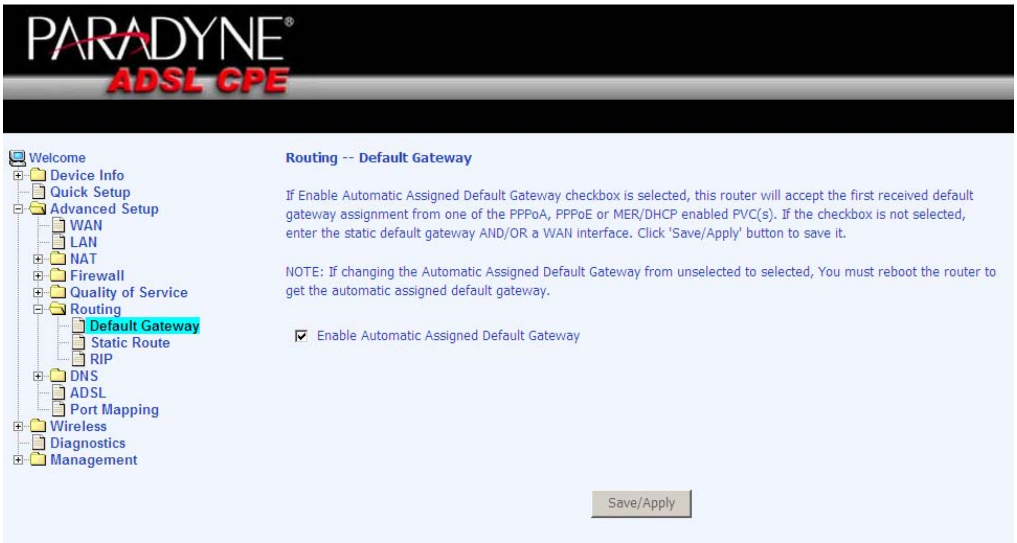
SET-2

802.1p Priority:

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.



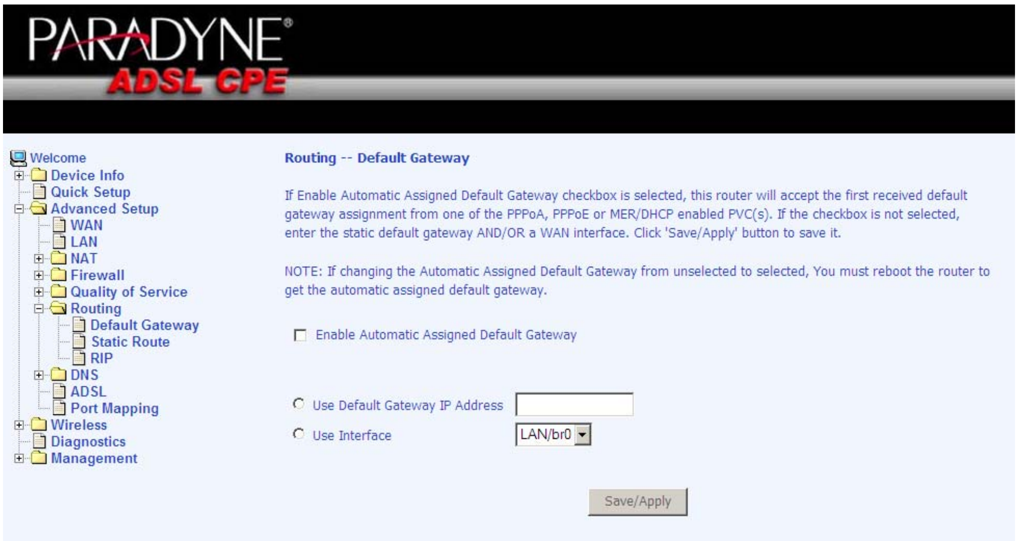
Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☑ Enable Automatic Assigned Default Gateway

If automatic assigned default gateway is not selected, then enter the preferred default gateway IP address or select the interface.



Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

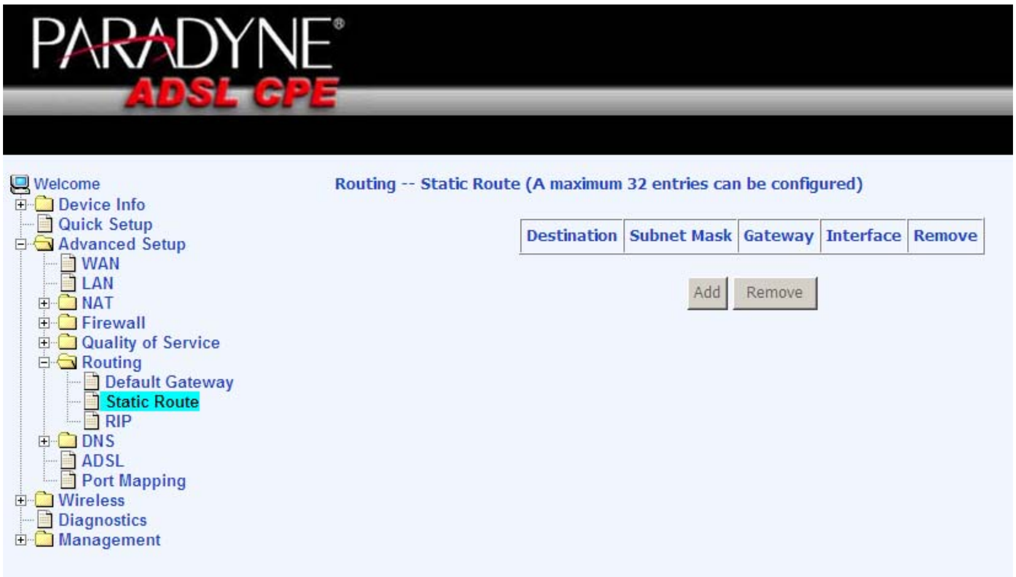
□ Enable Automatic Assigned Default Gateway

○ Use Default Gateway IP Address

○ Use Interface LAN/br0

Static Route

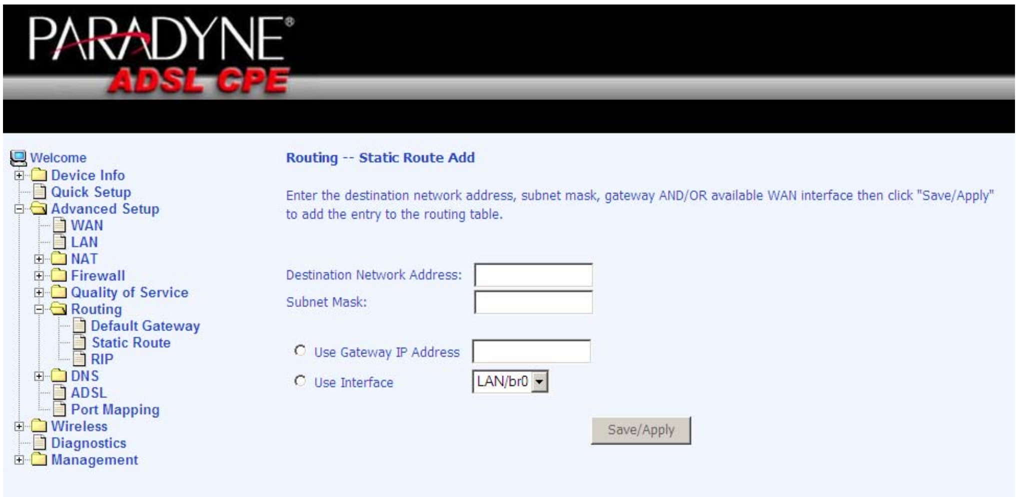
Use the Routing – Static Route screen to add a static route to the routing table.



Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove

Enter the route information and click on **Save/Apply**. No reboot is required.



Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:

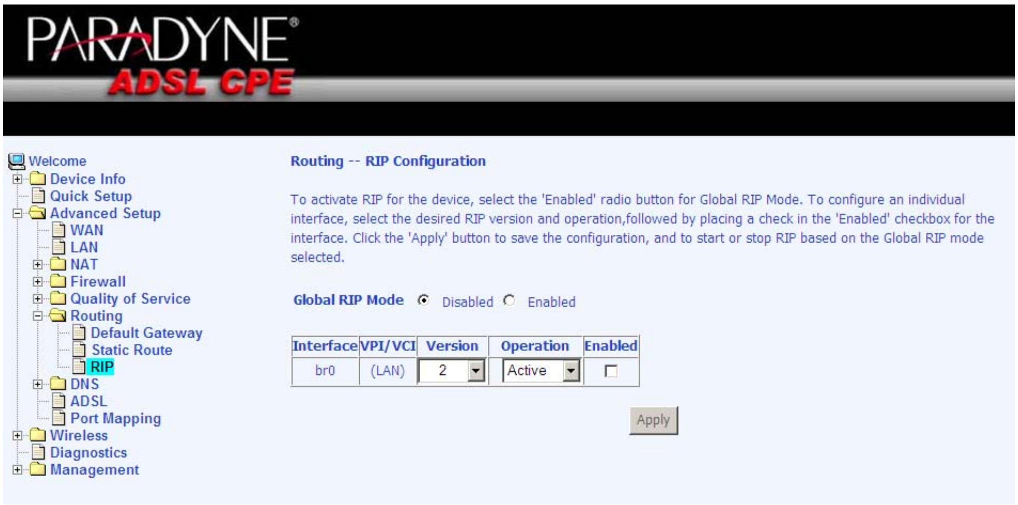
Subnet Mask:

○ Use Gateway IP Address

○ Use Interface LAN/br0

RIP

If RIP is enabled, the router operation can be configured as active or passive.



Routing -- RIP Configuration

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation,followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

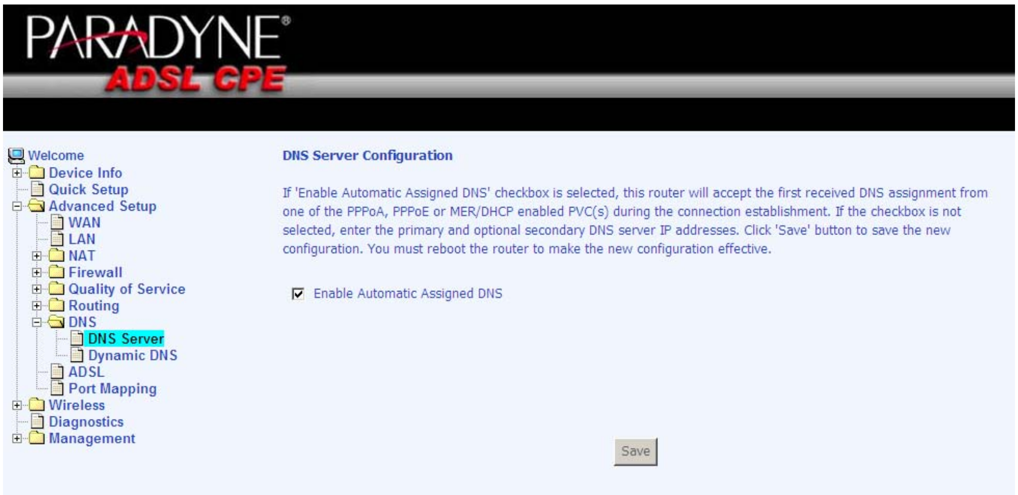
Global RIP Mode ● Disabled ○ Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	□

DNS

DNS Server

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

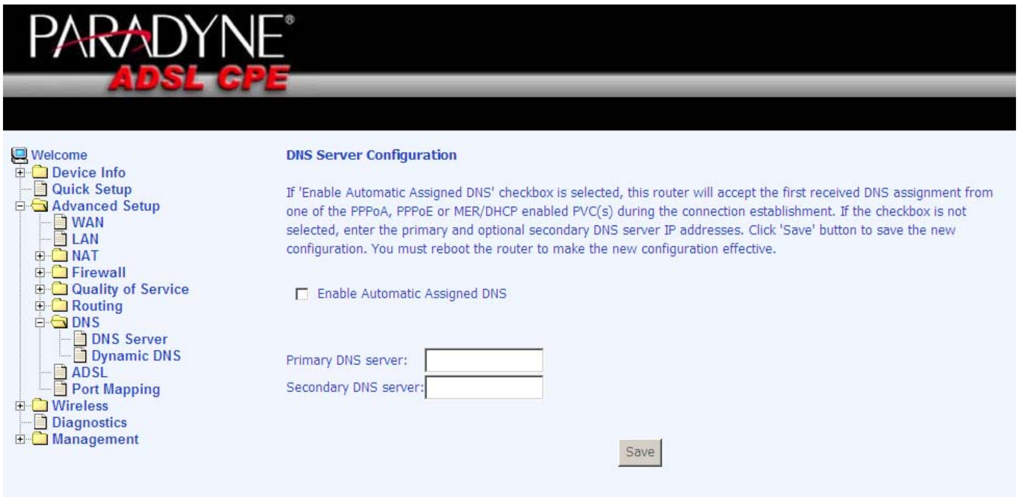


DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

☑ Enable Automatic Assigned DNS

If the automatic assigned DNS checkbox is not selected, then enter the primary and secondary DNS Server IP addresses as illustrated below.



DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

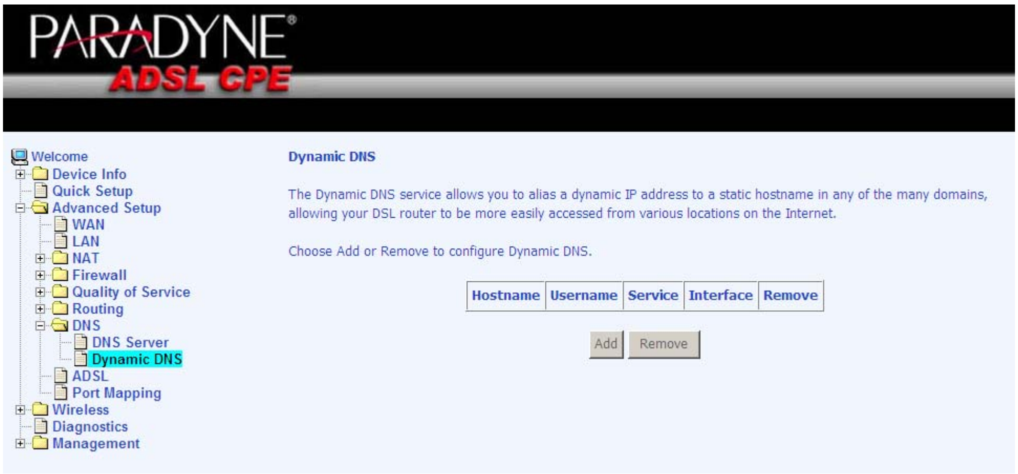
□ Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

Dynamic DNS

Dynamic DNS (D-DNS) allows you to have your own permanent domain name linked to your dynamic IP address. To configure a dynamic DNS, click on **Add**. If you have already created a dynamic DNS that you want to delete, click on **Remove**.



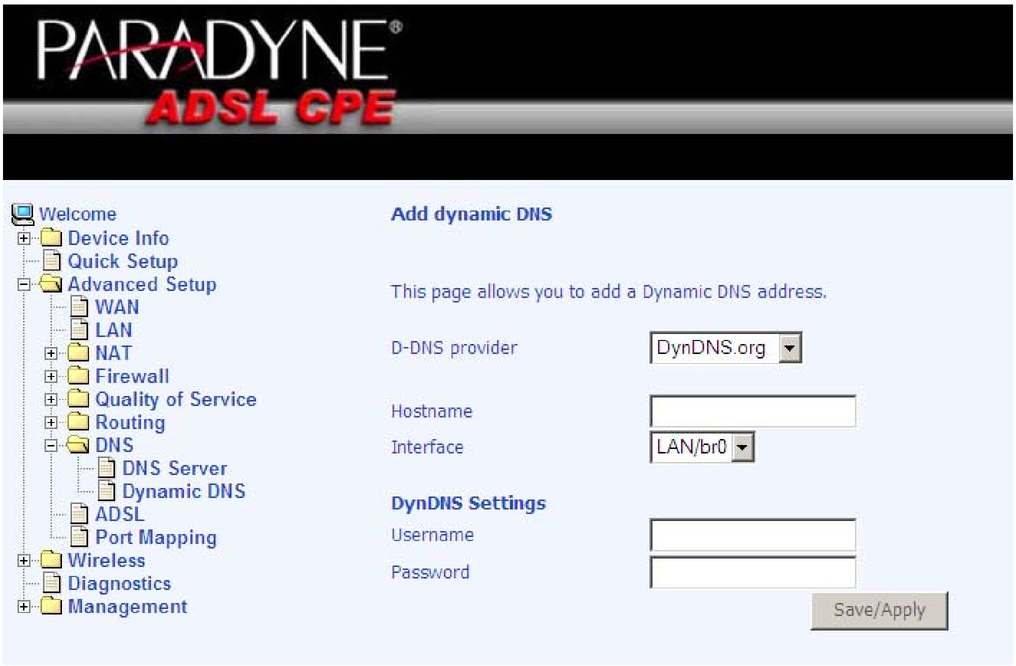
Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

The below screen allows you to set up the Dynamic DNS provider. Note that you will have to first register at the Dynamic DNS site that you wish to use. Select from either DynDNS.org or TZO. Then enter the hostname and the interface that you want to establish the D-DNS address to. Enter the username / password for the D-DNS account that you have signed up for and then click on **Save / Apply**.



Add dynamic DNS

This page allows you to add a Dynamic DNS address.

D-DNS provider: DynDNS.org

Hostname:

Interface: LAN/br0

DynDNS Settings

Username:

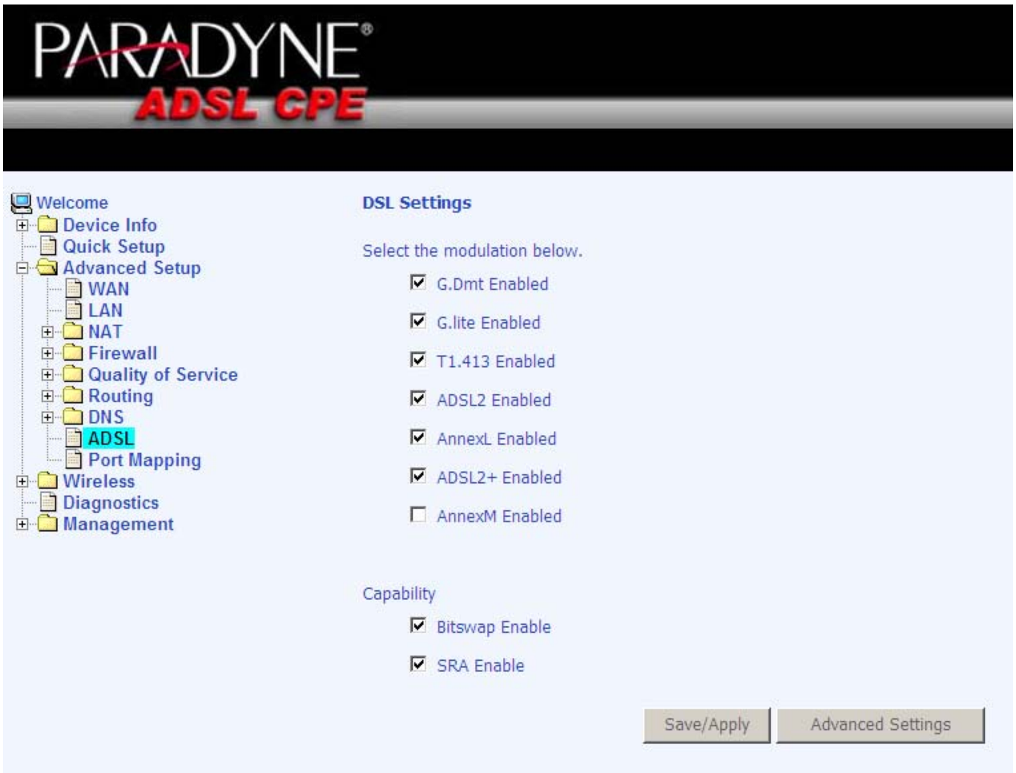
Password:

ADSL

There are three major items in the ADSL settings:

Modulation Methods
Six modulation methods for different linking speed are supported by the 6211 ADSL router: G.Dmt Enabled, G.lite Enabled, T1.413 Enabled, ADSL Enabled, Annex L Enabled, and ADSL2+ Enabled. Set this value only as directed by your ISP.

Capability
Do not change these settings unless directed by your ISP.



DSL Settings

Select the modulation below.

☑ G.Dmt Enabled

☑ G.lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ AnnexL Enabled

☑ ADSL2+ Enabled

☐ AnnexM Enabled

Capability

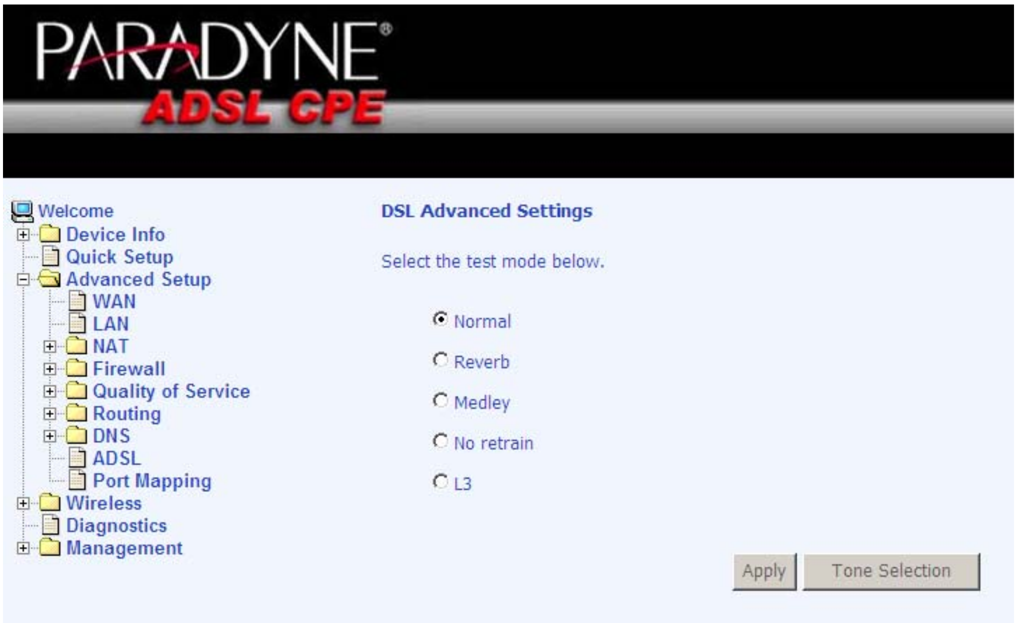
☑ Bitswap Enable

☑ SRA Enable

DSL Advanced Settings

The test mode can be selected from the DSL Advanced Settings page. Test modes are as follows—

- Normal
- Reverb
- Medley
- No retrain
- L3



DSL Advanced Settings

Select the test mode below.

● Normal

○ Reverb

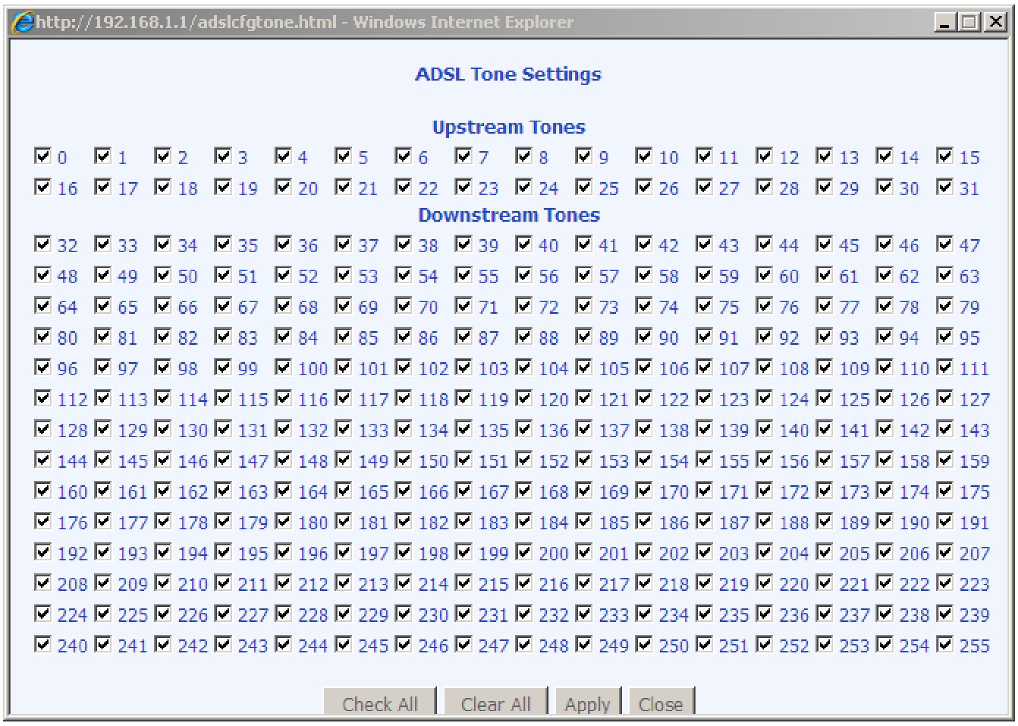
○ Medley

○ No retrain

○ L3

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 instructed by your ISP.


http://192.168.1.1/adslcfgtone.html - Windows Internet Explorer
Check All
Clear All
Apply
Close

ADSL Tone Settings

Upstream Tones

☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15
☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31

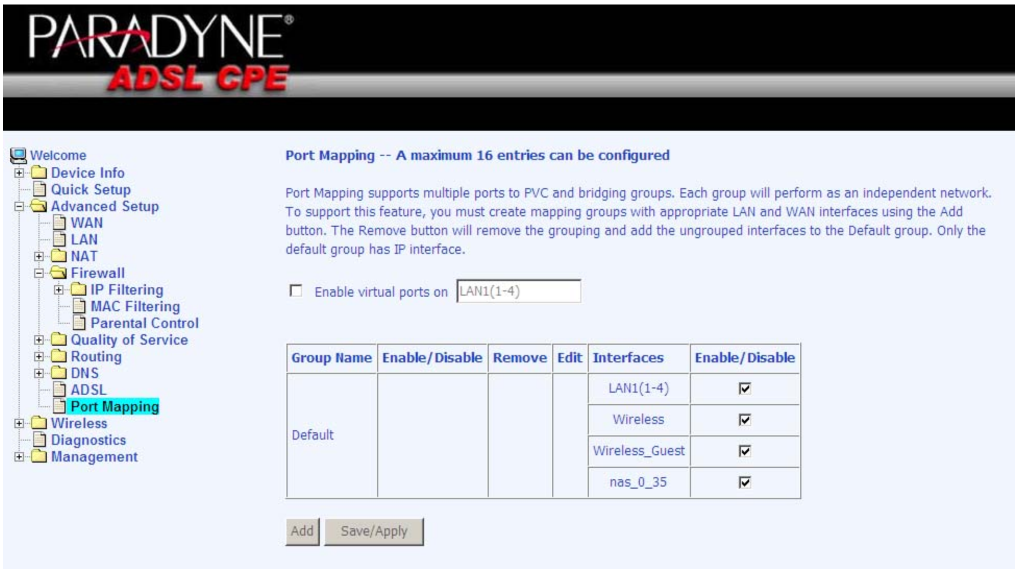
Downstream Tones

☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45 ☑ 46 ☑ 47
☑ 48 ☑ 49 ☑ 50 ☑ 51 ☑ 52 ☑ 53 ☑ 54 ☑ 55 ☑ 56 ☑ 57 ☑ 58 ☑ 59 ☑ 60 ☑ 61 ☑ 62 ☑ 63
☑ 64 ☑ 65 ☑ 66 ☑ 67 ☑ 68 ☑ 69 ☑ 70 ☑ 71 ☑ 72 ☑ 73 ☑ 74 ☑ 75 ☑ 76 ☑ 77 ☑ 78 ☑ 79
☑ 80 ☑ 81 ☑ 82 ☑ 83 ☑ 84 ☑ 85 ☑ 86 ☑ 87 ☑ 88 ☑ 89 ☑ 90 ☑ 91 ☑ 92 ☑ 93 ☑ 94 ☑ 95
☑ 96 ☑ 97 ☑ 98 ☑ 99 ☑ 100 ☑ 101 ☑ 102 ☑ 103 ☑ 104 ☑ 105 ☑ 106 ☑ 107 ☑ 108 ☑ 109 ☑ 110 ☑ 111
☑ 112 ☑ 113 ☑ 114 ☑ 115 ☑ 116 ☑ 117 ☑ 118 ☑ 119 ☑ 120 ☑ 121 ☑ 122 ☑ 123 ☑ 124 ☑ 125 ☑ 126 ☑ 127
☑ 128 ☑ 129 ☑ 130 ☑ 131 ☑ 132 ☑ 133 ☑ 134 ☑ 135 ☑ 136 ☑ 137 ☑ 138 ☑ 139 ☑ 140 ☑ 141 ☑ 142 ☑ 143
☑ 144 ☑ 145 ☑ 146 ☑ 147 ☑ 148 ☑ 149 ☑ 150 ☑ 151 ☑ 152 ☑ 153 ☑ 154 ☑ 155 ☑ 156 ☑ 157 ☑ 158 ☑ 159
☑ 160 ☑ 161 ☑ 162 ☑ 163 ☑ 164 ☑ 165 ☑ 166 ☑ 167 ☑ 168 ☑ 169 ☑ 170 ☑ 171 ☑ 172 ☑ 173 ☑ 174 ☑ 175
☑ 176 ☑ 177 ☑ 178 ☑ 179 ☑ 180 ☑ 181 ☑ 182 ☑ 183 ☑ 184 ☑ 185 ☑ 186 ☑ 187 ☑ 188 ☑ 189 ☑ 190 ☑ 191
☑ 192 ☑ 193 ☑ 194 ☑ 195 ☑ 196 ☑ 197 ☑ 198 ☑ 199 ☑ 200 ☑ 201 ☑ 202 ☑ 203 ☑ 204 ☑ 205 ☑ 206 ☑ 207
☑ 208 ☑ 209 ☑ 210 ☑ 211 ☑ 212 ☑ 213 ☑ 214 ☑ 215 ☑ 216 ☑ 217 ☑ 218 ☑ 219 ☑ 220 ☑ 221 ☑ 222 ☑ 223
☑ 224 ☑ 225 ☑ 226 ☑ 227 ☑ 228 ☑ 229 ☑ 230 ☑ 231 ☑ 232 ☑ 233 ☑ 234 ☑ 235 ☑ 236 ☑ 237 ☑ 238 ☑ 239
☑ 240 ☑ 241 ☑ 242 ☑ 243 ☑ 244 ☑ 245 ☑ 246 ☑ 247 ☑ 248 ☑ 249 ☑ 250 ☑ 251 ☑ 252 ☑ 253 ☑ 254 ☑ 255

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.



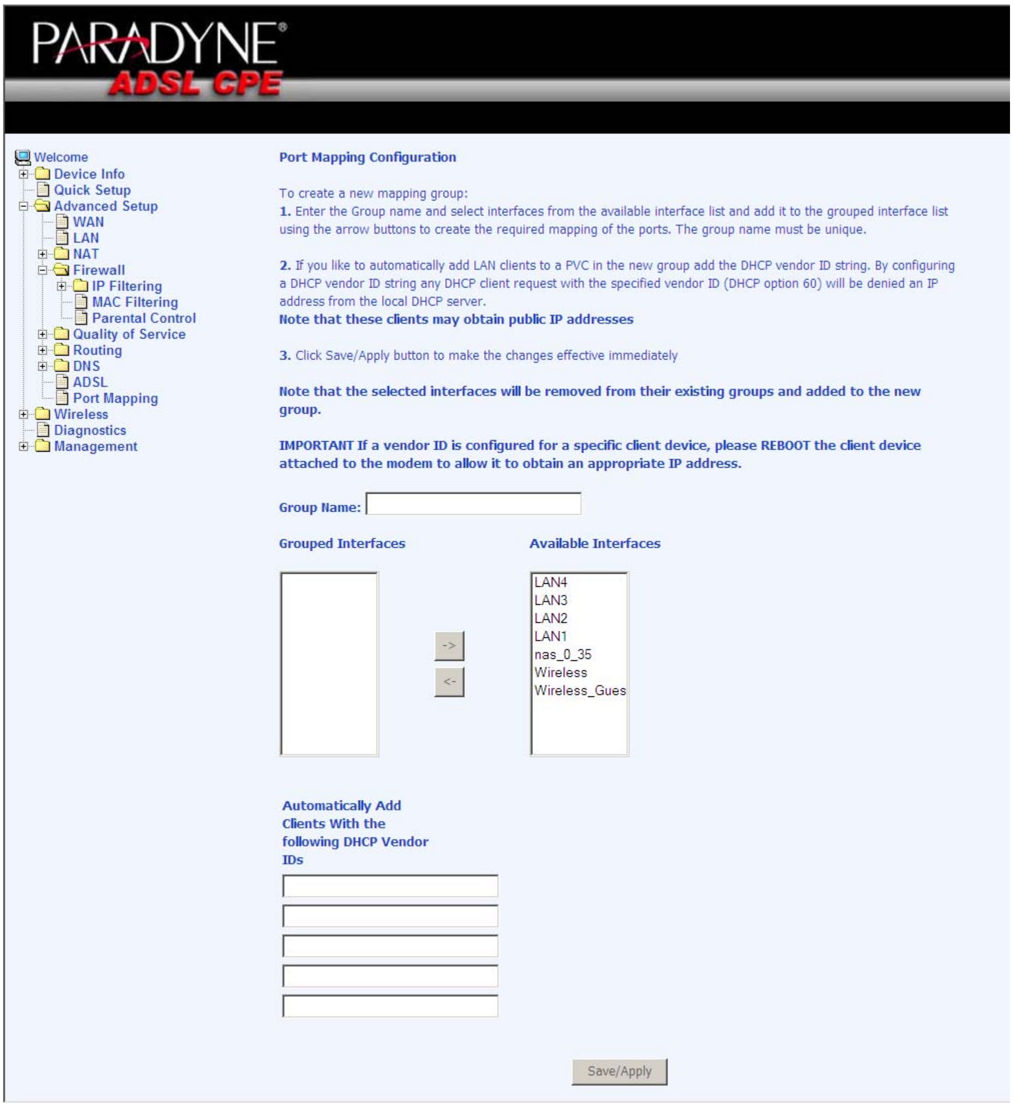
Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

☐ Enable virtual ports on LAN1(1-4)

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				LAN1(1-4)	☑
				Wireless	☑
				Wireless_Guest	☑
				nas_0_35	☑

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



Port Mapping Configuration

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses

3. Click Save/Apply button to make the changes effective immediately

Note that the selected interfaces will be removed from their existing groups and added to the new group.

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces

Available Interfaces

LAN4
LAN3
LAN2
LAN1
nas_0_35
Wireless
Wireless_Gues

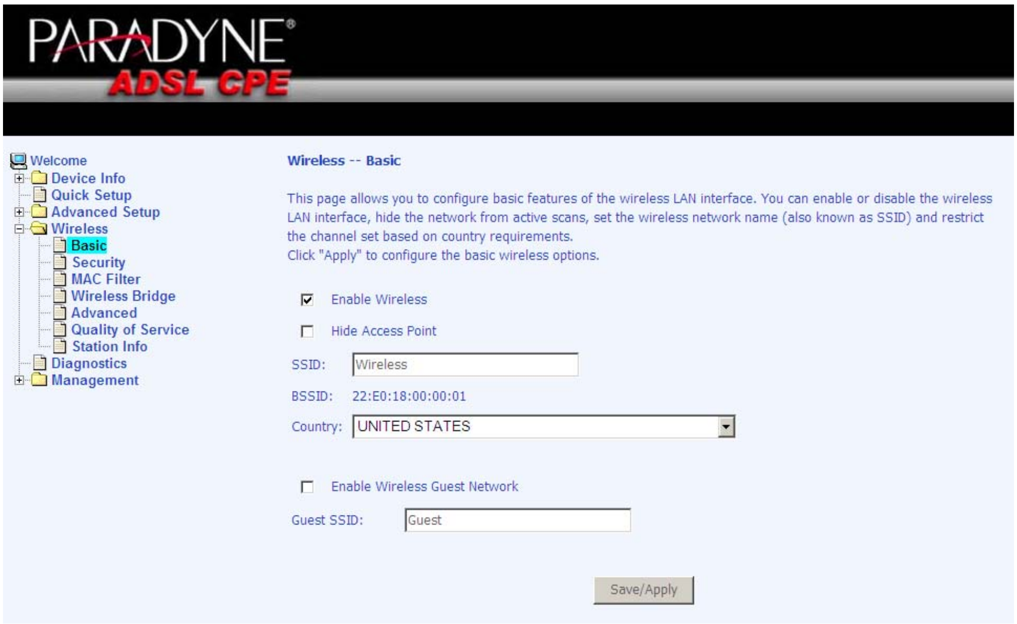
Automatically Add Clients With the following DHCP Vendor IDs

Wireless

This section allows you to configure wireless settings on your router.

Basic

The below Wireless—Basic screen lets you enable or disable wireless. The default setting for wireless is enabled. You can also hide the access point so others cannot see your ID on the network.



Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

SSID: Wireless

BSSID: 22:E0:18:00:00:01

Country: UNITED STATES

□ Enable Wireless Guest Network

Guest SSID: Guest

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.

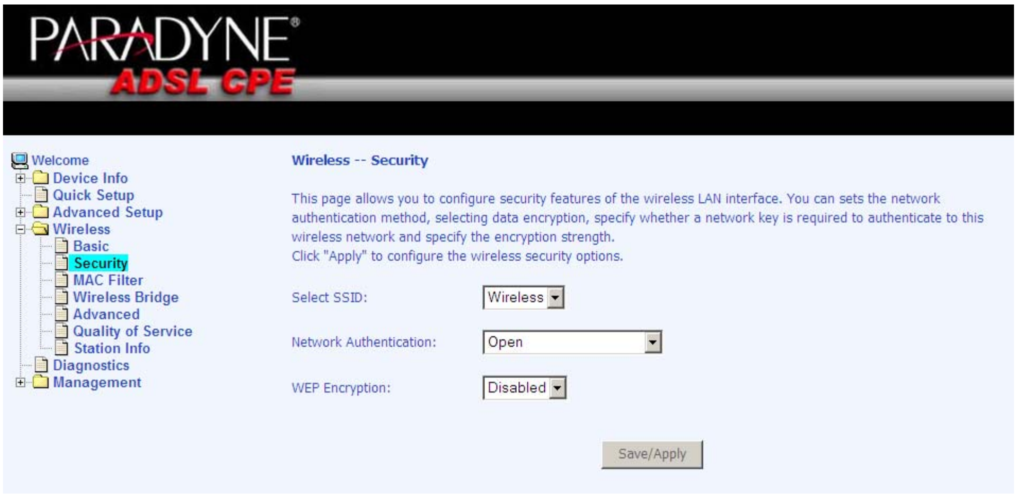
- **WPA—(Wi-Fi Protected Access)**— usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses128-bit dynamic session keys (per user, per session, and per packet keys).
- **WPA-PSK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



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

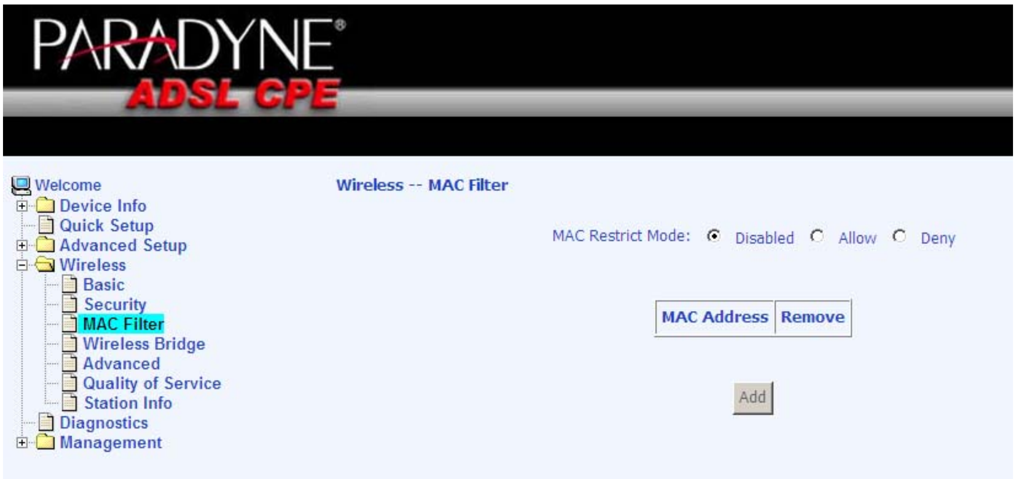
Select SSID: Wireless

Network Authentication: Open

WEP Encryption: Disabled

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.

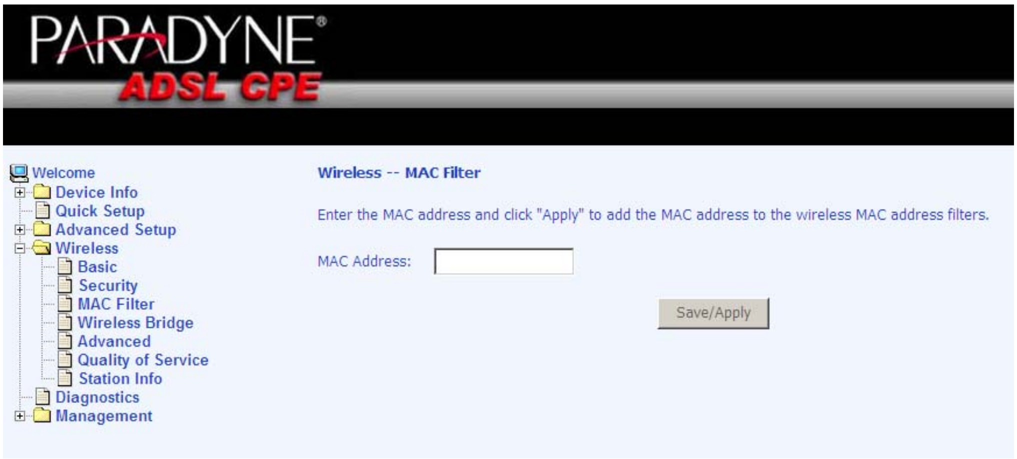


Wireless -- MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

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



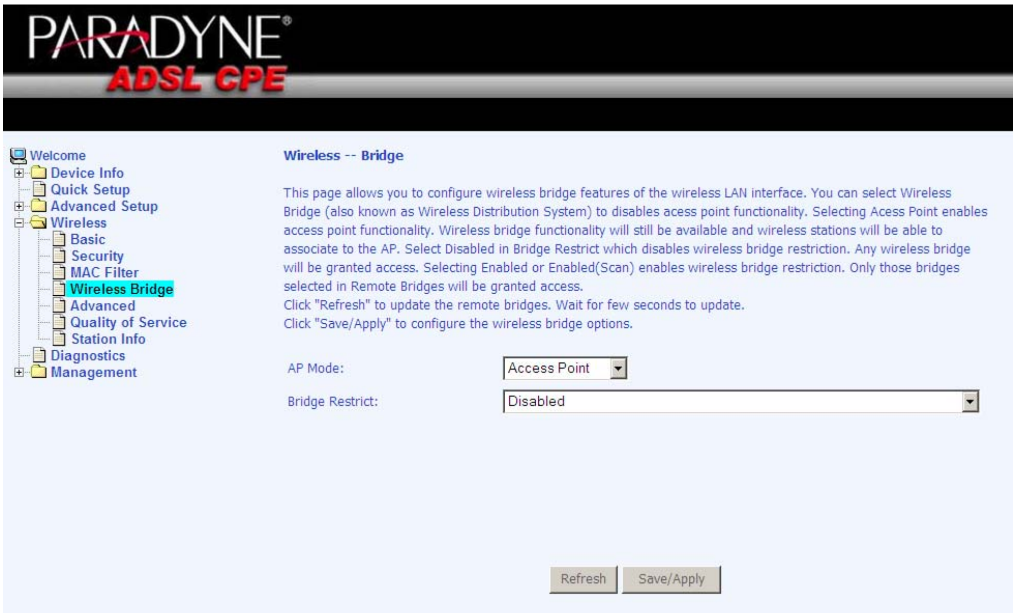
Wireless -- MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:

Wireless Bridge

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



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables acess point functionality. Selecting Acess Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.

AP Mode: Access Point

Bridge Restrict: Disabled

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.

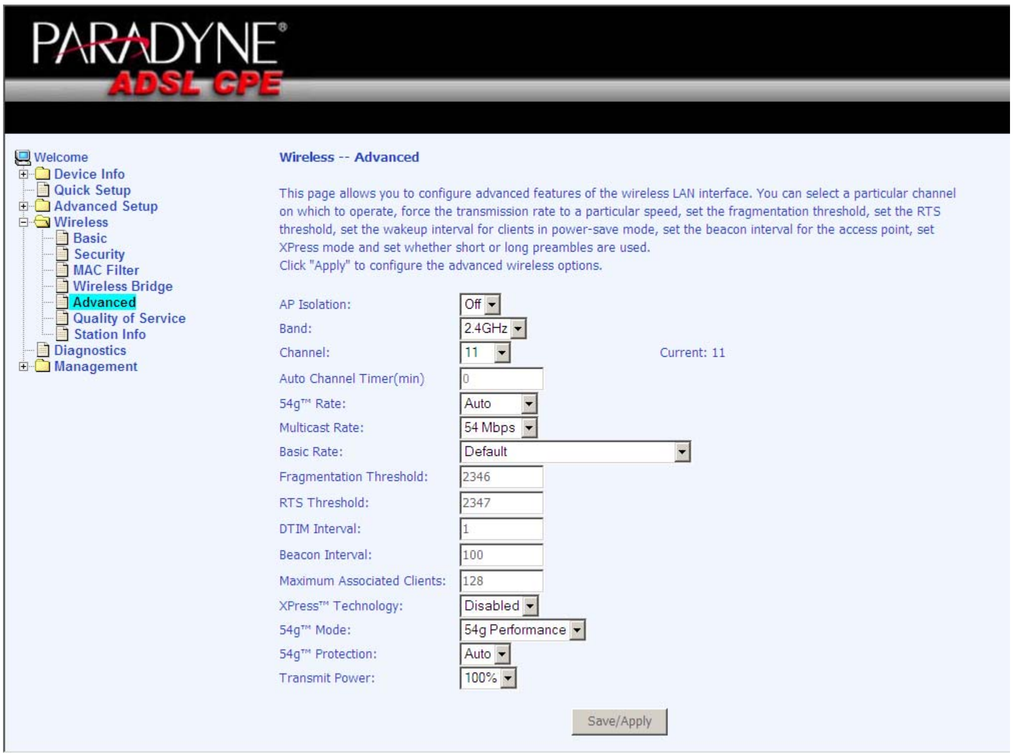
- **Beacon Interval**—a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (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.

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



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.

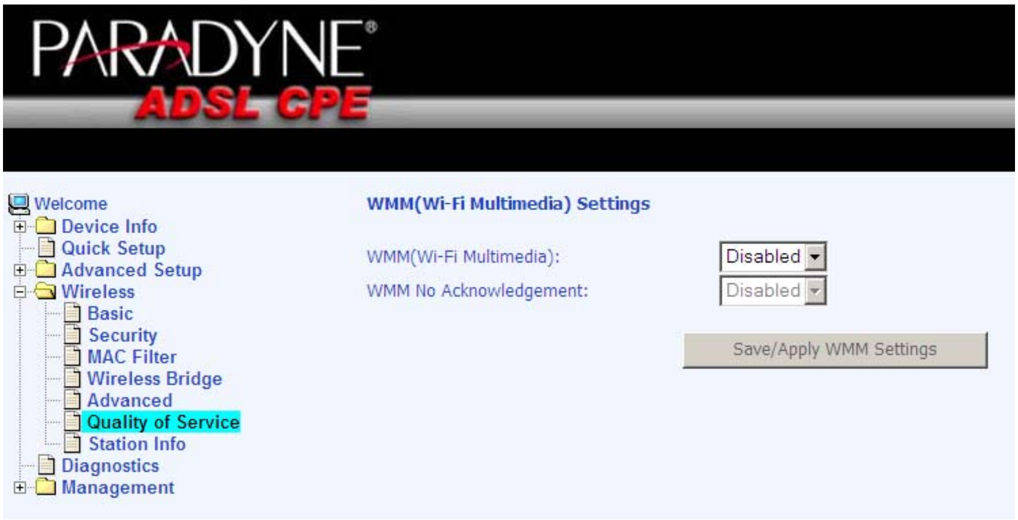
AP Isolation:	Off	
Band:	2.4GHz	
Channel:	11	Current: 11
Auto Channel Timer(min)	0	
54g™ Rate:	Auto	
Multicast Rate:	54 Mbps	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Maximum Associated Clients:	128	
XPress™ Technology:	Disabled	
54g™ Mode:	54g Performance	
54g™ Protection:	Auto	
Transmit Power:	100%	

Quality of Service

WMM (Wi-Fi Multimedia) technology is available on the wireless router, allowing you to give multimedia applications a higher quality of service and priority in a wireless network so applications such as videos will be of higher quality. Enabling WMM may delay the network traffic of other lower assigned quality applications.

WMM No Acknowledgement can be enabled if you enable WMM which refers to the acknowledgement policy used at the MAC level.

To create a QoS entry, click the **Add QoS Entry** button to proceed to add or remove traffic class rules for your network. Click on **Save/Apply WME Settings**.

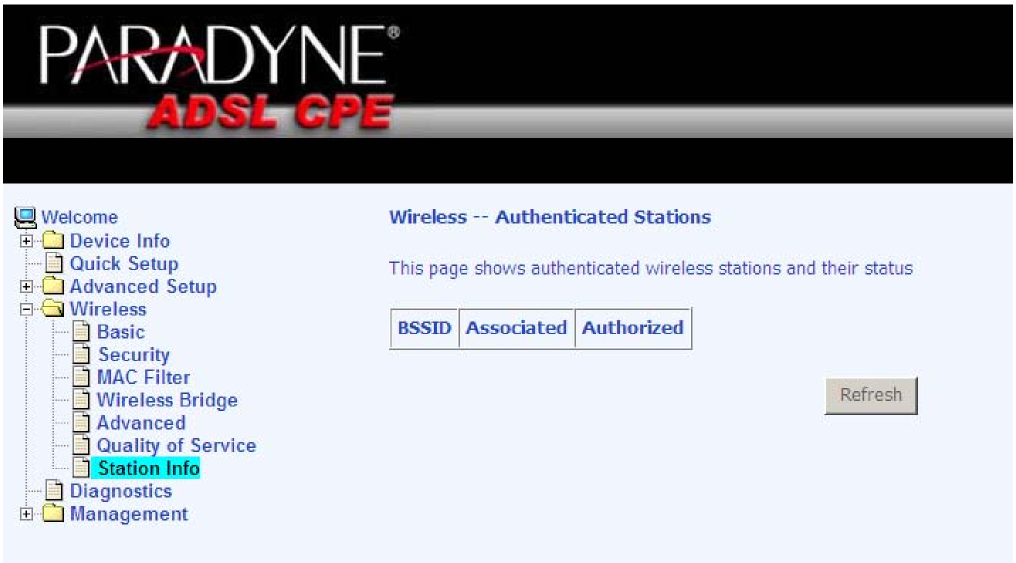


WMM(Wi-Fi Multimedia) Settings

WMM(Wi-Fi Multimedia):	Disabled
WMM No Acknowledgement:	Disabled

Station Info

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



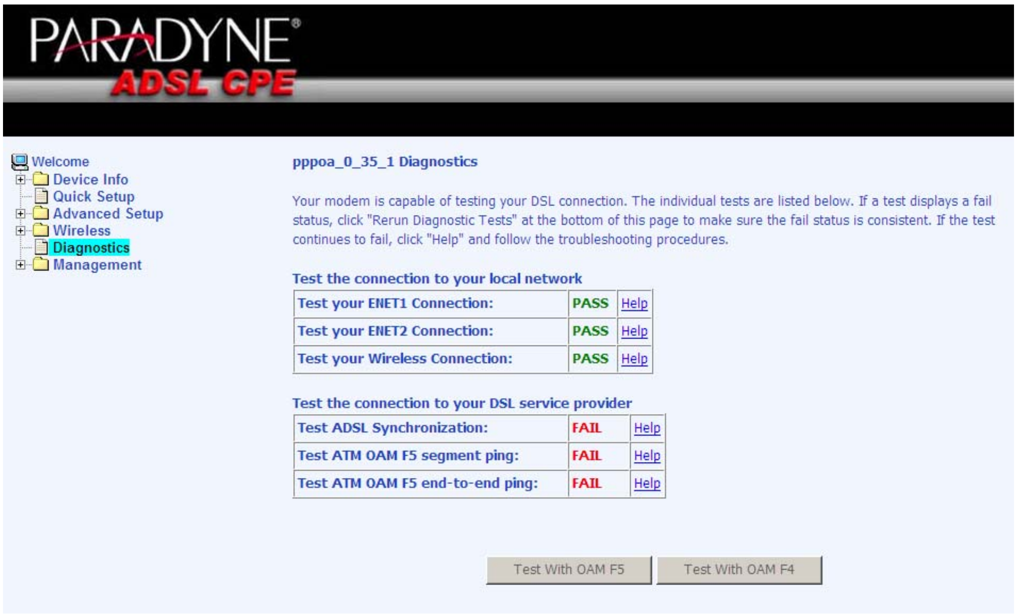
Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status

BSSID	Associated	Authorized

Troubleshooting—Diagnostics

The diagnostics screen allows you to run diagnostic tests to check your DSL connection. In addition, you can test the connection to your DSL service provider.



pppoa_0_35_1 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ENET1 Connection:	PASS	Help
Test your ENET2 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

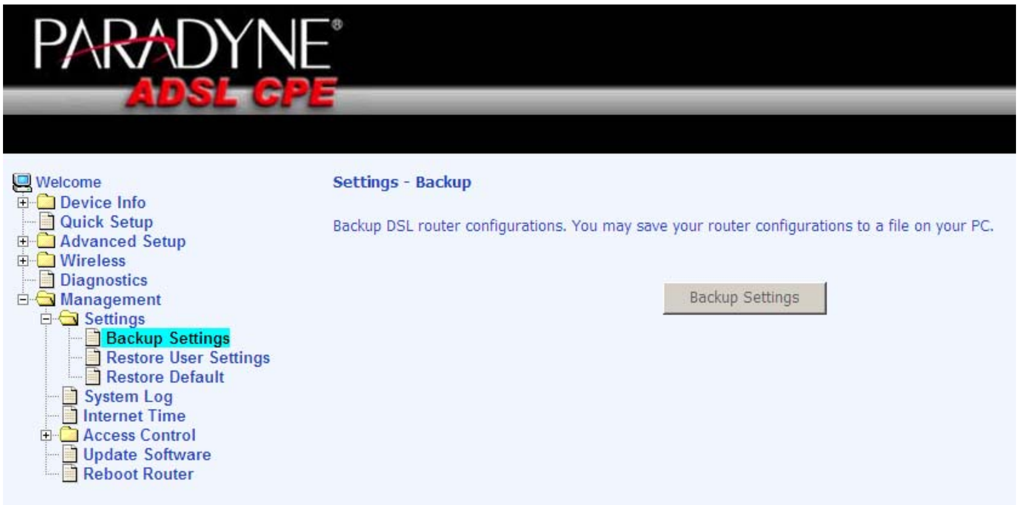
Management

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

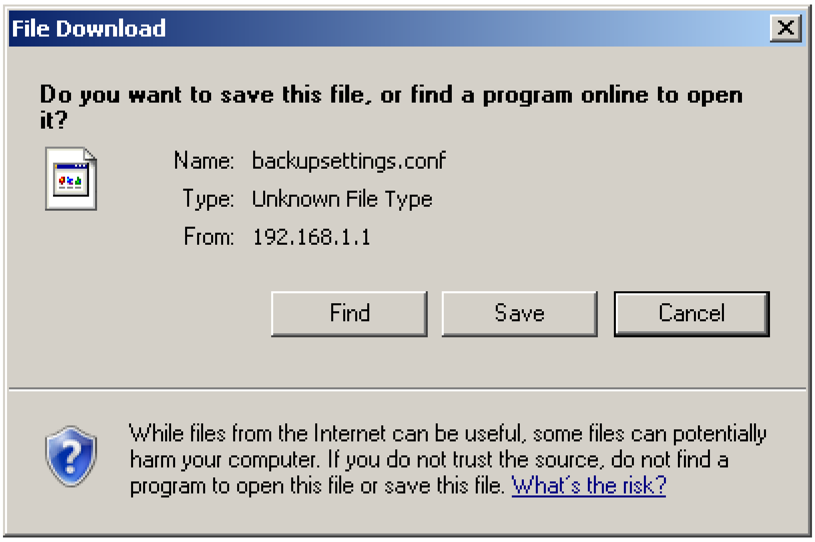
To save a copy of the configurations that you have made on your router, click on the *Management* and then *Settings* and *Backup.* Click on the **Backup Settings** button initiate the settings backup process.



Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

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



Do you want to save this file, or find a program online to open it?

Name: backupsettings.conf

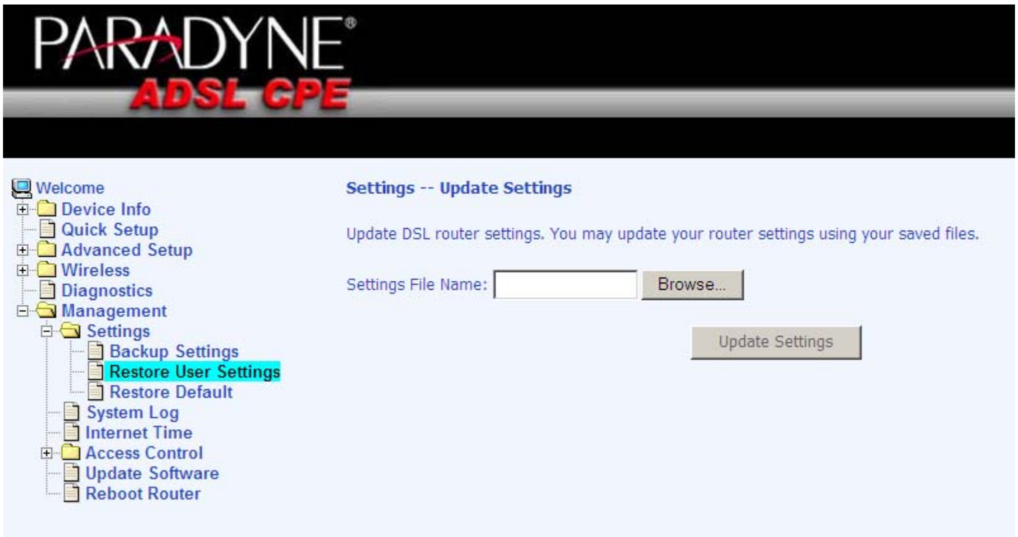
Type: Unknown File Type

From: 192.168.1.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

Update Settings

To restore saved settings, select *Management* and then *Settings* and *Update*. Then select the backup file you want to restore and click on **Update Settings**.



Settings -- Update Settings

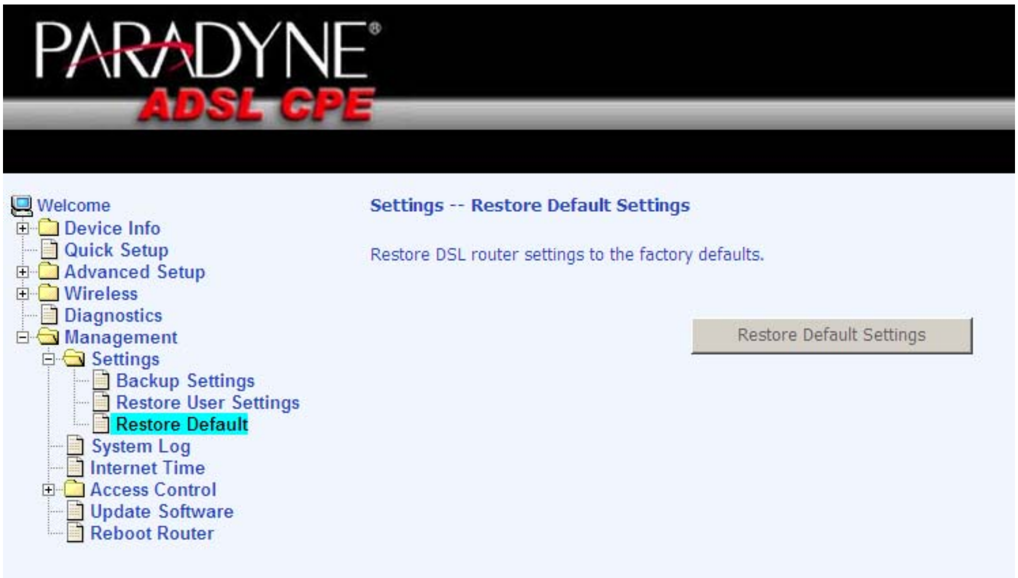
Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

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

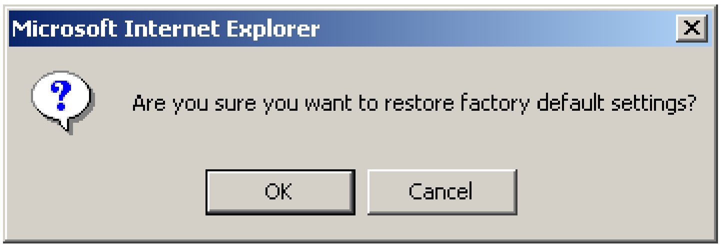
Restore Default

Restore Default will remove all current settings and restore the router to factory default settings. To restore the router to factory default settings, select *Management* and then *Settings* and *Restore Default*. Click on the **Restore Default Settings** button and when the confirmation dialog appears, reply OK.



Settings -- Restore Default Settings

Restore DSL router settings to the factory defaults.



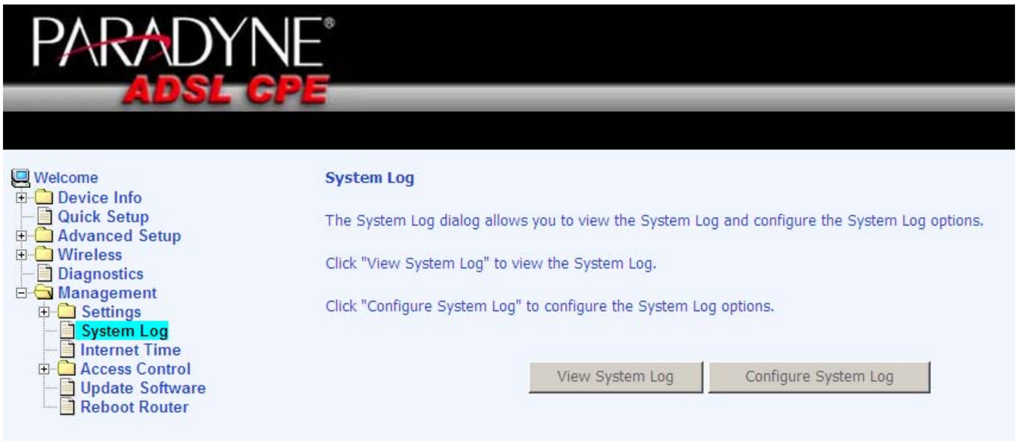
Are you sure you want to restore factory default settings?

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.



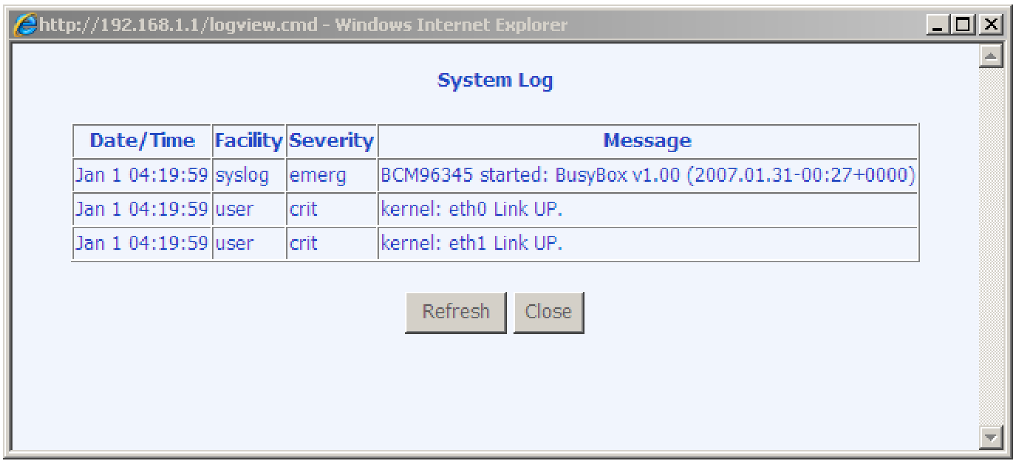
System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

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

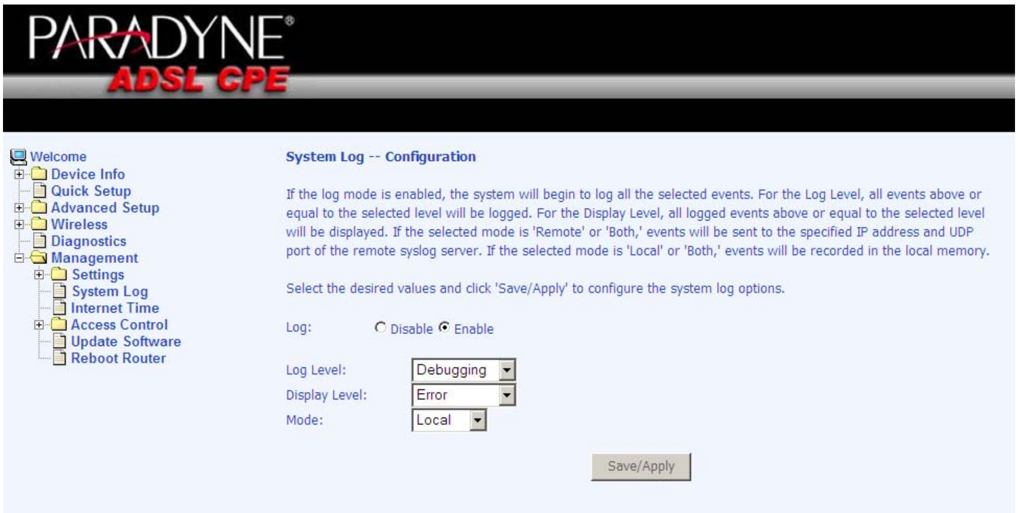


System Log

Date/Time	Facility	Severity	Message
Jan 1 04:19:59	syslog	emerg	BCM96345 started: BusyBox v1.00 (2007.01.31-00:27+0000)
Jan 1 04:19:59	user	crit	kernel: eth0 Link UP.
Jan 1 04:19:59	user	crit	kernel: eth1 Link UP.

System Log – Configuration

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



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ○ Disable ● Enable

Log Level: Debugging

Display Level: Error

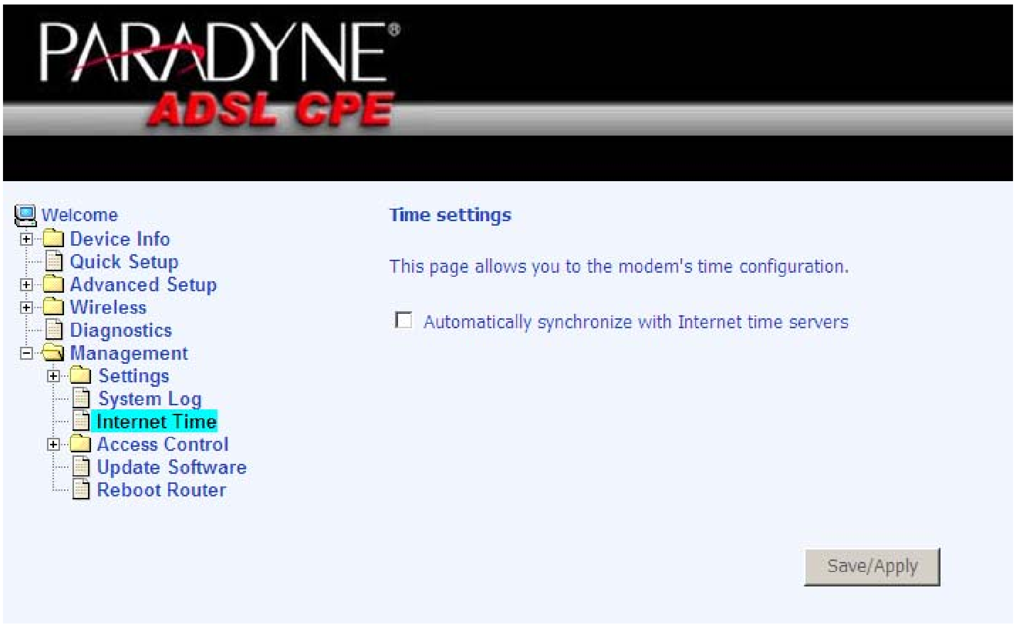
Mode: Local

Save/Apply

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.

Internet Time

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



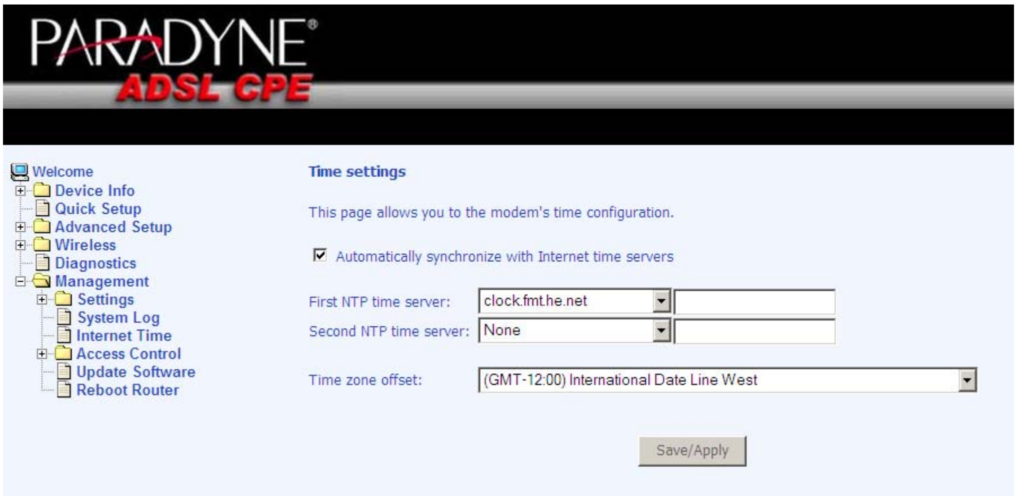
Time settings

This page allows you to the modem's time configuration.

☐ Automatically synchronize with Internet time servers

Save/Apply

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.



Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server: clock.fmt.he.net

Second NTP time server: None

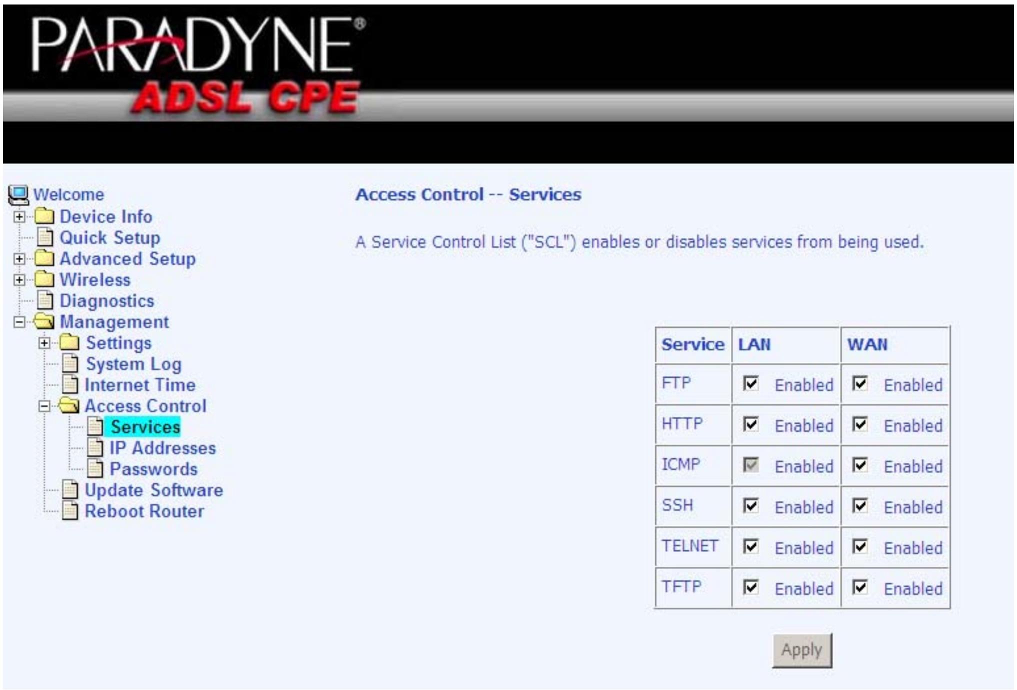
Time zone offset: (GMT-12:00) International Date Line West

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 or disabled on the LAN / WAN are FTP, HTTP, ICMP, SNMP, SSH, Telnet, and TFTP.



Access Control -- Services

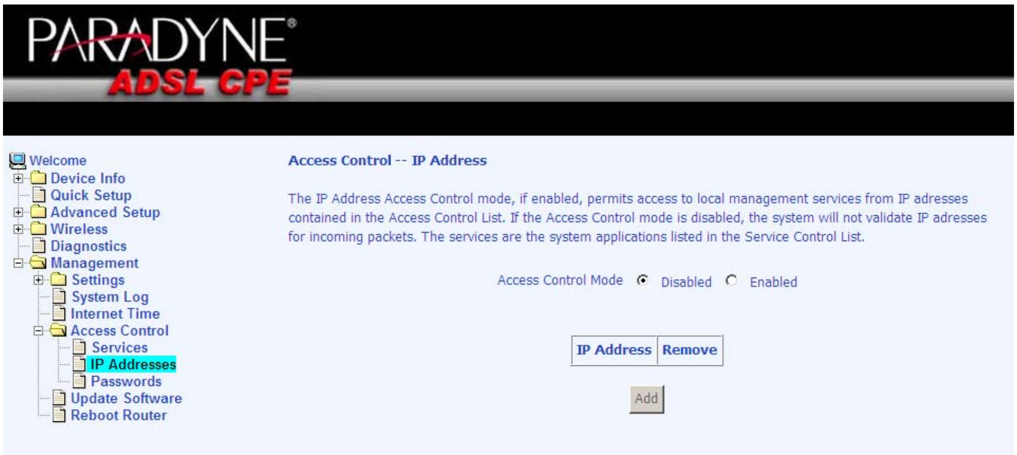
A Service Control List ("SCL") enables or disables services from being used.

Service	LAN	WAN
FTP	☑ Enabled	☑ Enabled
HTTP	☑ Enabled	☑ Enabled
ICMP	☑ Enabled	☑ Enabled
SSH	☑ Enabled	☑ Enabled
TELNET	☑ Enabled	☑ Enabled
TFTP	☑ Enabled	☑ Enabled

IP Addresses

Web access to the router can be limited when Access Control Mode is enabled. To add the IP addresses of allowed hosts click on *Access Control* and then *IP Address.*.

Add the IP address to the IP address list by clicking on the **Add** button, then select "**Enabled**" to enable Access Control Mode.



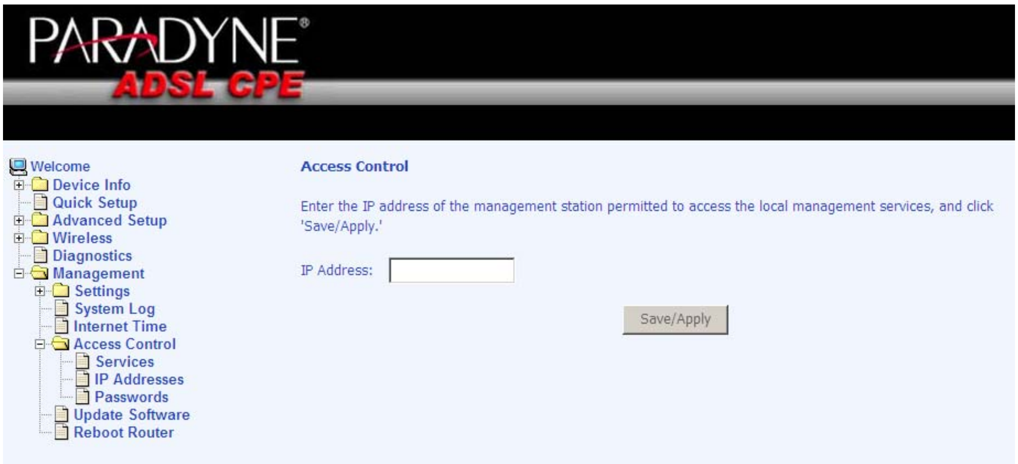
Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP adresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP adresses for incoming packets. The services are the system applications listed in the Service Control List.

Access Control Mode ● Disabled ○ Enabled

IP Address	Remove

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.



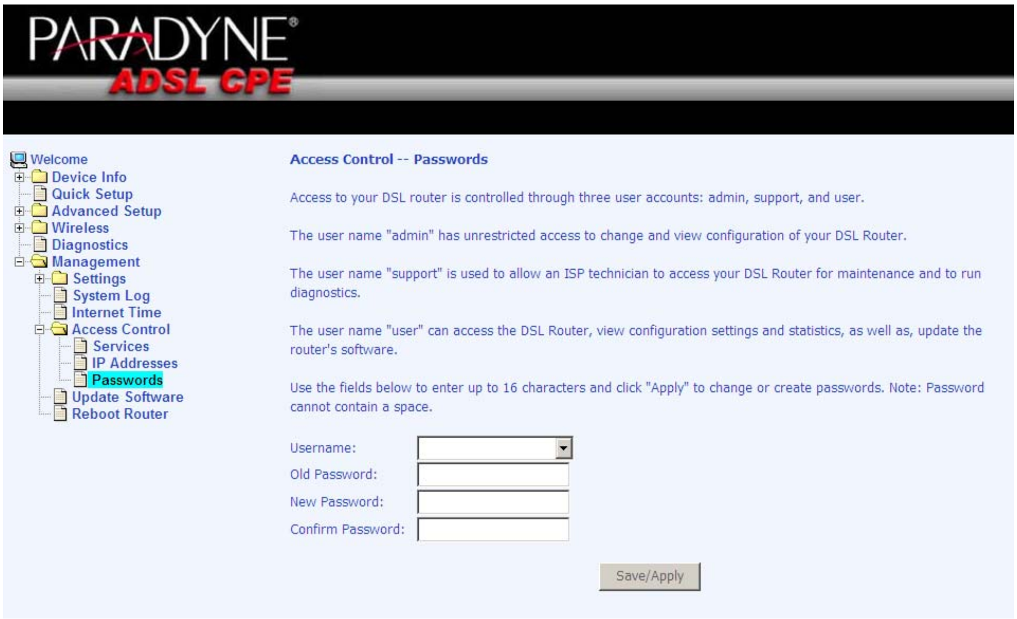
Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

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.



Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

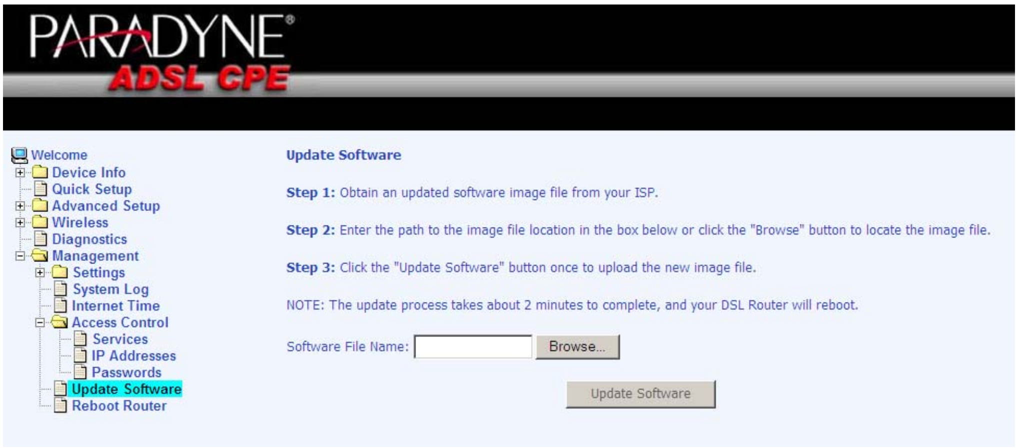
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:
Old Password:
New Password:
Confirm Password:

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.



Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

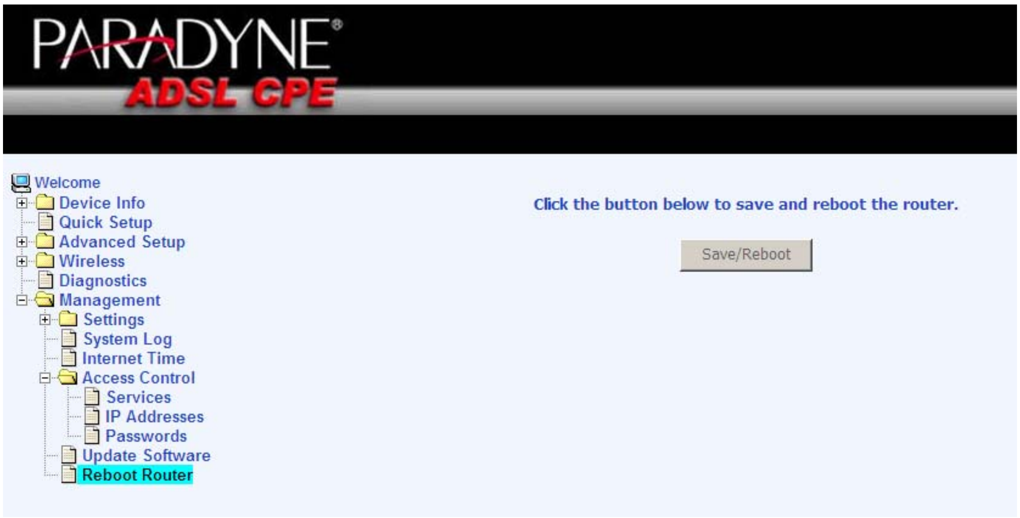
Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

Save / Reboot

To reboot the device, click on *Management* and then *Save/Reboot* to save the configurations and/or changes made and to reboot the device using the web interface. The CPE will save the current configuration and reboot itself using the new configuration.



Click the button below to save and reboot the router.