NetComm®

www.netcomm.com.au

User Guide

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be broken or malfunctioning, please contact technical support for immediate service by email at technicalsupport@netcomm.com.au

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.NetComm.com.au

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

⚠ **WARNING**

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix D

Copyright

NOTE:This document is subject to change without notice.

Save Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Table of Contents

1.Introduction

The **NB11W Multi-DSL Router** is designed for ADSL2+/VDSL2 over POTS (Annex A) connections. It is best suited for residential and business users who need to integrate ADSL2+/VDSL2 and WLAN functionality. Including the latest VDSL2 broadband technology, the **NB11W** is perfect for triple-play (Video, Voice and Data) applications. It also offers users easy access to the Internet via WLAN or Ethernet.

The **NB11W** features flexible connectivity with a single port for ADSL2/2+ or VDSL2 access, four 10/100 Base-T Ethernet ports, two optional USB ports, and an 802.11g wireless LAN access point. It has robust routing capabilities to segment and direct data streams and allows for multiple data encapsulations. It provides higher level performance with embedded security, QoS, VPN and remote management functions. As an added bonus, the USB host acts as a printer hub and will enable future product enhancements available by software upgrade.

1.1 Features

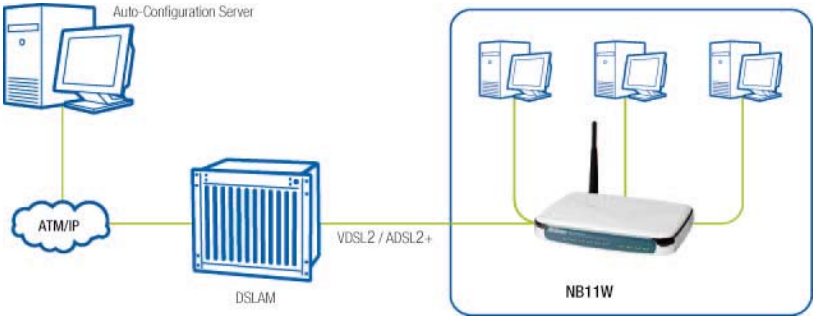
- Annex A (POTS)
- Up to 16 PVCs
- Auto selects ADSL2+/VDSL2 modes based on DSLAM settings
- Auto PVC configuration
- Dynamic IP assignment
- Embedded SNMP agent
- Automatic firmware upgrade & configuration
- Configuration backup and restoration
- Remote administration
- Time-of-day parental control
- IP/MAC address filtering
- Supports VPN Pass-Through
- Static route/RIP/RIP v2 routing functions
- WPA and WPA2
- IP QoS
- Per-VC packet level QoS

- NAT/PAT
- DNS Proxy
- IGMP Proxy and fast leave
- Integrated 802.11g AP (802.11b backward compatible)
- TR-069/TR-098/TR-104/TR-111
- User Friendly Color connections
- Web-based management
- DHCP Server/Relay/Client
- FTP/TFTP server
- RADIUS client

For a complete list of features, please consult Appendix D: Specifications.

1.2 Application

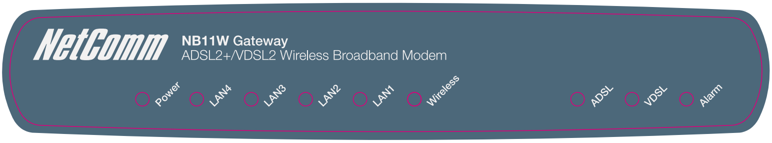
The diagram below depicts a typical application of the **NB11W** series.



Our related product, **NB11W**, is an Annex B device for ISDN connections.

1.3 Front Panel LED Indicators

The front panel LED indicators are shown and explained below.



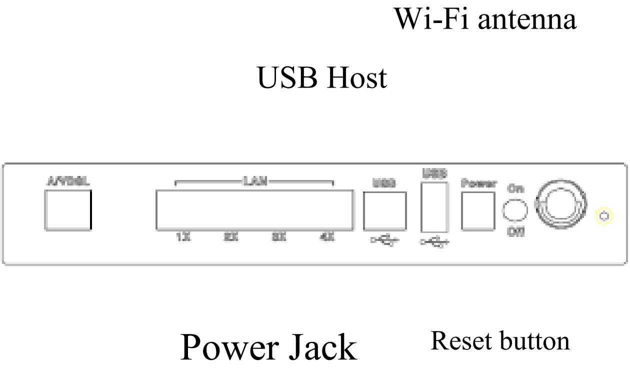
LED	Color	Mode	Description
POWER	Green	On	The router is powered up.
		Off	The router is powered down.
LAN 4~1	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
WIRELESS	Green	On	The wireless function is ready and idle.
		Off	The wireless function is unavailable.
		Blink	Data transmitting or receiving over WLAN
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
		Blink	ADSL link is training.
VDSL	Green	On	The VDSL link is established.
		Off	The VDSL link is not established.
		Blink	VDSL link is training.
ALARM	Red	On	The ADSL or VDSL link is terminated.
		Off	Normal operating status.

Installation

2.Installation

2.1 Hardware Installation

Follow the instructions below to complete the hardware installation.



Connection to A/VDSL port

Connect to an ADSL2/2+ or VDSL with this RJ11 Port. This device contains a micro filter which removes the analog phone signal. If you wish, you can connect a regular telephone to the same line by using a POTS splitter.

Connection to LAN ports

To connect to a hub or PC, use RJ45 Ethernet cable. You can connect the router to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to USB host port

This router is equipped with one high-speed USB 2.0 host connection.

With software support, users can connect USB devices such as printers or a hard disc to the router. For this software release, only printer service is supported.

Connection to Power

Connect the power jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source. After powering on, the router will perform a self-test. Wait a few moments and the router will be ready to operate.

Caution 1: If the router fails to power up, or if it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

Reset Button

In the back panel, there is a reset button (see **BACK PANEL** diagram). Restore the default parameters of the device by holding down this button until the front panel LED indicators start blinking simultaneously (about 10 seconds). If held down longer, the device may go into a firmware update state (CFE boot mode). The user can then update the device from any web browser using the default IP address (http://192.168.1.1) without login.

Web User Interface

3.Web User Interface

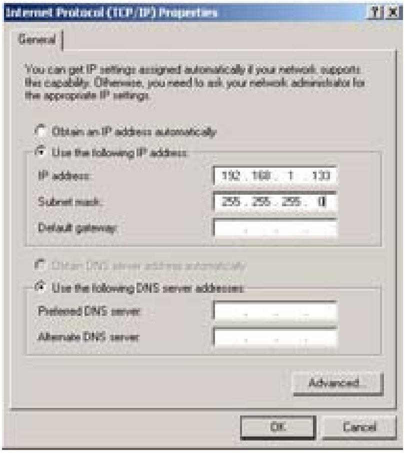
This section describes the setup procedure to access the web user interface.

3.1 TCP/IP Settings

The default IP address of the router (LAN port) is 192.168.1.1. To configure the router for the first time, the configuration PC can use DHCP a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

1: Right click on the Local Area Connection under the Network and Dial-Up connection window and select Properties.

2: Enter the TCP/IP window and change the IP address to 192.168.1.x/24



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 133

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

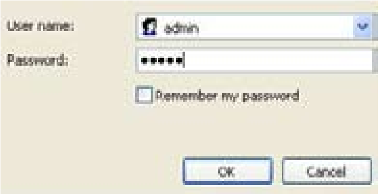
3: Click **OK** to submit settings.

3.2 Login Procedure

Follow these steps to login to the web user interface.

1: Open an Internet browser (e.g. Microsoft Internet Explorer) and enter the default IP address for the router in the URL address field at top. For example, if the IP address is 192.168.1.1, enter “http://192.168.1.1”.

2: Next, you will be prompted to enter your user name and password. Enter **admin** as the user name and **admin** as the password, and then click **OK**. These values can be changed later (see section 9.6.3).

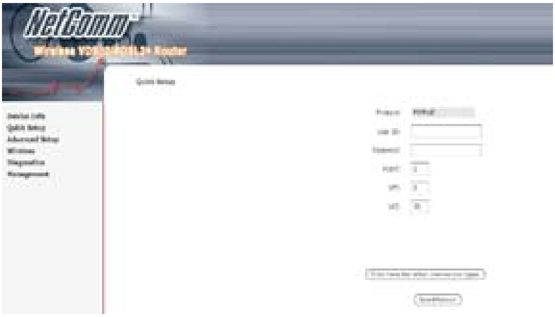


User name: admin

Password: •••••

□ Remember my password

3: After successfully logging in, you will reach the Quick Setup menu.



Quick Setup

3.3 Default Settings

The following list shows the factory default settings for this router.

- LAN port IP address: 192.168.1.1
- Local administrator account name: admin
- Local administrator account password: admin
- Local non-administrator account name: user
- Local non-administrator account password: user
- Remote WAN access: disabled (except for ICMP)
- Remote WAN access account name: support
- Remote WAN access account password: support
- NAT and firewall:Disabled for MER, IPoA and Bridge modes Enabled for PPPoE and PPPoA modes
- DHCP server on LAN interface: enabled
- WAN IP address: none

- Wireless access: enabled
- SSID: Wireless
- Wireless authentication: enabled Password a1b2c3d4e5
- Annex A enabled / Annex M disabled

This router supports the following connection types.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

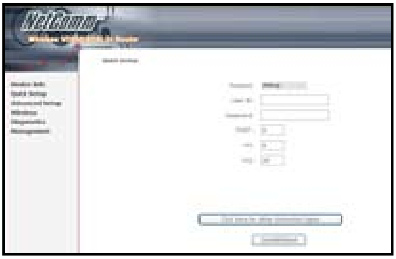
Technical Note:

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Default screen, section 9.1.3.

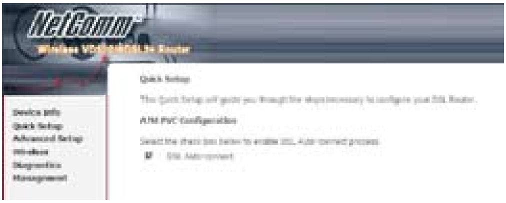
Quick Setup

4.Quick Setup

After login, the **Quick Setup** screen will appear as shown. For this, need to click on “Click here for other connection types”.



PPoE setup is the default connection type. If you have a PPoE connection you can proceed from here to setup your DSL Connection. If you are unsure or have a different connection type, select the Click here for other connection types button to go to the next screen.



Quick Setup

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

Select the check box below to enable DSL Auto-connect process.

☑ DSL Auto-connect

NOTE: The selections available on this menu are based upon configured connection settings and user account privileges.

The Quick Setup screen allows the user to configure the router for DSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either manually customize the router or follow the online instruction to set up the router.

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider’s configuration in the Central Office and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the router is to run the PPPoE client. The router can support both cases simultaneously.

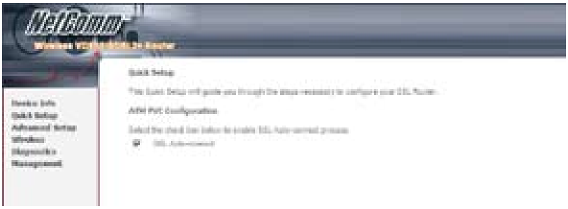
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge In PPPoE mode, the router also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices. In most cases, NAT and firewall should always be enabled when PPPoE or PPPoA mode are selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

NOTE: Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you must navigate through all the Quick Setup screens until the last summary screen, and then click on the Save/Reboot button.

4.1 Auto Quick Setup

The auto quick setup requires the DSL link to be up. The router will automatically detect the best connection type. You need only to follow the online prompts.

1: Select **Quick Setup** to display the Quick Setup screen and “Click for other” connections button.



Quick Setup

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

Select the check box below to enable DSL Auto-connect process.

☑ DSL Auto-connect

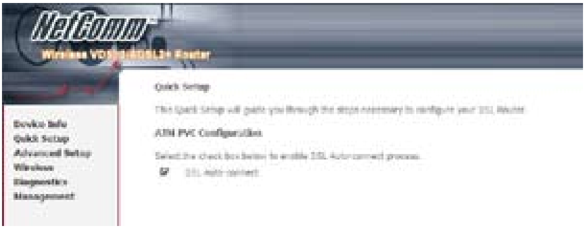
2. Then select “DSL Auto-Connect”

3: Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some advanced options, such as the PVC index and encapsulation screen.

4: After the process is complete, you can use the DSL service.

4.2 Manual Quick Setup

1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.



Quick Setup

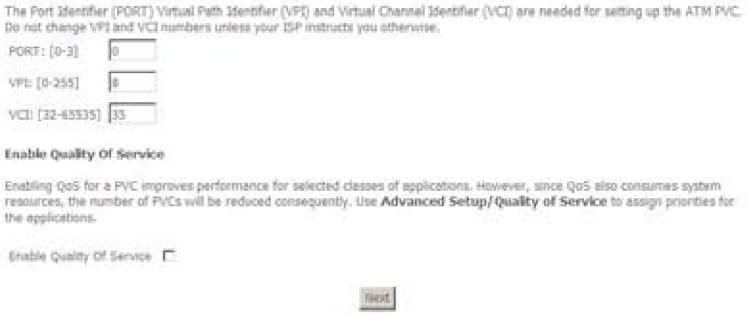
This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

Select the check box below to enable DSL Auto-connect process.

☑ DSL Auto-connect

Untick this checkbox to display the following screen.



The Port Identifier (PORT) Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.

PORT: [0-3] 0

VPI: [0-255] 8

VCI: [32-65535] 35

Enable Quality Of Service

Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

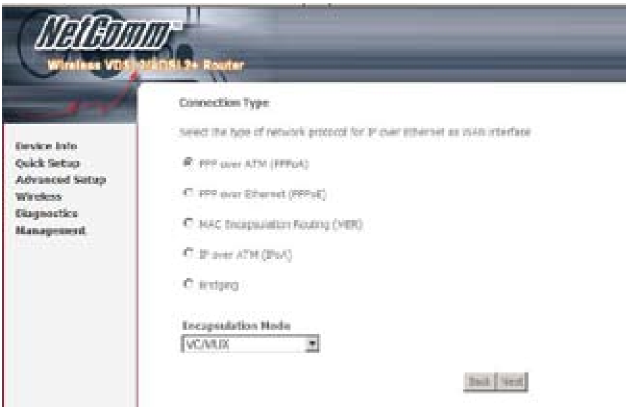
Enable Quality Of Service □

2: Enter the PORT, Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values. Select Enable Quality Of Service if required and click Next.

3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

● PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

○ Bridging

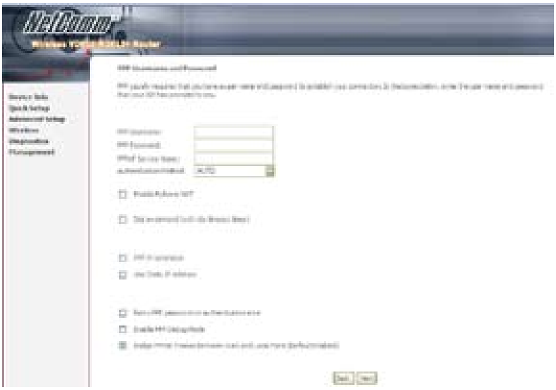
Encapsulation Mode: VC/MUX

NOTE: The sections that follow describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter appropriate settings that are required by your service provider.

4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click Next. The following screen appears.



PPP Username and Password

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Use Static IP Address

□ Retry PPP password on authentication error

□ Enable PPP Debug Mode

☑ Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

PPP Username/PPP Password

The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the DSL service provider. The web user interface allows a maximum of 256 characters for the PPP username and a maximum of 32 characters for PPP password.

PPPoE service name

PADI requests contain a service label. Some PPPoE servers (or BRAS) of ISP check this service label to make a connection.

Enable Fullcone NAT

Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Disconnect if no activity

The router can be configured to disconnect if there is no activity for a period of time by selecting the Dial on demand check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.

PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the router has a single IP address to assign to a LAN device.
- NAT and firewall are disabled when this option is selected.
- The router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

Use Static IP Address

Unless your service provider specially requires this setup, do not select it.

If selected, enter your static IP address.

Retry PPP password on authentication error

Tick the box to select.

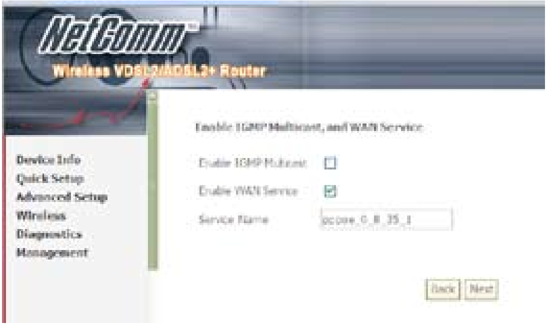
Enable PPP Debug Mode

Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don’t enable in normal usage.

Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

If Enabled, the function can create a local PPPoE connection to the WAN side.

5: Click **Next** to display the following screen.



Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name pppoe_0_8_35_1

Enable IGMP Multicast checkbox:

Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

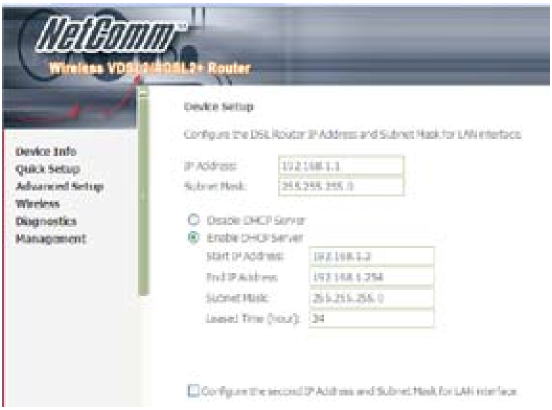
Enable WAN Service checkbox:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name:

This is user-defined.

6: After entering your settings, select Next. The following screen appears.



Device Setup

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

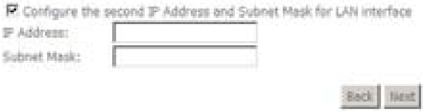
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Leased Time (hour): 24

□ Configure the second IP Address and Subnet Mask for LAN interface

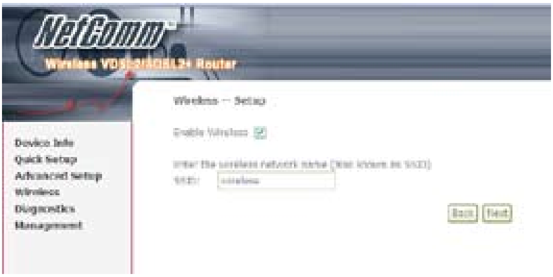
This screen allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button Enable DHCP server and enter the Start and End IP addresses and DHCP leased time.

To configure a secondary IP address for the LAN port, tick the checkbox shown.



☑ Configure the second IP Address and Subnet Mask for LAN interface
IP Address:
Subnet Mask:

7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click Next.



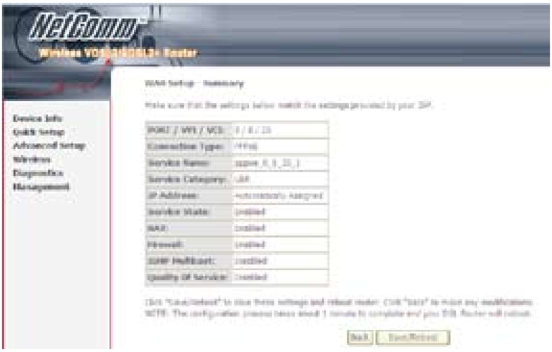
Wireless -- Setup

Enable Wireless ☑

Enter the wireless network name (also known as SSID).

SSID: wireless

8: Click Next to display the WAN Setup-Summary screen that presents the entire configuration summary. Click Save/Reboot if the settings are correct. Click Back if you wish to modify the settings.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_8_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

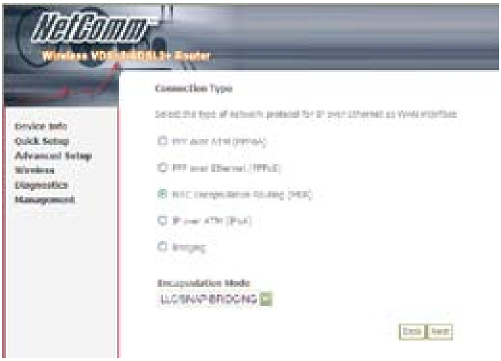
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

9: After clicking **Save/Reboot**, the router will save the configuration to flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The router is ready for operation when the LED indicators display as described in **Error! Reference source not found.**

4.2.2 MAC Encapsulation Routing (MER)

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the MAC Encapsulation Routing (MER) radio button and click Next.



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

● MAC Encapsulation Routing (MER)

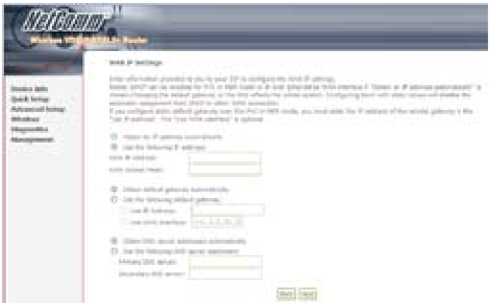
○ IP over ATM (IPoA)

○ Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

The following screen appears.



WAN IP Settings

[illegible]

○ Obtain an IP address automatically

● Use the following IP address:

WAN IP Address:

WAN Subnet Mask:

● Obtain default gateway automatically

○ Use the following default gateway:

Use IP Address:

Use WAN Interface:

● Obtain DNS server addresses automatically

○ Use the following DNS server addresses:

Primary DNS server:

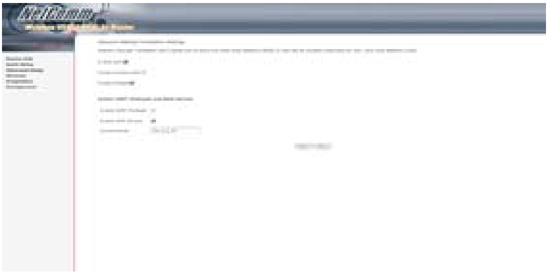
Secondary DNS server:

Enter information provided to you by your ISP to configure the WAN IP settings.

NOTE: DHCP can be enabled for PVC in MER mode if Obtain an IP address automatically is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address" field. The ISP will provide the values to enter in these fields.

5: Click **Next** to display the following screen.



Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will be gone.

Enable Fullcone NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will be gone.

Enable IGMP Multicast

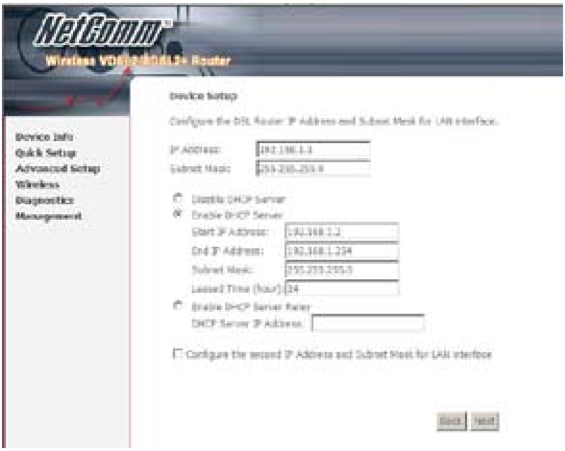
Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service

Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service.

Service Name: This is User-defined.

6: Upon completion click **Next**. The following screen appears.



Device Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Leased Time (hour): 24
○ Enable DHCP Server Relay
DHCP Server IP Address:

□ Configure the second IP Address and Subnet Mask for LAN interface

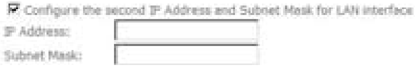
Consult the following paragraphs for more details about these settings.

The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP** server to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

NOTE: If NAT is enabled, Enable DHCP Server Relay won't display.

To configure a secondary IP address for the LAN port, tick the checkbox shown.

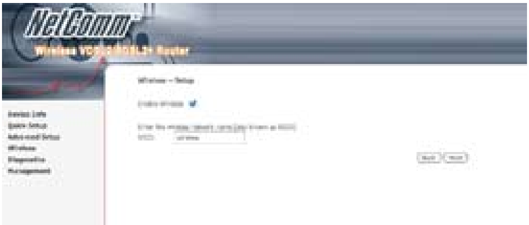


☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next.**



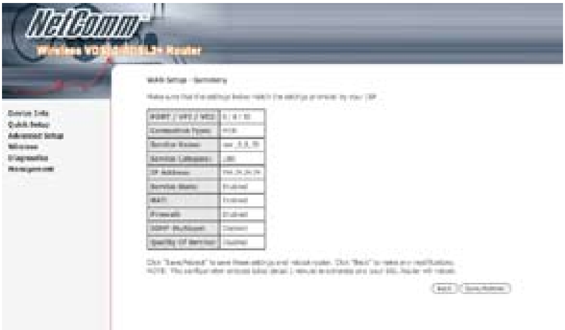
Wireless -- Setup

Enable Wireless ☑

Enter the wireless network name (also known as SSID).

SSID: wireless

The following screen will display.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	[illegible]
Connection Type:	[illegible]
Service Name:	[illegible]
Service Category:	[illegible]
IP Address:	[illegible]
Service State:	[illegible]
NAT:	[illegible]
Firewall:	[illegible]
IGMP Multicast:	[illegible]
Quality Of Service:	[illegible]

[illegible]

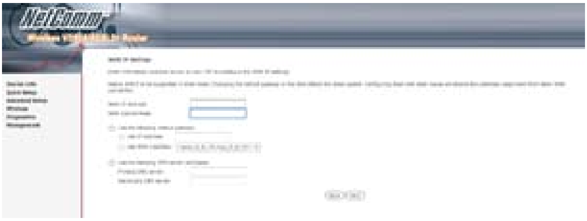
8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/ Reboot**, the router will save the configuration to flash memory and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically. The router is ready for operation when the LED indicators display as described in **Error! Reference source not found..**

4.2.3 IP Over ATM

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the IP over ATM (IPoA) radio button and click **Next**.

The following screen appears.



WAN IP Settings

[illegible]

[illegible]

WAN IP Address:

WAN Subnet Mask:

○ Use the following default gateway:

○ Use IP Address:

○ Use WAN Interface: [illegible]

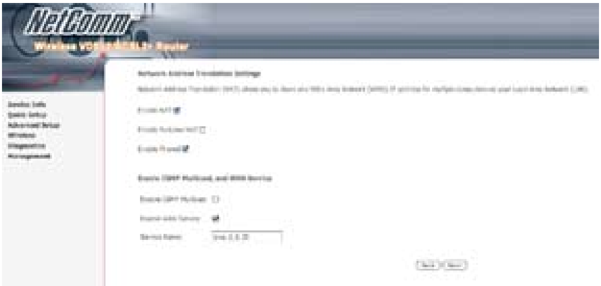
○ Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

NOTE: DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses provided by the ISP.

5: Click **Next**. The following screen appears.



Network Address Translation Settings

[illegible]

Enable NAT ☑

Enable Fullcone NAT □

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: [illegible]

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will be gone.

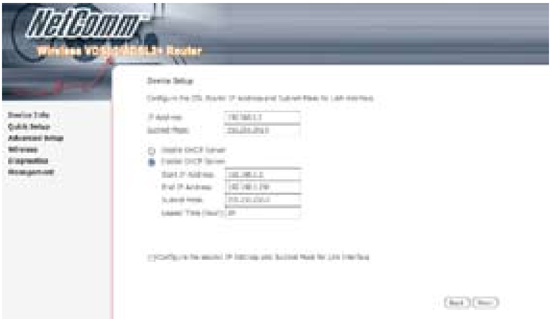
Enable Fullcone NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will be gone.

6: Click **Next** to display the following screen.



Device Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Leased Time (hour): 24

□ Configure the second IP Address and Subnet Mask for LAN interface

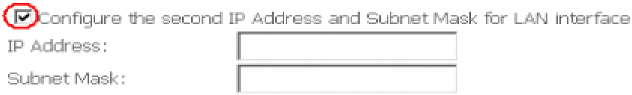
The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.

The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

NOTE: If NAT is enabled, Enable DHCP Server Relay won't display.

To configure a secondary IP address for the LAN port, click the box as shown below.

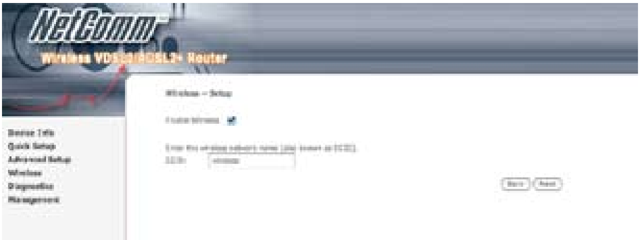


☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.



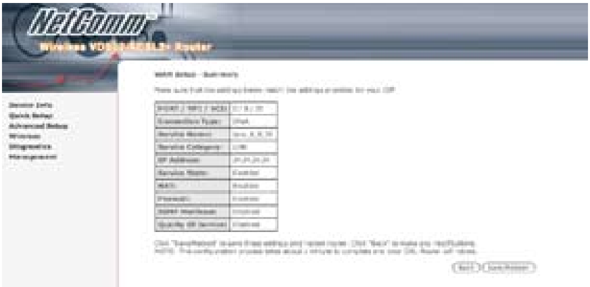
Wireless -- Setup

Enable Wireless ☑

Enter the wireless network name (also known as SSID).

SSID: wireless

The following screen will be displayed.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

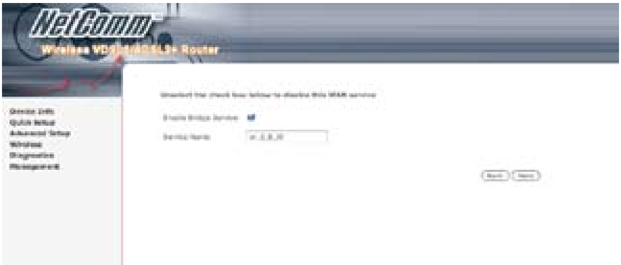
PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	[illegible]
Service Name:	[illegible]
Service Category:	UBR
IP Address:	[illegible]
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/ Reboot**, the router will save the configuration to the flash memory, and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically. The router is ready for operation when the LED indicators display as described in **Error! Reference source not found..**

4.2.4 Bridging

4: Select the Bridging radio button and click **Next**. The following screen appears. To use the bridge service, tick the **Enable Bridge Service** checkbox and enter a service name (user defined).

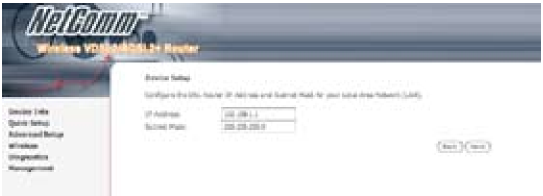


Unselect the check box below to disable this WAN service

Enable Bridge Service ☑

Service Name: br_0_8_35

5: Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the router. Notice that there is no IP address for the WAN interface in bridge mode, and technical support cannot access the router remotely.



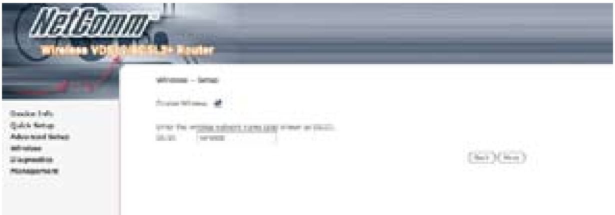
Device Setup

Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN).

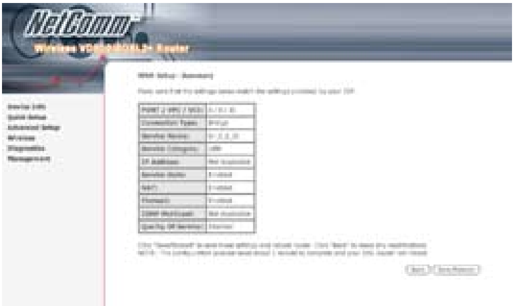
IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.



The following screen will be displayed.

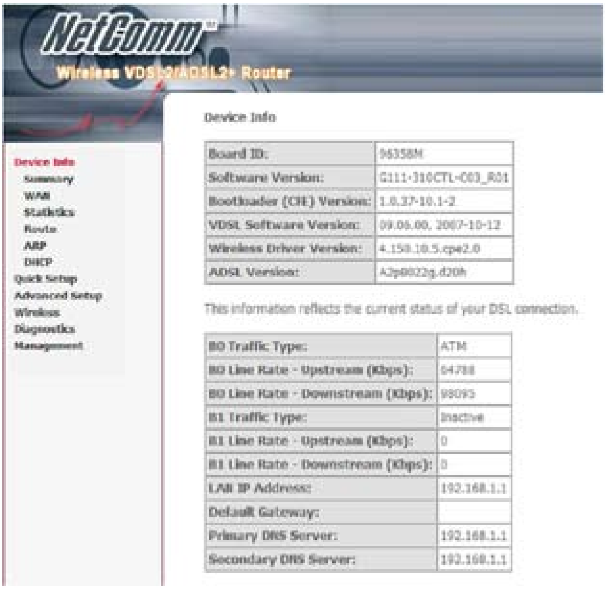


7: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically. The router is ready for operation when the LED indicators display as described in **Error! Reference source not found.**.

Device Info

Device Info

Select **Device Info** from the main menu to display Summary information as below.



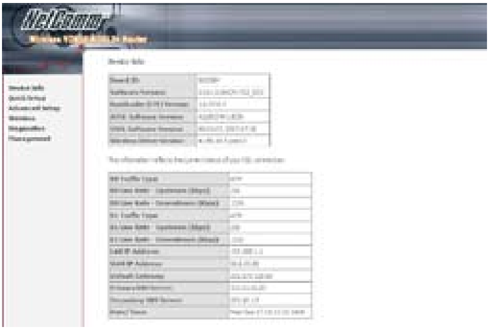
Device Info

Board ID:	96358M
Software Version:	G111-310CTL-C03_R01
Bootloader (CFE) Version:	1.0.37-10.1-2
VDSL Software Version:	09.06.00, 2007-10-12
Wireless Driver Version:	4.150.10.5.cpe2.0
ADSL Version:	A2pB022g.d20h

This information reflects the current status of your DSL connection.

B0 Traffic Type:	ATM
B0 Line Rate - Upstream (Kbps):	54788
B0 Line Rate - Downstream (Kbps):	98093
B1 Traffic Type:	Inactive
B1 Line Rate - Upstream (Kbps):	0
B1 Line Rate - Downstream (Kbps):	0
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

NOTE: The figure above shows the summary screen with a VDSL signal.



Device Info

Board ID:	[illegible]
Software Version:	[illegible]
Bootloader (CFE) Version:	[illegible]
ADSL Software Version:	[illegible]
VDSL Software Version:	[illegible]
Wireless Driver Version:	[illegible]

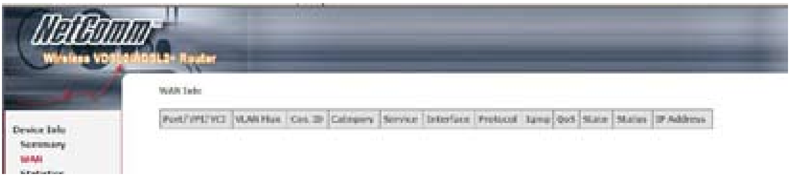
This information reflects the current status of your DSL connection.

B0 Traffic Type:	[illegible]
B0 Line Rate - Upstream (Kbps):	[illegible]
B0 Line Rate - Downstream (Kbps):	[illegible]
B1 Traffic Type:	[illegible]
B1 Line Rate - Upstream (Kbps):	[illegible]
B1 Line Rate - Downstream (Kbps):	[illegible]
LAN IP Address:	[illegible]
WAN IP Address:	[illegible]
Default Gateway:	[illegible]
Primary DNS Server:	[illegible]
Secondary DNS Server:	[illegible]
Date/Time:	[illegible]

NOTE: The figure above shows the summary screen with an ADSL signal.

5.1 WAN

Select WAN from the Device Info menu to display the status of all configured PVC(s).



WAN Info

Port/VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address

Port/VPI/VCI	Shows the values of the ATM Port/VPI/VCI
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type (e.g. PPPoE, PPPoA, etc.)
IGMP	Shows the status of the IGMP function
QoS	Shows the status of the QoS function
State	Shows the connection state of the WAN connection
Status	Lists the status of the PVC.
IP Address	Shows IP address for WAN interface

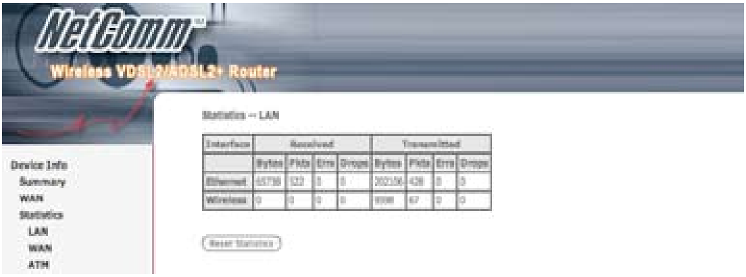
5.2 Statistics

This submenu provides statistics for LAN, WAN, ATM, ADSL and VDSL connections.

NOTE: These statistics refresh every 10 seconds.

5.2.1 LAN Statistics

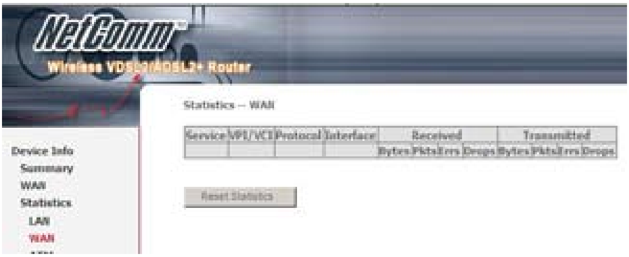
The Network Statistics screen shows interface statistics for Ethernet and Wireless interfaces. (The Network Statistics screen shows interface statistics of LAN. Eg; Here provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	65738	322	1	0	202156	428	0	0
Wireless	0	0	0	0	9598	67	0	0

5.2.2 WAN Statistics



Statistics -- WAN

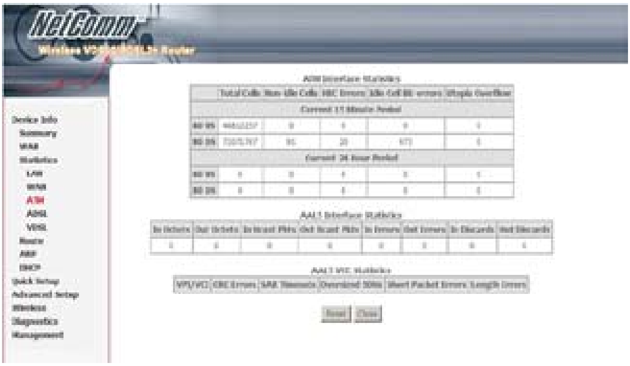
Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

Service		Shows the service type
VPI/VCI		Shows the values of the ATM VPI/VCI
Protocol		Shows the connection type
Interface		Shows connection interfaces
Received/Transmitted	- Bytes	Rx/TX (receive/transmit) packet in Byte
	- Pkts	Rx/TX (receive/transmit) packets
	- Errs	Rx/TX (receive/transmit) packets with errors
	- Drops	Rx/TX (receive/transmit) dropped packets

5.2.3 ATM statistics

VDSL

The figure below shows the ATM statistics screen when using VDSL.



ATM Interface Statistics

	Total Cells	Non-idle Cells	HEC Errors	Idle Cell Bit-errors	Utopia Overflow
Current 15 Minute Period					
B0 US	[illegible]	0	0	0	0
B0 DS	[illegible]	91	20	671	0
Current 24 Hour Period					
B0 US	0	0	0	0	0
B0 DS	0	0	0	0	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors

ATM Interface Statistics (VDSL)

This data is grouped according to bearer (B0/B1) and time period (15 min/24 hour).

Field	Description
Total Cells	Number of Total Cells
Non-idle Cells	Number of Non-idle Cells
HEC Errors	Number of cells dropped due to uncorrectable HEC errors
Idle Cell Bit-errors	Number of Bit errors in Idle Cells
Utopia Overflow	Number of cells dropped coming from the UTOPIA bus

AAL5 Interface Statistics

Field	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDUs octets transmitted
In Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission

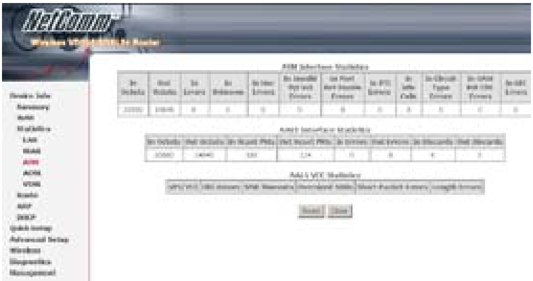
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmissions
In Errors	Number of received AAL5/AAL0 CPCS PDUs received that contain an error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

AAL5 VCC Statistics

Field	Description
VPI/VCI	Shows the values of the ATM VPI/VCI
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Oversized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packet Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

ADSL

The figure below shows the ATM statistics screen when using ADSL.

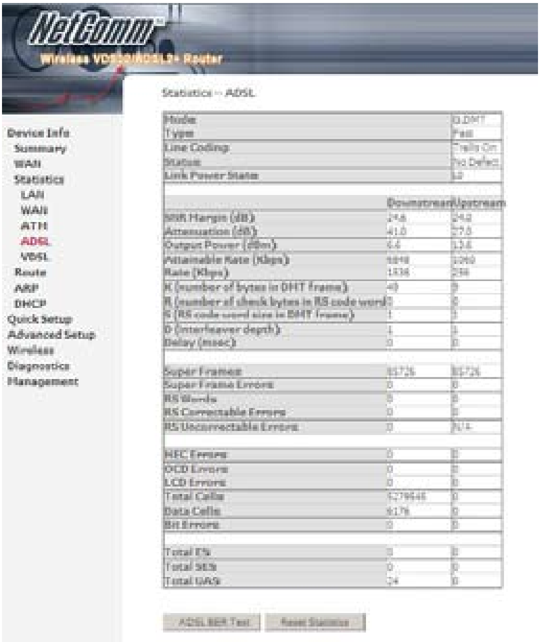


ATM Interface Statistics (ADSL)

Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEX error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In OAM RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

5.2.4 ADSL Statistics

The following graphic shows the ADSL Network Statistics screen. The **Reset** button (located at the bottom of the screen) can be used to reset statistics. The bit error rate can be tested by clicking the **ADSL BER** Test button.



Statistics -- ADSL

Mode	G.DMT
Type	Fast
Line Coding	Trellis On
Status	No Defect
Link Power State	L0

	Downstream	Upstream
SNR Margin (dB)	24.6	24.0
Attenuation (dB)	41.0	27.0
Output Power (dBm)	6.4	12.6
Attainable Rate (Kbps)	5848	1092
Rate (Kbps)	1536	256
K (number of bytes in DMT frame)	49	9
R (number of check bytes in RS code word)	0	0
S (RS code word size in DMT frame)	1	1
D (interleaver depth)	1	1
Delay (msec)	0	0
Super Frames	85726	85726
Super Frame Errors	0	0
RS Words	0	0
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	N/A
HEC Errors	0	0
OCD Errors	0	0
LCD Errors	0	0
Total Cells	5279646	0
Data Cells	6176	0
Bit Errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	24	0

Consult the table that follows for field descriptions.

Field	Description
Mode	Line Coding format (e.g. G.dmt, G.lite, T1.413, ADSL2)
Type	Channel type (Interleave or Fast)
Line Coding	Trellis On/Off
Status	Lists the status of the ADSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.

n G.DMT mode the following section is inserted here.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

In ADSL2+ mode the following section is inserted here.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

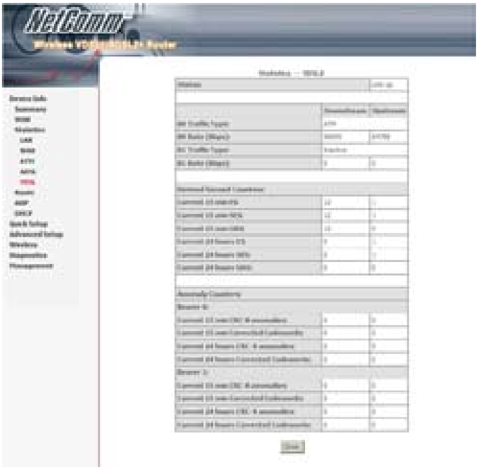
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle and data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

In ADSL2+ mode the following section is inserted here.

Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

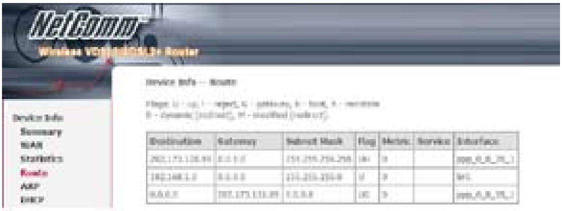
5.2.5 VDSL Statistics



Field	Description
Status:	VDSL link status.
B0 Traffic Type:	ATM or PTM
B0 Rate (Kbps):	Bearer 0 current sync rate.
B1 Traffic Type:	ATM or PTM
B1 Rate (Kbps):	Bearer 1 current sync rate.
Derived Second Counters:	
Current 15 min ES:	An accumulative total for current 15 minute ES.
Current 15 min SES:	An accumulative total for current 15 minute SES.
Current 15 min UAS:	An accumulative total for current 15 minutes UAS.
Current 24 hours ES:	An accumulative total for current 24 hours ES.
Current 24 hours SES:	An accumulative total for current 24 hours SES.
Current 24 hours UAS:	An accumulative total for current 24 hours UAS.

Anomaly Counters:	
Bearer 0:	
Current 15 min CRC-8 anomalies:	An accumulative total for current 15 minute CRC-8 anomalies
Current 15 min Corrected Codewords:	An accumulative total for current 15 minute Corrected Codewords
Current 24 hours CRC-8 anomalies:	An accumulative total for current 24 hours CRC-8 anomalies
Current 24 hours Corrected Codewords:	An accumulative total for current 24 hours CRC-8 Corrected Codewords
Bearer 1:	
Current 15 min CRC-8 anomalies:	An accumulative total for current 15 minute CRC-8 anomalies
Current 15 min Corrected Codewords:	An accumulative total for current 15 minute Corrected Codewords
Current 24 hours CRC-8 anomalies:	An accumulative total for current 24 hours CRC-8 anomalies
Current 24 hours Corrected Codewords:	An accumulative total for current 24 hours CRC-8 Corrected Codewords

5.3 Route



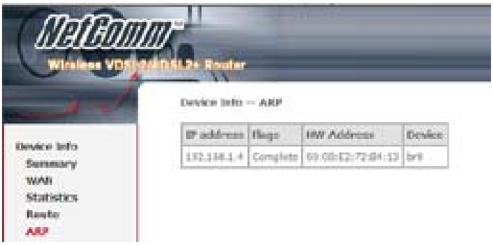
Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
[illegible]	0.0.0.0	255.255.255.255	UH	0		ppp_0_8_35_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	[illegible]	0.0.0.0	UG	0		ppp_0_8_35_1

Clicking on ‘Device Info’, then ‘Route’ shows the advanced route configuration of your NB11WD

5.4 ARP

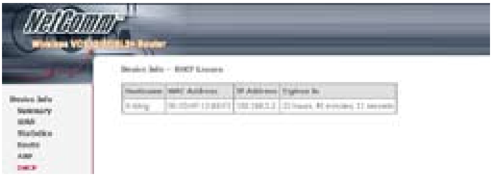


Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.4	Complete	[illegible]	br0

Clicking on ‘Device Info’, then ‘ARP’ shows the current ARP table (The automatic mapping of IP Addresses to MAC addresses) on the NB11WD.

5.5 DHCP



Device Info -- DHCP Leases

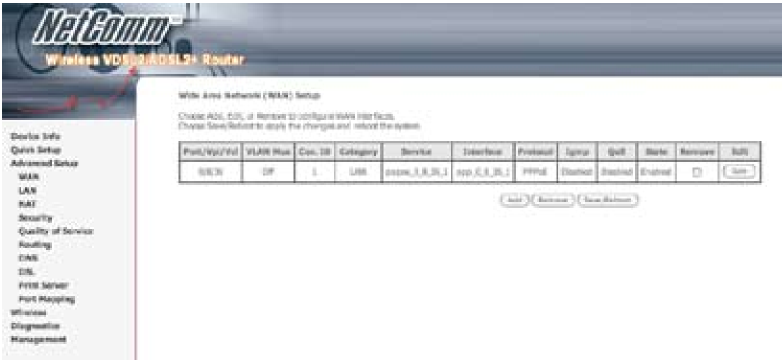
Hostname	MAC Address	IP Address	Expires In
[illegible]	[illegible]	[illegible]	[illegible]

Clicking on ‘Device Info’, then ‘DHCP’ shows the current DHCP lease table of your NB11WD. This table shows the IP addresses that have been assigned by the NB11WD, to which devices they have been assigned, and when the DHCP lease will expire.

Advanced Setup

6.Advanced Setup

This chapter explains the Advanced Setup menu options outlined below.



Wide Area Network (WAN) Setup

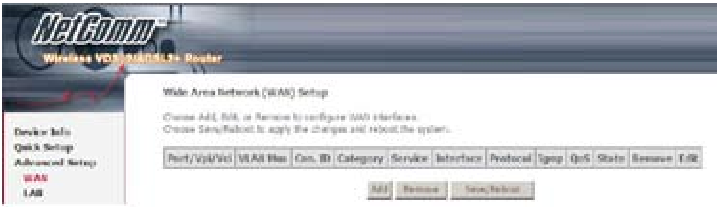
Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	□	Edit

NOTE: The selections available on this menu are based on configured connection settings and/or user account privileges. For example, NAT is not an available option in Bridge mode and may be disabled in MER or IPoA.

6.1 WAN

This screen allows for the advanced configuration of WAN interfaces.



Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit

- To Add a WAN connection, click the **Add** button. To edit an existing connection, click the Edit button next to the connection. To complete the Add or Edit, on the opening screen, select VLAN Mux (see section 6.1.1VLAN Mux) and then proceed to STEP 2 in section 4.2 Manual Quick Setup.

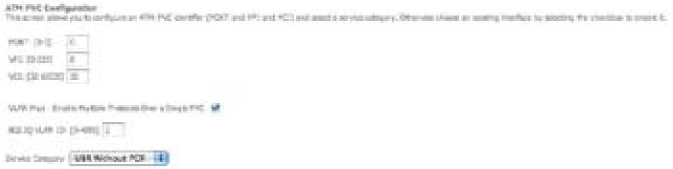
- To remove a connection select its radio button under the Remove column in the table and click the **Remove** button under the table.
- **Save/Reboot** activates the new configuration.

Port/VPI/VCI	ATM Port (0-3) / VPI (0-255) / VCI (32-65535)
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	ID for WAN connection
Category	ATM service category, e.g. UBR, CBR…
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows bridge or router mode
IGMP	Shows enable or disable IGMP proxy
QoS	Shows enable or disable QoS
State	Shows enable or disable WAN connection

6.1.1 VLAN Mux

VLAN Mux is a form of VLAN tagging that allows multiple protocols over a single connection. It is especially useful for VDSL2 connections in packet transfer mode.

Adding a new connection with VLAN Mux is accomplished by selecting the VLAN Mux – Enable Multiple Protocols Over a Single PVC check box (as outlined in red below). Enter a value for 802.Q VLAN ID in the box that appears below.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

PORT: [0-3] 0

VPI: [0-255] 8

VCI: [32-65535] 35

VLAN Mux - Enable Multiple Protocols Over a Single PVC ☑

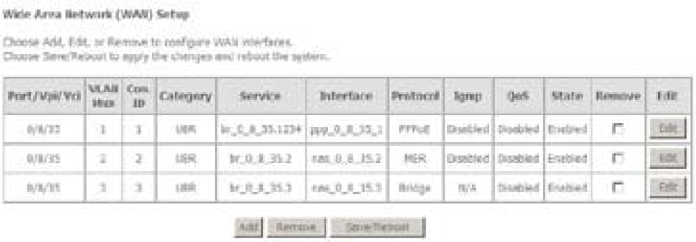
802.1Q VLAN ID: [0-4095] 1

Service Category: UBR Without PCR

After proceeding to STEP 3 in section 4.2 Manual Quick Setup, the screen will appear as follows. Notice that PPPoA and IPoA are not available.

PVCs can be added using the regular procedure, however, now multiple protocols can exist over the same connection, as long as the 802.1Q VLAN IDs differ.

The graphic below shows an example of three protocols over the same connection.



Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/8/35	1	1	UBR	br_0_8_35.1234	ppp_0_8_35_1	PPPoE	Disabled	Disabled	Enabled	□	Edit
0/8/35	2	2	UBR	br_0_8_35.2	nas_0_8_35.2	MER	Disabled	Disabled	Enabled	□	Edit
0/8/35	3	3	UBR	br_0_8_35.3	nas_0_8_35.3	Bridge	N/A	Disabled	Enabled	□	Edit

6.1.2 MSP

Multi-Service over PVC (MSP) supports multiple protocols over a single connection. As with the VLAN Mux function, PPPoE, Bridge and MER protocols can coexist, while IPoA and PPPoA are not supported. This function supports remote management by bridge protocol in addition to multimedia applications over a single PVC.

Configuring MSP is a two-part process:

Part 1 - Create multiple PVCs (One Bridge + multiple PPPoE / One MER)

Part 2 - Use Port Mapping to connect LAN / WAN interfaces

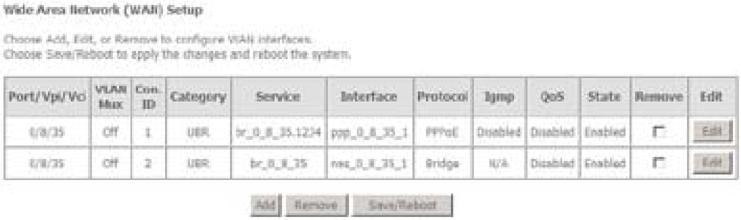
NOTE: The example below shows how to configure a Bridge / PPPoE MSP connection. Use the same process for Bridge / MER MSP connections.

If QoS is configured on the first MSP connection, it will be configured by default for all subsequent connections.

If a MSP connection is removed every other MSP connection should be removed to avoid port mapping configuration problems.

Part 1 – Create Multiple PVCs

On the Advanced Setup – WAN screen, create one PPPoE connection and one Bridge connection on the MSP supporting PVC. The screen will display as follows.



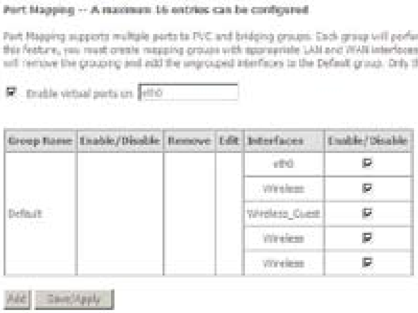
Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/8/35	Off	1	UBR	br_0_8_35.1234	ppp_0_8_35_1	PPPoE	Disabled	Disabled	Enabled	□	Edit
0/8/35	Off	2	UBR	br_0_8_35	nas_0_8_35_1	Bridge	N/A	Disabled	Enabled	□	Edit

Part 2

Go to Advanced Setup – Port Mapping screen (see section 6.10 Port Mapping) and select the Enable Virtual Ports checkbox. The screen will display as follows.



Port Mapping -- A maximum 16 entries can be configured

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

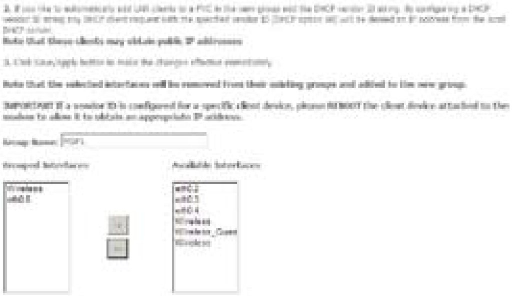
☑ Enable virtual ports on: eth0

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				eth0	☑
				Wireless	☑
				Wireless_Guest	☑
				Wireless	☑
				Wireless	☑

NOTE: Only hardware ports and bridge PVCs are listed as interfaces. The bridge interface is shown as “nas_x_y_z” where x=port, y=vpi, and z=vci.

To continue, click the **Add** button at the bottom of the screen shown above.

On the screen shown below, select the bridge connection and one Ethernet virtual port (ENET 1-4). Enter a group name, such as “MSP1”, and click **Save/Apply**.



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

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

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

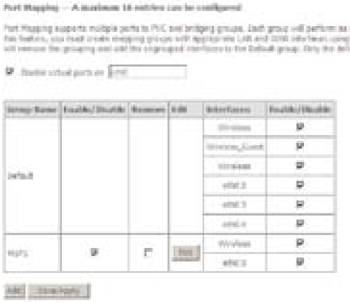
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name: MSP1

Grouped Interfaces
Wireless
eth0.5

Available Interfaces
eth0.2
eth0.3
eth0.4
Wireless
Wireless_Guest
Wireless

If successfully configured, the Port Mapping screen will display as follows.



Port Mapping -- A maximum 16 entries can be configured

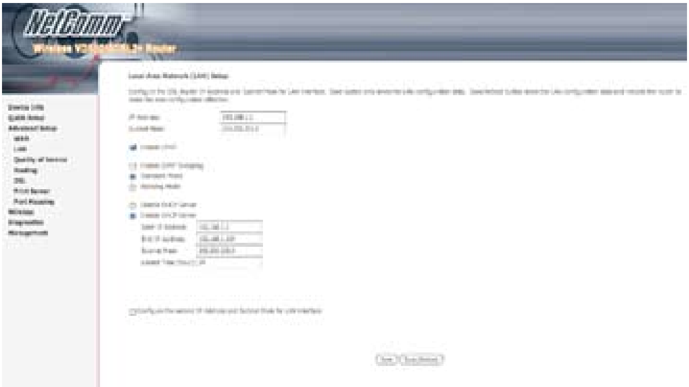
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces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

☑ Enable virtual ports on ENET

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				Wireless	☑
				Wireless_Guest	☑
				Wireless	☑
				eth0.2	☑
				eth0.3	☑
				eth0.4	☑
MSP1	☑	□	Edit	Wireless	☑
				eth0.5	☑

6.2 LAN

Use this screen to configure LAN interface settings.



Local Area Network (LAN) Setup

[illegible]

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☑ Enable UPnP

□ Enable IGMP Snooping

● Standard Mode

○ Blocking Mode

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: [illegible]

End IP Address: [illegible]

Subnet Mask: 255.255.255.0

Leased Time (hour): 24

□ Configure the second IP Address and Subnet Mask for LAN interface

NOTE: NAT is enabled so Enable UPnP is shown above while DHCP Server Relay is hidden. Consult the field descriptions below for more details.

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable UPnP: Tick the box to enable Universal Plug and Play.

This option is hidden when NAT disabled or if no PVC exists

Enable IGMP Snooping: Enable by ticking the box.

Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

DHCP Server: To enable DHCP, select Enable DHCP server and enter starting and ending IP addresses and the leased time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

DHCP Server Relay: Enable with checkbox and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. This option is hidden if NAT is enabled

Configure the second IP address by ticking the checkbox shown.

IP Address: Enter the secondary IP address for the LAN port.

Subnet Mask: Enter the secondary subnet mask for the LAN port.

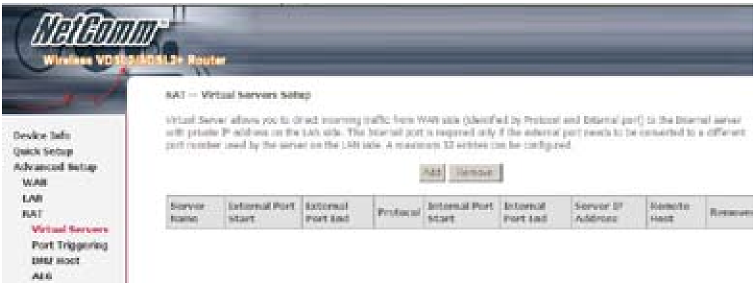
NOTE: The Save button saves new settings to allow continued configuration while the Save/Reboot button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

6.3 NAT

To display this option, NAT must be enabled in at least one PVC shown on the Advanced Setup - WAN screen. (NAT is not an available option in Bridge mode)

6.3.1 Virtual Servers

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

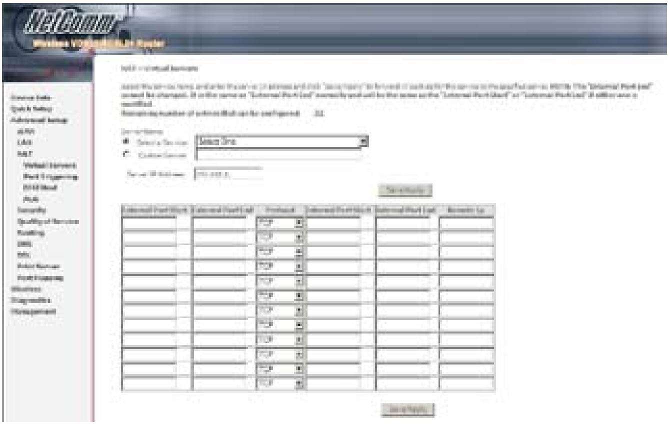


NAT -- Virtual Servers Setup

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove

To add a Virtual Server, click **Add**. The following screen will be displayed.



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.
Remaining number of entries that can be configured: 32

Server Name:
● Select a Service: Select One
○ Custom Server:

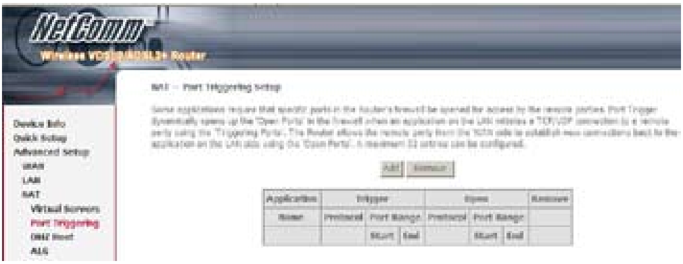
Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

Select a Service or Custom Server	User should select the service from the list. or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Remote IP	The IP address of the remote host

6.3.2 Port Triggering

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

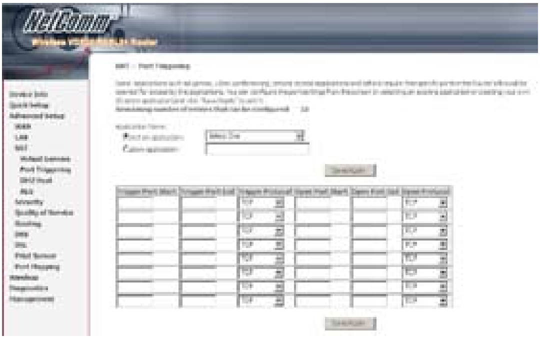


NAT -- Port Triggering Setup

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

Application	Trigger			Open			Remove
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	

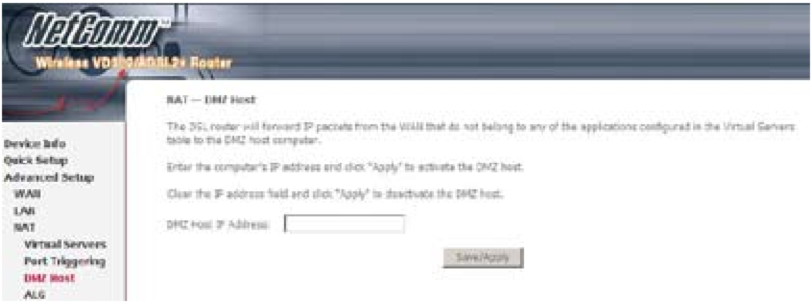
To add a Trigger Port, simply click the **Add** button. The following will be displayed.



Select an Application	
Or Custom Application	User should select the application from the list.
Or User can enter the name of their choice.	
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

6.3.3 DMZ Host

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



NAT -- DMZ Host

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

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

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

DMZ Host IP Address:

Enter the DMZ Host IP address and click **Save/Apply** to activate DMZ host.

Clear the IP address field and click **Save/Apply** to deactivate DMZ host.

6.3.4 ALG

SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication, while ALG stands for Application Layer Gateway. If the user has an IP phone (SIP) or VoIP gateway (SIP) behind the router, the SIP ALG can help VoIP packet passthrough the router (NAT enabled).

NOTE: This ALG is only valid for SIP protocol running on UDP port 5060.

6.4 Security

To display this option, the Firewall checkbox must be enabled in at least one PVC shown on the Advanced Setup - WAN screen.

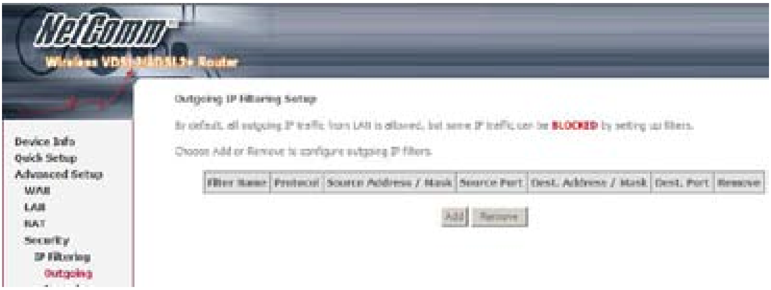
NOTE: For a more technical discussion of this topic see Appendix B: Firewall.

6.4.1 IP Filtering

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

Outgoing

The default setting for all Outgoing traffic is **ACCEPTED**.



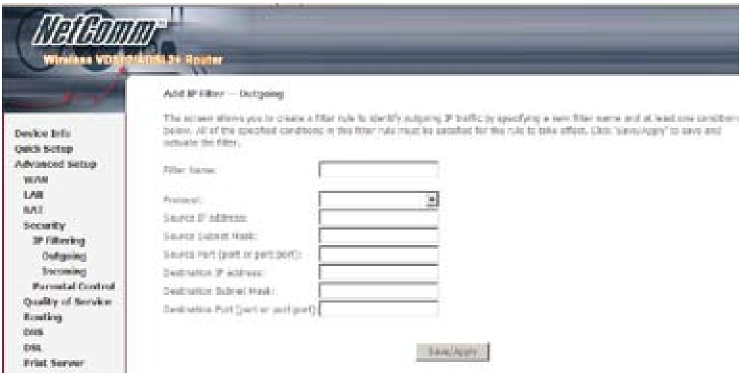
Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filtering rule, click the **Add** button. The following screen will be displayed.



Add IP Filter -- Outgoing

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

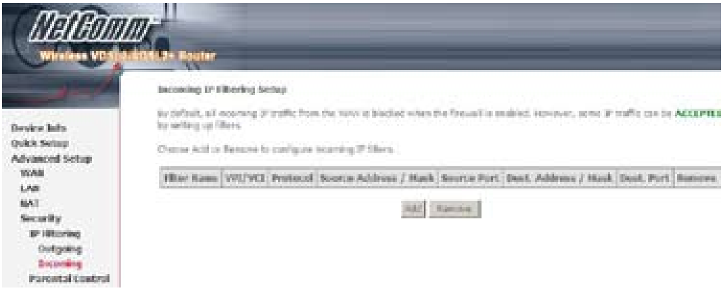
Destination Subnet Mask:

Destination Port (port or port:port):

Filter Name	Type a name for the filter rule.
Protocol	User can select: TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port **(port or port:port)**	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination Port **(port or port:port)**	Enter destination port number or range.

Incoming

The default setting for all Incoming traffic is Blocked.



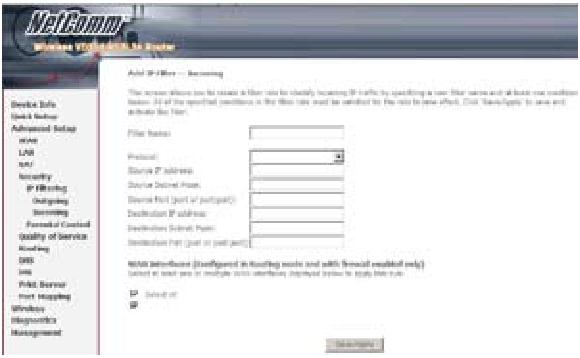
Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filtering rule, click the **Add** button. The following screen will be displayed.



Add IP Filter -- Incoming

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

Filter Name:	
Protocol:	
Source IP address:	
Source Subnet Mask:	
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	

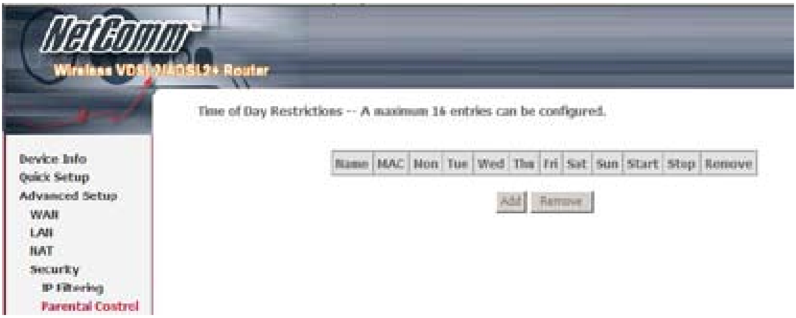
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All
☑

To configure the parameters, please reference the Outgoing table above. The Incoming IP Filter applies only to the PVCs selected at the bottom of the screen in the WAN Interfaces list. Only PVCs configured in routing mode (PPPoE, PPPoA, MER, or IPoA) with firewall enabled are available for selection.

6.4.2 Parental Control

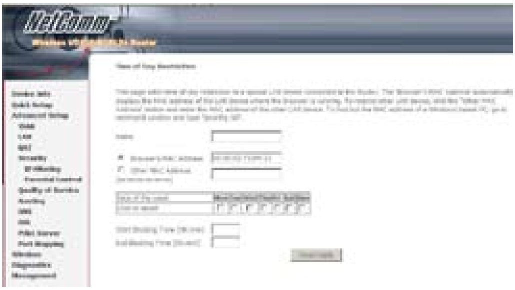
This allows parents, schools, and libraries to set access times for Internet use.



Time of Day Restrictions -- A maximum 16 entries can be configured.

Name	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

To add a time of day restriction click **Add**. The following screen will display.



User Name	Name of the Filter.
Browser's or Other MAC Address	Displays MAC address of the device on which the WUI is running or another MAC address.
Days of the week	Days when restrictions are applied. Click the checkbox under the days of the week.
Start/End Blocking Time	The times when restrictions start and stop.

NOTE: Parental Control must be activated to use Internet Time. Also, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP time server.

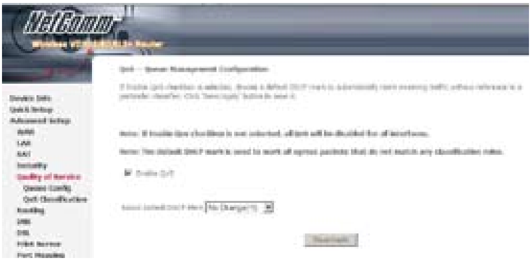
6.5 Quality of Service

Quality of Service (QoS) can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

NOTE: QoS must be enabled in at least one PVC to display this option. (see Advanced Setup - WAN for detailed PVC setup instructions).

6.5.1 Queue Management Configuration

To Enable QoS tick the checkbox, select Default DSCP Mark and click **Save/Apply**.

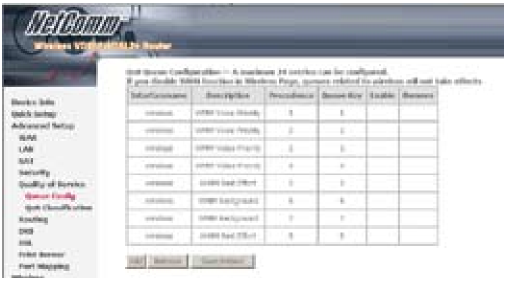


Select Default Differentiated Services Code Point (DSCP) Mark

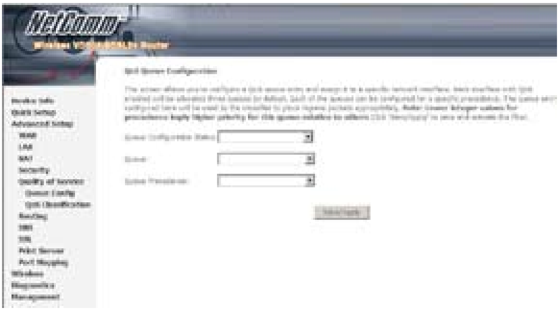
With this drop-down box you can assign a DSCP mark in the Internet Protocol (IP) header that specifies the per hop behavior for a given flow of incoming packets that do not match any other QoS rule.

6.5.2 QoS Queue Configuration

This function follows the **Differentiated Services** rule of IP QoS. You can create a new Queue rule by assigning an Interface, Enable/Disable and Precedence. The router uses various queuing strategies to tailor performance to user requirements



Click **Add** to display the following screen.

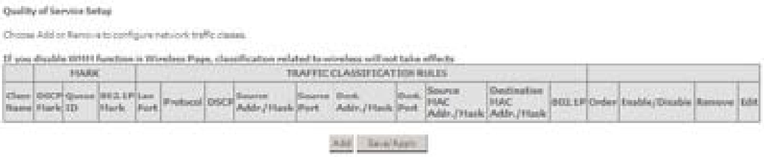


Queue Configuration Status: Enable or Disable the queue.

Queue: Assign queue to a specific network interface whose QoS is enabled.

Queue Precedence: Configure precedence for the queue. Lower integer values for precedence imply higher priority for this queue relative to others.

6.5.3 QoS Classification



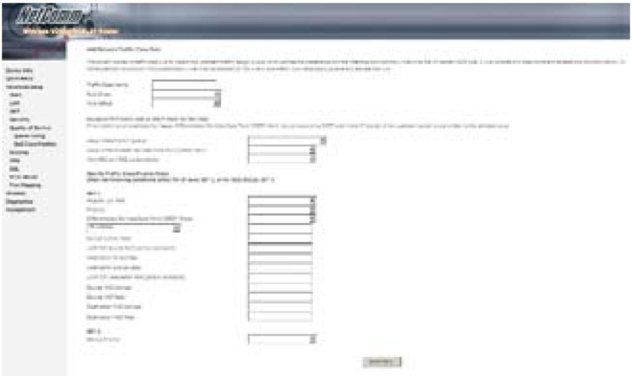
Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

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

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

Click **Add** to configure network traffic classes.



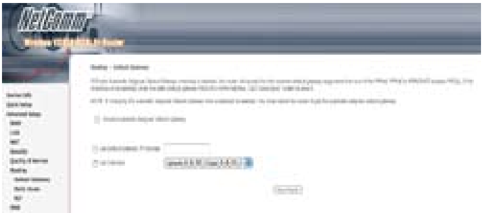
This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click **Save/Apply** to save and activate the rule.

6.6 Routing

6.6.1 Default Gateway

If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this router will accept the first received default gateway assignment from the DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway and/or WAN interface. Click **Save/Apply**.



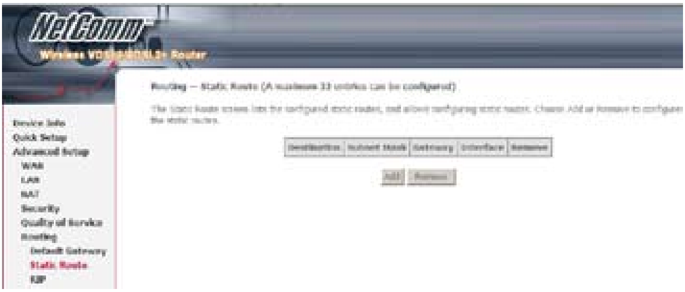
Routing -- Default Gateway

[illegible]

NOTE: After enabling Automatic Assigned Default Gateway, you must click the Save/Apply button to put it into effect. The router will reboot.

6.6.2 Static Route

This screen lists the configured static routes and allows for the configuration of static routes. Choose Add or Remove to configure the static routes.

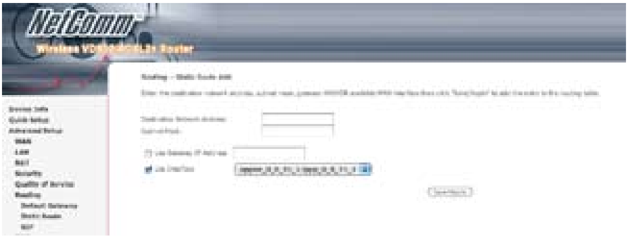


Routing -- Static Route (A maximum 32 entries can be configured)

The Static Route screen lists the configured static routes, and allows configuring static routes. Choose Add or Remove to configure the static routes.

Destination	Subnet Mask	Gateway	Interface	Remove

To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.



Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

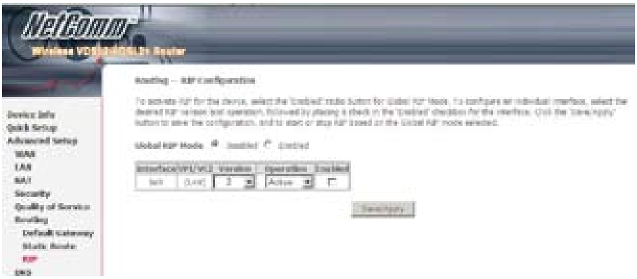
☐ Use Gateway IP Address

☑ Use Interface [illegible]

Save/Apply

6.6.3 RIP

To activate RIP for the router, select the Enabled radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the Enabled checkbox for the interface. Click **Save/Apply** to save settings and start/stop RIP (based on Global RIP mode).



Routing -- RIP Configuration

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

Global RIP Mode ● Disabled ○ Enabled

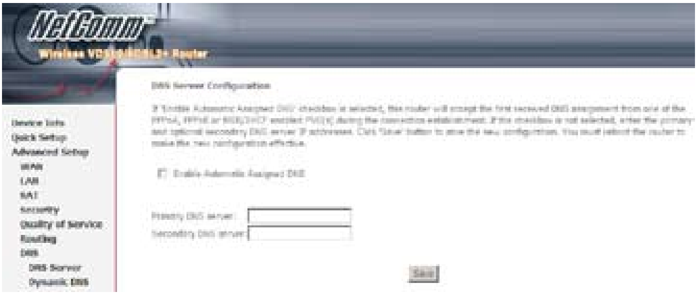
Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	☐

Save/Apply

6.7 DNS

6.7.1 DNS Server

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



DNS Server Configuration

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

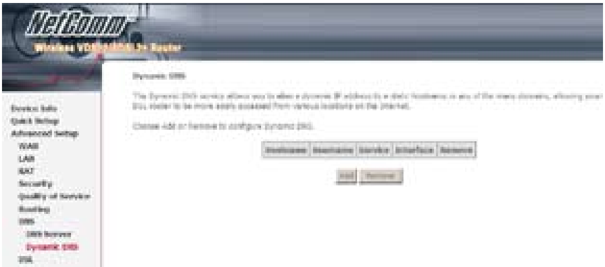
□ Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

6.7.2 Dynamic DNS

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



Dynamic DNS

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

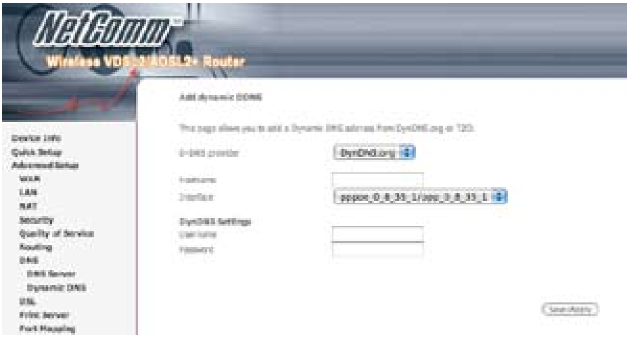
Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Add | Remove

NOTE: The Add and Remove buttons will only be displayed if the CPE has already been assigned an IP address from the remote server.

To add a dynamic DNS service, click **Add** and the following screen will display.



Add dynamic DDNS

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

D-DNS provider: DynDNS.org

Hostname:

Interface: pppoe_0_8_35_1/ppp_0_8_35_1

DynDNS Settings

User name:

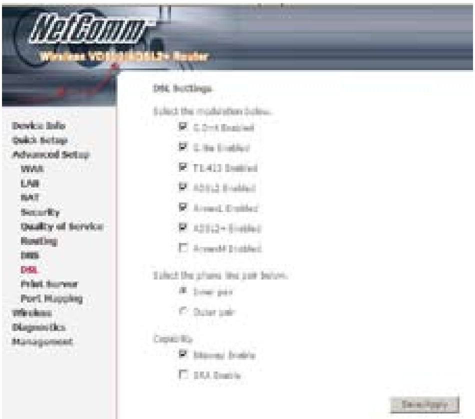
Password:

Save/Apply

D-DNS provider	Select a dynamic DNS provider from the list.
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list.
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

6.8 DSL

This screen is used to select ADSL modulations and capabilities.



DSL Settings

Select the modulation below.

☑ G.Dmt Enabled
☑ G.lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
□ AnnexM Enabled

Select the phone line pair below.

● Inner pair
○ Outer pair

Capability

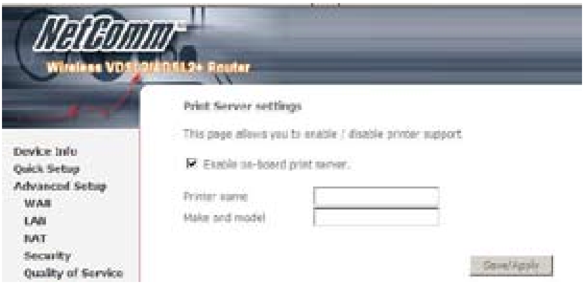
☑ Bitswap Enable
□ SRA Enable

The following table describes these DSL settings

Option	Description
G.dmt	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite	Sets G.Lite if you want the system to use G.Lite mode.
T1.413	Sets the T1.413 if you want the system to use T1.413 mode.
ADSL2	The router can support the functions of ADSL2.
AnnexL	The router can support/enhance the long loop test.
ADSL2+	The router can support the functions of ADSL2+.
AnnexM	Enables a higher “upstream” data rate, by making use of some downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswapping function
SRA Enable	Allows seamless rate adaptation

6.9 Print Server

This router is equipped with one high-speed USB2.0 host connection. With software support, users can connect USB devices such as a printer and hard drive to the router. For this software release, only the print server is supported.



Print Server settings

This page allows you to enable / disable printer support.

☑ Enable on-board print server.

Printer name

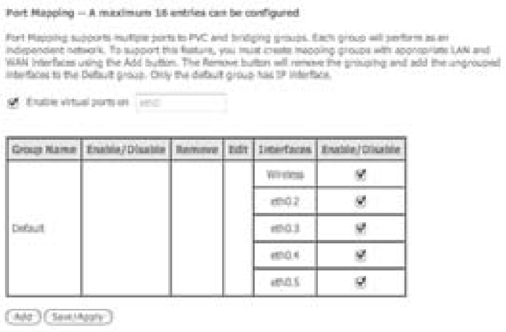
Make and model

NOTE: Please refer to Appendix A: Printer Server for detailed setup instructions.

6.10 Port Mapping

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

As shown below, when you tick the Enable virtual ports on checkbox, all of the LAN interfaces will be put together as a default group.

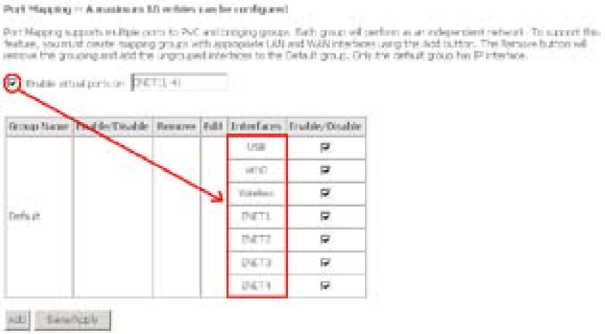


Port Mapping -- A maximum 16 entries can be configured

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

☑ Enable virtual ports on eth0

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				Wireless	☑
				eth0.2	☑
				eth0.3	☑
				eth0.4	☑
				eth0.5	☑



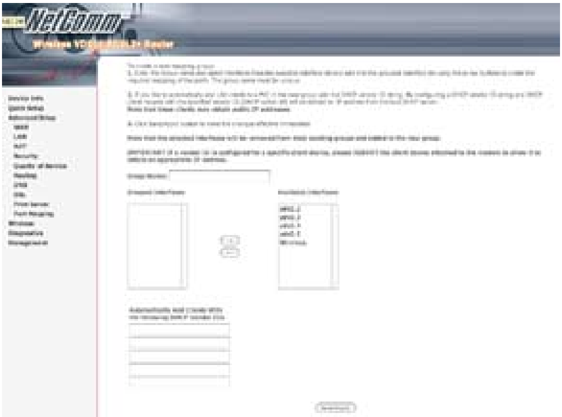
Port Mapping -- A maximum 16 entries can be configured

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

☑ Enable virtual ports on ENET(1-4)

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				USB	☑
				ath0	☑
				Wireless	☑
				ENET1	☑
				ENET2	☑
				ENET3	☑
				ENET4	☑

To add a port mapping group, click the **Add** button.



To create a group from the list, first enter the group name and then select from the available interfaces on the list with the arrow buttons -> <-.

Automatically Add Clients With the Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces including Wireless and USB to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when PortMapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE and the others are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, ENET4, Wireless and USB. Port mapping configuration is:

1. Default: ENET1, ENET2, ENET3, ENET4, Wireless and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38. The DHCP vendor ID is "Video".

The CPE deco server is running on "Default". And ISP's deco server is running on PVC 0/36. It is for set-top box use only.

On the LAN side, the PC can get IP address from CPE deco server and access the Internet via PPPoE (0/33).

If the set-top box was connected with interface "ENET1" and send a deco request with vendor id "Video", the CPE deco server would forward this request to ISP's deco server. Then the CPE will change the PortMapping configuration automatically.

The PortMapping configuration would become:

1. Default: ENET1, ENET2, ENET3, ENET4, Wireless and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38 and ENET1.

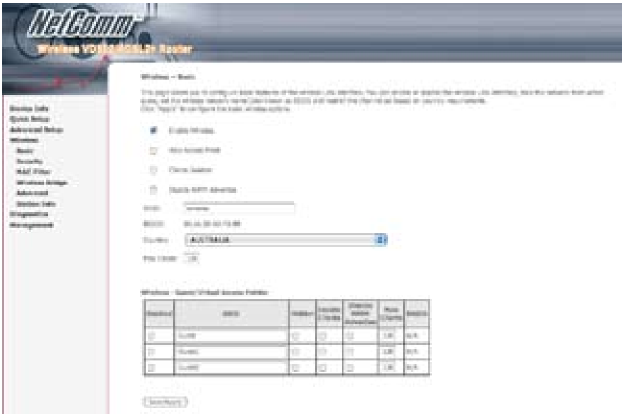
Wireless

Wireless

The Wireless dialog box allows you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.

7.1 Basic

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



Click **Save/Apply** to configure the basic wireless options.

Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected. The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration. In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.
Clients Isolation	1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood.
	2. Prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video). (wireless software version 3.10 and above)
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the radio buttons under the Enable heading. To hide a Guest SSID select its radio button under the Hidden heading.
	Do the same for Isolate Client and Disable WMM Advertise functions. For a description of these two functions, see the entries for "Client Isolation" and "Disable WMM Advertise" in this table. Similarly, for Max Clients and BSSID headings, consult the matching entries in this table.
	NOTE: Remote wireless hosts are unable to scan Guest SSIDs.

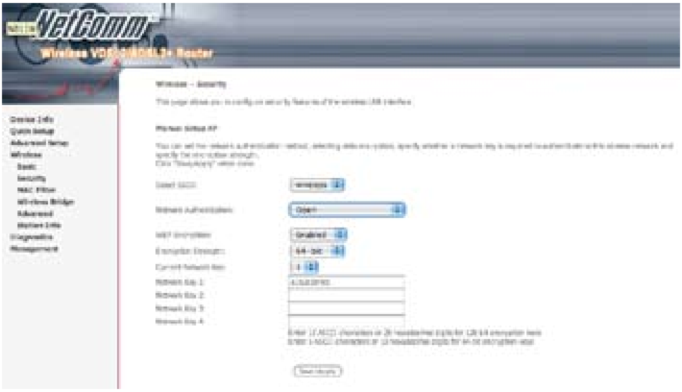
7.2 Security

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from 802.11 wireless network communications channel.

The following screen appears when Security is selected. The Security screen allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click **Apply** to configure the wireless security options.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.

Select SSID: [illegible]

Network Authentication: Open

WEP Encryption: Enabled

Encryption Strength: 64-bit

Current Network Key: 1

Network Key 1: [illegible]

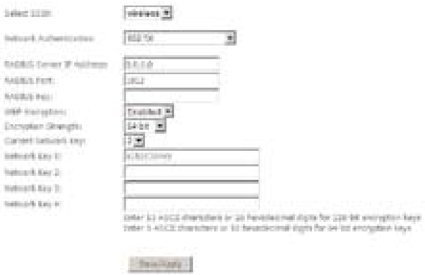
Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Option	Description
Select SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
Network Authentication	It specifies the network authentication. When this checkbox is selected, it specifies that a network key be used for authentication to the wireless network. If the Network Authentication (Shared mode) checkbox is not shared (that is, if open system authentication is used), no authentication is provided. Open system authentication only performs identity verifications. Different authentication type pops up different settings requests. Choosing 802.1X, enter RADIUS Server IP address, RADIUS Port, and RADIUS key. Also, enable WEP Encryption and the Encryption Strength.

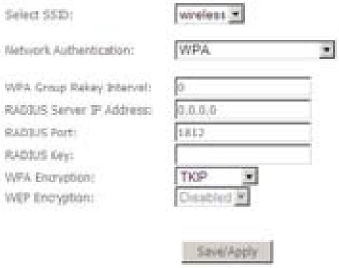


Select SSID:	wireless
Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled
Encryption Strength:	64-bit
Current Network Key:	1
Network Key 1:	[illegible]
Network Key 2:	
Network Key 3:	
Network Key 4:	

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

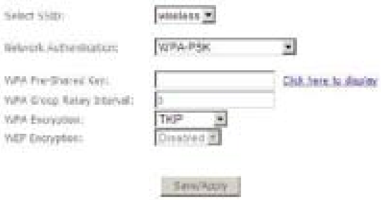
Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Choosing WPA, you must enter WPA Group Rekey Interval.



Select SSID:	wireless
Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP
WEP Encryption:	Disabled

Choosing WPA-PSK, you must enter WPA Pre-Shared Key and Group Rekey Interval.



Select SSID: wireless

Network Authentication: WPA-PSK

WPA Pre-Shared Key:

WPA Group Rekey Interval: 0

WPA Encryption: TKIP

WEP Encryption: Disabled

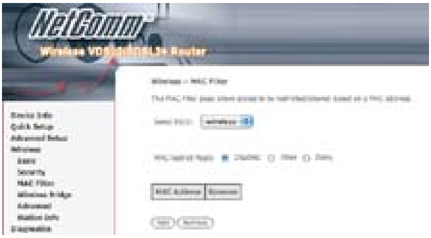
WEP Encryption	It specifies that a network key is used to encrypt the data is sent over the network. When this checkbox is selected, it enables data encryption and prompts the Encryption Strength drop-down menu. Data Encryption (WEP Enabled) and Network Authentication use the same key.
Encryption strength	A session's key strength is proportional to the number of binary bits comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode. This drop-down menu sets either a 64 8-bit (5-ASCII character or 10-hexadecimal character) or 128 8-bit (13-ASCII character or 26-hexadecimal character) key. If you set a minimum 128-bit key strength, users attempting to establish a secure communications channel with your server must use a browser capable of communicating with a 128-bit session key. The Encryption Strength settings do not display unless the network Authentication (shared Mode) check box is selected.

7.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers. When MAC address filtering is enabled, it restricts the devices that can connect to your access point.

To add a MAC Address filter, click the **Add** button shown below.

To delete a filter, select it from the table below and click the **Remove** button.



Wireless -- MAC Filter

The MAC Filter page allows access to be restricted/allowed based on a MAC address.

Select SSID: wireless

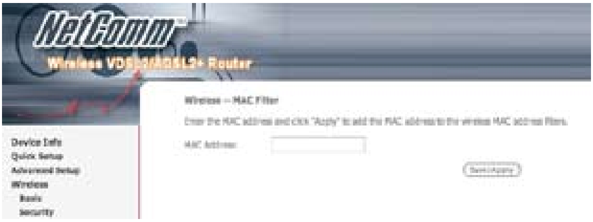
MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

Option	Description
MAC Restrict Mode	Disabled: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears.

Enter the MAC address in the box provided and click **Save/Apply**.



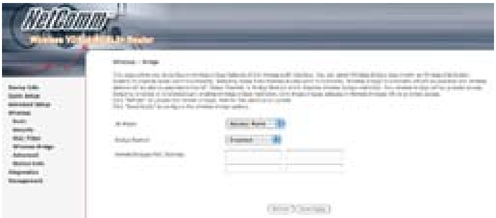
Wireless -- MAC Filter

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

MAC Address:

7.4 Wireless Bridge

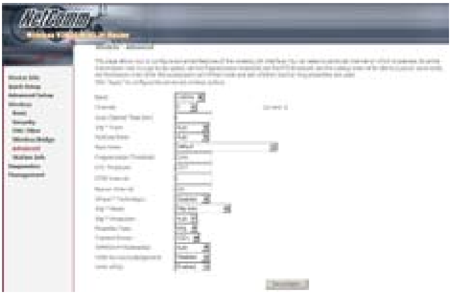
This screen allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict, which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.



7.5 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface.   You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click **Apply** to configure the advanced wireless options.

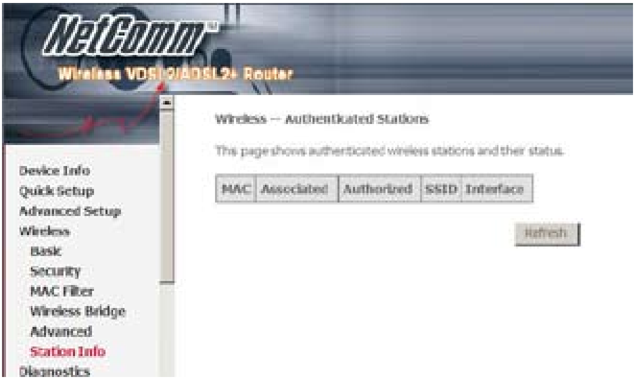


Option	Description
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Xpress TM Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
54g TM Mode	Set the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.

54g Protection	In Auto mode the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for application where maximum throughput is desired but it doesn't cooperate with the legacy. Long preamble interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	The router will set different power output (by percentage) according to this selection.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

7.6 Station Info

This screen shows authenticated wireless stations and their status.



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

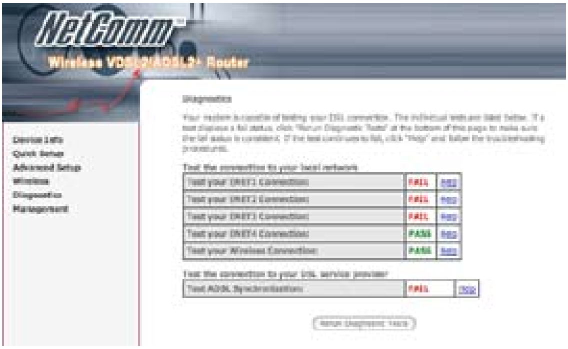
MAC	Associated	Authorized	SSID	Interface

Diagnostics

8.Diagnostics

The Diagnostics menu provides feedback on the connection status of the router and the DSL link. The individual tests are listed below. If a test displays a fail status, click Rerun Diagnostic Tests at the bottom of this screen to make sure the fail status is consistent. If the test continues to fail, click Help and follow the troubleshooting procedures provided onscreen.

MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.



Diagnostics

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

Test the connection to your local network

Test your ENET1 Connection:	FAIL	Help
Test your ENET2 Connection:	FAIL	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

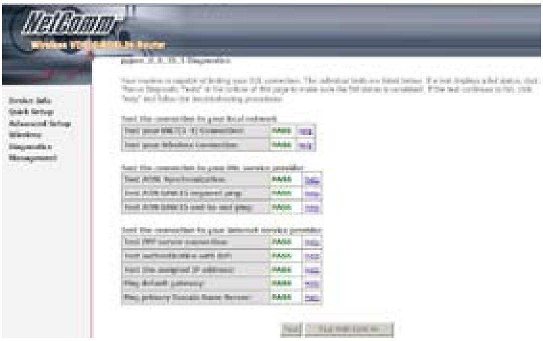
Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help

Test	Description
Ethernet Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of your router. Fail: Indicates that the router does not detect the Ethernet interface on your computer.
Wireless Connection	Pass: Indicates that the Wireless interface from your computer is connected to the wireless network. Down: Indicates that the router does not detect the wireless network.
ADSL Synchronization	Pass: Indicates that the router has detected an ADSL signal from the telephone company. Fail: Indicates that the router does not detect a signal from the telephone company's DSL network.

Additional tests are added here based upon connection type.

An example is provided below of the diagnostics screen for a PPPoE connection.



Ping Default Gateway	Pass: Indicates that the device can communicate with the first entry point to the network. It is usually the IP address of the ISP local router. Fail: Indicates that the device was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	Pass: Indicates that the device can communicate with the primary Domain Name Server (DNS). Fail: Indicates that the device was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

If multiple PVCs are configured you will have the option of testing each one in turn.

Click the Next Connection button at the bottom of the screen to do so.

The Management section includes the following functions and processes.

Settings	Internet Time
System Log	Access Control
SNMP Agent	Update Software
TR-069 Client	Save/Reboot

Management

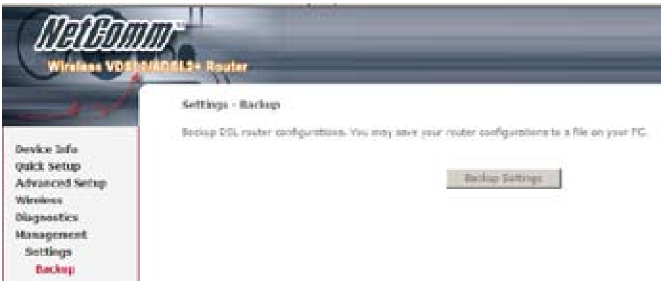
Management

9.1 Settings

The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.

9.1.1 Backup

The Backup option under Management > Settings saves your router configurations to a file on your PC. Click Backup Settings in the main menu. You will be prompted to define the location of the backup file to save. After choosing the file location, click Backup Settings. The file will then be saved to the assigned location.

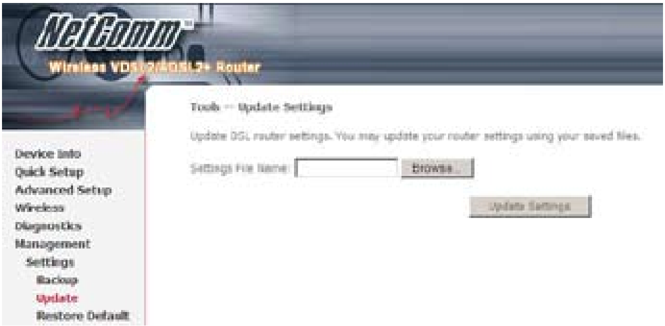


Settings - Backup

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

9.1.2 Update

This option updates your router settings using a previously saved settings file.



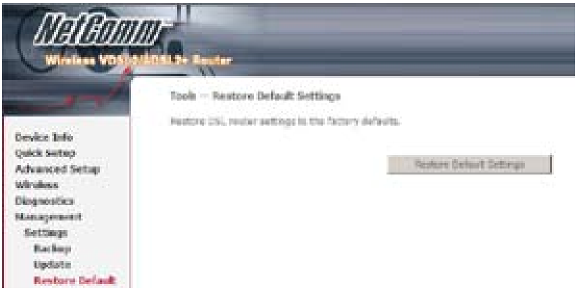
Tools -- Update Settings

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

Settings File Name:

9.1.3 Restore Default

Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings (see section 3.3 Default Settings).



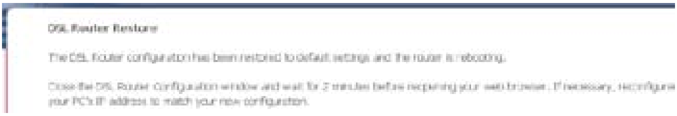
Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

NOTE 1: This option has the same effect as the hardware reset-to-default button on the rear panel of the router. The device board hardware and the boot loader support the reset to default button. If the reset button is pressed for more than 10 seconds, the configuration data will be erased.

NOTE 2: Restoring system settings requires a system reboot. The current Web UI session must be closed and restarted. Before restarting it, the IP configuration may need to be configured with a static IP address.

After the Restore Default Configuration button is selected, the following screen appears. Close the window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC IP address to match your new configuration.



DSL Router Restore

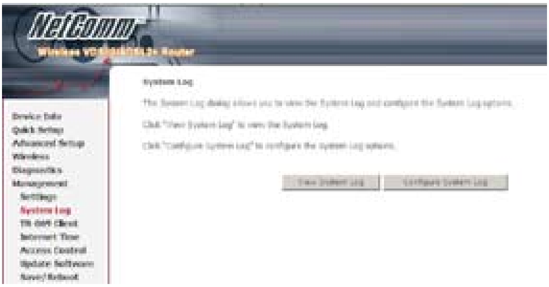
The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

9.2 System Log

The System Log option under Management > Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

1: Click **Configure System Log** to display the following screen.



System Log

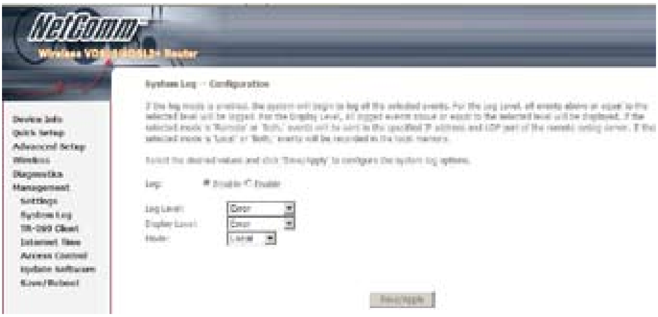
The System Log dialog allows you to view the System Log and configure the System Log options.

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

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

View System Log | Configure System Log

2: Select from the desired Log options described in the following table, and then click **Save/Apply**.



System Log -- Configuration

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

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

Log: ● Disable ○ Enable

Log Level: Error

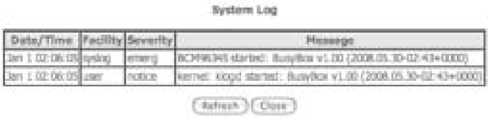
Display Level: Error

Mode: Local

Save/Apply

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the device SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the View System Log screen for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

3: Click **View System Log**. The results are displayed as follows.

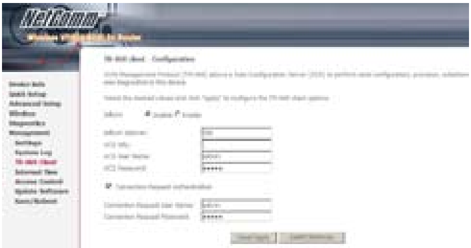


System Log

Date/Time	Facility	Severity	Message
Jan 1 02:06:05	syslog	emerg	BCM96345 started: BusyBox v1.00 (2008.05.30-02:43+0000)
Jan 1 02:06:05	user	notice	kernel: klogd started: BusyBox v1.00 (2008.05.30-02:43+0000)

9.3 TR-069 Client

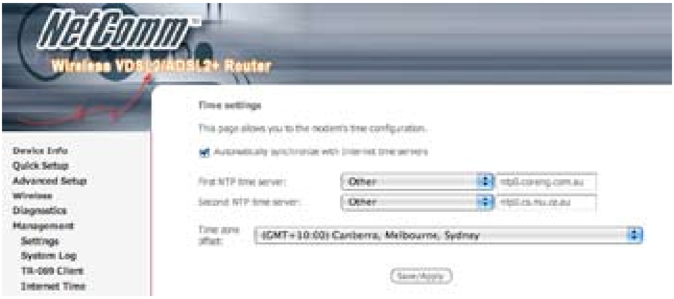
WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this router.



Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The “host” portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Connection Request Authentication	Enable/Disable authentication of ACS making a Connection Request to the CPE.
Connection Request User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to establish an immediate connection to the ACS.

9.4 Internet Time

The Internet Time option under the Management submenu configures the time settings of the device. To automatically synchronize with Internet time servers, tick the corresponding box displayed on this screen shown below.



Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server: Other ntp0.cornerg.com.au

Second NTP time server: Other ntp0.cs.mu.oz.au

Time zone offset: (GMT+10:00) Canberra, Melbourne, Sydney

First NTP time server: Select the required server.

Second NTP time server:	Select second time server, if required.
Time zone offset:	Select the local time zone.

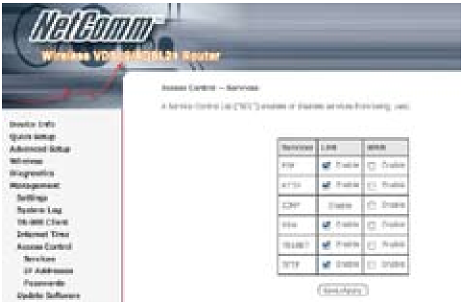
Configure these options and then click Save/Apply to activate.

9.5 Access Control

The Access Control option under the Management menu configures three access-related parameters: Services, IP Address and Passwords.

9.5.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SSH (Security Socket Share), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.



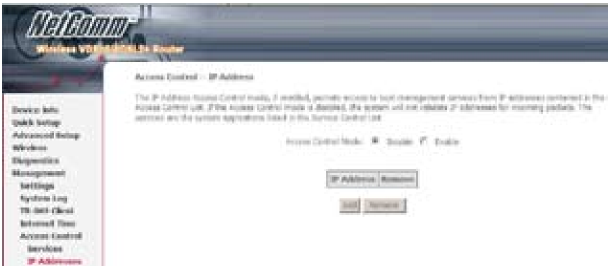
Access Control -- Services

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

Services	LAN	WAN
FTP	☑ Enable	☐ Enable
HTTP	☑ Enable	☐ Enable
ICMP	Enable	☐ Enable
SSH	☑ Enable	☐ Enable
TELNET	☑ Enable	☐ Enable
TFTP	☑ Enable	☐ Enable

9.5.2 Access IP Addresses

The IP Addresses option limits access by IP address. If Access Control Mode is enabled, only the IP addresses listed here can access the router. Before enabling it, configure the IP addresses by clicking the **Add** button. Enter the IP address and click **Apply** to allow the PC with this IP address to manage the device.

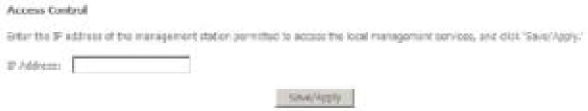


Access Control -- IP Address

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

Access Control Mode: ● Disable ○ Enable

IP Address	Remove



Access Control

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

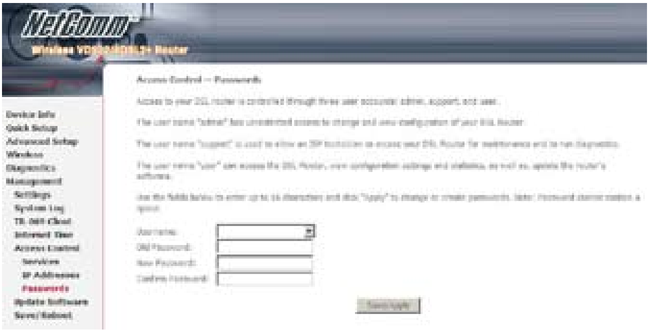
IP Address:

9.5.3 Passwords

The Passwords option configures the access passwords for the router. Access to your router is controlled through three user accounts: root, support, and user.

- root has unrestricted access to change and view the configuration of your router. It is the top administrative account.
- support is intended to allow limited access so that a technical support representative can conduct maintenance and run diagnostics.
- user provides the least access control but allows for viewing configuration settings and statistics, as well as, updating software.

Use the fields below to enter up to 16 characters and click Save/Apply to change or create passwords. See section 3.3 Default Settings for the default passwords.



Access Control -- Passwords

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

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

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

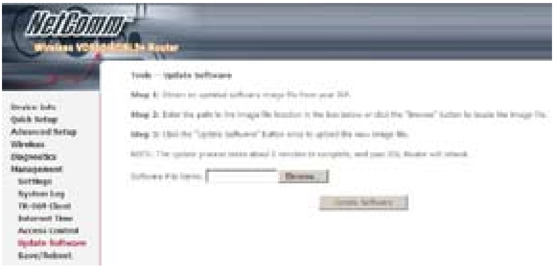
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

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

Username:
Old Password:
New Password:
Confirm Password:

9.6 Update Software

The Update Software screen allows you to update the software of the device. Manual software upgrades from a locally stored file can be performed using the following screen. Your ISP will provide this file to you, if necessary.



Tools -- Update Software

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

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

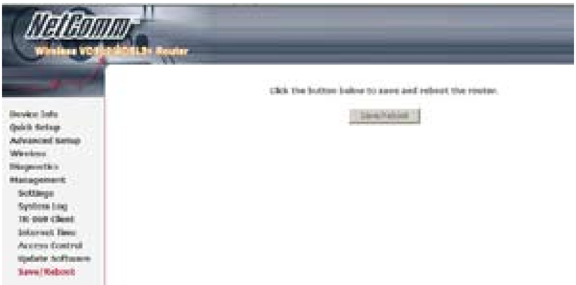
Step 3: Click the "Update Software" button once to upload the new image file.

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

Software File Name:

9.7 Save and Reboot

The Save/Reboot button saves the configurations and reboots the router. After clicking it, wait for 2 minutes before attempting to use the user interface. You may need to close and restart the web browser if it does not refresh automatically. You may need to reconfigure your PC IP address to match your new configuration. In this case, see section 3.1 TCP/IP Settings for detailed instructions.



Click the button below to save and reboot the router.

Appendix

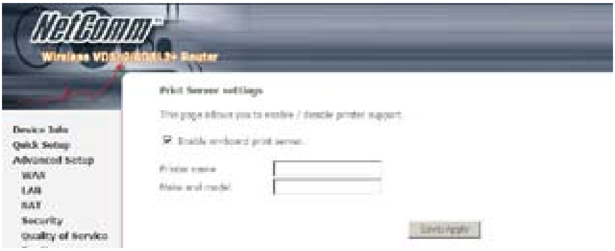
Appendix A: Printer Server

These steps explain the procedure for enabling the Printer Server.

1: Enable Print Server from Web User Interface.

Select **Enable on-board print server** checkbox and enter Printer name and Make and model

NOTE: The Printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.



Print Server settings

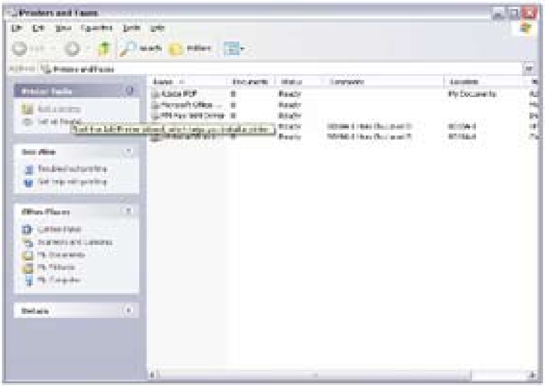
This page allows you to enable / disable printer support.

☑ Enable on-board print server.

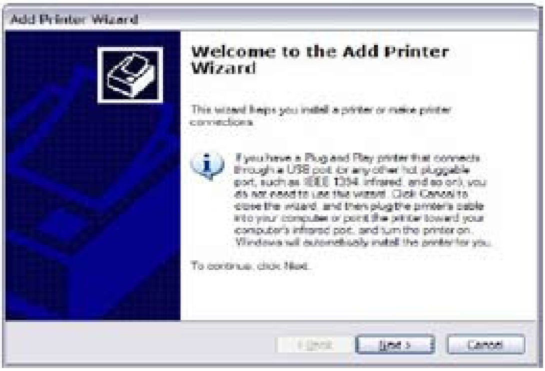
Printer name

Make and model

2: Go to the Printers and Faxes application in the Control Panel and select the Add a printer function (as located on the side menu below).



3: Click **Next** to continue, when you see the dialog box below.



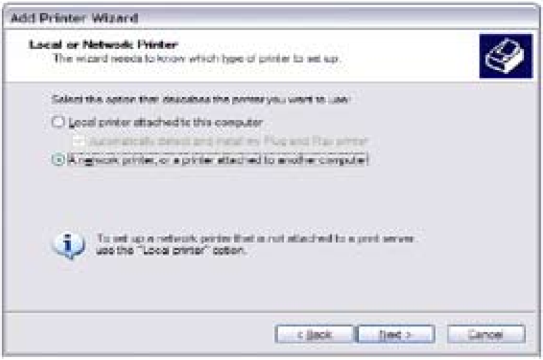
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

4: Select Network Printer and click **Next**.



Local or Network Printer
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

○ Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

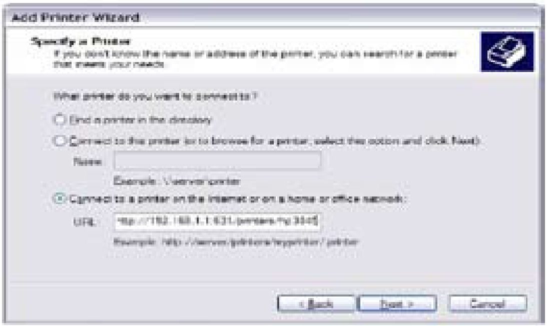
● A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

5: Select **Connect** to a printer on the Internet and enter your printer link.

(e.g. http://192.168.1.1:631/printers/hp3845) and click **Next**.

NOTE: The printer name must be the same name entered in the web user interface “printer server setting” as in step 1.



Add Printer Wizard

Specify a Printer

If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

○ Find a printer in the directory

○ Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

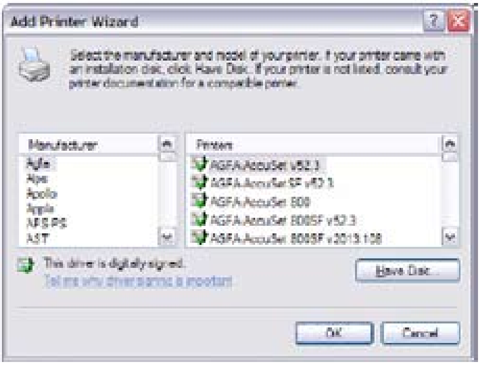
Example: \\server\printer

● Connect to a printer on the Internet or on a home or office network:

URL: http://192.168.1.1:631/printers/hp3845

Example: http://server/printers/myprinter/.printer

6: Click Have **Disk** and insert the printer driver CD.



Add Printer Wizard

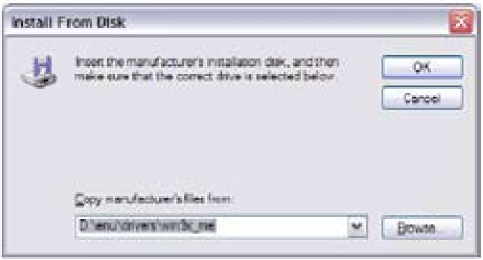
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer	Printers
Agfa	AGFA-AccuSet v52.3
Alps	AGFA-AccuSet SF v52.3
Apollo	AGFA-AccuSet 800
Apple	AGFA-AccuSet 800SF v52.3
APS-PS	
AST	AGFA-AccuSet 800SF v2013.108

This driver is digitally signed.

Tell me why driver signing is important

7: Select driver file directory on CD-ROM and click **OK**.



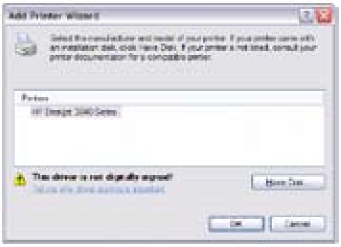
Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

D:\emu\drivers\win9x_me

8: Once the printer name appears, click **OK**.



Add Printer Wizard

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

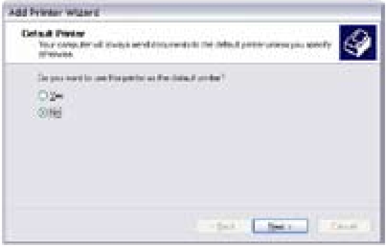
Printers

HP Deskjet 3840 Series

This driver is not digitally signed!

Tell me why driver signing is important

9: Choose Yes or No for default printer setting and click **Next**.



Add Printer Wizard

Default Printer

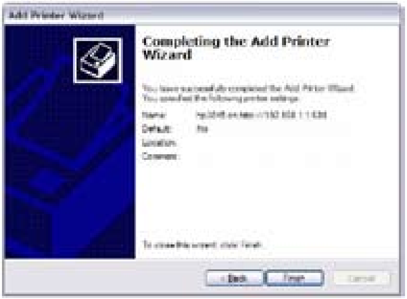
Your computer will always send documents to the default printer unless you specify otherwise.

Do you want to use this printer as the default printer?

○ Yes

● No

10: Click “**Finish**”.



Add Printer Wizard

Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard. You specified the following printer settings:

Name: hp2015 on http://192.168.1.1:631

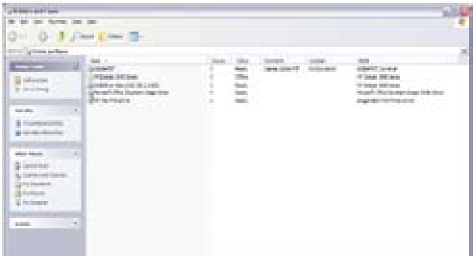
Default: No

Location:

Comment:

To close this wizard, click Finish.

11: Check the status of printer from Windows Control Panel, printer window. Status should show as Ready.



Appendix B: Firewall

Stateful Packet Inspection

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service attack

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the router can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3.

When a Routing interface is created “Enable Firewall” must be checked.

Navigate to Advanced Setup -> Security -> IP Filtering, web page.

Outgoing IP Filtering: Helps in setting rules to DROP packets from the LAN

interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular “Source IP Address/Source Subnet Mask” combination will be dropped.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular “Destination IP Address/ Destination Subnet Mask” combination will be dropped.

Destination Port: This can take on either a single port number or a range

of port numbers. Packets having a destination port equal to this value or falling

within the range of port numbers (portX : portY) will be dropped.

Examples:

1.	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Dest. Address	: NA
	Dest. Sub. Mask	: NA
	Dest. Port	: NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2.	Filter Name	: Out_Filter2
	Protocol	: UDP
	Source Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 5060:6060
	Dest. Address	: 172.16.13.4
	Dest. Sub. Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070

Incoming IP Filtering:

Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IPtraffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular

"Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

Examples:

1.	Filter Name	: In_Filter1
	Protocol	: TCP
	Source Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 80
	Dest. Address	: NA
	Dest. Sub. Mask	: NA
	Dest. Port	: NA

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2.	Filter Name	: In_Filter2
	Protocol	: UDP
	Source Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 5060:6060
	Dest. Address	:192.168.1.45
	Dest. Sub. Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 and a

source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering:

These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Security -> MAC Filtering web page.

Global Policy:

When set to Forwarded the default filter behavior is to

Forward all MAC layer frames except those explicitly stated in the rules.

Setting it to Blocked changes the default filter behavior to Drop all

MAC layer frames except those explicitly stated in the rules.

To setup a rule:

Protocol Type: Can be PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI or IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with

this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction:

LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.

WAN => LAN --> All Frames coming from WAN destined to LAN.

LAN => WAN --> All Frames coming from LAN destined to WAN

User needs to select the interface on which this rule is applied.

1.	Global Policy:	Forwarded
	Protocol Type:	PPPoE
	Dest. MAC Addr:	00:12:34:56:78
	Source MAC Addr:	NA
	Frame Direction:	LAN => WAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Dest. MAC Addr. of 00:12:34:56:78 irrespective of its Source MAC Addr. on the br_0_34 WAN interface. All other frames on this interface are forwarded.

Protocol Type:	PPPoE
Dest. MAC Addr:	00:12:34:56:78:90
Source MAC Addr:	00:34:12:78:90:56
Frame Direction:	WAN => LAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78 and Source MAC Addr. of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Daytime Parental Control

This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device

are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

Example:

User Name:	FilterJohn
Browser's MAC Address:	00:25:46:78:63:21
Days of the Week:	Mon, Wed, Fri
Start Blocking Time:	14:00
End Blocking Time:	18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays and Fridays, from 2pm to 6pm. On all other days and time this device will have access to the outside Network.

Appendix C: Pin Assignments

Line Port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix D: Specifications

Back Panel

RJ11 X1 for ADSL2+/VDSL2, RJ45 X 4 for LAN, Reset Button X 1, Power Jack X 1, WiFi antenna, USB host/device

DSL

ADSL2+ Downstream : 24 Mbps **Upstream :** 1.3 Mbps

Standards: ITU-T G.992.5, G.992.3, G.992.1; ANSI T1.413 Issue 2; AnnexM

VDSL2 Downstream : 100 Mbps **Upstream :** 50 Mbps

Standards:ITU-T G.993.2 (profiles 8a,8b,8c,8d,12a,12b,17a)

Ethernet

Standard	IEEE 802.3, IEEE 802.3u
10/100 BaseT	Auto-sense
MDI/MDX support	Yes

Wireless

Standard	IEEE802.11g, backward compatible with 802.11b
Encryption	64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
Channels	11 Channels (US, Canada)
	13 Channels (Europe)
	14 Channels (Japan)
Data Rate	Up to 54Mbps

WPA/WPA2, IEEE 802.1x, WMM, MAC address filtering, Variable output power levels (10, 25, 50, 100 mW @ 22 MHz channel bandwidth)

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);

RFC 1577 (IPoA)

Support PVCs	16
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI 3.1/4.0
OAM F4/F5	Yes

Management

TR-069/TR-098/TR-104/TR-111, SNMP, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP, TFTP server, or FTP server

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
VLAN support	Yes
Spanning Tree Algorithm	Yes
IGMP Proxy	Yes

Routing Functions

Static route, RIP v1/v2, NAT/PAT, DHCP Client/Server/Relay, DNS, ARP

Security Functions

Authentication protocols: PAP, CHAP, TCP/IP/Port filtering rules, Packet and MAC address filtering, Access Control

Encryption protocol: SSH

Port triggering/Forwarding, Stateful Packet Inspection, Denial Of Service protection, Traffic Conditioning, WFQ-based Bandwidth Management, HTTP proxy

Application Passthrough

PPTP, L2TP, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc

QoS: L3 policy-based QoS, IP QoS, ToS

OS Supported for USB driver

Windows Vista/2000/XP/ME/98SE

Power Supply: External power adapter 100 - 240 Vac, 15VDC / 1.6A

Environment Condition

Operating temperature: 0 ~ 50 degrees Celsius

Relative humidity: 5 ~ 95% (non-condensing)

Dimensions: 205 mm (W) x 48 mm (H) x 145 mm (D)

Kit Weight: 1 kg ~ 1 x NB11W

1 x RJ-11 cable

1 x RJ-45 cable

1 x USB cable

1 x power adapter

1 x cd-rom

NOTE: Specifications are subject to change without notice

Linux OS comes with ssh client. Microsoft Windows does not have ssh client but there is a public domain one “putty” that you can download.

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the router using Linux ssh client:

Appendix E: SSH Client

From LAN: Use the router WEB UI to enable SSH access from LAN.

(default is enabled)

type: ssh -l admin 192.168.1.1

From WAN: From the router, use WEB UI to enable SSH access from WAN.

type: ssh -l support xx.xx.xx.xx (router WAN IP address)

To access the router using Windows putty ssh client:

From LAN: Use the router WEB UI to enable SSH access from LAN

(default is enabled)

type: putty -ssh -l admin 192.168.1.1

From WAN: From the router, use WEB UI to enable SSH access from WAN.

type: putty -ssh -l support xx.xx.xx.xx (router WAN IP address)

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website **www.netcomm.com.au**.

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.

NetComm®
www.netcomm.com.au

NETCOMM LIMITED PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: sales@netcomm.com.au **W:** www.netcomm.com.au

Dynalink
www.dynalink.co.nz

DYNALINK NZ 224b Bush Road, Albany, Auckland, New Zealand
P: 09 448 5548 **F:** 09 448 5549
E: sales@dynalink.co.nz **W:** www.dynalink.co.nz