

# Shiro

## **ADSL 2/2+ Ethernet USB Combo Router**

User Manual

VERSION 1.0



# Contents

<b>About this Manual .....</b>	<b>6</b>
<b>About the Router .....</b>	<b>7</b>
Requirements .....	7
Software .....	7
Hardware .....	7
Package Contents .....	8
Device Design.....	9
Front Panel .....	9
Back Panel .....	10
<b>Getting Started.....</b>	<b>11</b>
Remove or Disable Conflicts .....	12
Internet Sharing, Proxy, and Security Applications .....	12
Configuring TCP/IP Settings .....	13
Configuring Internet Properties .....	13
Removing Temporary Internet Files .....	13
Hardware Setup.....	15
Ethernet Connection.....	15
USB Connection .....	16
Connecting to the Internet .....	17

---

## **About the Web Manager ..... 19**

Accessing the Web Manager..... 19

Menus ..... 20

    Basic Menu..... 21

    Advanced Menu..... 22

    Help Menu ..... 23

## **Basic Menu ..... 24**

Home ..... 24

    Connection Information ..... 24

    Router Information..... 25

    Local Network Information..... 25

Quick Start ..... 25

## **Advanced Menu ..... 26**

WAN ..... 27

    New Connection ..... 27

    ADSL Modulation..... 33

    Connection Scan ..... 33

    Quickstart ..... 34

LAN ..... 35

    LAN Configuration ..... 35

    LAN Clients..... 40

Applications ..... 41

    Simple Network Timing Protocol (SNTP) ..... 42

    IGMP Proxy ..... 44

TR-068 WAN Access.....	46
DNS Proxy.....	47
Dynamic DNS Client.....	48
Port Forwarding.....	49
Bridge Filters.....	52
Web Access Control.....	53
<b>Quality of Service (QoS).....</b>	<b>54</b>
Egress.....	56
Ingress.....	59
QoS Shaper Configuration.....	63
Policy Routing Configuration.....	67
<b>Routing.....</b>	<b>70</b>
Static Routing.....	70
Routing Table.....	71
<b>Security.....</b>	<b>72</b>
IP Filters.....	72
LAN Isolation.....	74
<b>Status.....</b>	<b>75</b>
Connection Status.....	76
System Log.....	77
Remote Log.....	78
Network Statistics.....	80
DHCP Clients.....	81
QoS Status.....	82
Modem Status.....	83
Product Information.....	84
<b>Diagnostics.....</b>	<b>85</b>
Ping Test.....	85

---

Full Modem Test.....	86
<b>System Password .....</b>	<b>87</b>
Changing the System Password .....	87
Changing the Timeout Settings .....	88
<b>Firmware Upgrade .....</b>	<b>89</b>
<b>Save Settings.....</b>	<b>90</b>
<b>Restart Router .....</b>	<b>90</b>
<b>Restore to Default.....</b>	<b>90</b>
<b>Help Menu.....</b>	<b>91</b>

# About this Manual

This manual provides a description of the components, basic operation, and advanced configuration options of the router.

## Scope

This manual provides the installation instructions, router components, and configuration information through the Web manager.

## Target Audience

This manual is designed for users who are required to install and maintain the router. It assumes the user of this manual has basic knowledge and experience in configuring routers, computer networks, and computer systems.

## Document Structure

The manual is divided into the following sections:

<b>Chapter</b>	<b>About</b>
1	About this manual
2	About the router
3	Getting Started
4	About the Web Manager
5	Basic Menu
6	Advanced Menu
7	Help Menu

# About the Router

Congratulations on the purchase of your router. This router provides advanced features that allow you to converge your computer, Internet, and other network appliances into a single network through wired connection.

## Requirements

Your computer must meet the following minimum requirements.

### Software

#### Operating System:

- Any operating system can be used

#### Browser:

- Internet Explorer 4.0
- Netscape Navigator 3.02

### Hardware

- 233MHz processor
- CD-ROM Drive
- Ethernet network adapter
- USB port

# Package Contents

Package contents are listed below. For any missing items, please contact your dealer immediately.

Product contents vary for different models.

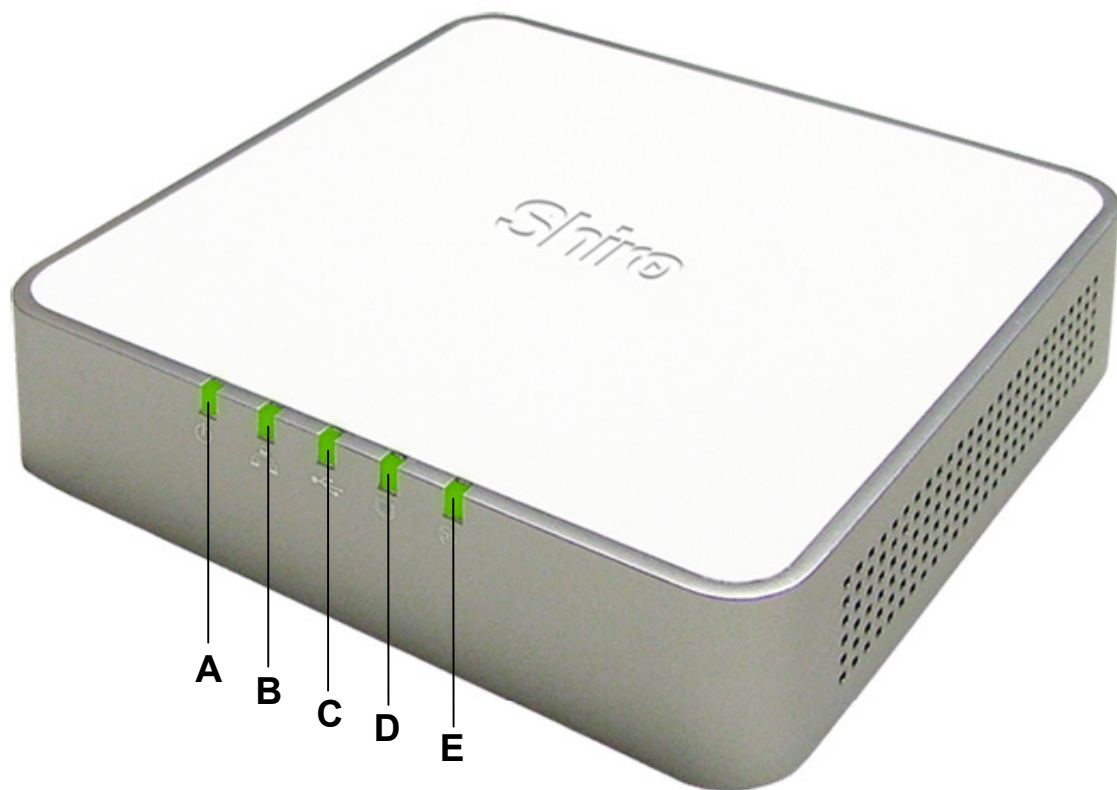
- Router
- Ethernet Cable
- USB Cable
- Telephone Cable
- POTS Splitter
- Power Adapter
- Installation CD
- Quick Start Guide
- Vertical Stand



# Device Design

## Front Panel

The LEDs on the front panel gives you an idea about the power and connection status.



	Label	Action	Description
<b>A</b>	<b>POWER</b>	Off	No power is supplied to the device
		Steady light	Connected to an AC power supply
<b>B</b>	<b>ETHERNET</b>	Off	No Ethernet connection
		Steady light	Connected to an Ethernet port
		Blinking light	Transmitting/Receiving data
<b>C</b>	<b>USB</b>	Off	No USB connection
		Steady light	Connected to a USB port
<b>D</b>	<b>DSL</b>	Off	No DSL signal

		Blinking light	Establishing DSL signal
		Steady light	DSL signal is established
<b>E</b>	<b>INTERNET</b>	Off	No Internet connection
		Steady green light	Connected to the Internet
		Blinking green light	Transmitting/Receiving data
		Red	Connection attempt failed

## Back Panel

The back panel provides ports to power up and connect the router into the network.

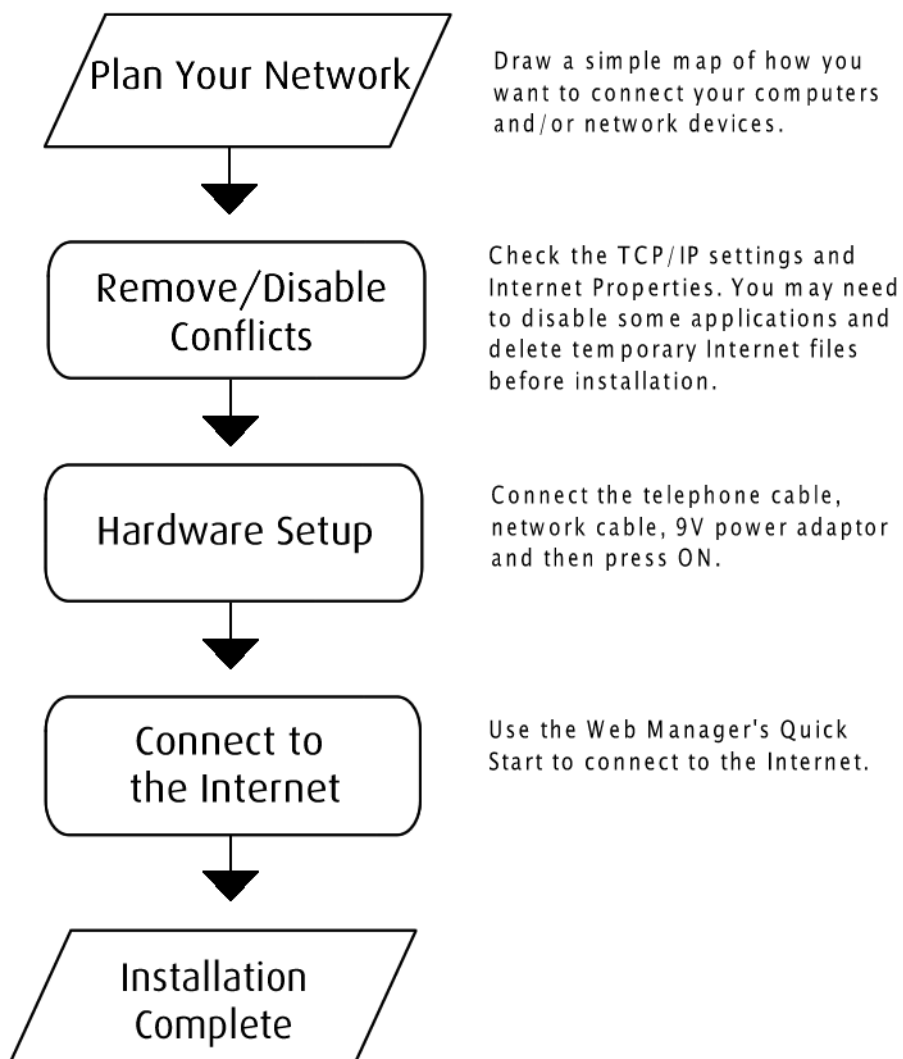


### Back Panel

Label	Used for...
<b>DSL</b>	Connecting the telephone cable
<b>USB</b>	Connecting with computers/devices through USB cable
<b>ETHERNET</b>	Connecting with computers/devices through Ethernet cable
<b>RESET</b>	Resetting the device. Press for 10 seconds to reset.
<b>9V DC</b>	Connecting with the 9V power adapter
<b>ON/OFF</b>	Switching the device on/off

# Getting Started

Setting up the device is easy. The flowchart below provides an outline of the steps you need to complete the installation. There are brief descriptions beside each step to help you along. Detailed instructions are provided in the subsequent pages.



## Remove or Disable Conflicts

To make sure the router installation moves on smoothly, you need to remove or disable conflicts that may interfere the installation. Probable conflicts may include:

- Internet sharing applications
- Proxy software
- Security software
- TCP/IP settings
- Internet properties
- Temporary Internet files

### Internet Sharing, Proxy, and Security Applications

Internet sharing, proxy software, and firewall applications may interfere with the router installation. These should be removed or disabled before you install and configure the router.

If you have any of the following or similar applications installed on your computer, remove or disable them according to the manufacturer's instructions.

---

<b>Internet Sharing Applications</b>	<b>Proxy Software</b>	<b>Security Software</b>
Microsoft Internet Sharing	WinGate	Symantec
	WinProxy	Zone Alarm

---

## Configuring TCP/IP Settings

Use the default TCP/IP settings to allow the router to provide a network address to the computer,

### To set the TCP/IP properties:

1. Select **Start > Run**. This opens the **Run** dialog box.
2. Enter **control ncpa.cpl** and then click **OK**. This opens the **Network Connections** in your computer.
3. Right-click **LAN** and then select **Properties**. This opens the **Local Area Connection Properties** dialog box.
4. Select **Internet Protocol (TCP/IP)** and then click **Properties**. This opens the **Internet Protocol (TCP/IP)** dialog box.
5. Select **Obtain an IP address automatically**.
6. Click **OK** to close the **Internet Protocol (TCP/IP)** dialog box.
7. Click **OK** to close the **Local Area Connection Properties** dialog box.

## Configuring Internet Properties

### To set the Internet Properties:

1. Select **Start > Run**. This opens the **Run** dialog box.
2. Enter **control inetcpl.cpl** and then click **OK**. This opens the **Internet Properties** dialog box.
3. Click **Connections** tab.
4. In the **Dial-up and Virtual Private Network settings** pane, select **Never dial a connection**.
5. Click **OK** to close the **Internet Properties** dialog box.

## Removing Temporary Internet Files

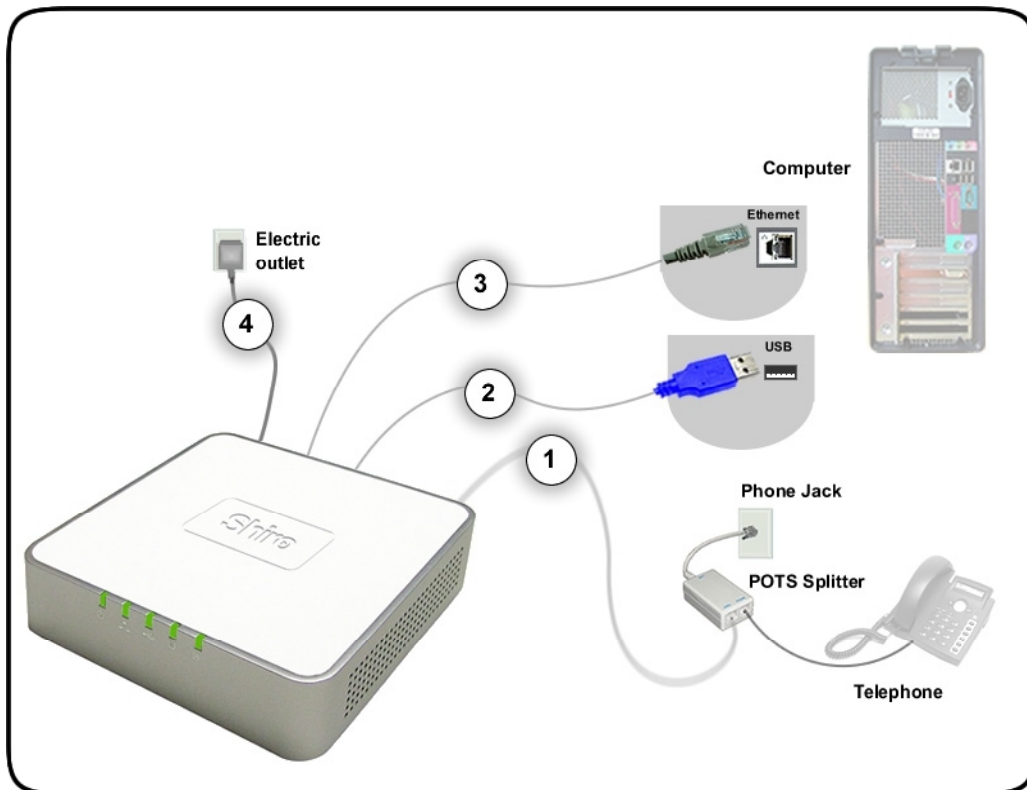
Temporary Internet files are files from Web sites that are stored in your computer. Delete these files to purge the Internet cache and remove footprints left by the Web pages you visited.

**To remove temporary Internet files:**

1. Select **Start > Run**. This opens the **Run** dialog box.
2. Enter **control** and then click **OK**. This opens the **Control Panel**.
3. Double-click **Internet Options**. This opens the Internet Options dialog box.
4. In the **Temporary Internet Files** pane, click **Delete Cookies**.
5. Click **Delete Files**.
6. Click **OK** to close the **Internet Properties** dialog box.

# Hardware Setup

When installing the router, the common practice is to have the router, the main computer, and phone jack in the same room. The room should also have enough electrical outlets to match your needs.



## Ethernet Connection

In terms of data transfer speed, the Ethernet provides the fastest mode of connection between the router and the computer.

### To connect through Ethernet:

1. Plug one end of the telephone cable from the POTS Splitter's **ADSL** port and then plug the other end into the router's **DSL** port

#### POTS Splitter

A phone line can carry phone call and Internet signals. When you enable the phone line for high speed Internet, the connection produces high-pitched tones when using the phone. Installing a Plain Old Telephone Service (POTS) splitter separates the two signals and eliminates the noise.

#### To setup the telephone POTS Splitter:

1. Locate the phone jack in your house.
2. Insert the POTS Splitter into the phone jack.
3. Plug one end of the telephone cable from the POTS Splitter's **TEL** port and then plug the other end into the telephone.

2. Plug one end of the Ethernet cable from the router's **ETHERNET** port and then plug the other end into the Ethernet port in your computer.
3. Connect the power adapter from the router's **9V DC** port into the electrical outlet and then press **ON**.

## USB Connection

You can also establish an additional connection with the computer using the USB port. When using the USB, you need to install the USB driver.

### **To install the USB driver and connect through USB:**

1. Plug one end of the USB cable from the router's **USB** port and then plug the other end into the computer's USB port.
2. Insert the **Resource CD** into your CD-ROM.
3. When the **Add Hardware Wizard** opens, follow the on-screen instructions. If asked to identify where to search for drivers, select **CD-ROM drivers**.
4. Follow the on screen instructions.

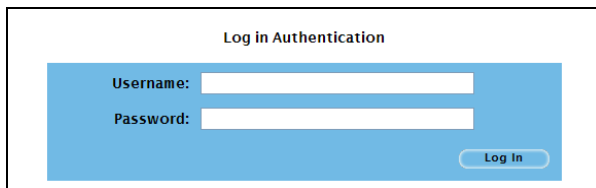


# Connecting to the Internet

Use Web Manager's Quick Start to connect to the Internet.

## To use Quick Start:

1. Open your browser.
2. Enter **192.168.1.1** in the address field and then press **Enter**. This opens the **Log In** page of Web Manager.
3. Enter the **Username** and **Password** for the Web Manager. The default Username and Password is **admin**.



Log In

4. Click **Log In**.

5. From the **Basic Menu**, click **Quick Start**.
6. Enter the **Username** and **Password** for your Internet account and then click **Connect**.

When the connection attempt is successful, the **Basic Home** page appears. When the connection attempt is not successful, a message will ask you to verify the Username and Password.

**Basic**  
Home  
Quick Start

**Advanced**  
WAN  
LAN  
Application  
QoS  
Routing  
Security  
Status  
Diagnostics  
System Password  
Firmware Upgrade  
Save Settings  
Restart Router  
Restore To Default

**Help**  
PPP Connection Help  
LAN Configuration  
Help  
LAN Clients Help  
Firewall Help  
Bridge Filters Help  
UPnP Help  
RIP Help  
QoS Help

**Basic > Home**

---

Connection Information		Router Information	
<b>DSL</b>	Down	<b>System Uptime</b>	0 hours 0 minutes
<b>Downstream / Upstream (Mbps)</b>	0/0	<b>Model</b>	DSL805EU
<b>Internet</b>	Not Connected	<b>Firmware Version</b>	113.100.1
<b>Connected Time</b>	0	<b>Build</b>	004
<b>Connection Type</b>	PPPoE	<b>Ethernet MAC address</b>	00:30:0A:77:0B:77
<b>Username</b>	username@ispname	<b>DSL MAC address</b>	00:30:0A:77:0B:79
<b>IP Address</b>	N/A	<b>NAT</b>	Enabled
<b>Default Gateway</b>	N/A	<b>Firewall</b>	Enabled
<b>Primary DNS</b>	N/A		
<b>Secondary DNS</b>	N/A		

[Connect](#)

---

**Local Network Information**

<b>LAN IP Address</b>	192.168.1.1
<b>DHCP</b>	Enabled
<b>DHCP Range</b>	192.168.1.2 - 192.168.1.254
<b>Ethernet</b>	Connected
<b>USB</b>	Connected

**Basic Home**

# About the Web Manager

The Web Manager is used to configure the router settings.

## Accessing the Web Manager

### To access the Web Manager:

1. Open a browser.
2. Enter the router's IP Address. The default IP Address is **192.168.1.1**.
3. When authentication is enabled, the log in page will appear. In the login page, enter the **Username** and **Password**. The default Username and Password is admin.
4. Click **Login**.

# Menus

The web interface includes the following menus:

- Basic Menu
- Advanced Menu
- Help Menu

# Basic Menu

The Basic Menu includes the Home and Quick Start links.

**Basic**  
Home  
Quick Start

**Advanced**  
WAN  
LAN  
Application  
QoS  
Routing  
Security  
Status  
Diagnostics  
System Password  
Firmware Upgrade  
Save Settings  
Restart Router  
Restore To Default

**Help**  
PPP Connection Help  
LAN Configuration  
Help  
LAN Clients Help  
Firewall Help  
Bridge Filters Help  
UPnP Help  
RIP Help  
QoS Help

**Basic > Home**

---

Connection Information		Router Information	
<b>DSL</b>	Down	<b>System Uptime</b>	0 hours 0 minutes
<b>Downstream / Upstream (Kbps)</b>	0/0	<b>Model</b>	DSL805EU
<b>Internet</b>	Not Connected	<b>Firmware Version</b>	113.100.1
<b>Connected Time</b>	0	<b>Build</b>	004
<b>Connection Type</b>	PPPoE	<b>Ethernet MAC address</b>	00:30:0A:77:08:77
<b>Username</b>	username@ispname	<b>DSL MAC address</b>	00:30:0A:77:08:79
<b>IP Address</b>	N/A	<b>NAT</b>	Enabled
<b>Default Gateway</b>	N/A	<b>Firewall</b>	Enabled
<b>Primary DNS</b>	N/A		
<b>Secondary DNS</b>	N/A		

[Connect](#)

---

**Local Network Information**

<b>LAN IP Address</b>	192.168.1.1
<b>DHCP</b>	Enabled
<b>DHCP Range</b>	192.168.1.2 - 192.168.1.254
<b>Ethernet</b>	Connected
<b>USB</b>	Connected

## Basic Menu

## Advanced Menu

The Advanced Menu provides advanced configuration settings for existing connections. At least one WAN connection must be configured before implementing advanced WAN configuration features. At least one LAN group must be defined before implementing advanced LAN configuration features.

The screenshot shows the 'Advanced > WAN > quickstart Setup' configuration page. The left sidebar contains a navigation menu with sections: Basic (Home, Quick Start), Advanced (WAN, LAN, Application, QoS, Routing, Security, Status, Diagnostics, System Password, Firmware Upgrade, Save Settings, Restart Router, Restore To Default), and Help (PPP Connection Help, LAN Configuration Help, LAN Clients Help, Firewall Help, Bridge Filters Help, UPnP Help, RIP Help, QoS Help). The main content area is titled 'Advanced > WAN > quickstart Setup' and contains the following configuration sections:

- PPPoE Connection:** Connection Name: quickstart, Type: PPPoE, Sharing: Disable, Options:  NAT  Firewall, VLAN ID: 0, Priority Bits: 0.
- PPP Settings:** Encapsulation:  LLC  VC, Username: username@ispne, Password: [masked], Idle Timeout: 60 secs, Keep Alive: 10 min, Authentication:  Auto  CHAP  PAP, MTU: 1492 bytes, On Demand: , Enforce MTU: , PPP Unnumbered: , Host Trigger: . Default Gateway: , Debug: , Valid Rx: .
- PVC Settings:** PVC: New, VPI: 0, VCI: 35, QoS: UBR, PCR: 0 cps, SCR: 0 cps, MBS: 0 cells, CDVT: 0 usecs, Auto PVC: .

Buttons at the bottom include 'Configure', 'Connect', 'Disconnect', 'Submit', and 'Delete'.

### Advanced Menu

# Help Menu

The Help Menu provides documentation about various router features.

**Basic**  
Home  
Quick Start

**Advanced**  
WAN  
LAN  
Application  
QoS  
Routing  
Security  
Status  
Diagnostics  
System Password  
Firmware Upgrade  
Save Settings  
Restart Router  
Restore To Default

**Help**  
PPP Connection Help  
LAN Configuration  
Help  
LAN Clients Help  
Firewall Help  
Bridge Filters Help  
UPnP Help  
RIP Help  
QoS Help

## Help > PPP Help

---

**PPP Connection Help**

**Username:** The username for the DSL access.

**Password:** The password for the DSL access.

**Authentication:** Specifies the authentication protocol required to establish connection.

**On-Demand:** Enable on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.

**Valid Rx:** Configurable only if on-demand is enabled. If enabled, PPP link is kept alive for valid packets accepted over PPP link. If disabled, PPP link is kept alive for packets received over PPP link.

**Host Trigger:** Configurable only if on-demand is enabled. Enable/Disable on-demand originated traffic.

**Configure:** Configurable only if on-demand is enabled. Configure on-demand originated traffic based on protocol and port.

**Idle Timeout:** Specifies that DSL should disconnect if the link has no activity detected for n seconds. A non-zero value.

**Keep Alive:** When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. A non-zero value.

**Set Defaultroute:** Specify connection as the default-route.

**MRU:** Maximum Receive Unit the DSL connection can receive. It is an negotiated value that ask the provider to send packets of no more than n bytes. The minimum MRU value is 128.

## Help Menu

# Basic Menu

The options for the Basic Menu include:

- Home
- Quick Start

## Home

The Home page provides a one-page summary about the Connection Information, Router Information, and Local Network settings.

### Basic>Home

Connection Information		Router Information	
<b>DSL</b>	Down	<b>System Uptime</b>	0 hours 0 minutes
<b>Downstream / Upstream (Kbps)</b>	0/0	<b>Model</b>	DSL805EU
<b>Internet</b>	Not Connected	<b>Firmware Version</b>	113.100.1
<b>Connected Time</b>	0	<b>Build</b>	004
<b>Connection Type</b>	PPPoE	<b>Ethernet MAC address</b>	00:30:0A:77:0B:77
<b>Username</b>	username@ispname	<b>DSL MAC address</b>	00:30:0A:77:0B:79
<b>IP Address</b>	N/A	<b>NAT</b>	Enabled
<b>Default Gateway</b>	N/A	<b>Firewall</b>	Enabled
<b>Primary DNS</b>	N/A		
<b>Secondary DNS</b>	N/A		
<a href="#">Connect</a>			
Local Network Information			
<b>LAN IP Address</b>	192.168.1.1		
<b>DHCP</b>	Enabled		
<b>DHCP Range</b>	192.168.1.2 - 192.168.1.254		
<b>Ethernet</b>	Connected		
<b>USB</b>	Connected		

### Basic Home

## Connection Information

The Connection Information pane gives you an idea about the status of your Internet connection. This pane includes a Connect/Disconnect button. When clicked, the router makes an attempt to connect to the Internet using the parameters saved in the router.



---

## Router Information

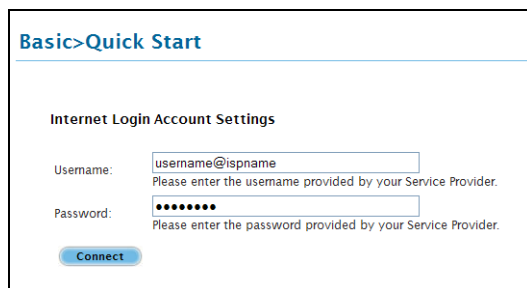
This pane provides all the necessary information to determine the model, firmware version, build, Ethernet MAC Address, NAT status, and Firewall status.

## Local Network Information

The Local Network pane displays the current IP address of the router. It also provides the DHCP status, DHCP Range, and Ethernet status.

## Quick Start

Quick Start gives you the ability to instantly connect to the Internet.



The screenshot shows a web interface titled "Basic > Quick Start". Under the heading "Internet Login Account Settings", there are two input fields. The first is labeled "Username:" and contains the placeholder text "username@ispname" with a subtext "Please enter the username provided by your Service Provider." The second is labeled "Password:" and contains seven dots with a subtext "Please enter the password provided by your Service Provider." Below the fields is a blue "Connect" button.

### Quick Start

# Advanced Menu

The Advanced Menu provides advanced configuration options. These include:

- WAN
- LAN
- Application
- QoS
- Routing
- Security
- Status
- Diagnostics
- System Password
- Firmware Upgrade
- Save Settings
- Restart Router
- Restore Default

# WAN

Wide Area Network refers to the configurations you perform to establish an Internet connection. There are several types of WAN connections that require different settings.

## New Connection

Your router supports the creation of new connections. If you have multiple virtual connections, you may need to utilize the static routing capabilities of the modem to pass data correctly.

WAN connection types include:

- PPPoE Connection
- PPPoA Connection
- Static Connection
- DHCP Connection
- Bridge Connection

## PPPoE Connection

PPPoE is a common WAN connection type used to connect to the Internet. PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. PPPoE is a protocol for encapsulating PPP frames in Ethernet frames and is described in RFC 2516. PPPoE provides the ability to connect to a network of hosts over a simple bridging access device to a remote access concentrator. With this model, each router uses its own PPP stack. Access control, billing, and type of service control can all be done on a per-user rather than per-site basis.

### Advanced>New Connection

---

#### PPPoE Connection

Connection Name:  Type: **PPPoE** Sharing: **Disable**

Options:  NAT  Firewall VLAN ID:  Priority Bits:

PPP Settings	PVC Settings
Encapsulation: <input checked="" type="radio"/> LLC <input type="radio"/> VC	PVC: <input type="text"/>
Username: <input type="text"/>	VPI: <input type="text"/>
Password: <input type="text"/>	VCI: <input type="text"/>
Idle Timeout: <input type="text"/> secs	QoS: <b>UBR</b>
Keep Alive: <input type="text"/> min	PCR: <input type="text"/> cps
Authentication: <input checked="" type="radio"/> Auto <input type="radio"/> CHAP <input type="radio"/> PAP	SCR: <input type="text"/> cps
MTU: <input type="text"/> bytes	MBS: <input type="text"/> cells
On Demand: <input type="checkbox"/>	CDVT: <input type="text"/> usecs
Enforce MTU: <input checked="" type="checkbox"/>	Auto PVC: <input type="checkbox"/>
PPP Unnumbered: <input type="checkbox"/>	
Host Trigger: <input type="checkbox"/>	

Default Gateway:  Debug:

Valid Rx:

### New PPPoE Connection Setup

## PPPoA Connection

Another commonly used WAN connection type is PPPoA. PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets in ATM cells that are carried over the DSL line. PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users. Logical Link Control (LLC) and Virtual Circuit (VC) are two different methods of encapsulating the PPP packet. Contact your service provider to determine which encapsulation is being used on your Internet connection.

### Advanced>New Connection

---

#### PPPoA Connection

Connection Name:  Type: **PPPoA** Sharing: **Disable**  
Options:  NAT  Firewall VLAN ID:  Priority Bits:

PPP Settings	PVC Settings
Encapsulation: <input checked="" type="radio"/> LLC <input type="radio"/> VC	PVC: <b>New</b>
Username: <input type="text" value="username@ispns"/>	VPI: <input type="text" value="0"/>
Password: <input type="password" value="*****"/>	VCI: <input type="text" value="0"/>
Idle Timeout: <input type="text" value="60"/> secs	QoS: <b>UBR</b>
Keep Alive: <input type="text" value="10"/> min	PCR: <input type="text" value="0"/> cps
Authentication: <input checked="" type="radio"/> Auto <input type="radio"/> CHAP <input type="radio"/> PAP	SCR: <input type="text" value="0"/> cps
MTU: <input type="text" value="1500"/> bytes	MBS: <input type="text" value="0"/> cells
On Demand: <input type="checkbox"/>	CDVT: <input type="text" value="0"/> usecs
PPP Unnumbered: <input type="checkbox"/>	Auto PVC: <input type="checkbox"/>
Host Trigger: <input type="checkbox"/>	

Default Gateway:  Debug:   
Valid Rx:

### New PPPoA Connection Setup

## Static Connection

Static connection type is used whenever a known static IP address is assigned to the router. Additional addressing information such as the Subnet Mask and the Default Gateway must also be specified. Up to three Domain Name Server (DNS) addresses can be identified. These servers resolve the name of the computer to the IP address mapped to it and thus enable you to access other web servers by typing the symbolic name (host name).

**Advanced > New Connection**

---

**Static Connection**

Connection Name:  Type:  Sharing:   
Options:  NAT  Firewall VLAN ID:  Priority Bits:

**Static Settings**

Encapsulation:  LLC  VC  
IP Address:   
Mask:   
Default Gateway:   
DNS 1:   
DNS 2:   
DNS 3:   
Mode:  Bridged  Routed

**PVC Settings**

PVC:   
VPI:   
VCI:   
QoS:   
PCR:  cps  
SCR:  cps  
MBS:  cells  
CDVT:  usecs  
Auto PVC:

### New Static Connection Setup

## DHCP Connection

DHCP allows the router to automatically obtain the IP address from the server. This option is commonly used when the IP is dynamically assigned and is not known prior to assignment.

**Advanced>New Connection**

---

**DHCP Connection**

Connection Name:  Type: **DHCP** Sharing: **Disable**

Options:  NAT  Firewall VLAN ID:  Priority Bits:

**DHCP Settings**

Encapsulation:  LLC  VC

IP Address:

Mask:

Gateway:

Default Gateway:

**PVC Settings**

PVC: **New**

VPI:

VCI:

QoS: **UBR**

PCR:  cps

SCR:  cps

MBS:  cells

CDVT:  usecs

Auto PVC:

**Renew** **Release** **Submit** **Delete**

### New DHCP Connection Setup

## Bridge Connection

A bridge connection does not assign any IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the router act as a bridge for passing packets between the WAN interface and the LAN interface.

### Advanced>New Connection

---

#### Bridged Connection

Connection Name:  Type: **Bridge** Sharing: **Disable**  
Options: VLAN ID:  Priority Bits:

**Bridge Settings**  
Encapsulation:  LLC  VC  
Select LAN: **LAN group 1**

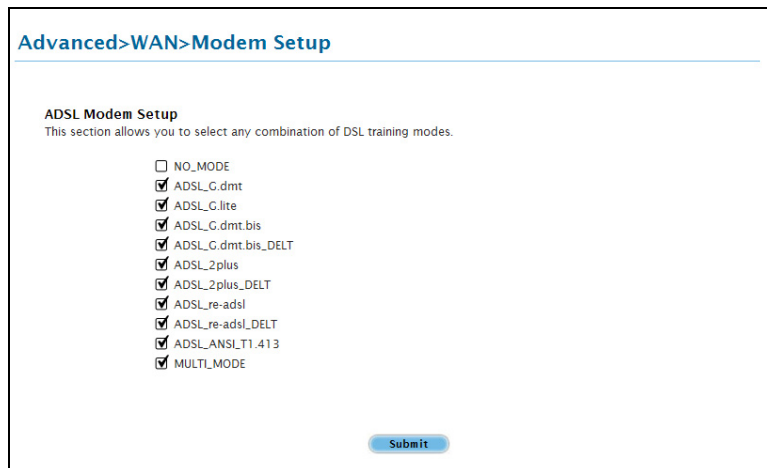
**PVC Settings**  
PVC: **New**  
VPI:   
VCI:   
QoS: **UBR**  
PCR:  cps  
SCR:  cps  
MBS:  cells  
CDVT:  usecs  
Auto PVC:

### New Bridge Connection Setup



## ADSL Modulation

ADSL Modulation allows you to select any combination of DSL training modes. Leave the default value if you are unsure or the service provider did not provide this information. In most cases, this screen should not be modified.



The screenshot shows a web interface for configuring ADSL Modem Setup. The breadcrumb path is "Advanced > WAN > Modem Setup". The page title is "ADSL Modem Setup" with a subtitle "This section allows you to select any combination of DSL training modes." Below this, there is a list of checkboxes for different DSL training modes. The "NO\_MODE" option is unchecked, while all other options are checked. A "Submit" button is located at the bottom right of the form area.

Mode	Selected
NO_MODE	<input type="checkbox"/>
ADSL_G.dmt	<input checked="" type="checkbox"/>
ADSL_G.lite	<input checked="" type="checkbox"/>
ADSL_G.dmt.bis	<input checked="" type="checkbox"/>
ADSL_G.dmt.bis_DELT	<input checked="" type="checkbox"/>
ADSL_2plus	<input checked="" type="checkbox"/>
ADSL_2plus_DELT	<input checked="" type="checkbox"/>
ADSL_re-adsl	<input checked="" type="checkbox"/>
ADSL_re-adsl_DELT	<input checked="" type="checkbox"/>
ADSL_ANSLT1.413	<input checked="" type="checkbox"/>
MULTI.MODE	<input checked="" type="checkbox"/>

### ADSL Modulation

## Connection Scan

This feature helps users to detect the PVC settings provided by the service provider. Before the router can begin scanning the connection, the telephone line has to be plugged into the router.

### To perform connections scan:

1. From the **Advanced Menu**, select **WAN > Connection Scan**.
2. Click **Scan**.

# Quickstart

Click to open the Quickstart Setup page. Quickstart is the connection name of the default PPPoE WAN Connection. In this page, you can change the connection details.

**Advanced>WAN>quickstart Setup**

**Bridged Connection**

Connection Name:  Type:  Sharing:   
Options:  VLAN ID:  Priority Bits:

**Bridge Settings**

Encapsulation:  LLC  VC  
Select LAN:

**PVC Settings**

PVC:   
VPI:   
VCI:   
QoS:   
PCR:  cps  
SCR:  cps  
MBS:  cells  
CDVT:  usecs  
Auto PVC:

## Quickstart

# LAN

The router is preconfigured to automatically provide an IP address to each Ethernet device connected in the local area network (LAN). However, if you are familiar with your network setup, you can manually configure the LAN settings.

## LAN Configuration

Your router's default IP address and subnet mask are 192.168.1.1 and 255.255.255.0, respectively. This subnet mask allows the router to support 254 users. If you want to support more users, you need to edit the subnet mask but remember that the DHCP server function can only provide up to 255 IP addresses. If you change your gateways' IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet. The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway Address.

The screenshot shows the 'LAN Configuration' page in a web browser. The breadcrumb trail at the top reads 'Advanced > LAN > LAN Configuration'. The main content area is titled 'LAN Configuration' and is divided into two main sections: 'Interfaces' and 'LAN Configuration'. The 'Interfaces' section is an empty rectangular box. The 'LAN Configuration' section contains two groups: 'LAN group 1' and 'LAN group 2'. 'LAN group 1' has an 'Add >' button, a list containing 'USB' and 'Ethernet', a '< Remove' button, and a 'Configure' link. 'LAN group 2' has an 'Add >' button and an empty list box with a '< Remove' button. A 'Submit' button is located at the bottom right of the configuration area.

LAN Configuration

**To configure the LAN groupings:**

1. From the **Advanced Menu**, select **LAN > LAN Configuration**.
2. Select **ETHERNET** in **LAN group 1** and then click **< Remove**. No packets will be sent to the ETHERNET interface because it does not belong to any LAN group.
3. Select **ETHERNET** from **Interfaces** and then click **Add >** under **LAN group 2**. Just like in LAN group 1, **Configure** will appear in **LAN group 2** to allow the definition of additional configurations.
4. To temporarily activate the settings, click **Submit**.
5. To make changes permanent, click **Save Settings**.

## LAN Group Configuration

LAN Group Configuration allows you to configure settings for each LAN group. Notice that you can also view the status of advanced services that can be applied to a LAN group. Green indicates that the service is enabled, while red indicates that the service is disabled.

**Advanced>LAN>LAN Configuration**

---

**LAN Group 1 Configuration**

**IP Settings**

Unmanaged

Obtain an IP address automatically

IP Address:  Release

Netmask:  Renew

PPP IP Address

IP Address:

Use the following Static IP address

IP Address:

Netmask:

Default Gateway:

Host Name:

Domain:

Enable DHCP Server  Assign ISP/DNS/SNTP

Start IP:

End IP:

Lease Time:  Seconds

Enable DHCP Relay

Relay IP:

Server and Relay Off

Submit

**Services Status**

IP Filters ●

Bridge Filters ●

UPnP ●

LAN Clients ●

Static Routing ●

### LAN Group Configuration

Category	Field	Description
Unmanaged		Unmanaged is a state when the LAN group is not configured and no IP address has been assigned to the bridge.
Obtain an IP address automatically		When this function is enabled, your router acts like a client and requests an IP address from the DHCP server on the LAN side.
	IP Address	You can retrieve/renew an IP address from the DHCP server using the Release and Renew buttons.
	Netmask	The subnet mask of your router.
PPP IP Address		Enables/disables PPP unnumbered feature.
	IP Address	The IP address should be different but within the same subnet as the WAN-side IP address.
Use the following Static IP address		This field enables you to change the IP address of the router.
	IP Address	The default IP address of the router (as shown) is 192.168.1.1.
	Netmask	The default subnet mask of your router is 255.255.255.0. This

		subnet allows the router to support 254 users. If you want to support a larger number of users you can change the subnet mask.
	Default Gateway	The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP provides you with the IP address of the default gateway.
	Host Name	The host name is used in conjunction with the domain name to uniquely identify the router. It can be any alphanumeric word that does not contain spaces.
	Domain	The domain name is used in conjunction with the host name to uniquely identify the router. To access the web pages of the router you can type 192.168.1.1 (the IP address) or mygateway1.ar7 (Host Name.Domain).
Enable DHCP Server		Enables/disables DHCP. By default, your router has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of the two DHCP servers.
	Assign ISP DNS, SNTP	Enable/disables the Assign ISP DNS, SNTP feature when the DHCP server of your router has been enabled. To learn more, please refer to <a href="#">Assign ISP DNS, SNTP</a> .
	Start IP	The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the IP address value of the router. For example, if the IP address of the router is 192.168.1.1 (default), then the starting IP address must be 192.168.1.2 (or higher).
	End IP	The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254; hence the max value for the default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users do not get access to network resources. If this happens, you can increase the Ending IP address (to the limit of 254) or reduce the lease time.
	Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the router using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or the DHCP server issues a new IP. The amount of time is in units of seconds. The default value is 3600 seconds (1 hour). The maximum value is 999999 seconds (About 278 hours).
Enable DHCP Relay		In addition to the DHCP server feature, the router supports the

		DHCP relay function. When the router is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiated between the DHCP clients and the server.
	Relay IP	The IP address of the DHCP relay server.
Server and Relay Off		When the DHCP server and relay functions are turned off, the network administrator must carefully configure the IP address, Subnet Mask, and DNS settings of every host on your network. Do not assign the same IP address to more than one host. Also, your router must reside on the same subnet as all the other hosts.

## Assign ISP DNS, SNTP

When you enable the DHCP server, the router dynamically assigns IP addresses to computers in the local network. The router provides its own LAN IP address (192.168.1.1) as both the gateway and the DNS server.

The router has a choice of advertising its own IP address (192.168.1.1) as the DNS server or providing the DNS that was received from the WAN. This can be configured by enabling/disabling **Assign ISP DNS SNTP** on the **LAN Group Configuration** page.

**Note:** ISP DNS, SNTP only applies when the DHCP server is enabled on the LAN Group Configuration page.

## LAN Clients

LAN Clients allows you to view and add computers in a LAN group. Each computer either has a dynamic or static (manually-configured) IP address.

You can add a static IP address (belonging to the router's LAN subnet) using the LAN Clients page. Any existing static entry falling within the DHCP server's range can be deleted.

**Advanced > LAN > LAN Clients**

---

**LAN Clients**

LAN Clients allows you to view and add computers in LAN group.  
Each computer either has a dynamic or static (manually-configured) IP address.  
To add a LAN Client, input the IP Address and Hostname, then click on Submit.

Select LAN Connection:

Enter IP Address:

Hostname:

MAC Address:

---

**Dynamic Addresses**

<u>Reserve</u>	<u>IP Address</u>	<u>Hostname</u>	<u>MAC</u>	<u>Type</u>
<input type="checkbox"/>	192.168.1.2	joserubicruz	00:11:43:b7:e7:f2	Dynamic

### LAN Clients

#### To add LAN Clients:

1. From the **Advanced Menu**, select **LAN > LAN Clients**. This opens the **LAN Clients** page.
2. Select a **LAN Connection**, and then enter **IP Address**, **Hostname**, and **MAC Address**.
3. (Optional) You can convert the dynamic into a static entry by clicking **Reserve**
4. To temporarily implement the settings, click **Submit**.
5. To make changes permanent, click **Save Settings**.



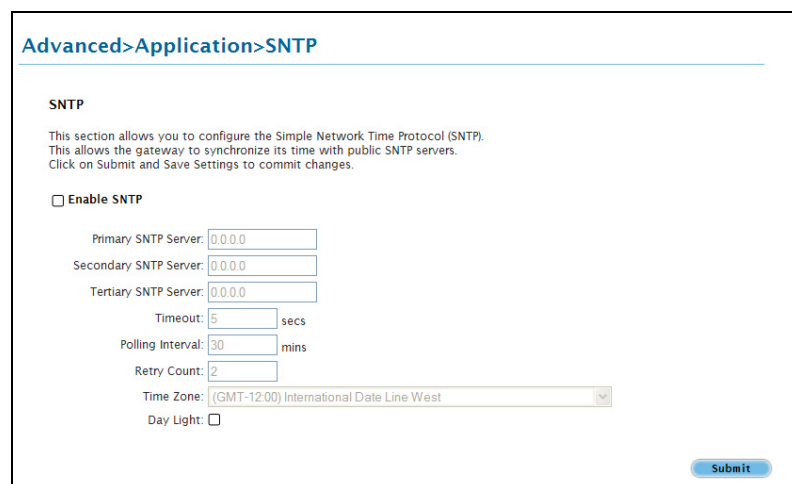
# Applications

Applications include:

- Simple Network Timing Protocol
- Internet Group Management Protocol (IGMP) Proxy
- TR-068 WAN Access
- DNS Proxy
- Dynamic DNS Client
- Port Forwarding
- Bridge Filters
- Web Access Control

## Simple Network Timing Protocol (SNTP)

Simple network timing protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers.



The screenshot shows a web configuration page for SNTP. The breadcrumb navigation is "Advanced > Application > SNTP". The page title is "SNTP". Below the title, there is a descriptive paragraph: "This section allows you to configure the Simple Network Time Protocol (SNTP). This allows the gateway to synchronize its time with public SNTP servers. Click on Submit and Save Settings to commit changes." There is a checkbox labeled "Enable SNTP" which is currently unchecked. Below this are several input fields: "Primary SNTP Server" with value "0.0.0.0", "Secondary SNTP Server" with value "0.0.0.0", and "Tertiary SNTP Server" with value "0.0.0.0". There are also fields for "Timeout" (5 secs), "Polling Interval" (30 mins), and "Retry Count" (2). A "Time Zone" dropdown menu is set to "(GMT-12:00) International Date Line West". There is a "Day Light" checkbox which is unchecked. A "Submit" button is located at the bottom right of the form area.

### SNTP

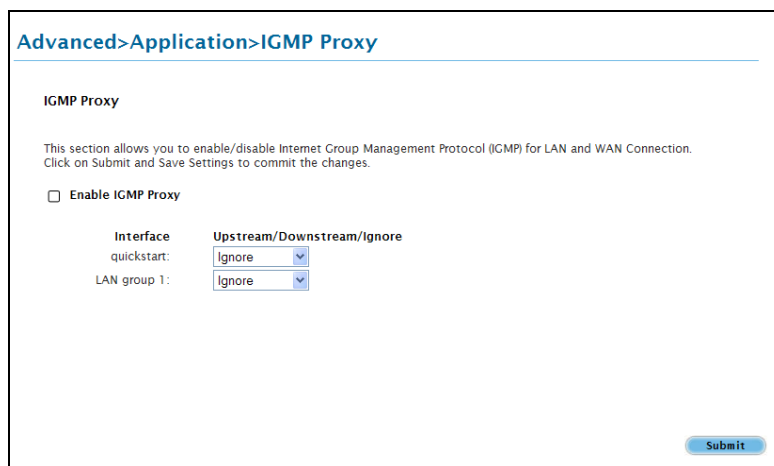
#### To enable SNTP:

1. From the **Advanced Menu**, select **Application > SNTP**.
2. Check **Enable SNTP**.
3. Configure the following fields:
  - **Primary SNTP Server** The IP address or the host name of the primary SNTP server. This can be provided by ISP or defined by user.
  - **Secondary SNTP Server** The IP address or the host name of the secondary SNTP server. This can be provided by ISP or defined by user.
  - **Tertiary SNTP Server** The IP address or the host name of the tertiary SNTP server. This can be provided by ISP or defined by user.
  - **Timeout** If the router failed to connect to an SNTP server within the Timeout period, it retries the connection.
  - **Polling Interval** The amount of time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.

- **Retry Count** The number of times the router tries to connect to an SNTP server before it tries to connect to the next server in line.
  - **Time Zone** The time zone in which the router resides.
  - **Day Light** Select this option to enable/disable daylight saving time (DST). DST is not automatically enabled or disabled. You need to manually enable and disable it.
4. Click **Submit** to temporarily apply the settings.
  5. To make changes permanent, click **Save Settings**.

## IGMP Proxy

IP hosts use Internet group management protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your router supports IGMP proxy that handles IGMP messages. When enabled, your router acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side.



The screenshot shows a web configuration page titled "Advanced>Application>IGMP Proxy". The page has a sub-header "IGMP Proxy" and a descriptive paragraph: "This section allows you to enable/disable Internet Group Management Protocol (IGMP) for LAN and WAN Connection. Click on Submit and Save Settings to commit the changes." Below this is a checkbox labeled "Enable IGMP Proxy" which is currently unchecked. Underneath, there are two rows of configuration options. The first row is labeled "Interface" and has a dropdown menu with "Upstream/Downstream/Ignore" selected. The second row is labeled "quickstart:" and has a dropdown menu with "Ignore" selected. Below that, there is a row labeled "LAN group 1:" with a dropdown menu also set to "Ignore". A blue "Submit" button is located at the bottom right of the form area.

### IGMP Proxy

Multicasting is a form of limited broadcast. UDP is used to send datagram's to all hosts that belong to what is called a Host Group. A host group is a set of one or more hosts identified by a single IP destination address. The following statements apply to host groups:

- Anyone can join or leave a host group at will.
- There are no restrictions on a host's location.
- There are no restrictions on the number of members that may belong to a host group.
- A host may belong to multiple host groups.
- Non-group members may send UDP datagram's to the host group.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers.

The IGMP Proxy page allows you to enable multicast on available WAN and LAN connections. You can configure the WAN or LAN interface as one of the following:

- **Upstream** The interface that IGMP requests from hosts are sent to the multicast router.
- **Downstream** The interface data from the multicast router are sent to hosts in the multicast group database.
- **Ignore** No IGMP request nor data multicast are forwarded.

You can perform one of the two options:

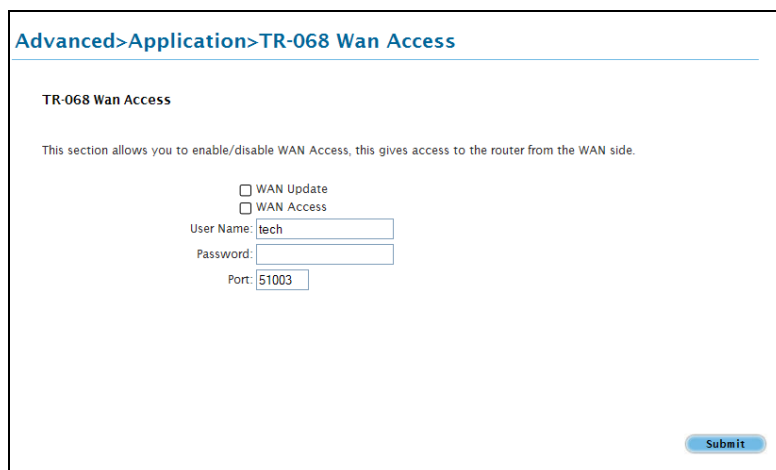
1. Configure one or more WAN interface as the upstream interface.
2. Configure one or more LAN interface as the upstream interface.

**To configure the IGMP Proxy:**

1. From the **Advanced Menu**, select **Application > IGMP Proxy**.
2. Check **Enable IGMP Proxy**.
3. Configure the listed interfaces.
4. Click **Submit** to temporarily apply the settings.
5. To make changes permanent, click **Save Settings**.

## TR-068 WAN Access (Optional)

The TR-068 WAN Access page enables you to give temporary permission to someone (such as technical support staff) to be able to access your router from the WAN side. From the moment the account is enabled the user is expected to log in within 20 minutes, otherwise the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.



The screenshot shows a web interface for configuring TR-068 WAN Access. The breadcrumb path is "Advanced > Application > TR-068 Wan Access". The page title is "TR-068 Wan Access". Below the title, there is a descriptive text: "This section allows you to enable/disable WAN Access, this gives access to the router from the WAN side." There are two checkboxes: "WAN Update" and "WAN Access", both of which are currently unchecked. Below these are three input fields: "User Name" with the value "tech", "Password" (empty), and "Port" with the value "51003". A "Submit" button is located at the bottom right of the form area.

### Enable WAN Access Update

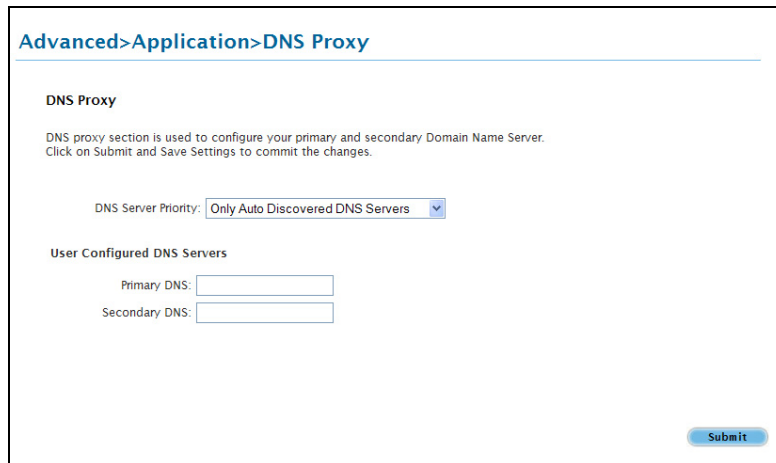
#### To create a temporary user account for remote access:

1. From the **Advanced Menu**, select **Application > TR-068 WAN Access**.
2. Check **WAN Update**.
3. Check **WAN Access**.
4. Enter a user name and password in the **User Name** and **Password** fields.
5. Enter a port number In the **Port** field.
6. Click **Submit** to temporarily apply the settings.
7. To make changes permanent, click **Save Settings**.

**Note:** To access your router remotely, enter the WAN Router IP and Port Number in your browser.  
For example, <http://10.10.10.5:51003>.

# DNS Proxy

DNS Proxy determines the primary Domain Name Server and secondary DNS to be used.



The screenshot shows a web interface for configuring DNS Proxy. At the top, there is a breadcrumb trail: **Advanced > Application > DNS Proxy**. Below this, the section is titled **DNS Proxy**. A descriptive text reads: "DNS proxy section is used to configure your primary and secondary Domain Name Server. Click on Submit and Save Settings to commit the changes." There is a dropdown menu for "DNS Server Priority" currently set to "Only Auto Discovered DNS Servers". Under the heading "User Configured DNS Servers", there are two input fields: "Primary DNS:" and "Secondary DNS:". A blue "Submit" button is located at the bottom right of the form area.

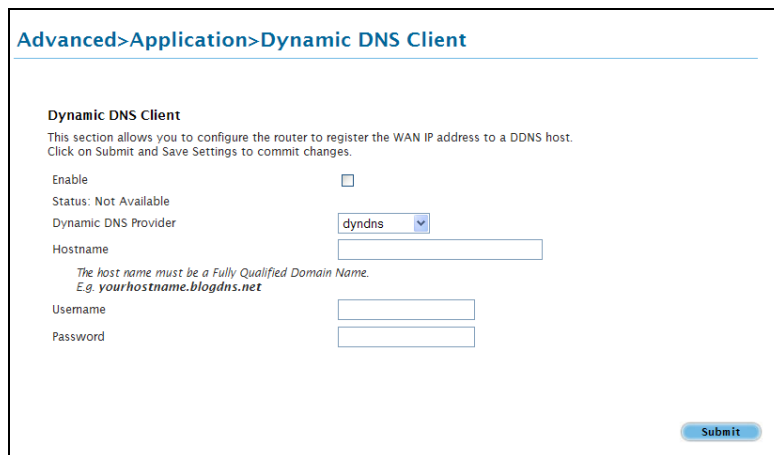
## DNS Proxy

### To select the DNS Server Priority:

1. From the **Advanced Menu**, Select **Application > DNS Proxy**.
2. Select the **DNS Server Priority**:
  - Only Auto Discovered DNS Servers
  - Only User Configured DNS Servers
  - Auto Discovered then User Configured
  - User Configured then Auto Discovered
3. Click **Submit** to temporarily apply settings.
4. To make changes permanent, click **Save Settings**.

## Dynamic DNS Client

Dynamic DNS allows the user to register with a Dynamic DNS Provider. The Dynamic DNS will be linked with the WAN IP of the router even after the ISP update the WAN IP to another IP address. It can be useful in web hosting and FTP services.



The screenshot shows the 'Dynamic DNS Client' configuration page. At the top, there is a breadcrumb trail: 'Advanced > Application > Dynamic DNS Client'. Below this, the page title is 'Dynamic DNS Client'. A descriptive paragraph states: 'This section allows you to configure the router to register the WAN IP address to a DDNS host. Click on Submit and Save Settings to commit changes.' The configuration fields include: 'Enable' with an unchecked checkbox; 'Status: Not Available'; 'Dynamic DNS Provider' with a dropdown menu set to 'dyndns'; 'Hostname' with an empty text input field and a note below it: 'The host name must be a Fully Qualified Domain Name. E.g. yourhostname.blogdns.net'; 'Username' with an empty text input field; and 'Password' with an empty text input field. A blue 'Submit' button is located at the bottom right of the form area.

### Dynamic DNS Client

**Note:** The Username/Password entered should be similar to the Username/Password you have specified during the registration of the DNS hostname.

### To enable Dynamic DNS:

1. From the **Advanced Menu**, select **Application > Dynamic DNS Client**.
2. Configure the following fields:
  - Dynamic DNS Provider
  - Hostname
  - Username
  - Password
3. Click **Submit** to temporarily apply the settings.
4. To make changes permanent, click Save **Settings**.



## Port Forwarding

Port forwarding (or virtual server) allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol. Using the Port Forwarding page, you can provide local services (for example, web hosting) for people on the Internet or play Internet games. Port forwarding is configurable per LAN group.

The screenshot shows the 'Port Forwarding' configuration page. At the top, the breadcrumb navigation is 'Advanced > Application > Port Forwarding'. Below this, the page title is 'Port Forwarding'. A brief description states: 'Port Forwarding allows incoming traffic to specific LAN host based on the protocol port number. This page allows you to configure the port forwarding parameters. Click on Submit and Save Settings to commit the changes.'

The configuration options include:

- WAN Connection: quickstart (dropdown menu)
- Allow Incoming Ping:
- Select LAN Group: LAN group 1 (dropdown menu)
- LAN IP: 192.168.1.2 (dropdown menu)
- Buttons: New IP, DMZ, Custom Port Forwarding

Below these options are two main sections:

- Available Rules:** A list of predefined rules categorized by type. The 'Games' category is selected. The list includes: Alien vs Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirecX (7.6) Games, EliteForce, EverQuest, and Fighter Ace II. A 'View' button is located below this list.
- Applied Rules:** An empty box where selected rules are moved. It contains 'Add >' and '< Remove' buttons.

A 'Submit' button is located at the bottom right of the page.

### Port Forwarding

A database of predefined port forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category and add the available rules for a given category. You can also create, edit, or delete your own port forwarding rules.

#### To configure port forwarding:

1. From the **Advanced Menu**, select **Application > Port Forwarding**.
2. Select a **WAN Connection**.
3. Select a **LAN Group**.
4. Select a **LAN IP**. If the desired LAN IP is not available in the **LAN IP** drop-down menu, you can add it using the **LAN Client page**, which is accessed by clicking **New IP**.
5. Select the available rules for a given category then click **Add** to apply the rule for this category.

If a rule is not in the list, you can create your own rule in the **User** category. To create a new rule, select **User** as the **Category**, and then click **New**. The Rule Management page opens. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map**, and then click **Submit**.

6. Click **Submit** to temporarily activate the settings.
7. To make changes permanent, click **Save Settings**.

## DMZ Settings

Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the Port Forwarding feature to the IP address of the host. This opens the access to the DMZ host from the Internet. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall.

**Advanced>Application>DMZ Settings**

---

**DMZ**

Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the port forwarding feature to the IP address of the host. This opens the access to the DMZ host from the Internet. This function is disabled by default. Click on Submit and Save Settings to Commit the changes.

Enable DMZ

Select your WAN Connection:

Select LAN Group:

Select a LAN IP Address:  [LAN Clients](#)

### DMZ Settings

**To enable DMZ Settings:**

1. From the **Advanced Menu**, select **Application > Port Forwarding**.
2. Select **DMZ**. This opens the DMZ Settings page.
3. Select **Enable DMZ**.
4. Select the **WAN Connection**.
5. Select a **LAN Group**.
6. Select a **LAN IP Address**.
7. Click **Submit** to temporarily apply the settings.
8. To make changes permanent, click **Save Settings**.

## Custom Port Forwarding

The Custom Port Forwarding page allows you to create up to 15 custom Port Forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operation.

**Advanced>Application>Custom Port Forwarding**

---

**Custom Port Forwarding**

Connection:       Enable:

Application:       Protocol:

Source IP Address:       Source Netmask:

Destination IP Address:       Destination Netmask:

Destination Port Start:       Destination Port End:

Destination Port Map:

Enabled	Name	Source IP Mask	Destination IP Mask	Port Start Port End Port Map	Protocol	Edit	Delete

### Custom Port Forwarding

## Bridge Filters

The Bridge Filters allows you to enable, add, edit, or delete the filter rules. When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed. Up to 20 filter rules are supported with bridge filtering.

**Advanced>Application>Bridge Filters**

---

**Bridge Filters**

This Bridge Filters allows you to enable, add, edit, or delete the filter rules. When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed. Click on Submit and Save Settings to commit the changes.

Enable Bridge Filters

Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet1

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny	Add
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete

Submit

### Bridge Filters

#### To configure Bridge Filters:

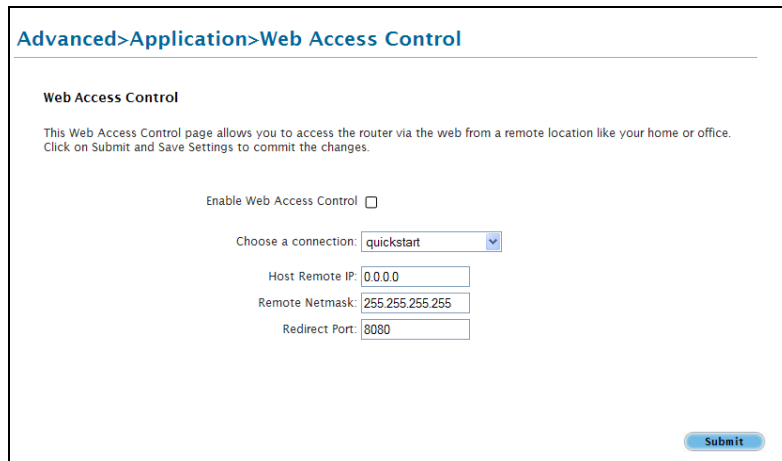
1. From the **Advanced Menu**, select **Application > Bridge Filters**. This opens the Bridge Filters page.
2. Check **Enable Bridge Filters**.
3. To add a rule, enter **Src MAC address**, **Src Port**, **Dest MAC address**, **Dest Port**, **Protocol**, and **Mode**, then click **Add**.

**Note:** You can also edit a rule that you created using the **Edit** checkbox. You can delete using **Delete**.

4. Click **Submit** to temporarily activate the settings.
5. To make changes permanent, click **Save Settings**.

# Web Access Control

The Web Access Control page allows you to access the router via the web from a remote location like your home or office.



The screenshot shows the 'Web Access Control' configuration page. At the top, there is a breadcrumb trail: 'Advanced > Application > Web Access Control'. Below this, the page title 'Web Access Control' is followed by a brief description: 'This Web Access Control page allows you to access the router via the web from a remote location like your home or office. Click on Submit and Save Settings to commit the changes.' The main configuration area includes a checkbox for 'Enable Web Access Control' which is currently unchecked. Below the checkbox is a dropdown menu labeled 'Choose a connection:' with 'quickstart' selected. There are three input fields: 'Host Remote IP:' with the value '0.0.0.0', 'Remote Netmask:' with the value '255.255.255.255', and 'Redirect Port:' with the value '8080'. A blue 'Submit' button is located at the bottom right of the form area.

## Web Access Control

### To configure Web Access:

1. From the **Advanced Menu**, select **Application > Web Access Control**.
2. Select **Enable Web Access Control**.
3. Select the **Connection**.
4. Configure the following fields:
  - Remote Host IP
  - Remote Netmask
  - Redirect Port
5. Click **Submit** to temporarily activate the settings on the page. The WAN address is now added into the IP Access List. This allows you to access you router remotely.
6. To make changes permanent, click **Save Settings**.

## Quality of Service (QoS)

Quality of service allows network administrators to configure the routers to meet the real time requirements for voice and video.

Different networks use different QoS markings like:

- ToS network: ToS bits in the IP header
- VLAN network: priority bits in the VLAN header
- DSCP network: uses only 5 bits of the CoS
- WLAN: WLAN QoS header.

The QoS framework is supported on all the above domains. How do you make them talk to each other? How can you make sure the priority from one network is carried over to another network? Class of service (CoS) is introduced as the common language for the QoS mappings. When QoS is enabled, the router has full control over packets from the time they enter the router till they leave the router.

This is how it works: The domain mapping (ToS bits, priority bits, etc.) of a packet needs to be translated to CoS when the packet enters the router, and vice versa, the CoS of a packet needs to be translated back to the domain mapping when the packet leaves the router.

There are 6 types of CoS (in descending priority):

- CoS1
- CoS2
- CoS3
- CoS4
- CoS5
- CoS6

The rules are:

1. CoS1 has absolute priority and is used for expedited forwarding (EF) traffic. This is always serviced till completion.
2. CoS2-CoS5 is used for assured forwarding (AF) classes. They are serviced in a strict round robin manner using the following priority scheme:  
  
CoS2 > CoS3 > CoS4 > CoS5
3. CoS6 is for best effort (BE) traffic. This is only serviced when there is no other class of service. If QoS is not enabled on your router, all traffic will be treated as best effort.

There are some additional terms you should get familiarize with:

- Ingress: Packets arriving into the router from a WAN/LAN interface.
- Egress: Packets sent from the router to a WAN/LAN interface.
- Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).
- Untrusted mode: Does not honor domain mapping. This is the default QoS setting.
- Traffic Conditioning Agreement (TCA): The TCA needs to be defined for each interface:
  - Ingress mappings (Domain =>CoS)
  - Egress Mappings (CoS => Domain)
  - Untrusted mode (default)
- Shaper

## Egress

For packets going out of the router, the markings (CoS) need to be translated to the mappings understood by the network domains. The reverse CoS and domain mapping is configured using the Egress. To access **Egress**, select **QoS > Egress** from the **Advanced Menu**. There are three Egress modes:

- No Egress mode
- Layer 2
- Layer 3

### No Egress Mode

The default Egress page setting for all interfaces is No Egress. In this mode, the domain mapping of the packets are untouched.

Advanced > Egress

Egress

Connection : Ethernet1

No Egress  Layer2  Layer3

No Egress TCA defined

Cancel

### Egress



## Layer 2

The Egress Layer 2 page allows you to map the CoS of an outgoing packet to user priority bits, which is honored by the VLAN network. Again, this feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current release.

**Advanced> Egress**

---

**Egress**

Connection : NA ▼

No Egress
  Layer2
  Layer3

Unclassified Packet : CoS1 ▼

Class of Service : CoS1 ▼    User Priority : 0 ▼

Reset   Apply   Cancel

### Layer 2

Field	Description
Interface	Select the WAN interface to configure the QoS for outgoing packets; LAN interface cannot be selected as VLAN is currently supported on the WAN side only.
Unclassified Packet	Some locally generated packets might not have been classified and thus do not have a CoS value, such as PPP control packet and ARP packet. You can define the CoS for all unclassified outgoing packets on layer 2 using this field, which will then pick up the user priority bits based on the mapping rules you create. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, and 7.

## Layer 3

Egress Layer 3 enables you to map CoS to ToS so that the priority marking of outgoing packets can be carried over to the IP network.

**Advanced > Egress**

---

**Egress**

Connection : Ethernet1

No Egress  
  Layer2  
  Layer3

Default Non-IP: CoS1

Class of Service : CoS1 Translated Tos:

Class of Service  
 Translated TOS

Reset
Apply
Cancel

### Layer 3

Field	Description
Interface	Select the WAN interface to configure the QoS for outgoing packets; LAN interface cannot be selected as VLAN is currently supported on the WAN side only.
Default Non-IP	Locally generated packets (such as ARP packets) do not have a CoS marking. You can define the CoS for all unclassified outgoing packets on layer 3 using this field. The selections are in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
Translated TOS	The Type of Service field takes values from 1 to 255. The selections are 0, 1, 2, 3, 4, 5, 6, and 7.

# Ingress

Ingress enables you to configure QoS for packets as soon as they come into the router. The domain mappings are converted to CoS (the common language) so that the priority marking is carried over.

There are four Ingress modes:

- Untrusted mode
- Layer 2
- Layer 3
- Static

## Untrusted Mode

Untrusted is the default Ingress page setting for all interfaces. In this mode, no domain mapping is honored in the router. All packets are treated as CoS6 (best effort).

Advanced > QoS > Ingress

**Ingress**

Interface : Ethernet1

Untrusted  Layer2  Layer3  Static

TOS	Class of Service
All	CoS6

Cancel

### Untrusted mode

## Layer 2

Layer 2 allows you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current software release.

### Layer 2

Field	Description
Interface	Select the WAN interface here to configure the CoS for incoming traffic. Only WAN interface can be selected as VLAN is currently supported only on the WAN side.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, and 7.

### To access Ingress Layer 2:

From the **Advanced Menu**, select **QoS > Ingress**.

## Layer 3

The Layer 3 page allows you to map ToS bits of incoming packets from the IP network to CoS for each WAN/LAN interface.

### Layer 3

Field	Description
Interface	For both WAN and LAN interfaces, you can configure QoS for layer 3 (IP) data traffic.
Class of Service	This CoS field allows you to map incoming layer 3 WAN/LAN packets to one of the following CoS (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
ToS	The Type of Service field takes values from 0 to 255.
Default Non-IP	A static CoS can be assigned to all layer 3 incoming packets (per interface) that do not have an IP header, such as PPP control packets and ARP packets. The default is CoS1 (recommended).

### To access Ingress Layer 3:

From the **Advanced Menu**, select **QoS > Ingress**.

## Static

The Ingress - Static page enables you to configure a static CoS for all packets received on a WAN or LAN interface.

**Advanced > Ingress**

**Ingress**

Interface :

Untrusted  Layer2  Layer3  Static

Class of Service :

### Static

#### **To access Ingress Layer 3:**

From the **Advanced Menu**, select **QoS > Ingress**.

## QoS Shaper Configuration

The Shaper Configuration page is accessed by selecting Shaper on the Advanced main page. Three shaper algorithms are supported:

- HTB
- Low Latency Queue Discipline
- PRIOWRR

**Advanced>QoS>QoS Shaper Configuration**

---

**QoS Shaper Configuration**

Interface : Ethernet1

HTB Queue Discipline      Max Rate:  

Low Latency Queue Discipline

CoS1 :   Kbits      CoS2 :   Kbits  
 CoS3 :   Kbits      CoS4 :   Kbits  
 CoS5 :   Kbits      CoS6 :   Kbits

PRIOWRR

CoS2 :   %    CoS3 :   %    CoS4 :   %    CoS5 :   %    CoS6 :   %

Reset    Submit

### QoS Shaper Configuration

**Note:** Egress TCA is required if shaper is configured for that interface.

Field	Description
Interface	The selections are WAN/LAN interfaces except WLAN, which does not support Shaper feature. This field needs to be selected before shaper configuration.
Max Rate	This field is applicable for the HTB Queue Discipline and Low Latency Queue Discipline, both are rate-based shaping algorithms.
HTB Queue Discipline	The hierarchical token bucket queue discipline is a rate-based shaping algorithm. This algorithm rate shapes the traffic of a class over a specific interface. All CoSx traffic uses a specific rate to which data will be shaped. For example: If CoS1 is configured to 100Kbps then even if 300Kbps of CoS1 data is being transmitted to the interface only 100Kbps will be sent out.
Low Latency Queue Discipline	This is similar to the above algorithm except that CoS1 is not rate limited. So in the example above CoS1 data is not rate limited to 100Kbps but instead all 300Kbps is transmitted. The side effect is that a misconfigured stream can potentially take all bandwidth.

PRIOWRR	This is a priority based weighted round robin algorithm operating on CoS2-CoS6. CoS1 queues have the highest priority and are not controlled by the WRR algorithm.
---------	--

Of the three shaping algorithms available on the Shaper Configuration page, only one can be enabled at a time. An example of each configuration is given as follows.

### Example 1: HTB Queue Discipline Enabled

In the example below, HTB Queue Discipline is enabled. The PPPoE1 connection has a total of 300 Kbps of bandwidth, of which 100 Kbps is given to CoS1 and another 100 Kbps is given to CoS2. When there is no CoS1 or CoS2 packet, CoS6 packets have the whole 300 Kbps of bandwidth.

The screenshot shows the 'QoS Shaper Configuration' page. The interface is set to 'Ethernet1'. The 'HTB Queue Discipline' checkbox is checked, and the 'Max Rate' is set to 300. The 'Low Latency Queue Discipline' checkbox is unchecked. There are input fields for CoS1 through CoS6 in Kbits. The 'PRIOWRR' checkbox is unchecked, and there are input fields for CoS2 through CoS6 in percentage. 'Reset' and 'Submit' buttons are at the bottom right.

**HTB Queue Discipline enabled**



## Example 2: Low Latency Queue Discipline Enabled

In this second example, Low Latency Queue Discipline is enabled. CoS1 is not rate controlled (hence the field is disabled). CoS2 takes 100 Kbps when there are no CoS1 packets. CoS6 has 300 Kbps when there is no CoS1 or CoS2 packets. This is similar to the HTB queue discipline as they are both rate-based algorithm, except that CoS1 is handled differently.

**Advanced>QoS>QoS Shaper Configuration**

---

**QoS Shaper Configuration**

Interface :

HTB Queue Discipline      Max Rate:

Low Latency Queue Discipline

CoS1 :  Kbits      CoS2 :  Kbits

CoS3 :  Kbits      CoS4 :  Kbits

CoS5 :  Kbits      CoS6 :  Kbits

PRIOWRR

CoS2 : %    CoS3 : %    CoS4 : %    CoS5 : %    CoS6 : %

**Low Latency Queue Discipline enabled**

## Example 3: PRIOWRR Enabled

In this third example, PRIOWRR is enabled. Since PRIOWRR operates only on the number of packets being transmitted, the max rate field has been disabled. Only percentage can be assigned to the CoS2 - CoS6. CoS1 is not rate controlled (hence the field is not displayed). When there are no CoS1 packets, CoS2, CoS3, CoS4 each has 10 percent, and CoS6 has 70 percent. This is similarly to the Low Latency Queue discipline, except that one is packet-based, and the other is rate-based.

**Advanced>QoS>QoS Shaper Configuration**

---

**QoS Shaper Configuration**

Interface :

HTB Queue Discipline      Max Rate:

Low Latency Queue Discipline

CoS1 :  Kbits      CoS2 :  Kbits

CoS3 :  Kbits      CoS4 :  Kbits

CoS5 :  Kbits      CoS6 :  Kbits

**PRIOWRR**

CoS2 :  %    CoS3 :  %    CoS4 :  %    CoS5 :  %    CoS6 :  %

**PRIOWRR enabled**

# Policy Routing Configuration

The Policy Routing Configuration enables you to configure policy routing and QoS.

**Advanced>QoS>Policy Routing Configuration**

**Policy Routing Configuration**

Ingress Interface :       Destination Interface :

DiffServ Code Point :       Class of Service :

Source IP :       Destination IP :

Mask :       Mask :

Protocol :

Source Port Start :       Source Port End :

Destination Port Start :       Destination Port End :

Source MAC :

Local Routing Mark :

Ingress Interface	DSCP	Source IP	Destination IP	Source Port Start	Destination Port Start	Protocol	Local Mark	Delete
	Dest Interface	CoS	Mask	Mask	Source Port End	Destination Port End	Source MAC	

## Policy Routing Configuration

Field	Description
Ingress Interface	The incoming traffic interface for a Policy Routing rule. Selections include LAN interfaces, WAN interfaces, Locally generated (traffic), and not applicable. Examples of Locally generated traffic are: voice packets, packets generated by applications such as DNS, DHCP, etc.
Destination Interface	The outgoing traffic interfaces for a Policy Routing rule. Selections include LAN Interfaces and WAN interfaces.
DiffServ Code Point	The diffServ code point (DSCP) field value ranges from 1 to 255. This field cannot be configured alone, additional fields like IP, Source MAC, and/or Ingress Interface should be configured.
Class of Service	The selections are (in the order of priority): CoS1, CoS2, CoS3, CoS4, CoS5, CoS6, and N/A.
Source IP	The IP address of the traffic source.
Mask	The source IP Netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Mask	The Netmask of the destination. This field is required if the destination IP has been entered.
Protocol	The selections are TCP, UDP, ICMP, Specify, and none. If you choose Specify, you need to enter the protocol number in the box next to the Protocol field. This field cannot be configured alone, additional fields like IP, Source MAC, and/or Ingress Interface should be configured. This field is also required if the source port or destination port has been entered.
Source Port	The source protocol port. You cannot configure this field without entering the protocol first.
Destination Port	The destination protocol port or port range. You cannot configure this field without entering the

	protocol first.
Source MAC	The MAC address of the traffic source.
Local Routing MAC	<p>This field is enabled only when Locally Generated is selected in the Ingress Interface field. The mark for DNS traffic generated by different applications are described below:</p> <ul style="list-style-type: none"><li>▪ Dynamic DNS: 0xE1</li><li>▪ Dynamic Proxy: 0xE2</li><li>▪ Web Server: 0xE3</li><li>▪ MSNTP: 0xE4</li><li>▪ DHCP Server: 0xE5</li><li>▪ IP tables Utility: 0xE6</li><li>▪ PPP Deamon: 0xE7</li><li>▪ IP Route: 0xE8</li><li>▪ ATM Library: 0xE9</li><li>▪ NET Tools: 0xEA</li><li>▪ RIP: 0xEB</li><li>▪ RIP v2: 0xEC</li><li>▪ UPNP: 0xEE</li><li>▪ Busybox Utility: 0xEF</li><li>▪ Configuration Manager: 0xF0</li><li>▪ DropBear Utility: 0xF1</li><li>▪ Voice: 0</li></ul>

Currently routing algorithms make decision based on destination address, i.e. only Destination IP address and subnet mask is supported. The Policy Routing page enables you to route packets on the basis of various fields in the packet.

The following fields can be configured for Policy Routing:

- Destination IP address/mask
- Source IP address/mask
- Source MAC address
- Protocol (TCP, UDP, ICMP, etc)
- Source port
- Destination port
- Incoming interface
- DSCP

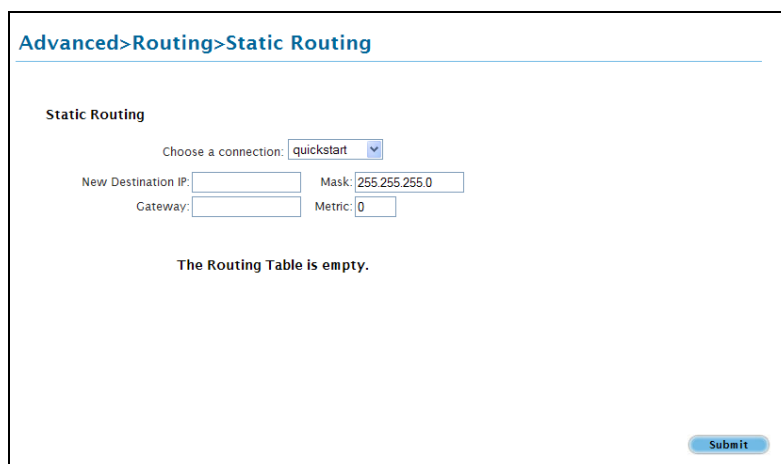
# Routing

Routing options include:

- Static Routing
- Routing Table

## Static Routing

If the router is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the router.



The screenshot shows a web interface for configuring static routing. The breadcrumb path is "Advanced > Routing > Static Routing". The page title is "Static Routing". There is a dropdown menu labeled "Choose a connection:" with "quickstart" selected. Below this are four input fields: "New Destination IP:" (empty), "Mask:" (containing "255.255.255.0"), "Gateway:" (empty), and "Metric:" (containing "0"). A message in the center states "The Routing Table is empty." A "Submit" button is located in the bottom right corner.

### Static Routing

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.

## Routing Table

Routing Table displays the information used by routers when making packet-forwarding decisions. Packets are routed according to the packet's destination IP address.

### Advanced>Routing>Routing Table

#### Routing Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	1	0	0	br0

#### Routing Table

# Security

Security options include:

- IP Filters
- LAN Isolation

## IP Filters

IP filtering allows you to block specific applications/services based on the IP address of the LAN device. In this page, you can block specific traffic (for example, block web access) or any traffic from a host on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter and add the available rules for a given category. You can also create, edit, or delete your own IP filter rules.

The screenshot shows the 'Advanced > Security > IP Filters' configuration page. At the top, it says 'IP Filters' and provides a brief description: 'Port Forwarding allows incoming traffic to specific LAN host based on the protocol port number. This page allows you to configure the port forwarding parameters. Click on Submit and Save Settings to commit the changes.'

Configuration options include:

- Select LAN Group: LAN group 1
- LAN IP: 192.168.1.2
- New IP button
- Block All Traffic:
- Block Outgoing Ping:  [Custom IP Filters](#)

Below these are two main sections:

- Available Rules:** A list of predefined rules categorized by type. The 'Games' category is selected. The list includes: Alien vs Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirectX (7,8) Games, EliteForce, EverQuest, and Fighter Ace II. A 'View' button is at the bottom of this list.
- Applied Rules:** An empty box where selected rules are moved. It has 'Add >' and '< Remove' buttons between it and the available rules list.

A 'Submit' button is located at the bottom right of the page.

### IP Filters



**To configure IP Filters:**

1. From the **Advanced Menu**, select **Security > IP Filters**.
2. Select a **LAN Group**.
3. Select a **LAN IP**. If the desired LAN IP is not available in the LAN IP drop-down menu, click **New IP** to add an IP.
4. Select Available Rules and then move them into Applied Rules.

To select a rule, select a **Category** then select an available rule based on the selected Category. Click **View** to view the rule settings.

If a rule is not in the list, you can create your own rule. Select **User**, and then click **New**. The Rule Management page opens for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, **Port Map**, and then click **Apply**.

5. Click **Add** to move the rule into **Applied Rules**.
6. To temporarily implement the changes, click **Submit**.
7. To make the change permanent, click **Save Settings**.

# LAN Isolation

LAN isolation allows you to disable the flow of packets between two LAN groups. This allows you to secure information in private portions of the LAN from other publicly accessible LAN segments.

**Advanced>Security>LAN Isolation**

---

**LAN Isolation**  
To block traffic from one LAN to another LAN, check the Disable check box.

- Disable traffic between LAN group 1 and LAN group 2
- Disable traffic between LAN group 1 and LAN group 3
- Disable traffic between LAN group 1 and LAN group 4
- Disable traffic between LAN group 1 and LAN group 5
- Disable traffic between LAN group 2 and LAN group 3
- Disable traffic between LAN group 2 and LAN group 4
- Disable traffic between LAN group 2 and LAN group 5
- Disable traffic between LAN group 3 and LAN group 4
- Disable traffic between LAN group 3 and LAN group 5
- Disable traffic between LAN group 4 and LAN group 5

## LAN Isolation

### To enable LAN Isolation:

1. From the **Advanced Menu**, select **Security > LAN Isolation**.
2. Check an option.
3. To temporarily implement the changes, click **Submit**.
4. To make changes permanent, click **Save Settings**.

# Status

This chapter provides information about monitoring the router status and viewing product information.

Your router allows you to view the following status and product information:

- Connection Status
- System Log
- Remote Log
- Network Statistics
- DHCP Clients
- QoS Status
- Modem Status
- Product Information

## Connection Status

Connection Status displays the type of protocol, the WAN IP address, the connection state and the duration of your Internet connection. To view the Connection Status from the **Advanced Menu**, select **Status > Connection Status**.

[Advanced](#)>[Status](#)>[Connection Status](#)

---

Connection Status (1)

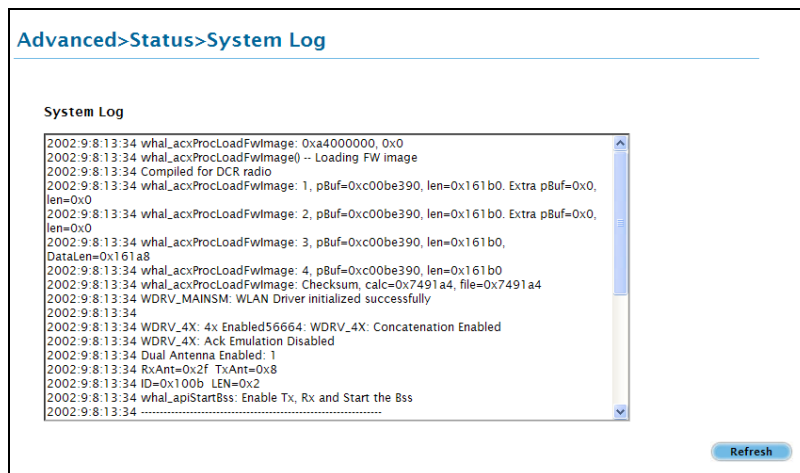
Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	N/A	Not Connected	0	DSL line is Disconnected

[Refresh](#)

### Connection Status

## System Log

System Log displays the router log. Depending on the severity level, the information log will generate log reports to a remote host if remote logging is enabled. To view the System Log from the **Advanced Menu**, select **Status > System Log**.

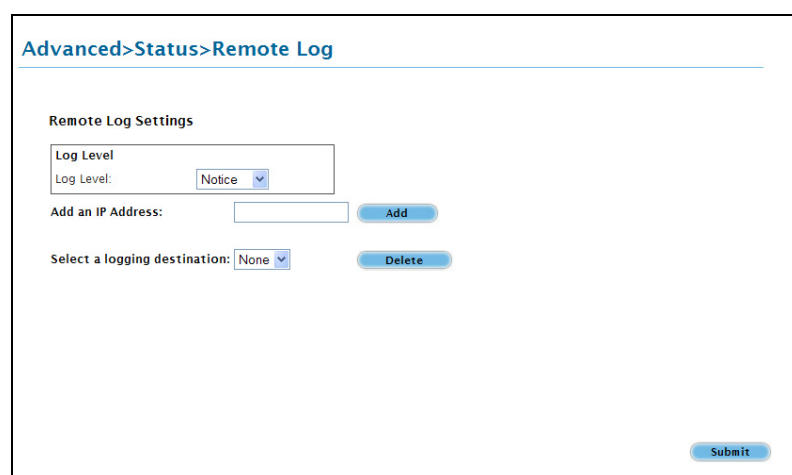


### System Log

## Remote Log

Remote Log allows you to forward all logged information to one (or more) remote computer. The type of information forwarded to the remote computer depends on the Log level. Each log message belongs to a certain log level, which indicates the severity of the event.

When you configure remote logging, you must specify a severity level. Log messages that are rated at that level or higher are sent to the log server and can be viewed using the server log application, which can be downloaded from the web.



The screenshot shows a web interface for configuring Remote Log Settings. The breadcrumb path is "Advanced > Status > Remote Log". Under the heading "Remote Log Settings", there is a "Log Level" dropdown menu currently set to "Notice". Below this is a field for "Add an IP Address:" with an "Add" button. Further down is a "Select a logging destination:" dropdown menu currently set to "None" with a "Delete" button. A "Submit" button is located at the bottom right of the form area.

### Remote Log Settings

#### To enable remote logging:

1. From the **Advanced Menu**, select **Status > Remote Log**.
2. Select a **Log Level**. There are 8 log levels listed below in order of severity.
  - **Panic** System panic or other condition that causes the router to stop functioning.
  - **Alert** Conditions that require immediate correction, such as a corrupted system database.
  - **Critical** Critical conditions such as hard drive errors.
  - **Error** Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
  - **Warning** Conditions that warrant monitoring.
  - **Notice** (Default) Conditions that are not errors but might warrant special handling.

- **Info** Events or non-error conditions of interest.
  - **Debug** Software debugging message. Specify this level only when directed by a technical support representative.
3. Enter the **IP Address** where the log will be sent to.
  4. Click **Add**.
  5. Click **Submit**. The IP address will appear in the **Select a logging destination** drop-down menu.
  6. To make changes permanent, click **Save Settings**.

**Note:** When you select a log level, all log information within this severity level and levels above (meaning, more severe levels) will be sent to the remote host.

**To disable a remote log:**

1. Select the IP address to be deleted from the **Select a logging destination** drop-down menu.
2. Click **Delete**.
3. To temporarily implement the changes, click **Submit**.
4. To make changes permanent, click **Save Settings**.

## Network Statistics

The Ethernet and DSL line statuses are displayed in this page. To view the Network Statistics from the **Advanced Menu**, select **Status > Network Statistics**. There are three categories for Network Statistics. These include Ethernet and DSL.

### Advanced>Status>Network Statistics

---

#### Network Statistics

Choose an interface to view your network statistics:

Ethernet  DSL

Transmit

Good Tx Frames	3187
Good Tx Broadcast Frames	6
Good Tx Multicast Frames	0
Tx Total Bytes	2920881
Collisions	0
Error Frames	0
Carrier Sense Errors	0

Receive

Good Rx Frames	1927
Good Rx Broadcast Frames	140
Good Rx Multicast Frames	15
Rx Total Bytes	160872
CRC Errors	0
Undersized Frames	0
Overruns	0

[Refresh](#)

### Ethernet

### Advanced>Status>Network Statistics

---

#### Network Statistics

Choose an interface to view your network statistics:

Ethernet  DSL

Transmit

Tx PDUs	0
Tx Total Bytes	0
Tx Total Error Counts	0

Receive

Rx PDUs	0
Rx Total Bytes	0
Rx Total Error Counts	0

[Refresh](#)

### DSL



## DHCP Clients

DHCP Clients displays the MAC address, IP address, host name, and lease time. To view the DHCP Clients from the **Advanced Menu**, select **Status > DHCP Clients**. The DHCP Clients are displayed according to LAN Group.

**Advanced>Status>DHCP Clients**

---

**DHCP Clients (1)**

Select LAN:

MAC Address	IP Address	Host Name	Lease Time
00:11:43:b7:e7:f2	192.168.1.2	josenubicruz	0 days 0:40:23

[Refresh](#)

### DHCP Clients

## QoS Status

This page displays the Quality of Service and the packet statistics. To view the QoS Status from the **Advanced Menu**, select **Status > QoS Status**.

**Advanced>Status>QoS status**

---

**QOS STATUS**

QOS Framework : Enabled  
Scheduling Algorithm : Strict Round-Robin

NQM Received Statistics	NQM Dropped Statistics
Cos1 Pkts received : 0	Cos1 Pkts received : 0
Cos2 Pkts received : 0	Cos2 Pkts received : 0
Cos3 Pkts received : 0	Cos3 Pkts received : 0
Cos4 Pkts received : 0	Cos4 Pkts received : 0
Cos5 Pkts received : 0	Cos5 Pkts received : 0
Cos6 Pkts received : 25277	Cos6 Pkts received : 0

NQM Congestion Control	Translation Statistics
Cos1 Queue : Empty	Packets Remarkd : 1806
Cos2 Queue : Empty	Packets Unchanged : 0
Cos3 Queue : Empty	Non-Ip Packets Marked : 7
Cos4 Queue : Empty	Unclassified Ip Packets Marked : 20
Cos5 Queue : Empty	Unclassified Non-Ip Packets Marked : 5
Cos6 Queue : Empty	Unclassified Layer2 Packets : 0

Congestion State : Not Congested

**Classification Statistics**  
Classification Errors : 0  
Unclassified Packets : 0  
Fragmented Packets = 0

### QoS Status

## Modem Status

This page displays the model status. To view the Modem Status from the **Advanced Menu**, select **Status > Modem Status**.

**Advanced>Status>Modem Status**

---

**Modem Status**

Modem Status

Connection Status	Disconnected
Us Rate (Kbps)	0
Ds Rate (Kbps)	0
US Margin	0
DS Margin	0
Trained Modulation	NO_MODE
LOS Errors	0
DS Line Attenuation	0
US Line Attenuation	0
Peak Cell Rate	0 cells per sec
CRC Rx Fast	0
CRC Tx Fast	0
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path
DSL Statistics	
Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

[Refresh](#)

### Modem Status

## Product Information

This page displays the product information and software versions. To view the Product Information from the **Advanced Menu**, select **Status > Product Information**.

### Advanced>Status>Product Information

---

#### Product Information

##### Product Information

Model Number	DSL805E
Ethernet MAC	00:30:0A:77:0C:5D
DSL MAC	00:00:02:03:04:05
Wireless MAC0	00:12:0e:54:e9:d2

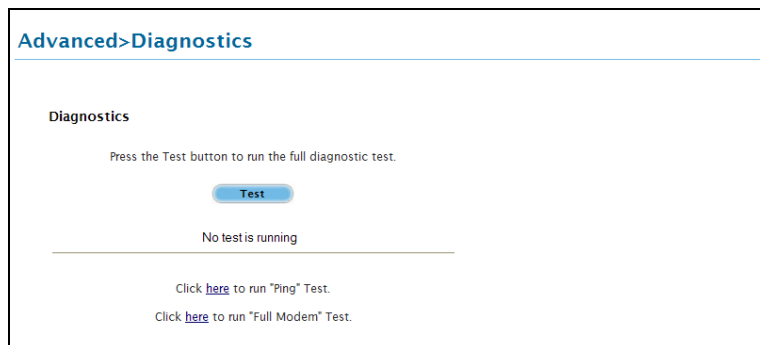
##### Software Versions

Gateway	3.7.0
Firmware	120.53.1
Build	002
ATM Driver	6.00.01.00
DSL HAL	6.00.01.00
DSL Datapump	6.00.04.00 Annex A
SAR HAL	01.07.2b
PDSP Firmware	0.54
Wireless Firmware	3.4.0.41
Wireless APDK	6.4.4.27
Boot Loader	1.4.0.4

#### Product Information

# Diagnostics

Diagnostic Test is used for investigating whether the router is properly connected to the WAN Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and click **Test**. Before running this test, make sure you have a valid DSL link.



## Diagnostics

### To run diagnostic test:

1. From the **Advanced Menu**, select **Diagnostics**. This opens the **Diagnostics** page.
2. Click **Test**. The test status will appear after running the diagnostic test. If a test failed, click **Help** to get the solution.

## Ping Test

Once you have your router configured, it is a good idea to make sure you can ping the network. If you can ping an IP on the WAN side successfully, you should be able to surf the Internet.

### To perform a ping test:

1. From the **Advanced Menu**, select **Diagnostics**. This opens the **Diagnostics** page.
2. Click **Ping Test**. This opens the **Ping Test** page.
3. Change or leave the default settings for the following fields:
  - IP address to ping
  - Packet size
  - Number of echo request

4. Click **Test**.

The ping results are displayed in the page. If the ping test was successful, it means that the TCP/IP protocol is up and running. If the Ping test failed, you should restart the router.

## Full Modem Test

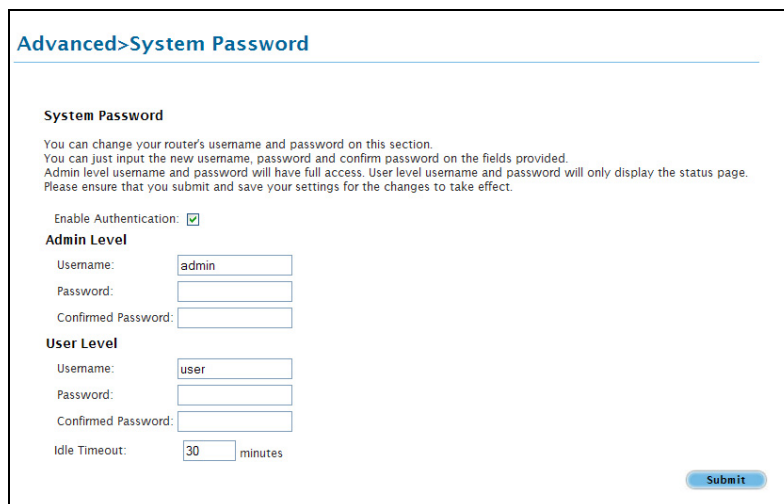
This test is used to check if your modem is properly connected to the network.

### **To perform a Full Modem test:**

1. From the **Advanced Menu**, select **Diagnostics**. This opens the **Diagnostics** page.
2. Click **Full Modem Test**. This opens the **Modem Test** page.
3. Select your connection and then click **Test**.

# System Password

Anyone who can access the web interface can be considered an Administrator. To restrict access to the web interface, you need to set the System Password.



The screenshot shows a web interface for configuring the system password. The page title is "Advanced>System Password". Below the title, there is a section titled "System Password" with a brief instruction: "You can change your router's username and password on this section. You can just input the new username, password and confirm password on the fields provided. Admin level username and password will have full access. User level username and password will only display the status page. Please ensure that you submit and save your settings for the changes to take effect." Below this, there is a checkbox for "Enable Authentication" which is checked. There are two sections: "Admin Level" and "User Level". Each section has three input fields: "Username", "Password", and "Confirmed Password". In the "Admin Level" section, the "Username" field contains the text "admin". In the "User Level" section, the "Username" field contains the text "user". At the bottom left, there is an "Idle Timeout" field with a value of "30" and the unit "minutes". A "Submit" button is located at the bottom right of the form.

## System Password

## Changing the System Password

To change the System Password:

1. From the **Advanced Menu**, select **System Password**. This opens the **System Password** page.
2. Check **Enable Authentication**.
3. Enter your password.
4. Reenter your password in the **Confirm Password** text box.
5. To temporarily implement the settings, click **Submit**.
6. To make changes permanent, click **Save Settings**.

**Note:** Remember your account information. If you forget the User Name and System Password, you will need to reset the router to its default settings. To reset, press **RESET** at the router's back panel for 10 seconds.

## Changing the Timeout Settings

To change the timeout settings:

1. From the **Advanced Menu**, select **System Password**.
2. Select **Enable Authentication**.
3. Enter the number of minutes in the **Idle Timeout** text field.
4. To temporarily implement the settings, click **Submit**.
5. To make changes permanent, click **Save Settings**.



# Firmware Upgrade

When updating the firmware, make sure you are using the correct file. Once the upgrade is complete the router will reboot. You will need to log back into the router after the firmware upgrade is completed.

**Advanced>Firmware Upgrade**

---

### Firmware Upgrade

This section allows you to upgrade the router's firmware and configuration and to get the current configuration of the router. Click on the **Browse** button to locate the updated image file or configuration file. Click on **Upgrade** to upgrade the firmware or upload the configuration file. The router will be restarted automatically upon successful file system upgrade. Router needs to be manually restarted upon successful configuration upload.

Please select the file:  **Browse**

Firmware image can be combined as a single image with or without digital signature, maximum size is 3.5MB.

**Update Gateway**

Click on **Get Configuration** to save the router's current configuration to a file.

**Get Configuration**

Status:None

## Firmware upgrade

### To update the firmware:

1. From the **Advanced Menu**, select **Firmware Upgrade**. This opens the **Firmware Upgrade** page.
2. Click **Browse** and then locate the firmware file.
3. Click **Update Gateway**. The update may take a few minutes. Make sure that the power is not turned off during the update process.

## **Save Settings**

Select to apply configuration changes permanently.

## **Restart Router**

Select to restart the router.

## **Restore to Default**

Select to reset the router to its factory default settings.

# Help Menu

To access Help, select the **Help Menu**. The Help Menu provides documentation for topics that include:

- PPP Connection
- LAN Configuration
- LAN Clients
- Firewall
- Bridge Filters
- QoS (Quality of Service)

## Safety Precautions

- Do not open, service, or change any component.
- Only qualified technical specialists are allowed to service the equipment.
- Observe safety precautions to avoid electric shock.
- Check voltage before connecting to the power supply. Connecting to the wrong voltage will damage the equipment.

**Reminder:** Product warranty does not apply to damage caused by lightning, power surges, or wrong voltage usage.

Copyright © 2007. All rights reserved.

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission of the owner. Product specifications contained in this document are subject to change without notice. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>