



***ADSL2/2+ 4 Ports Switch 11N WiFi Router
Freeway DSL User's Manual***

**Rev. 1.0
May. 2009**

Table of Contents

1. INTRODUCTION.....	1
1.1 GENERAL FEATURES	1
1.2 SYSTEM REQUIREMENT.....	1
2. FREEWAY DSL OVERVIEW	2
2.1 LED DESCRIPTION	2
2.2 PORTS AND BUTTONS.....	3
2.3 INSTALLING YOUR FREEWAY DSL.....	3
3. CONFIGURING TCP/IP	4
4. 5.1 LOGIN TO YOUR FREEWAY DSL.....	5
5. DEVICE INFO.....	6
5.1 SUMMARY	6
5.2 WAN	6
5.3 STATISTICS.....	7
5.3.1 LAN.....	7
5.3.2 WAN Service.....	7
5.3.3 xTM.....	7
5.3.4 xDSL.....	8
5.4 ROUTE.....	9
5.5 ARP.....	9
5.6 DHCP.....	9
6. ADVANCED SETUP.....	10
6.1 LAYER2 INTERFACE-ATM INTERFACE.....	10
6.2 WAN SERVICE.....	11
6.3 LAN.....	16
6.4 NAT.....	17
6.4.1 Virtual Servers.....	17
6.4.2 Port Triggering.....	19
6.4.3 DMZ Host	20
6.5 SECURITY – IP FILTERING	21
6.5.1 Outgoing	21
6.5.2 Incoming.....	22
6.6 PARENTAL CONTROL	23
6.6.1 Time Restriction.....	23
6.6.2 URL Filter.....	24
6.7 QUALITY OF SERVICE.....	25
6.7.1 Queue Config.....	26
6.7.2 QoS Classification.....	27
6.8 ROUTING.....	28
6.8.1 Default Gateway.....	28
6.8.2 Static Route.....	28
6.8.3 RIP.....	29
6.9 DNS.....	29
6.9.1 DNS Server.....	29
6.9.2 Dynamic DNS (DDNS).....	30
6.10 DSL	31
6.11 UPnP	32
6.12 DNS PROXY.....	32
6.13 USB STORAGE	32
6.14 PRINT SERVER.....	33
6.15 INTERFACE GROUPING	34
6.16 LAN PORTS.....	36
6.17 IPSEC.....	36
6.18 CERTIFICATE.....	38
6.18.1 Local.....	38

6.18.2	Trusted CA.....	40
7.	WIRELESS.....	41
7.1	BASIC.....	41
7.2	SECURITY.....	42
7.3	MAC FILTER.....	45
7.4	WIRELESS BRIDGE.....	46
7.5	ADVANCED.....	47
7.6	STATION INFO.....	49
8.	DIAGNOSTICS.....	50
9.	MANAGEMENT.....	51
9.1	SETTINGS.....	51
9.1.1	Backup.....	51
9.1.2	Update.....	51
9.1.3	Restore Default.....	51
9.2	SYSTEM LOG.....	52
9.2.1	Configure System Log.....	52
9.2.2	View System Log.....	53
9.3	SNMP AGENT.....	53
9.4	TR-069 CLIENT.....	54
9.5	INTERNET TIME.....	55
9.6	ACCESS CONTROL.....	55
9.6.1	Passwords.....	55
9.6.2	Services.....	56
9.7	UPDATE SOFTWARE.....	56
9.8	REBOOT.....	57
10.	WALL MOUNTING (OPTIONAL).....	58
	APPENDIX A. TROUBLESHOOTING.....	59
	APPENDIX B. SPECIFICATIONS.....	61

Federal Communication Commission Interference Statement

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 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.

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FEDERAL COMMUNICATIONS COMMISSION

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.
--

CAUTION

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

1. Introduction

The Freeway DSL is a highly integrated device which enables ADSL2+, 11N WLAN, Router, Switch,] and File server together. It is positioned to enhance the user's triple play broadband experience with excellent QoS (Quality of Service) and traffic management. This new generation of platforms not only eases the deployment of DSL-based ADSL2+ but also provides new opportunities for the service provider to derive additional value from the emerging IP Video service.

The Draft 2.0 IEEE802.11N solution of Freeway DSL can take advantage of the high throughput and extended range with MIMO core technology. Freeway DSL adopts the easy-to-use web-GUI management interface. Its user friendly interface will amaze you with total difference experience. Freeway DSL also supports SNMP agent and TR-069 which enable central management from the central offices and benefit the ISP much.

1.1 General Features

- Comply with ITU ADSL, ADSL 2 and ADSL2+ standards
- Compliant to DSL Forum TR-048, TR-067 and TR-100 Interoperability Test
- Feature-Rich TR-069 supports Remote Registration / Remote Authentication / Remote Configuration
- Complete solution for integration of ADSL, Router, Switch, and 11N Draft 2.0 WLAN
- Advanced MIMO technology provides enhanced wireless speed/range and wide coverage area
- WPS support for easy WLAN client setup
- Easily expands network coverage using compatible WDS-enabled AP
- Improves on the experience of user for audio, video and voice applications by QoS configuration
- Easy to use file server for mass storage file sharing
- Security supports WPA/WPA2-PSK, & 64/128-bit WEP Encryption
- Remote / Local configuration & management through Web / Telnet configuration & management
- Three levels access account management
- Support Universal Plug and Play (UPnP)
- Device management access control based on source IP addresses and incoming interfaces

1.2 System Requirement

In order to use the Freeway DSL, you must have the following:

- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN
- One or more computers each containing an Ethernet network interface card (NIC) and/or a single computer with a USB port
- An Ethernet hub/switch, if you are connecting the device to more than one computer on an Ethernet network
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, Firefox v2.0 or later, or Netscape v6.1 or later

2. Freeway DSL Overview

2.1 LED Description

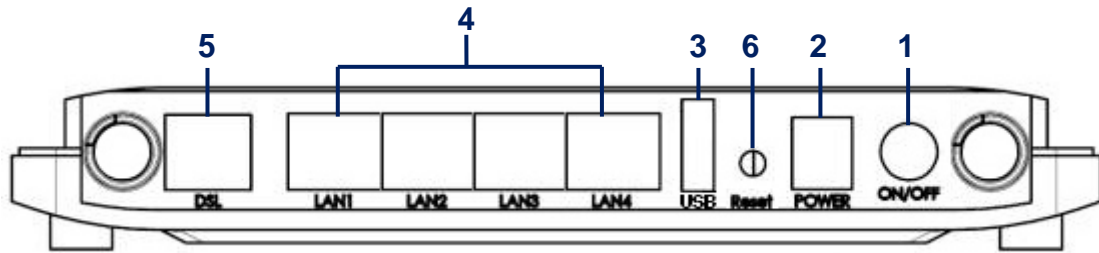
The front panel contains lights called LEDs that indicate the status of the Freeway DSL.



LED	Color	Status	Description
POWER	Green	On	The device is power on.
		Off	The device is power off.
	Red	On	The device is booting up.
WPS	Green	On	The WPS is in progress and success status.
	Red	On	The WPS encounters problem or session overlap.
LAN1-4	Green	On	The LAN port is connected to a power-on Ethernet device.
		Blinking	The data is sending/receiving via LAN port.
		Off	The LAN port is not connected to any Ethernet device.
WLAN	Green	On	The wireless feature is enabled.
		Blinking	The IAD is sending/receiving wirelessly.
		Off	The wireless feature is disabled.
USB	Green	On	A powered device has connected to the USB port.
		Blinking	The data is sending/receiving via USB port.
		Off	No powered device has connected to the USB port.
DSL	Green	On	The device is successfully linked with ADSL head-end.
		Slow Blinking	The device is trying to link with ADSL head-end.
		Fast Blinking	The device is handshaking with the ADSL head-end.
		Off	The device is not linked with ADSL head-end.
Internet	Green	On	The device is successfully connected to the Internet.
		Blinking	The device is sending/receiving data via the Internet.
		Off	The device is not connected to the Internet.
	Red	On	The device is failed to authenticate with the ISP due to username or password error.

2.2 Ports and Buttons

The rear panel contains the ports for the Freeway DSL's data and power connections.



1. **ON/OFF:** Power switch to power on/off the Freeway DSL.
2. **POWER:** Connector for a power adapter. Using a power supply with a different voltage rating will damage this product. Make sure to observe the proper power requirements. The requirement of adapter is 12V/1A.
3. **USB:** Connects for USB supported printer or USB mass storage.
4. **LAN1-4:** Connectors for Ethernet network devices, such as a PC, hub, switch or router.
5. **DSL:** Connector for accessing the Internet through ADSL line.
6. **Reset:** Restore the default settings. You may need to restore the Freeway DSL to its factory defaults if the configuration is changed, you lose the ability to enter the Freeway DSL via the web interface, or following a software upgrade, and you lose the ability to enter the Freeway DSL. To reset the Freeway DSL, simply press the reset button for more than 8 seconds. The Freeway DSL will be reset to its factory defaults. The reboot process will take a about 30 seconds and the Freeway DSL will become operational again.

2.3 Installing your Freeway DSL

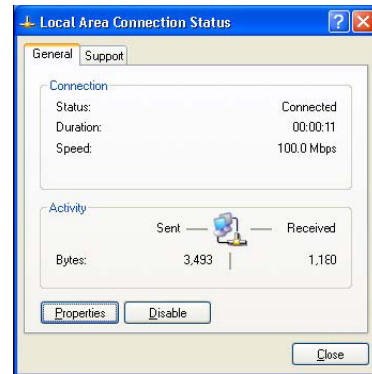
1. Locate an optimum location for the Freeway DSL.
2. For connections to the Ethernet and DSL interfaces, refer to the Quick Start Guide.
3. Connect the Power Adapter. Depending upon the type of network, you may want to put the power supply on an uninterruptible supply. Use only the power adapter supplied with the Freeway DSL. A different adapter may damage the product.

3. Configuring TCP/IP

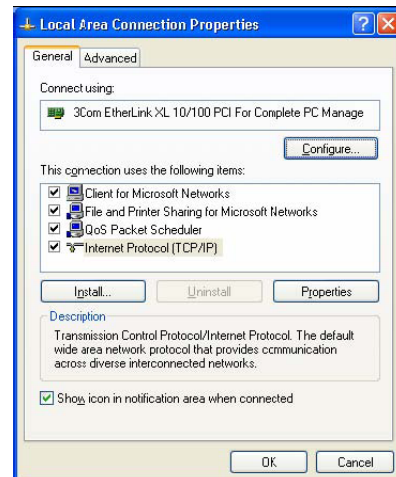
This section will help you to establish a connection between a PC and the Freeway DSL. Each computer that will be part of your network needs to communicate with the Freeway DSL. To do this, you may need to configure each PC's network settings to automatically obtain an IP address.

This configuration assumes you have retained the default interface for Windows XP. If you are running the 'Classic' interface, please follow the instructions for Windows XP.

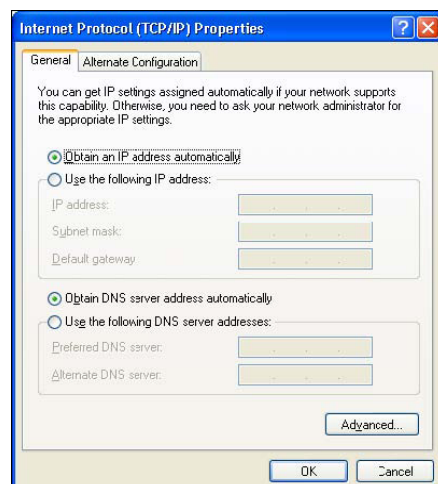
1. Select **Start > Settings > Control Panel**.
2. Double-click **Network and Dial-Up Connections**.
3. Double-click the **Local Area Connection** appropriate for your Ethernet adapter.
4. Click **Properties**.
The Local Area Properties window is displayed.



5. Ensure the box next to Internet Protocol (TCP/IP) is selected.
6. Click to highlight **Internet Protocol (TCP/IP)** and click **Properties**.
The Internet Protocol (TCP/IP) Properties window is displayed.



7. Select **Obtain an IP address automatically** if you are connecting the Freeway DSL to the PC via Ethernet. Otherwise, select **Use the following IP address** and specify an IP address within the subnet such as 192.168.1.5 (assuming the IP address of the Freeway DSL is 192.168.1.1) if you are connecting the Freeway DSL to the PC via USB.
8. Click **OK** twice to exit and save your settings.

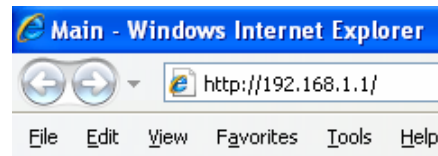


4. 5.1 Login to Your Freeway DSL

This section guides you through configuring your Freeway DSL. You should have your computers configured for DHCP mode and have proxies disabled on your browser. If you do not get the page as shown below, you may need to delete your temporary Internet files by flushing the cached web pages.

Follow the procedures below to login to your Freeway DSL.

1. Open your web browser. Type the default IP address of the Freeway DSL **http://192.168.1.1** and press **Enter**.
The Log In page appears.
2. Enter user name as **admin** and password as **admin** (case sensitive).
3. Click **OK**.
The main page appears.



Note

There are two default user name and password combinations. The **user / user** name and password combination allow you to view the device status, but you cannot change or save configurations. The **admin / admin** combination allows you to perform all functions. Passwords can be changed at any time. You can change the password in **Management->Access Control->Passwords** page at any time.

This web page layout of Freeway DSL is shown as below.

<p>Easy configurator Device Info Advanced Setup Wireless Diagnostics Management</p>	<p>Device Info</p> <table border="1"> <tr> <td>Firmware Version:</td> <td>8423.090512a1_87_50</td> </tr> <tr> <td>Board ID:</td> <td>96358VW2</td> </tr> <tr> <td>SDK Version:</td> <td>090512_1126-4.02L.03.A2p8025c1.d21j2</td> </tr> <tr> <td>Bootloader (CFE) Version:</td> <td>1.0.37-102.9</td> </tr> <tr> <td>Wireless Driver Version:</td> <td>5.10.85.0.cpe4.402.0</td> </tr> </table> <p>This information reflects the current status of your DSL connection.</p> <table border="1"> <tr> <td>Line Rate - Upstream (Kbps):</td> <td>64</td> </tr> <tr> <td>Line Rate - Downstream (Kbps):</td> <td>1024</td> </tr> <tr> <td>LAN IPv4 Address:</td> <td>192.168.1.1</td> </tr> <tr> <td>Default Gateway:</td> <td>ppp0</td> </tr> <tr> <td>Primary DNS Server:</td> <td>168.95.192.1</td> </tr> <tr> <td>Secondary DNS Server:</td> <td>168.95.1.1</td> </tr> </table>	Firmware Version:	8423.090512a1_87_50	Board ID:	96358VW2	SDK Version:	090512_1126-4.02L.03.A2p8025c1.d21j2	Bootloader (CFE) Version:	1.0.37-102.9	Wireless Driver Version:	5.10.85.0.cpe4.402.0	Line Rate - Upstream (Kbps):	64	Line Rate - Downstream (Kbps):	1024	LAN IPv4 Address:	192.168.1.1	Default Gateway:	ppp0	Primary DNS Server:	168.95.192.1	Secondary DNS Server:	168.95.1.1
Firmware Version:	8423.090512a1_87_50																						
Board ID:	96358VW2																						
SDK Version:	090512_1126-4.02L.03.A2p8025c1.d21j2																						
Bootloader (CFE) Version:	1.0.37-102.9																						
Wireless Driver Version:	5.10.85.0.cpe4.402.0																						
Line Rate - Upstream (Kbps):	64																						
Line Rate - Downstream (Kbps):	1024																						
LAN IPv4 Address:	192.168.1.1																						
Default Gateway:	ppp0																						
Primary DNS Server:	168.95.192.1																						
Secondary DNS Server:	168.95.1.1																						

5. Device Info

This is the first page you see when entering the Web Application.

5.1 Summary

This page shows the status summary of the Freeway DSL.

Device Info	
Firmware Version:	B423.090512a1_87_50
Board ID:	96358VW2
SDK Version:	090512_1126-4.02L.03.A2pB025c1.d21j2
Bootloader (CFE) Version:	1.0.37-102.9
Wireless Driver Version:	5.10.85.0.cpe4.402.0

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	64
Line Rate - Downstream (Kbps):	1024
LAN IPv4 Address:	192.168.1.1
Default Gateway:	ppp0
Primary DNS Server:	168.95.192.1
Secondary DNS Server:	168.95.1.1

5.2 WAN

This page shows the WAN information of Freeway DSL.

WAN Info								
Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
ppp0	pppoe_0_0_33	PPPoE	Disabled	Disabled	Enabled	Enabled	Connecting	

5.3 Statistics

This section shows the statistics information of Freeway.

5.3.1 LAN

This page shows the statistics of each connection on your LAN.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	132147	1385	0	0	316673	895	0	0
eth1	0	0	0	0	0	0	0	0
wl0	86265	594	0	0	247678	1082	3	0

5.3.2 WAN Service

This page shows the WAN statistics information.

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0	pppoe_0_0_33	39005	201	0	0	26630	189	0	0

5.3.3 xTM

This page shows the xTM interface statistics information.

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
<input type="button" value="Reset"/>										

5.3.4 xDSL

This page shows the DSL status and statistics.

Statistics -- xDSL				
Mode:	ADSL_G.dmt			
Traffic Type:	ATM			
Status:	Up			
Link Power State:	LO			
	Downstream	Upstream		
Line Coding(Trellis):	Off	Off		
SNR Margin (0.1 dB):	292	200		
Attenuation (0.1 dB):	260	190		
Output Power (0.1 dBm):	186	81		
Attainable Rate (Kbps):	10432	524		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	1024	64	0	0
K (number of bytes in DMT frame):	33	3	0	0
R (number of check bytes in RS code word):	16	16	0	0
S (RS code word size in DMT frame):	4.00	16.00	0.0	0.0
D (interleaver depth):	8	4	0	0
Delay (msec):	8.00	16.00	0.0	0.0
INP (DMT symbol):	0.43	0.11	0.0	0.0
Super Frames:	73572	73513	0	0
Super Frame Errors:	0	0	0	0
RS Words:	1250728	312430	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	0	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	3020697	0	0	0
Data Cells:	6412	0	0	0
Bit Errors:	0	0	0	0
Total ES:	0	0		
Total SES:	0	0		
Total UAS:	31	0		
<input type="button" value="xDSL BER Test"/> <input type="button" value="Reset Statistics"/>				

5.4 Route

This page shows the IP route for Freeway DSL.

Device Info -- Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
61.228.192.254	0.0.0.0	255.255.255.255	UH	0	pppoe_0_0_33	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_0_0_33	ppp0

5.5 ARP

This page shows the ARP (Address Resolution Protocol) table on Freeway DSL.

Device Info -- ARP			
IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:15:00:21:6B:A9	br0

5.6 DHCP

This page shows the client devices which are assigned IP addresses by the Freeway DSL.

Device Info -- DHCP Leases			
Hostname	MAC Address	IP Address	Expires In
your-275e71dd89	00:15:00:21:6b:a9	192.168.1.2	23 hours, 32 minutes, 0 seconds

6. Advanced Setup

This section allows you to make specific configurations to your Freeway DSL such as NAT, Quality of Service, DNS and so on.

6.1 Layer2 Interface-ATM Interface

This page shows the summary of the current ATM interfaces you have configured. You can set up more than one connection profiles on your Freeway DSL.

DSL ATM Interface Configuration								
Choose Add, or Remove to configure DSL ATM interfaces.								
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	33	Path0	UBR	EoA	DefaultMode	Disabled	<input type="checkbox"/>

Click **Add** to create ATM interface. Enter the information provided by your ISP and then click **Save/Apply**.

ATM PVC Configuration	
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.	
VPI: [0-255]	<input type="text" value="0"/>
VCI: [32-65535]	<input type="text" value="35"/>
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)	
<input checked="" type="radio"/> EoA <input type="radio"/> PPPoA <input type="radio"/> IPoA	
Encapsulation Mode:	<input type="text" value="LLCSNAP-BRIDGING"/>
Service Category:	<input type="text" value="UBR Without PCR"/>
Select Connection Mode	
<input checked="" type="radio"/> Default Mode - Single service over one connection <input type="radio"/> VLAN MUX Mode - Multiple Vlan service over one connection <input type="radio"/> MSC Mode - Multiple Service over one Connection	
Enable Quality Of Service	
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.	
<input type="checkbox"/> Enable Quality Of Service.	
<input type="button" value="Back"/> <input type="button" value="Apply/Save"/>	

Field	Description
VPI/VCI	Enter the PVC identifier (VPI and VCI) provided by your ISP.
DSL Link Type	Select the DSL link type for the connection. Your ISP should inform you which type to use.
Encapsulation Mode	Select the encapsulation mode for the connection. Your ISP should inform you which mode to use.
Service Category	Select the encapsulation mode for the connection. If you are not sure which type to select, just use the default type.
Connection Mode	Select the connection mode according to your application.
Enable Quality of Service	Check to enable QoS feature. It improves the performance for selected classes of applications.

6.2 WAN Service

This page shows the summary of the WAN service for a selected interface.

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
ppp0	pppoe_0_0_33	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>

Click **Add** to configure WAN service. Select an interface from the drop-down list and click **Next**.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

Select a WAN service type and enter a service description for this connection. Different mode will lead you to different configuration page. Click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

PPP over Ethernet (PPPoE) Mode

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

IPv4 Address:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

Enable IGMP Multicast

Field	Description
PPP Username	Enter the username of your PPP account.
PPP Password	Enter the password of your PPP account
PPPoE Service Name	Enter the service name if required by the ISP.

Authentication Method	Select the authentication method to be PAP, CHAP or MSCHAP. Select "Auto" to allow the Freeway DSL to negotiate with PPP server automatically.
Enable Fullcone NAT	Check to enable fullcone NAT feature.
Dial on Demand	Check to enable DOD feature.
Inactivity Timeout (minutes)	Specify the inactivity timeout (in minute) for DOD feature.
PPP IP Extension	Check to enable PPP IP extension.
Use Static IPv4 Address	Check and enter the static IPv4 address.
Enable PPP Debug Mode	Check to enable PPP debug mode.
Bridge PPPoE frames Between WAN and Local Ports	Check to enable the PPPoE frames bridging between WAN and Local Ports.
IGMP Multicast	Check to enable IGMP multicasting.

IP over Ethernet (MER) Mode

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically
 Use the following Static IP address:

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Field	Description
Obtain an IP Address Automatically	Select and select your preferred WAN interface from drop-down list. This allows the Freeway DSL to obtain the DNS server information automatically.
Option 60 Vendor ID	Your ISP will assign the Vendor Class IDentifier automatically. This option can be used by DHCP clients to identify the vendor and functionality of a DHCP client.
Option 61 IAID	Your ISP will assign the IAID (Identity Association IDentifier) automatically.
Option 61 DUID	Your ISP will assign the DUID (DHCP Unique IDentifier)) automatically.
Option 125	Select this item (Vendor-Identifying Vendor-Specific) to tell the Freeway DSL which firmware it has to download.
User the following Static IP Address	Select this mode and enter the static IP address, subnet mask and gateway IP address provided by your ISP.

Select a WAN interface as Freeway DSL default gateway. Click **Next**.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: ▼

DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:
 WAN Interface selected: ▼

Use the following Static DNS IP address:
 Primary DNS server:
 Secondary DNS server:

Field	Description
Obtain DNS Info from a WAN	Select the WAN interface to obtain the DSN info.
Use the Following Static DNS IP Address	Select to configure the static DNS IP address manually.
Primary DNS Sever	Enter the IP address of primary DNS server.
Secondary DNS Sever	(Optional) Enter the IP address of secondary DNS server.

The table below shows the summary of your WAN settings. Make sure they match the settings provided by your ISP so that you can connect to the Internet.

WAN Setup - Summary	
Make sure that the settings below match the settings provided by your ISP.	
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save" to save these settings and reboot router.
Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

6.3 LAN

This page shows the current setting of LAN interface. You can set IP address/subnet mask and DHCP server pool for the LAN interface.

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address:

Subnet Mask:

Enable IGMP Snooping

Standard Mode
 Blocking Mode

Enable LAN side firewall

Disable DHCP Server
 Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<div style="display: flex; justify-content: space-around;"> Add Entries Remove Entries </div>		

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

Apply/Save

Field	Description
Group Name	Select a group name for this LAN.
IP Address	Enter the IP address for this LAN.
Subnet Mask	Enter the subnet mask for this LAN.
Enable IGMP Snooping	Check to enable IGMP Snooping and select the mode to be Standard or Blocking.
Enable LAN Side Firewall	Check to enable LAN side Firewall.
DHCP Server	If Enabled, the Freeway DSL will assign IP addresses to PCs (DHCP clients) on your LAN when they start up. The default setting is Enabled.
Start/End IP Address	Configure the DHCP range used by the DHCP server when assigning IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported.
Leased Time (hour)	Configure the amount of time the clients will be allowed to connect to DHCP server. If set to 0, the allocated IP addresses will be effective forever.

Static IP Leased Time	Click Add Entries to configure static LAN IP according to its MAC address to the clients.
Second IP Address	Enter the second IP address for this LAN if needed.
Subnet Mask	Enter the subnet mask for this LAN.

6.4 NAT

6.4.1 Virtual Servers

You can configure the Freeway DSL as a virtual server. Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the internal server with private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Age of Kings	47624	47624	TCP	47624	47624	192.168.1.55	ppp0	<input type="checkbox"/>
Age of Kings	6073	6073	TCP	6073	6073	192.168.1.55	ppp0	<input type="checkbox"/>
Age of Kings	2300	2400	TCP	2300	2400	192.168.1.55	ppp0	<input type="checkbox"/>
Age of Kings	2300	2400	UDP	2300	2400	192.168.1.55	ppp0	<input type="checkbox"/>

Click **Add** to configure virtual server. Select the virtual server from the drop-down list or custom the service you need. Then complete the server IP address and click the **Apply/Save**.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text" value="443"/>	<input type="text" value="443"/>	TCP <input type="button" value="v"/>	<input type="text" value="443"/>	<input type="text" value="443"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>

6.4.2 Port Triggering

Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, require that specific ports in the Router's firewall be opened for access by the remote parties.

Port Trigger dynamically opens up the "Open Ports" in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the "Triggering Ports". The Freeway DSL allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the "Open Ports". A maximum 32 entries can be configured.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		
Napster	TCP	6699	6699	TCP	6699	6699	ppp0	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	6697	6697	ppp0	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	4444	4444	ppp0	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	5555	5555	ppp0	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	6666	6666	ppp0	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	7777	7777	ppp0	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	8888	8888	ppp0	<input type="checkbox"/>

Click **Add** to configure the Port Triggering. Select the applications that you want to set up the port settings and then click **Save/Apply**.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text" value="6801"/>	<input type="text" value="6801"/>	<input type="text" value="UDP"/>	<input type="text" value="6801"/>	<input type="text" value="6801"/>	<input type="text" value="UDP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>

6.4.3 DMZ Host

The Freeway DSL can forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

To activate the DMZ host, enter the computer's IP address and click **Save/Apply**. To deactivate the DMZ host, clear the IP address field and click **Save/Apply**.

6.5 Security – IP Filtering

6.5.1 Outgoing

The outgoing filter blocks the LAN traffic from entering the WAN side. By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting up filters.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Security	UDP	192.168.1.111 / 255.255.255.0	4567			<input type="checkbox"/>

Click **Add** to create a filter rule to identify outgoing IP traffic. Specify a new filter name and at least one condition. Then click **Save/Apply**. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Field	Description
Filter Name	Enter a name for this filter rule.
Protocol	Select the protocol to be used from the drop-down list.
Source IP Address / Subnet Mask / Port	Enter the source (from the LAN side) IP address, subnet mask and port number.
Destination IP Address / Subnet Mask / Port	Enter the destination (from the WAN side) IP address, subnet mask and port number.

6.5.2 Incoming

Incoming IP filter filters the WAN traffic to the LAN side. When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is blocked. This page allows you to configure filters for accepting some incoming IP traffic.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Extra	ppp0,br0	TCP			192.168.1.222 / 255.255.255.0	6789	<input type="checkbox"/>

Click **Add** to create a filter rule to identify outgoing IP traffic. Specify a new filter name and at least one condition. Then click **Save/Apply**. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All

pppoe_0_0_33/ppp0

br0/br0

Field	Description
Filter Name	Enter a name for this filter rule.
Protocol	Select the protocol to be used from the drop-down list.
Source IP Address / Subnet Mask/ Port	Enter the source (from the WAN side) IP address, subnet mask and port number.

Destination IP Address / Subnet Mask / Port	Enter the destination (from the LAN side) IP address, subnet mask and port number.
WAN/LAN Interface	Select the WAN and LAN interface to apply this rule.

6.6 Parental Control

Parental Control allows you to add the day of the week and URL restrictions to specific LAN clients.

6.6.1 Time Restriction

This page allows you to block Internet access from specified LAN clients for specified periods. Make sure that either the system time is specified directly or Internet time server is configured.

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Working	00:15:00:21:6b:a9	x	x	x	x	x			9:0	17:0	<input type="checkbox"/>

Click **Add** to configure the restriction. Enter the settings and then click **Save/Apply**.

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address

Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Field	Description
User Name	Enter a name for this restriction.
Browser's MAC Address	This is the MAC address of the LAN device where the browser is running.
Other MAC Address	Select and enter other LAN device's MAC address.
Select Days of the Week	Check the days of the week of blocking.
Start/End Blocking Time	Enter the start and end time of blocking.

6.6.2 URL Filter

This page allows you to block specified URLs from accessing. Maximum 100 entries can be configured.

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
www.xxx.com	80	<input type="checkbox"/>

Select the list type first and then click **Add** to configure the URL entries. Enter the URL address and port number. Then click **Save/Apply**.

Parental Control -- URL Filter Add

Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Field	Description
URL Address	Enter the URL address of blocking.
Port Number	Enter the port number of blocking.

6.7 Quality of Service

You can configure the Quality of Service to apply different priorities to traffic on the Freeway DSL. If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Select Default DSCP Mark v

To enable QoS, check **Enable QoS** checkbox and select a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Then click **Save/Apply**.

Field	Description
Select Default DSCP Mark	Select the DSCP mark to mark all egress packets that do not match any classification rules.

6.7.1 Queue Config

This page shows the QoS queue on the Freeway DSL. The Queue configuration allows you to configure a QoS queue entry and assign it to a specific network interface. 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. If you disable WMM function in Wireless Page, queues related to wireless will not take effects

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

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1			Enabled	
WMM Voice Priority	2	wl0	2			Enabled	
WMM Video Priority	3	wl0	3			Enabled	
WMM Video Priority	4	wl0	4			Enabled	
WMM Best Effort	5	wl0	5			Enabled	
WMM Background	6	wl0	6			Enabled	
WMM Background	7	wl0	7			Enabled	
WMM Best Effort	8	wl0	8			Enabled	

Click **Add** to configure QoS queue. Enter the settings and then click **Apply/Save**.

QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. 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 'Apply/Save' to save and activate the queue.

Name:

Enable: ▾

Interface:

Precedence: ▾

Field	Description
Name	Enter a name for the queue.
Enable	Select to enable or disable this queue.
Interface	Select an interface for this queue to apply.
Precedence	Select the precedence for this queue. Lower integer values imply higher

	priority for this queue relative to others.
--	---

Below is the table of precedence summary:

Precedence	Meaning	Precedence	Meaning
0	Routine	4	Flash Override
1	Priority	5	Critical
2	Immediate	6	Internetwork Control
3	Flash	7	Network Control

6.7.2 QoS Classification

This page allows you to create 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. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

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: ▼

Specify Classification Criteria
A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID:

Field	Description
Traffic Class Name	Enter a name for this traffic class.
Rule Order	Select a rule order for this traffic class.
Rule Status	Select to enable or disable this traffic class.
Class Interface	Select an interface for this traffic class to apply.
Ether Type	Select the Ether type from the drop-down list.
Source MAC Address/Mask	Enter the MAC address and the mask of the computer where packets are coming from.
Destination MAC Address/Mask	Enter the MAC address and the mask of the computer where the packets will be sent to.

Assign Classification Queue	Select the classification queue for the traffic class.
Mark DSCP	Select the DSCP to mark. Different markers representing different grades of service placed on various packet streams to be recognized by the router for route purposes.
Mark 802.1p Priority	If 802.1q was enabled on WAN, then select a value between 0-7.
Tag VLAN ID	Enter a VLAN ID for the packet to tag.

6.8 Routing

6.8.1 Default Gateway

This page allows you to select a preferred WAN interface to be the system's default gateway.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

6.8.2 Static Route

This page allows you to add the routing table. A maximum of 32 entries can be configured.

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

Destination	Subnet Mask	Gateway	Interface	Remove
192.168.1.244	255.255.255.0	192.168.1.1	ppp0	<input type="checkbox"/>

Click **Add** to configure the routing table. Enter the routing information and then click **Save/Apply**.

Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

Use Interface

Use Gateway IP Address

Field	Description
Destination Network Address	Enter the destination address of the LAN IP.
Subnet Mask	Enter the subnet mask of the LAN IP.
Use Interface	Check and select a WAN interface for static route.
Use Gateway IP Address	Check and enter the gateway address of the remote router.

6.8.3 RIP

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the "Enabled" checkbox. To stop RIP on the WAN Interface, uncheck the "Enabled" checkbox. Click **Save/Apply** to star/stop RIP and save the configuration.

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
WAN Interface not exist for RIP.			

6.9 DNS

6.9.1 DNS Server

This page allows you to enable automatic DNS from the ISP or specify their own DNS server address manually.

DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:

WAN Interface selected:

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Field	Description
Obtain DNS Info from a WAN	Select the WAN interface to obtain the DSN info.
Use the Following Static DNS IP Address	Select to configure the static DNS IP address manually.
Primary DNS Sever	Enter the IP address of primary DNS server.
Secondary DNS Sever	(Optional) Enter the IP address of secondary DNS server.

6.9.2 Dynamic DNS (DDNS)

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

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
dyndns	Lucky1	dyndns	ppp0	<input type="checkbox"/>

Click **Add** to configure the DDNS. This page allows you to set up DDNS address from DynDNS.org. You must register with the service provider first and obtain the necessary information. Enter the DDNS information and then click **Save/Apply**.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org.

D-DNS provider:

Hostname:

Interface:

DynDNS Settings

Username:

Password:

Field	Description
D-DNS Provider	Freeway DSL is pre-configured with the DynDNS.org as DDNS provider.
Hostname	Enter the host name.
Interface	Select a WAN interface to apply DDNS service.
DynDNS Username / Password	Enter username and password of your account on DynDNS.org.

6.10 DSL

This page allows you to select the modulation, phone line type and capability specified by your ISP. The default configuration in this page can work with most ADSL implementations. DO NOT change any setting unless you are instructed to do so. Then click **Save/Apply**.

DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

If you want to configure more advanced setting, click **Advanced Settings**. Select the test mode for DSL line.

DSL Advanced Settings

Select the test mode below.

- Normal
- Reverb
- Medley
- No retrain
- L3

6.11 UPnP

This page allows you to enable the UPnP function. The UPnP function allows devices to connect seamlessly and to simplify the implementation of networks such as data sharing, communications and entertainment.

The UPnP feature requires one active WAN interface. You must create one WAN connection before you can enable this function. In addition, the client connecting to the Freeway DSL should also support this feature.

Upnp Configuration

Enable Upnp protocol.

6.12 DNS Proxy

The Freeway DSL can act as a DNS proxy when you enable DNS proxy feature.

Dns Proxy Configuration

Enable Dns proxy.

Host name of the modem:

Domain name of the LAN network:

Field	Description
Enable DNS Proxy	Check to enable DNS proxy feature.
Host Name of the modem	Enter a host name for the Freeway DSL.
Domain name of the LAN Network	Enter a name for this LAN network.

6.13 USB Storage

This page shows the information of USB mass storage. Open a file explorer window and type in the address field:


\\192.168.1.1\DeviceName

where "DeviceName" is the name that was assigned to the storage device.

You can click **Browse** to access the contents on this USB drive.

USB Storage

This page show the USB mass storage!



usb1_1

3814Mb(2081Mb Free)

[Browse](#)

6.14 Print Server

This page allows you to enable the on-board print sever. A USB printer can be connected to the Freeway DSL and used as a network printer.

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name

Make and model

Before connecting your printer to the print server, be sure to install the driver provided by the printer manufacturer on each PC that will use the printer.

1. Plug your USB printer into one of the USB ports on your PC.
2. Install the printer by following the installation instructions included with your printer.
3. You may print a test page to ensure that the printer is working properly.
4. Power off your PC.
5. Disconnect the printer from your PC and plug this thin rectangular end of the USB cable into one of the USB host ports on the Freeway DSL.
6. Connect the power supply to your printer and turn it on.
7. Launch a Web browser. In the location or address field, enter 192.168.1.1 and press **Enter**.



Note

If you have modified your gateway's IP address, enter the new IP address instead of 192.168.1.1.

8. When the user name and password window appears, enter the user name and the password. Click **OK** to login to the Web Application.
9. Select **Print Server** from the **Advanced Setup** menu. Enter the printer name and its manufacturer/model information you want to save for it. Click **Save/Apply**.
10. Write down the printer location address. You need the address to set up the printer on computers that are connected to your network.
11. Windows XP Users: Click **Windows Start -> Printers and Faxes**; Windows 2000 Users: Click **Windows Start -> Settings -> Printers**.
12. Click **Add a Printer**. The Add Printer Wizard will start. Click **Next**.
13. Choose the radio button labeled **A network printer, or a printer attached to another computer**. Click **Next**.
14. Select **Connect to a printer on the Internet or on a home or office network**. In the URL field, enter the printer location address you wrote down at step 10. Click **Next**.



Note

The URL information is case-sensitive and must be exactly matched as it is shown on step 10.

15. Select the manufacturer and model of your printer. Click **OK**. If your printer does not appear in the list, please go back to step 1 to 4 to install the printer driver to this PC.
16. When prompted, you may select **Yes** to set this printer as your default printer.
17. The information of printer will be displayed. Click **Finish** to complete the installation.

6.15 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping 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.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0	ENET(1-3)	
			USB	
			wlan0	
			wl0_Guest1	
			wl0_Guest2	
			wl0_Guest3	

Click **Add** to create new interface group. To support Interface Grouping feature, you must create mapping groups with appropriate LAN and WAN interfaces. Then click **Save/Apply**. Only the default group has IP interface.

Group Name:

WAN Interface used in the grouping

Grouped LAN Interfaces

->

<-

Available LAN Interfaces

ENET(1-3)

USB

wlan0

wl0_Guest1

wl0_Guest2

wl0_Guest3

Automatically Add Clients With the following DHCP Vendor IDs

Field	Description
Group Name	Enter a name for this group.
WAN Interface used in the grouping	Select a WAN interface used in this grouping from the drop-down list.
Grouped LAN Interfaces	Select interfaces from the Available LAN Interfaces list and use the arrow buttons to map them to the Grouped LAN Interfaces list.
Available LAN interfaces	These are the available LAN interfaces on Freeway DSL.
Automatically Add Clients with the following DHCP Vendor IDs	Configure a DHCP vendor ID. Any DHCP client requests with the specified vendor ID will be denied an IP address from the local DHCP server.

IMPORTANT!

If a vendor ID is configured for a specific client device, you have to reboot the client device attached to the Freeway DSL to allow it to obtain an appropriate IP address.

6.16 LAN Ports

This page allows you to enable/disable the Virtual LAN Ports feature.

LAN Ports Configuration

Use this page to enable/disable the Virtual LAN Ports feature.

ENET(1-3)

Apply/Save

LAN Port
ENET4
ENET(1-3)
wlan0

6.17 IPSec

This page shows the IPSec Tunnel connection.

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
new connection	61.56.142.33	192.168.1.100	61.56.124.33	<input type="checkbox"/>

Click **Add New Connection** to add a new IPSec Tunnel connection. Enter the setting for IPSec connection and then click **Save/Apply**.

IPSec Settings	
IPSec Connection Name	<input type="text" value="new connection"/>
Remote IPSec Gateway Address (IP or Domain Name)	<input type="text" value="0.0.0.0"/>
Tunnel access from local IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Tunnel access from remote IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Key Exchange Method	<input type="text" value="Auto(IKE)"/>
Authentication Method	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key	<input type="text" value="key"/>
Perfect Forward Secrecy	<input type="text" value="Disable"/>
Advanced IKE Settings	<input type="button" value="Hide Advanced Settings"/>
Phase 1	
Mode	<input type="text" value="Main"/>
Encryption Algorithm	<input type="text" value="3DES"/>
Integrity Algorithm	<input type="text" value="MD5"/>
Select Diffie-Hellman Group for Key Exchange	<input type="text" value="1024bit"/>
Key Life Time	<input type="text" value="3600"/> Seconds
Phase 2	
Encryption Algorithm	<input type="text" value="3DES"/>
Integrity Algorithm	<input type="text" value="MD5"/>
Select Diffie-Hellman Group for Key Exchange	<input type="text" value="1024bit"/>
Key Life Time	<input type="text" value="3600"/> Seconds
<input type="button" value="Save / Apply"/>	

Field	Description
IPSec Connection Name	Enter a name for this IPSec connection.
Remote IPSec Gateway Address	Enter the IP address or domain name of the remote IPSec gateway.
Tunnel Access From Remote / Local IP Addresses	Select the range of local / remote IP addresses from the drop-down list.
IP Address for VPN	Specify the remote / local IP address for VPN.
IP Subnet Mask	Specify the subnet mask for the remote / local IP address.
Key Exchange Method	Select the key exchange method to be auto or manual.
Authentication Method	Select the authentication method to be Pre-Share Key or Certificate X.509.

Pre-Shared Key	Specify the Key if you select the authentication method as Pre-Shared Key.
Certificate	Select the certificate from drop-down list if you select the authentication method as Certificate X.509.
Perfect Forward Secrecy	Select to enable or disable Perfect Forward Secrecy (PFS) feature.
Encryption Algorithm	Select the encryption algorithm to be DES, 3DES or AES (aec-cbc).
Encryption Key	Enter the encryption key to be 3DES or AES (Advanced Encryption Standard).
Authentication Algorithm	Select the authentication algorithm from drop-down list.
Authentication Key	Enter the authentication key to be MD5 or SHA1.
SPI	Enter the SPI (Security Parameter Index) which is an identification tag added to the header tunneling the IP traffic.

There are two phases of IPSec:

Phase 1: Start to negotiate IKE parameters including encryption, integrity (hash), Diffie-Hellman parameter values and lifetime to protect the following IKE exchange. The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority to match with its policies. This sets up a secure tunnel for IKE Phase 2.

Phase 2: Start to negotiate IPSec security for the following IKE exchange and mutual examination of the secure tunnel establishment.



Note

It is critical that the exact same Phase 1 and Phase 2 proposals be entered at the remote client.

Field	Description
Advanced IKE Settings	This button is available when you select the Key Exchange Method as Auto mode.
Mode	Select the mode to be Main or Aggressive.
Encryption Algorithm	Select the encryption algorithm to be DES, 3DES, AES-128, AES-196 or AES-256.
Integrity Algorithm	Select the integrity algorithm to be MD5 or SHA1.
Select Diffie-Hellman Group for Key Exchange	Select the Diffie-Hellman group to be 768, 1024, 1536, 2048, 3072, 4096, 6144 or 8192-bit for key exchange.
Key Life Time	Configure the life time for Key (in second).

6.18 Certificate

This section allows you to create certificates.

6.18.1 Local

This page allows you to create local certificate. Local certificates are used by peers to verify your identity. You can either create certificate request or import the certificate to add local certificates. Maximum 4 certificates can be stored.

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
<input type="button" value="Import Certificate"/>				

Click **Import Certificate** to import the certificate.

Enter a certificate name, paste the certificate content and private key to create the certificate. Then click **Apply**.

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
h3w9G+zFH6LPLRwCBze13c7bpQu5MyXugwD
iH9fVRGQdPDEP1fZCWQBiIF3KzPEDk0CAwEA
AG6Ag0+cAKg14E4o5xoR8J6GehNPSKh/+oY
ats tq9G6Rs ch33Zq txJ tOq76R9D1jUnGSR8dsf
Y0ZYVavStvJBySkqTJM8j82r8kA/J8pbJ=
MIIB/TCCA WYCAQAwgbwx CzAJBgNVBAYTAk
BxMGS2FuYXRhMR8wHQYD VQKQExZKZWFuL
VQQLExRUCnV1IFdheSBTdXBw bGVtZW50czEj
dXBw bGVtZW50cy5jb20xKjAoBgkqhkiG9w0B
ZW11bnRzLmNvbTCBnzANBgkqhkiG9w0BAQE
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
g+uHJHj4fYzFNjCRksA92BVa/GHn3cPuwQJAVzJIR1eH/u
6XtJ3J9PKJDYXzGvMLa6pVG2mGLqM0nDpL06/wKVIz0+
3t6H0eE14Y4PzLiU4Pv+Z3K18hFgkTSbFLuKenXkwC+IKj
YCLSo tHXhLSvATXpwQJBAMrXc002WRJ9+bFokw3HZAI
8biqLXYJ aZLJqsMQBd/YB1vIMhf0JHUJKJTYtys tyt=
9KbJjh42/uSBMW5D1lGgREFjc+Bol/DZJii5zgINhKlSus3Ff
zNk fI03xNWAP0ELhysMYwyoV8BGHfD0b7MUfos8tHAIH
MndaYnaMKNP31B2qMqNW0EInFVuIf19VEZB08MQ+V9kJ
AoGA09sFz31cic/5xhWjY7zk4CP3JFz7+0bWTiU3539TNw
w8iEXO f0I72qY210f3mNhz2IhIB8P0ih07BnvapKEdAbs7
Iy8gmHtRJ+OyyfukXqfQxsEWF6ir90zr8wRORGaJ+T72G
9KbJjh42/uSBMW5D1lGgREFjc+Bol/DZJii5zgINhKlSus3Ff
wHT1iw6NAkEA8xdYaHbDS1EYD5UBTrvcfFmVAZA2qZk
-----END RSA PRIVATE KEY-----
```

6.18.2 Trusted CA

If an entity wants to utilize digital certificates, this entity should retrieve certificates of trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers. Maximum 4 certificates can be stored.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Name	Subject	Type	Action
<input type="button" value="Import Certificate"/>			

Click **Import Certificate** to import the certificate. Enter a certificate name and paste the certificate content to create the certificate. Then click **Apply**.

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

```

-----BEGIN CERTIFICATE-----
zNkf103xNWAP0BLhysMYwyoV8BGHfD0b7MUfos8tHAIH
9KbJjh42/uSBMW5D1lGgREFjc+Bo1/DZJii5zgINhKlSus3Ff
MndaYnaMGNP31B2qMqNW0EInFVuIf19VEZB08MQ+V9kJ
AoGA09sFz31cic/5xhWjY7zk4CP3JFz7+0bWTiU3539TNw
w8iHXOf0172qY210f3mNh2IhIB8P0ih07BnvapKEdAbs7
Iy8gmHtRJ+OyyfukXqfQxsEWF6ir90zr8wRORGaJ+T72G
g+uHJHj4fYzFNjCRksA92BVa/GHn3cPuwQJAVzJIR1eH/u
9KbJjh42/uSBMW5D1lGgREFjc+Bo1/DZJii5zgINhKlSus3Ff
wHT1iw6NAkEA8xdYaHbDS1EYD5UBTrvcfFmVAZA2qZk
6XtJ3J9PKJDYXzGvMLa6pVG2mGLqM0nDpL06/wKVIz0+
3t6H0eE14Y4PzLiU4Pv+Z3Ki8hFgkTSbFLuKenXkwC+IKj
YCLSothXhLSvATXpwQJBAMrXc002WRJ9+bfokw3HEAI
8biqLXYJaZLJqsMQBd/YBlvDMhfOJHUJKJTYtys tyt=
-----END CERTIFICATE-----

```

7. Wireless

This section allows you to configure wireless settings on the Freeway DSL.

7.1 Basic

This page allows you to configure basic features of wireless feature. 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.

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/Save" to configure the basic wireless options.

Enable Wireless
 Hide Access Point
 Clients Isolation
 Disable WMM Advertise
 Enable Wireless Multicast Forwarding (WMF)

SSID: BSSID: 00:1A:2B:14:D Country:
 Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wlo_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wlo_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wlo_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

Field	Description
Enable Wireless	Check to enable wireless feature.
Hide Access Point	Check to disable advertising the SSID of the access point (AP) in broadcast messages to wireless clients. Wireless clients will need to know the SSID if they want to join the network.
Clients Isolation	Check to prevent wireless clients from seeing each other.
Disable WMM Advertise	Check to disable WMM (Wi-Fi Multimedia). WMM allows the network packets of the multimedia application to have priority over regular data network packets, allowing multimedia applications to run smoother and with fewer errors.
Enable Wireless Multicast Forwarding (WMF)	Check to enable WMF feature.
SSID (Station Set Identifier)	Enter a name for your wireless network. Wireless clients must be configured with the correct SSID to access the wireless network.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS

	(Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC address of the AP and in Independent BSS or ad-hoc networks, the BSSID is generated randomly.
Country	Select your country from the drop-down list.
Max Clients	Enter the maximum number of wireless clients that are allowed to connect to the AP (Access Point) at the same period.
Wireless-Guest/Virtual Access Points	Check to enable virtual AP. It appears to be an independent physical AP, when in actuality there is only a single physical AP. Virtual AP allows you to control wireless clients' access and security settings. Wireless guests can access Internet through these guest accounts without compromising the integrity of your network.

7.2 Security

This page allows you to configure security features of the wireless LAN interface. You can set up configuration manually or through Wi-Fi protected Setup (WPS). WPS (WSC*) uses a push-button or a PIN to simplify the secure network setup. With WPS, Freeway DSL can automatically set the SSID or network name as part of the setup process and provide strong encryption keys to client devices. You do not need to configure SSID, wireless security setting, etc., in the client software. In order to use WPS (WSC), the wireless client software must also support WPS.

*WSC (Wi-Fi Simple Configuration) is a former name of WPS.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS(WSC) Setup

Enable WPS(WSC)

Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)

Push-Button PIN

[Help](#)

Set WSC AP Mode

Device PIN [Help](#)

WPS(WSC) Add External Registrar

Field	Description
Enable WSC (WSC)	Select to enable or disable WPS (WSC).
Setup AP by Push-Button / PIN	Select to set up the AP by push-button or PIN (Personal Identification Number) to simplify the secure network setup.
Push-Button	Select it to start WSC by simply pushing a button, either an actual button or a software one, on both WPS (WSC) AP and clients to connect. The push-button of WSC is labeled as WPS on the upper case of Freeway DSL.
PIN	Select it to start WPS (WSC) by using a same 8-digit PIN (Device PIN) in both AP and WPS (WSC) clients to make the connection.

Set WSC AP Mode	Select the WPS (WSC) AP mode.
Add Enrolee	Click it to start WSC by the means of push-button or PIN. This button acts the same function as the physical button on the upper case of the Freeway DSL when you select using Push-Button to be the setup AP method. The WPS LED on the Freeway DSL will blink slowly for 2 minutes when the Freeway DSL is waiting for incoming WSC request.
Device PIN	Device PIN is generated by the Freeway DSL. This PIN changes every time you reboot the Freeway DSL.
WSC Add External Registrar	Click Start AddER button to start external registrar.

You can also set up the AP manually. Depending on the network authentication you selected, the screen will change accordingly so that additional fields can be configured for the specific authentication method.

Manual Setup AP

You can set 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 "Save/Apply" when done.

Select SSID:

Network Authentication:

WEP Encryption:

Field	Description
Select SSID	Select the SSID from the drop-down list.
Network Authentication	<p>Select the authentication to be used.</p> <ul style="list-style-type: none"> • 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 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. • 802.1: 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, WPA uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption, which is disabled). TKIP uses 128-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, perpacket key construction, and key management that WPA provides in the enterprise environment. The main difference is that the password is entered manually. • WPA2 (Wi-Fi Protected Access 2): Second generation of WPA,

	<p>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.</p> <ul style="list-style-type: none"> • 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 a re-key interval time. • Mixed WPA2 / WPA: During transitional times for upgrades in the enterprise environment, this mixed authentication method allows upgraded users and users not yet upgraded to access the network via the router. RADIUS (Remote Authentication Dial-In User Service) 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.
WEP Encryption	Select to enable or disable WEP (Wired Equivalent Privacy).
Encryption Strength	Select the encryption strength to be 64 or 128-bit.
Current Network Key	Select the network key from 1 to 4 from drop-down list.
Network Key 1-4	Enter 4 sets of network key in each field.
RADIUS Server IP Address	Enter the IP address of RADIUS server.
RADIUS Port	Enter the port number for RADIUS server IP address.
RADIUS Key	Enter the key for RADIUS server. The key you set must be the same one as configured in the RADIUS server.
WPA Group Rekey Interval	Enter the re-key interval for WPA.
WPA Encryption	Select WPA encryption to be TKIP, AES or TKIP+AES.
WEP Encryption	Select to enable or disable WEP encryption.
WPA Pre-Shared Key	Enter the PSK for WPA.
WPA2 Preauthentication	Select to enable or disable WPA2 preauthentication.
Network Re-auth Interval	Specify the interval for network re-authentication.

7.3 MAC Filter

This function allows you to manage whether a wireless client is allowed to access the Freeway DSL or not based on the MAC address of device.

Select the **MAC Restrict Mode** you want to use and then click **Add** to add the MAC address to the wireless MAC address filters.

Wireless -- MAC Filter

Select SSID:

MAC Restrict Mode: Disabled Allow Deny

MAC Address	Remove
00:50:FF:CC:11:22	<input type="checkbox"/>

Field	Description
MAC Restrict Mode	Select to disable, allow or deny the access of Freeway DSL based on the client's MAC address.

Enter the MAC address to the wireless MAC address filters. Then click **Save/Apply**.

Wireless -- MAC Filter

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

MAC Address:

7.4 Wireless Bridge

This page allows you to configure the Freeway DSL as a bridge. Wireless bridge feature provides a wireless link between WLAN segments to extend the coverage range. If configure the Freeway DSL to bridge mode, then Access Point features is disabled.

In this next screen you can select the mode, either access point or wireless bridge that you want the router to be in. In the screen below, Bridge Restrict is enabled, therefore you see the Remote Bridges MAC Address fields. If Bridge Restrict is disabled, then there is nothing left to do afterwards. Click **Save/Apply** to continue.

AP Mode:	<input type="text" value="Access Point"/>
Bridge Restrict:	<input type="text" value="Enabled"/>
Remote Bridges MAC Address:	<input type="text"/> <input type="text"/>
	<input type="text"/> <input type="text"/>
<input type="button" value="Refresh"/> <input type="button" value="Save/Apply"/>	

Field	Description
AP Mode	Select to enable AP (Access Point) or disable AP (Wireless Bridge).
Bridge Restrict	If AP Mode is set to Bridge and this field set to Enabled, it allows you to specify the available bridges. If Bridge Restrict is disabled, any wireless bridge within range may connect. If you select Enabled(Scan), the AP will scan for available wireless bridges and display its MAC address it found.
Remote Bridges MAC Address	Enter (Bridge Restrict in Enabled mode) or select (Bridge Restrict in Enabled (Scan) mode) the remote bridge MAC address if Bridge Restrict is enabled.
Refresh	Click this button to update the remote bridges. Updating will take few seconds.

7.5 Advanced

This page allows you to configure setting for advanced wireless features.

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/Save" to configure the advanced wireless options.

Band: Current: 1

Channel: Current: 1

Auto Channel Timer(min):

802.11n/EWC:

Bandwidth: Current: 20MHz

Control Sideband: Current: None

802.11n Rate:

802.11n Protection:

Support 802.11n Client Only:

54g™ Rate:

Multicast Rate:

Basic Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Global Max Clients:

XPress™ Technology:

Transmit Power:

WMM(Wi-Fi Multimedia):

WMM No Acknowledgement:

WMM APSD:

Field	Description
Band	The supported band is 2.4GHz.
Channel	Select the channel you want to use. The wireless network is divided into several channels (region depends). Each channel broadcasts on a slightly different frequency; if you are experiencing interference with another device such as a baby monitor, security alarm, or cordless phone, then change the channel on your Freeway DSL.
Auto Channel Timer	This value cannot be changed.
802.11n/EWC	Enhanced Wireless Consortium
Bandwidth	Select the bandwidth to be either 20MHz or 40MHz (dual channel), that the Freeway DSL will use if 802.11n/EWC is configured as Auto and the Channel is configured as Auto . If the Freeway DSL detects other adjacent wireless networks, it will use 20 MHz operation so as to not interfere with the networks. If no other adjacent networks are detected, the Freeway DSL will use 40MHz operation. In both 20 MHz and 40 MHz operation, when the 802.11n/EWC is configured to Auto , the Freeway DSL will use

	dynamic channel selection to determine the best channels to transmit in order for optimal operation.
Control Sideband	Select the extension channel to be in the Upper or Lower sideband.
802.11n Rate	Set the 802.11n rate. These rates are only applicable when the 802.11n/EWC is configured as Auto .
802.11n Protection	Select Auto if there is a possibility that 802.11b or 802.11g devices will use your wireless network. In Auto mode, the wireless devices use RTS/CTS to improve 802.11n performance in mixed 802.11g/802.11b networks. Select Off to maximise 802.11n throughput under most conditions.
Support 802.11n Client Only	Select On to support 802.11n clients only
54g™ Rate	This value cannot be changed.
Multicast Rate	Use the default setting "Auto" unless there is a specific requirement for multicast.
Basic Rate	Use the default setting "Auto" unless there is a specific requirement for basic rate.
Fragmentation Threshold	Specify a value between 256 (min) and 2346 (max). This value determines whether packets will be fragmented and at what size.
RTS Threshold	Specify a value to determine the packet size of a transmission through the use of the router to help control traffic flow. The default value of 2347 (maximum length) disables RTS (Request To Send) Threshold.
DTIM Interval	Specify the wake-up interval for clients in power-saving mode. DTIM (Delivery Traffic Indication Message) is as known as Beacon Rate.
Beacon Interval	Specify the amount of time between beacon transmissions.
Global Max Clients	Specify the maximum clients that are allowed to connect to the Freeway DSL.
Xpress™ Technology	Select to enable or disable Xpress™ Technology. Xpress™ Technology is a Broadcom innovation. It 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.
Transmit Power	Select power output to be 20%, 40%, 60%, 80% and 100%.
WMM (Wi-Fi Multimedia)	Select the mode to "Auto" for automatically improves the experience for audio, video and voice applications over a Wi-Fi network.
WMM No Acknowledgement	Select to enable or disable WMM ACK. Enable this feature only when you are at a good communication quality and low interference area.
WMM APSD	Select to enable or disable ASPD (Automatic Power Save Delivery). It is a more efficient power management method for low power consumption.

7.6 Station Info

This page shows the connected wireless stations and their status.

Wireless -- Authenticated Stations				
This page shows authenticated wireless stations and their status.				
MAC	Associated	Authorized	SSID	Interface
00:21:00:21:6B:A9	Yes		BrcmAP0	wl0

8. Diagnostics

This page shows the ADSL diagnostic information. Usually, you do not have to view this data, but you may find it useful when working with your ISP to diagnose network and Internet data transmission problems.

pppoe_0_0_33 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 ENET4 Connection:	PASS	Help
Test your ENET(1-3) Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	PASS	Help
Test ATM OAM F5 segment ping:	PASS	Help
Test ATM OAM F5 end-to-end ping:	PASS	Help

Test the connection to your Internet service provider

Test PPP server connection:	PASS	Help
Test authentication with ISP:	PASS	Help
Test the assigned IP address:	PASS	Help
Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

9. Management

This section allows you to maintain the system, including backing up the configurations, viewing system log, maintaining access control and updating software.

9.1 Settings

9.1.1 Backup

This page allows you to backup (copy) current settings to a file on your PC.

Settings - Backup

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

9.1.2 Update

This page allows you to restore the settings from a previously saved file.

Tools -- Update Settings

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

Settings File Name:

To restore a previously saved configuration file onto the Freeway DSL, click **Browse** to find the file on your PC and click **Update Settings**. The Freeway DSL restores settings and reboots to activate the restored settings.

9.1.3 Restore Default

This page allows you to reset the configuration to default settings. It deletes all current settings and resets the Freeway DSL to factory default settings.

Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

Click **Restore Default Settings** and click **OK** when the pop-up window appears confirming that you want to restore factory default settings to your Freeway DSL. The Freeway DSL restores the default settings and reboots.

IMPORTANT!

DO NOT power off the Freeway DSL or press the reset button while this process is in progress.

9.2 System Log

This dialog allows you to view system log and configure system log options. To view the System Log, click **View System Log**. To configure System Log, click **Configure System Log**.

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.

9.2.1 Configure System Log

This page allows you to configure the system log level and display level. You must enable the System Log function so that the Freeway DSL can log the selected events.

Log: Disable Enable

Log Level:

Display Level:

Mode:

Server IP Address:

Server UDP Port:

Field	Description
Log Level	Select level of application events to log.
Display Level	Select level of application events to display.
Mode	Select to record the events in the local memory, sent them to a remote system log server or both.
Server IP Address	Enter the IP Address of remote system log server.
Server UDP Port	Enter the UDP port of the remote system log server.

9.2.2 View System Log

This page shows the events of Freeway DSL. If the system log feature is enabled, the system will log selected events. All events above or equal to the selected log level will be logged and displayed.

System Log			
Date/Time	Facility	Severity	Message
Jan 1 01:37:50	syslog	emerg	BCM96345 started: BusyBox v1.00 (2008.11.10-07:45+0000)

9.3 SNMP Agent

The SNMP (Simple Network Management Protocol) allows the management application to retrieve statistics and status from the SNMP agent in this device.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:

Set Community:

System Name:

System Location:

System Contact:

Trap Manager IP:

Field	Description
Read Community	Enter the password (character string) to specify the read privilege between the SNMP agent and manager.
Set Community	Enter the password (character string) to specify the write privilege between the SNMP agent and manager.
System Name	Enter the System name of the SNMP agent
System Location	Enter the System location of the SNMP agent
System Contact	Enter the System contact of the SNMP agent.
Trap Manager IP	Enter the IP address of the Trap Manager.

9.4 TR-069 Client

The Freeway DSL includes a TR-069 client which is a WAN management protocol. All the values are already filled in.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client: ▾

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Field	Description
Inform	Enable or disable the Freeway DSL to connect to the ACS periodically.
Inform Interval	Enter the amount of time (in second) between a successful connection with an ACS server and a new attempt to connect to an ACS server. This field is enabled only when the Inform Enabled is selected.
ACS URL	Enter the URL of the Auto Configuration Server (ACS) provided by the ISP.
ACS User Name	Enter the user name for the ACS to authenticate.
ACS Password	Enter the password for the ACS to authenticate.
WAN Interface Used by TR-069 Client	Select the WAN interface from the drop-down for TR-069 client to use.
Display SOAP messages on serial console	Enable or disable whether display SOAP messages on serial console or not.
Connection Request Authentication	Check to enable connection request authentication.
Connection Request User Name	Enter the username used to authenticate an ACS making a connection request to the Freeway DSL.
Connection Request Password	Enter the password used to authenticate an ACS making a connection request to the Freeway DSL.
Connection Request URL	This is the URL of connection request.
GetRPCMethods	Click this button to force the Freeway DSL to immediately establish a connection to the ACS.

9.5 Internet Time

This page allows you to manually configure the time and select Time Zone.

Time settings

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

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Third NTP time server:

Fourth NTP time server:

Fifth NTP time server:

Time zone offset:

Field	Description
Automatically synchronize with Internet time server	Check to enable the Freeway DSL to synchronize with Internet time server to update the system clock.
First/ Second/ Third/ Fourth/ Fifth NTP time server	Select at least one Internet time server from drop-down list or specify its IP address manually.
Time Zone Offset	Select The time zone in which the Freeway DSL resides.

9.6 Access Control

9.6.1 Passwords

This page allows you to change the password for all users account. Access to your Freeway 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 the Freeway DSL

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

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

Username:

Old Password:

New Password:

Confirm Password:

Field	Description
Username	Enter the pre-defined username from drop-down list.
Old Password	Enter the old password of this account.
New Password	Enter the new password for this account.
Confirmed Password	Enter the new password for this account again to confirm the password.

9.6.2 Services

This page allows you to enable or disable the services from being used for WAN.

Access Control -- Services

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

Services	WAN
FTP	<input type="checkbox"/> Enable
HTTP	<input type="checkbox"/> Enable
ICMP	<input type="checkbox"/> Enable
SNMP	<input type="checkbox"/> Enable
SSH	<input type="checkbox"/> Enable
TELNET	<input type="checkbox"/> Enable
TFTP	<input type="checkbox"/> Enable

9.7 Update Software

The system software used by this Freeway DSL is called "firmware". This page allows you to upgrade the firmware to a newer version.

Tools -- 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:

This page allows you to update the software (firmware) of Freeway DSL to a newer version. If your ISP releases new software for Freeway DSL, follow these steps to perform an upgrade.

1. Obtain an updated software image file from your ISP.
2. Click Browse to locate the image file.
3. Click Update Software to upload the new image file.

DSL Router Update

Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.



Note

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

IMPORTANT!

DO NOT power off the Freeway DSL or press the reset button while this process is in progress.

9.8 Reboot

This page allows you to reboot the Freeway DSL.

Click the button below to reboot the router.

IMPORTANT!

DO NOT power off the Freeway DSL or press the reset button while this process is in progress.

10. Wall Mounting (Optional)

This product can be mounted on wall. There are two holes in the lower case and you can use the screws to mount the device.

Appendix A. Troubleshooting

Below is a list of commonly asked questions. Before calling technical support, please look through these issues to see if they help solve your problem.

The Freeway DSL is not functional.

1. Check to see that the POWER LED is lit and that the network cables are installed correctly. Refer to the Quick Start Guide for more details.
2. Check to see that the LAN, DSL and Internet LEDs are lit.
3. Check the settings on your PC and Freeway DSL. Again, refer to the Quick Start Guide for more details.
4. From your PC, can you PING the Freeway DSL? Assuming that the Freeway DSL has DHCP enabled and your PC is on the same subnet as the Freeway DSL, you should be able to PING the Freeway DSL.
5. Can you PING the Internet? Your ISP should have provided the IP address of their server. If you can ping the Freeway DSL and your protocols are configured correctly, you should be able to ping the ISP's network. If you cannot PING the ISP's network, make sure you are using the correct protocols with the correct VPI/VCI values.

I can't connect to the Freeway DSL.

1. Check to see that the POWER LED is lit and that the network cables are installed correctly.
2. Make sure that the PC and Freeway DSL is on the same network segment. The Freeway DSL's default IP address is 192.168.1.1. If you are running a Windows based PC, you can open a DOS window and type IPCONFIG; make sure that the network adapter that is connected to the Freeway DSL is within the same subnet.
3. Also, your PC's Subnet Mask should match the Freeway DSL's subnet mask. The Freeway DSL has a default subnet mask of 255.255.255.0.
4. If this still does not work, press the Reset button. This will place the Freeway DSL into its factory default state. Go through the above procedures again.

The DSL LED continues to blink but does not go solid.

1. Make sure you have DSL service. You should get some kind of information from your ISP which states that DSL service is installed. You can usually tell if the service is installed by listening to the ADSL phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The main cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.
3. Verify that the DSL line is connected directly to the wall and to the line input on the Freeway DSL.

The Internet LED is always off.

1. Make sure you have DSL service. You should get some kind of information from your ISP which states that DSL service is installed. You can usually tell if the service is installed by listening to the phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. Verify that the phone line is connected directly to the wall and to the line input on the Freeway DSL. If the Freeway DSL is connected to the wall line outlet via a splitter, make sure you connect the Freeway DSL to the port labeled MODEM.

The Internet LED is always red.

Make sure your account for the DSL service is correct. Re-type your username and password for the Internet account. The username and password are usually case sensitive. Make sure your Caps Lock key is not locked when entering the account.

I cannot ping the Freeway DSL from the attached LAN.

1. Verify that the IP addresses are properly configured. In most cases, you enable the Freeway DSL's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Freeway DSL and any attached LAN devices.
2. Make sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP correctly.

I cannot connect using the web browser.

1. Make sure you have configured the Freeway DSL with a valid IP address, subnet mask and default gateway.
2. Make sure you have a valid network connection to the Freeway DSL and the port you are using has not been disabled.
3. Make sure the cable between the attached PC and the Freeway DSL is firmly installed.

I forgot or lost the password.

Press the Reset button on the rear panel (holding it down for at least 8 seconds) to restore the factory default settings.

Appendix B. Specifications

Physical Interfaces	One ADSL port for WAN
	Four 10/100 Mbps Fast Ethernet ports for LAN
	One USB 2.0 host port for USB mass storage or printer
	Two antennas built-in for wireless wide coverage
	IEEE 802.11 b/g/n Wireless AP with WPS auto setup
ADSL Compliance	G.994
	G.992.1 (G.dmt) - Annex A and B
	G.992.2 (G.lite) - Annex A
	ANSI T1.413
	G.992.3 (ADSL2) - Annex A, B, L, and M
	G.992.5 (ADSL2+) - Annex A, B, and M
ATM Protocols	Up to 16 PVCs
	OAM F4/F5 loop back
	Adaptation Layers AAL5, AAL2 and AAL0 are supported
PPP Support	PPP over ATM PVC (RFC2364&RFC1577)
	PPP over Ethernet (RFC2516)
	Multiple PPPoE sessions on single PVC
	PPPoE pass through
	PAP, CHAP, MS-CHAP authentication supported
NAT	Static Port Mappings
	NAT/NAPT
Bridging	IEEE 802.1d Bridge
Routing	Static Route
	RIP v1 / v2
Multicasting	IGMP Proxy v1/v2/v3, IGMP snooping v1/v2
Management	SNTP, DDNS, UPnP, HTTP, FTP, TFTP, Telnet, SSH, SNMP, TR-069, DHCP client/server
Firewall / Security	SPI (Stateful Packet Inspection) Firewall
	Intrusion Alert
	Application layer gateway for H.323, SIP and IPSec/L2TP/PPTP
	Mac/IP/TCP/interface Filtering
	Denial of Service (DOS)
	Advanced DMZ
Quality of Service (QoS)	IPSEC / PPTP Pass through
	ATM QoS: CBR, rt-VBR, nrt-VBR, UBR-with-PCR, UBR, IP/Bridge/802.1P QoS
Environmental Specification	Power Input Device input power: 12V/1A
	Power Consumption: 15W
	Operating Temperature: 0 °C to 40 °C
	Operating Humidity: 95% (non-condensing)
Wireless Standards	IEEE 802.11b/g/n for Wireless LAN
Frequency Band	2.400 to 2.4835 GHz ISM band
Modulation	802.11n: OFDM (64QAM, 16QAM, QPSK, BPSK)
	802.11g: OFDM (64QAM, 16QAM, QPSK, BPSK)
	802.11b: CCK (11Mbps, 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
Data Rate	11 b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
	11n Draft 2.0 (20MHz): 13, 26, 39, 52, 78, 104, 117, 130 Mbps
	11n Draft 2.0 (40MHz): 27, 54, 81, 108, 162, 216, 243, 270, 300 Mbps
Encryption	Hardware-based IEEE 802.11i encryption /decryption engine, Includes 64-bit/128-bit WEP, TKIP, 802.1x, WPA/WPA2 and AES
Operating Range	Open space: 100m ~ 300m
	Indoor: 35m ~ 100m