User Guide

DSL-N12HP

300Mbps Wi-Fi ADSL Modem Router

Inspiring Innovation • Persistent Perfection

E11002
First Edition
October 2015

Table of contents

Table of contents

Table of contents

1 Getting to know your ADSL modem router

1.1 Welcome!

Thank you for purchasing an ASUS DSL-N12HP Wi-Fi ADSL Modem Router!

DSL-N12HP is an 802.11n (300Mbps) Wireless ADSL2+ router comprising four 10/100 Base-T Ethernet ports, a Wi-Fi Protected Setup (WPS)/ Wi-Fi switch button, and is backward compatible with existing 802.11b (11Mbps) and 11g (54bps) equipment.

The DSL-N12HP ADSL2+ router provides state of the art security features such as 64/128 bit WEP encryption and WPA/WPA2 encryption, Firewall, and VPN pass through.

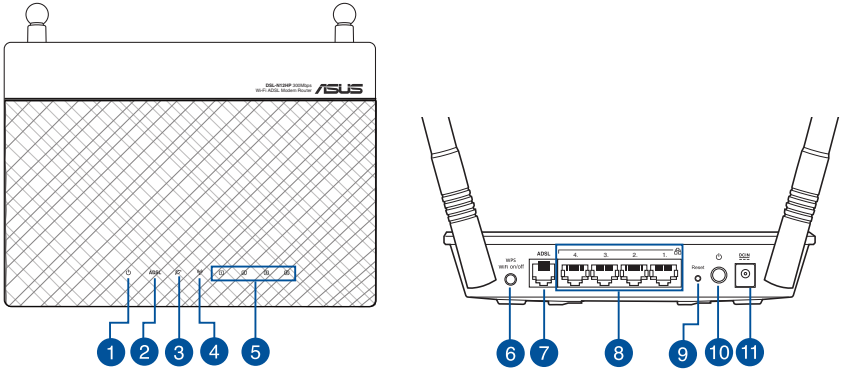
1.2 Package contents

- ☑ DSL-N12HP Wireless Modem Router
- ☑ 2 detachable antennas
- ☑ Antenna holder
- ☑ Power adapter
- ☑ Network cable (RJ-45 cable)
- ☑ DSL/phone cable (RJ-11 cable)
- ☑ Quick Start Guide
- ☑ Warranty card
- ☑ Splitter

NOTES:

- If any of the items are damaged or missing, contact ASUS for technical inquiries and support. Refer to the ASUS Support Hotline list at the back of this user manual.
- Keep the original packaging material in case you would need future warranty services such as repair or replacement.

1.3 Your ADSL modem router



1 **Power LED**

Off: No power.

Solid green: Device is ready.

Flashing green: Upgrade is in process.

Solid red: POST (Power On Self Test) failure (not bootable) or device malfunction.

NOTE: A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.

2 **ADSL LED**

Off: No ADSL link or unable to establish ADSL link.

Solid green: ADSL link is established.

Flashing green: ADSL is attempting to connect to a DSLAM.

3 **Internet LED**

Off: IP connected and no traffic detected (the device has a WAN IP address from IPCP or DHCP is up or a static IP address is configured, PPP negotiation has successfully complete.

If the IP or PPPoE session is dropped due to an idle timeout, the light will remain Blue.

Solid green: Modem power off, modem in bridged mode or WAN connection not present.

The light will turn off when it attempts to reconnect and DHCP or PPPoE fails.

Flashing green: IP connected and IP Traffic is passing through the device.

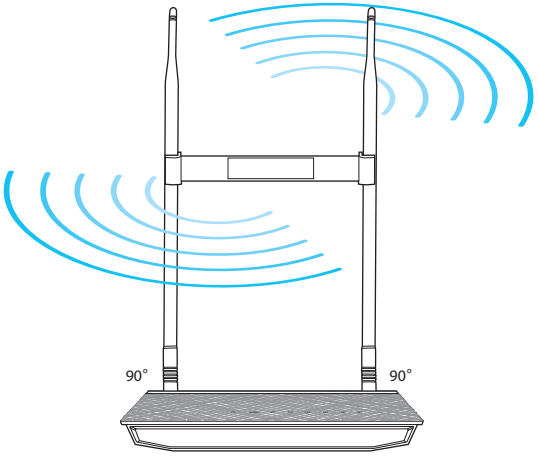
4	**Wi-Fi LED** **Off**: No Wi-Fi signal. **Solid green**: Wireless system is ready. **Flashing green**: Transmitting or receiving data via wireless connection.
5	**LAN 1~4 LED** **Off**: No power or no physical connection. **Solid green**: Has physical connection to an Ethernet network. **Flashing green**: Transmitting or receiving data via wireless connection.
6	**WPS and Wi-Fi on/off button** Press and hold this button more than 5 seconds to activate WPS. Ensure that the WPS is enabled in **Wireless** > **Security** page). Press and hold this button 2~3 seconds to enable/disable Wi-Fi.
7	**ADSL port** Connect to a splitter or to a telephone outlet via an RJ-11 cable.
8	**LAN 1 ~ 4 ports** Connect network cables into these ports to establish LAN connection.
9	**Reset button** Press this button for 10 seconds to reset or restore the system to its factory default settings.
10	**Power button** Press this button to power on or off the system.
11	**Power (DC-IN) port** Insert the bundled AC adapter into this port and connect your router to a power source.

NOTE: Use only the adapter that came with your package. Using other adapters may damage the device.

1.4 Positioning your ADSL modem router

For the best wireless signal transmission between the ADSL modem router and the network devices connected to it, ensure that you:

- Place the ADSL modem router in a centralized area for a maximum wireless coverage for the network devices.
- Keep the device away from metal obstructions and away from direct sunlight.
- To prevent signal interference or loss, keep the device away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment.
- Always update to the latest firmware. Visit the ASUS website at http://www.asus.com to get the latest firmware updates.
- To ensure the best wireless signal, orient the two detachable antennas using the bundled antenna holder as shown in the drawing below.



1.5 Setup Requirements

To set up your wireless network, you need a computer that meets the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX)
- IEEE 802.11b/g/n wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

NOTES:

- If your computer does not have built-in wireless capabilities, you may install an IEEE 802.11b/g/n WLAN adapter to your computer to connect to the network.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

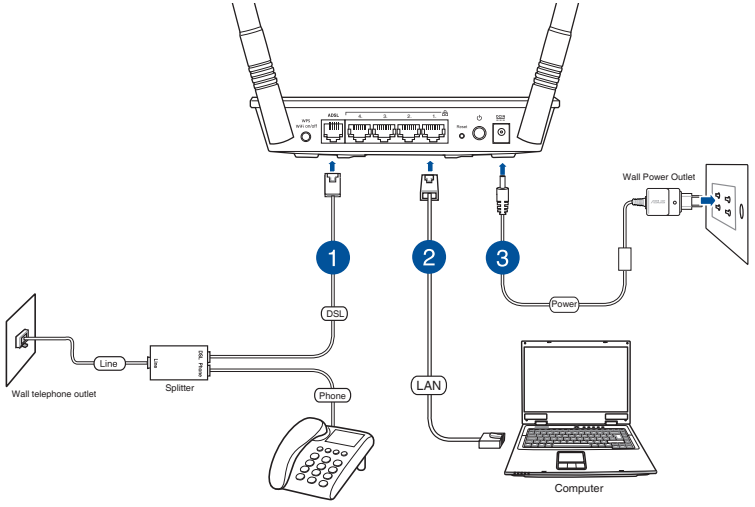
1.6 ADSL Modem Router Setup

IMPORTANT!

- Use a wired connection when setting up your ADSL modem router to avoid possible setup problems.
- Before setting up your ASUS ADSL modem router, do the following:
  - If you are replacing an existing ADSL modem router, disconnect it from your network.

Wired connection

NOTE: You can use either a straight-through cable or a crossover cable for wired connection.



To set up your ADSL modem router via wired connection:

1. Connect one end of the RJ-11 cable to the ADSL port of your ADSL modem router, and connect the other end to the ADSL port of your splitter.
2. Using a network cable, connect your computer to your ADSL modem router's LAN port.
3. Insert your ADSL modem router's power adapter to the DC-IN port and plug it to a power outlet.

IMPORTANT! After turning on your ADSL modem router, wait for a few minutes for Internet connection.

2 Getting started

2.1 Default settings

Your ASUS Wireless ADSL Modem Router comes with an intuitive web graphical user interface (GUI) that allows you to easily configure its various features through a web browser such as Internet Explorer, Firefox, Safari, or Google Chrome.

NOTE: The features may vary with different firmware versions.

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: admin , password: admin)
- Wi-Fi access: enabled

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 GUI 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 Settings screen.

2.2 IP configuration

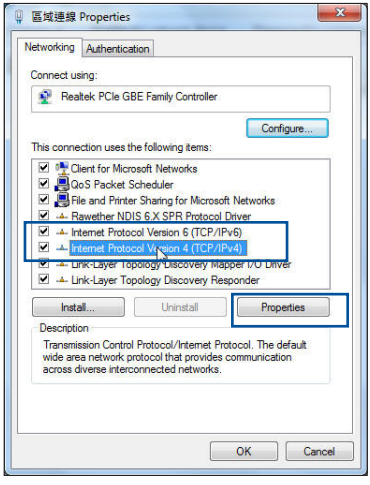
DHCP MODE

When the DSL-N12HP powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

To obtain an IP address from the DCHP server, follow the steps provided below.

NOTE: The following procedure assumes you are running Windows® 7. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

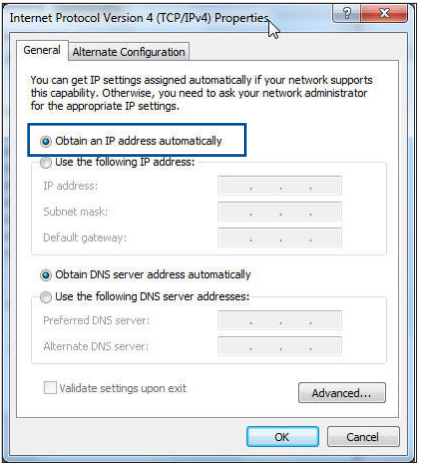
1. Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage network connections.**
2. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties**.



3. To obtain the IPv4 IP settings automatically, tick **Obtain an IP address automatically**.

   To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

4. Click **OK** when done.



If you experience difficulty with DHCP mode, you can try static IP mode instead.

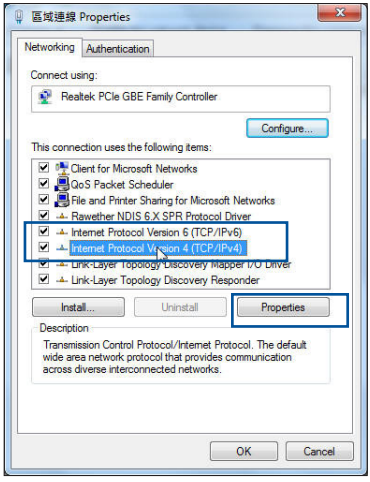
STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

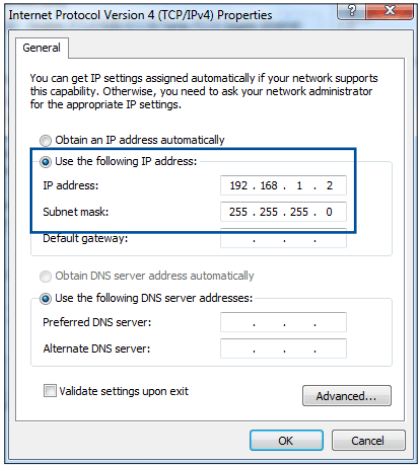
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

NOTE: The following procedure assumes you are running Windows® 7. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

1. Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage network connections.**
2. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties**.



3. Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0.
4. Click **OK** when done.



2.3 Logging into the Web GUI

To log into the web GUI:

1. On your web browser, manually key in the ADSL modem router's default IP address: **192.168.1.1**

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device.
For remote access (i.e. WAN), use the IP address shown on the **Device Information** screen and login with remote username and password.

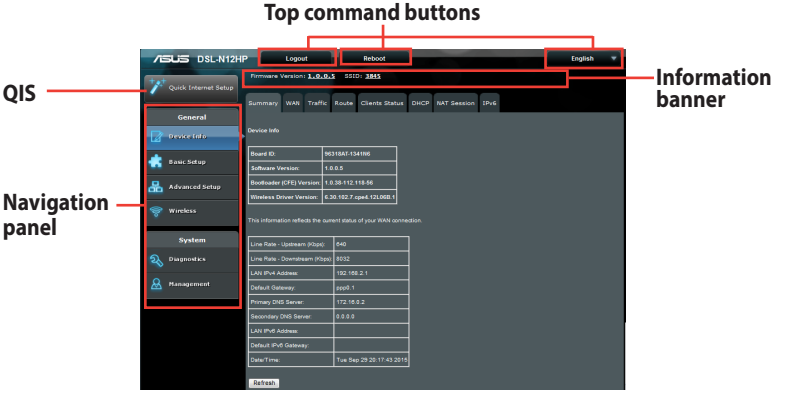
---

2. On the login page, key in the default user name (**admin**) and password (**admin**).

NOTE: For details on changing your ADSL modem router's login username and password, refer to section **4.2.4 Access Control**.

---

3. You can now use the Web GUI to configure various settings of your ASUS ADSL modem router.



NOTE: If you are logging into the Web GUI for the first time, you will be directed to the Quick Internet Setup (QIS) page automatically.

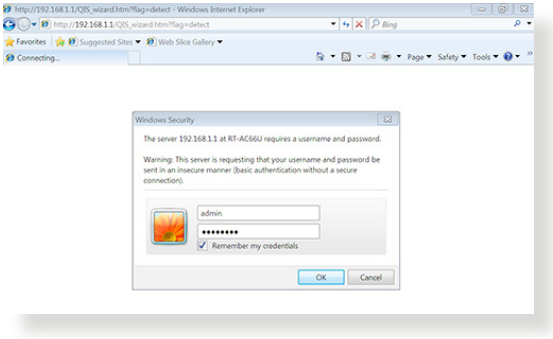
2.4 Quick Internet Setup (QIS) Wizard with Auto-detection

The Quick Internet Setup (QIS) function guides you in quickly setting up your Internet connection.

NOTE: When setting the Internet connection for the first time, press the Reset button on your ADSL modem router to reset it to its factory default settings. For more details, refer to the section **4.2.5 Update Software** of this user manual.

To use QIS with auto-detection:

1. Log into the Web GUI. The QIS page launches automatically.



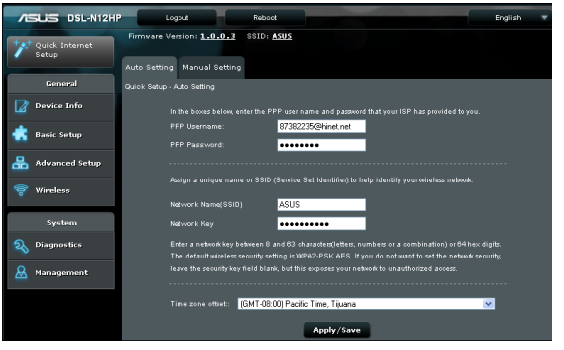
NOTES:

- By default, the login username and password for your ADSL modem router's Web GUI is **admin**. For details on changing your ADSL modem router's login username and password, refer to section **4.2.4 Access Control**.
- The ADSL modem router's login username and password allows you to log into your ADSL modem router's Web GUI to configure your ADSL modem router's settings. The network name (SSID) and security key allows Wi-Fi devices to log in and connect to your wireless network.

2. After successfully logging in for the first time, the Device Info page displays.

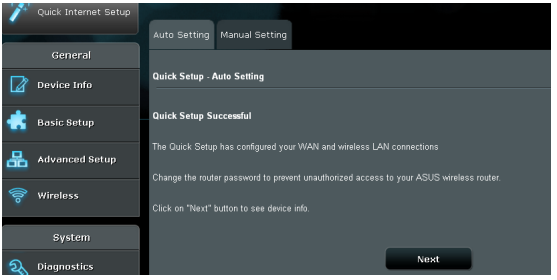
3. Click the **Quick Internet Setup** tab on the left side of the screen.

4. Key in the PPP username and PPP password that you obtained from your Internet Service Provider (ISP), assign the network name (SSID) and security key for your wireless connection, select your local time zone from the drop-down menu, and click **Apply/Save** when done.



5. Click **Next** to complete the setup and go to the Device Info page.

NOTE: Change the router password to prevent unauthorized access to your ASUS wireless router.



2.5 Connecting to your wireless network

After setting up your ADSL modem router via QIS, you can connect your computer or other smart devices to your wireless network.

To connect to your network:

1. On your computer, click the network icon in the notification area to display the available wireless networks.
2. Select the wireless network that you want to connect to, then click **Connect**.
3. You may need to key in the network security key for a secured wireless network, then click **OK**.
4. Wait while your computer establishes connection to the wireless network successfully. The connection status is displayed and the network icon displays the connected status.

NOTES:

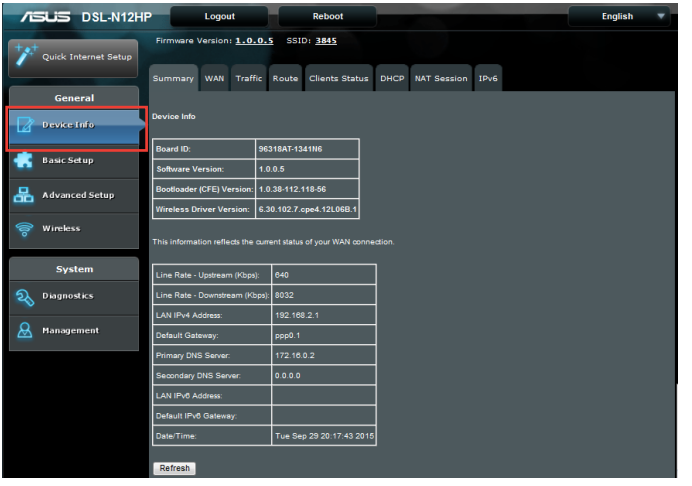
- Refer to the next chapters for more details on configuring your wireless network's settings.
- Refer to your device's user manual for more details on connecting it to your wireless network.

3 Configuring the General settings

3.1 Device Information

You can reach this page by clicking on the **Device Info** icon located on the left side of the screen.

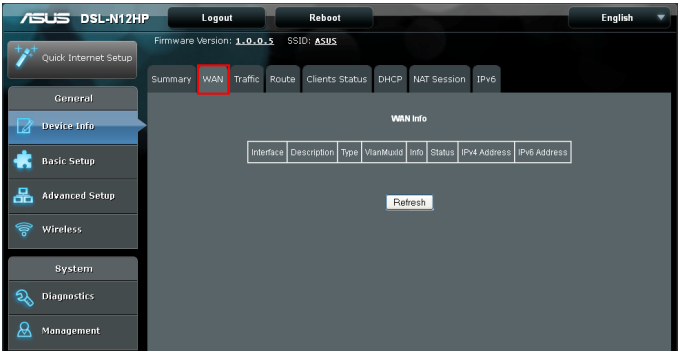
The Device Info Summary screen displays at startup.



This screen shows hardware, software, IP settings and other related information.

3.1.1 WAN

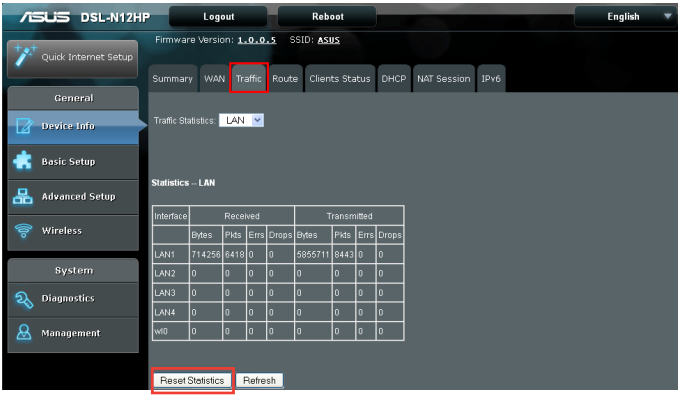
Click the WAN tab to display the configured PVC(s).



Field	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
Info	Shows the parameter setting value like, IPv6, IGMP, MLD, NAT, Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address
IPv6 Address	Shows WAN IPv6 address

3.1.2 Traffic Statistics

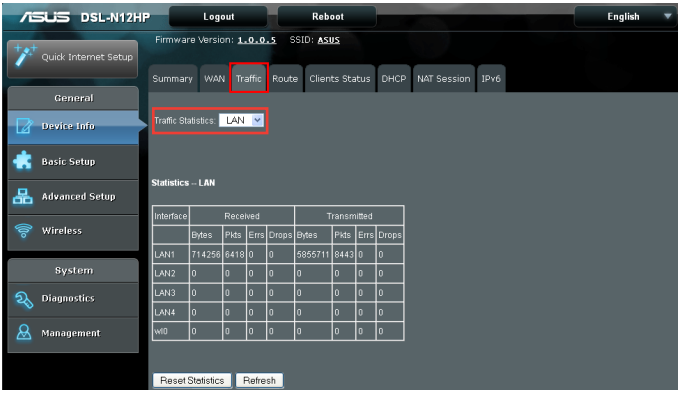
This selection provides LAN, WAN, xTM and xDSL statistics. Click the Traffic tab to display the following.



Click **Reset Statistics** to perform a manual update.

LAN Statistics

This screen shows data traffic statistics for each LAN interface.

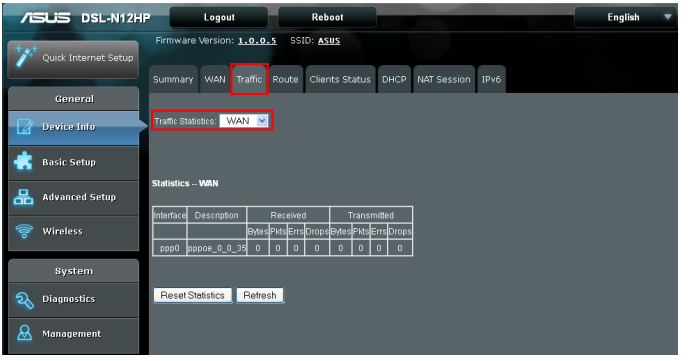


Select **LAN** from the drop-down menu.

Field		Description
Interface		LAN interface(s)
Received/Transmitted	Bytes	Number of Bytes
	Pkts	Number of Packets
	Errs	Number of packets with errors
	Drops	Number of dropped packets

WAN Statistics

This screen shows data traffic statistics for each WAN interface.

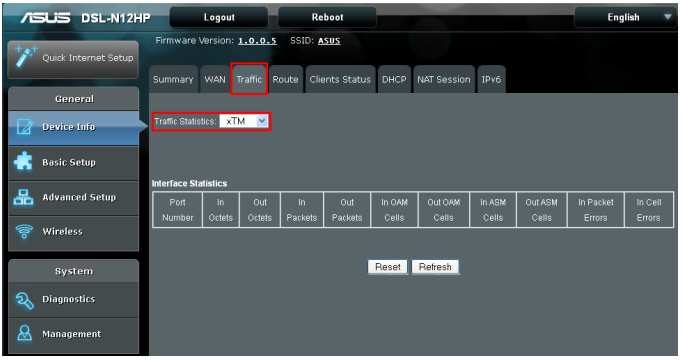


Select **WAN** from the drop-down menu.

Field		Description
Interface		WAN interface(s)
Description		WAN service label
Received/Transmitted	Bytes	Number of Bytes
	Pkts	Number of Packets
	Errs	Number of packets with errors
	Drops	Number of dropped packets

xTM Statistics

The following figure shows ATM (Asynchronous Transfer Mode)/ PTM (Packet Transfer Mode) statistics.



Select **xTM** from the drop-down menu.

Field	Description
Port Number	ATM PORT (0-3)
In Octets	Number of octets received over the interface
Out Octets	Number of octets transmitted over the interface
In Packets	Number of packets received over the interface
Out Packets	Number of packets transmitted over the interface
In OAM Cells	Number of OAM Cells received over the interface
Out OAM Cells	Number of OAM Cells transmitted over the interface.
In ASM Cells	Number of ASM Cells received over the interface
Out ASM Cells	Number of ASM Cells transmitted over the interface
In Packet Errors	Number of packets in Error
In Cell Errors	Number of cells in Error

xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type.

Click the **Reset Statistics** button to refresh this screen.

Field	Description
Mode	ADSL2, ADSL2+
Traffic Type	ATM
Status	Lists the status of the DSL link
Link Power State	Link output power state.
phyR Status	Shows the status of PhyR™ (Physical Layer Re-Transmission) impulse noise protection
Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin
Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction.
Output Power	
(0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rates downstream/upstream

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	Interleaver depth
Delay	The delay in milliseconds (msec)
INP	DMT symbol

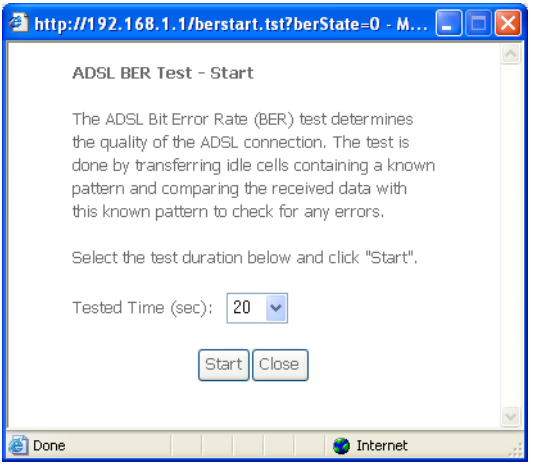
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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 + data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

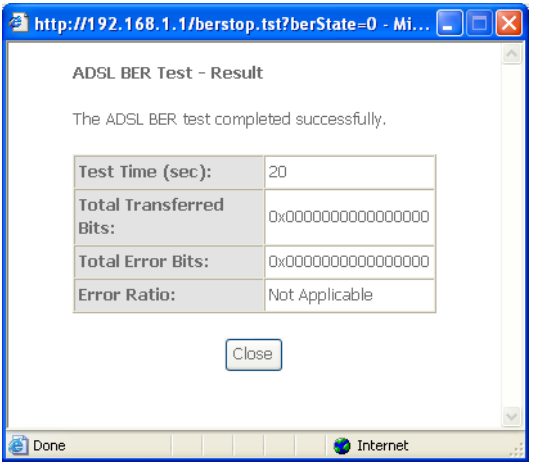
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

xDSL BER TEST

Click **xDSL BER Test** on the xDSL Statistics screen to test the Bit Error Rate (BER). A small pop-up window will open after the button is pressed, as shown below.

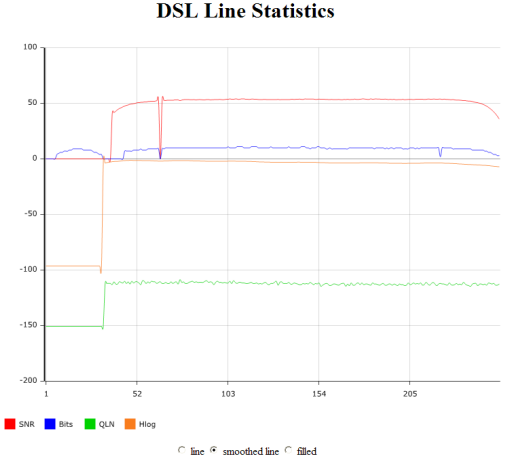


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



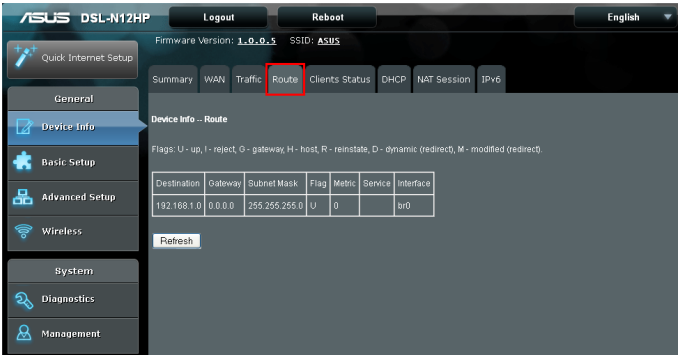
xDSL TONE GRAPH

Click **Draw Graph** on the xDSL Statistics screen and a pop-up window will display the DSL line statistics.



3.1.3 Route

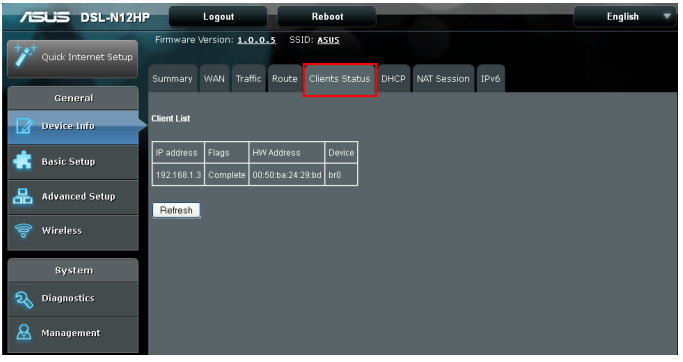
Click the Route tab to display the routes that the DSL-N12HP has found.



Field	Description
Destination	Destination network or destination host
Gateway	Next hop IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up
	!: reject route
	G: use gateway
	H: target is a host
	R: reinstate route for dynamic routing
	D: dynamically installed by daemon or redirect
	M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

3.1.4 Clients Status

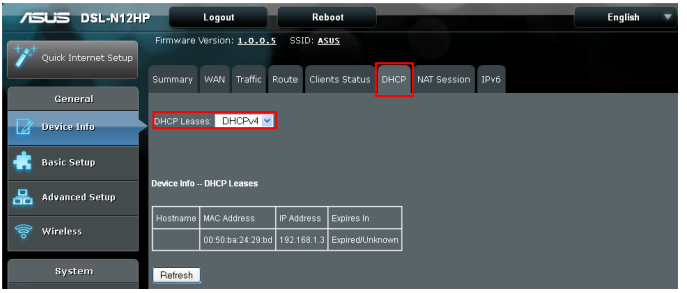
Click the Clients Status tab to display the Client information.



Field	Description
IP address	Shows IP address of host pc
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

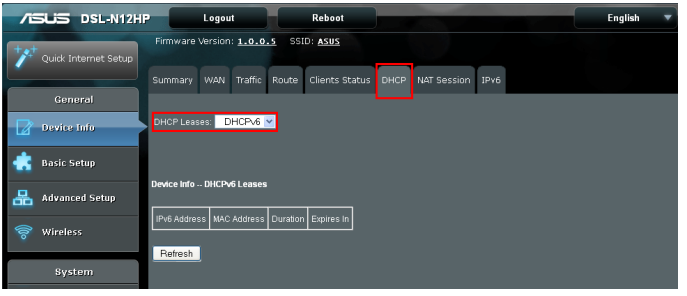
3.1.5 DHCP

Click the DHCP tab to display all DHCP Leases.



Select **DHCPv4** from the drop-down menu.

Field	Description
Hostname	Shows the host name of device/host/PC
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

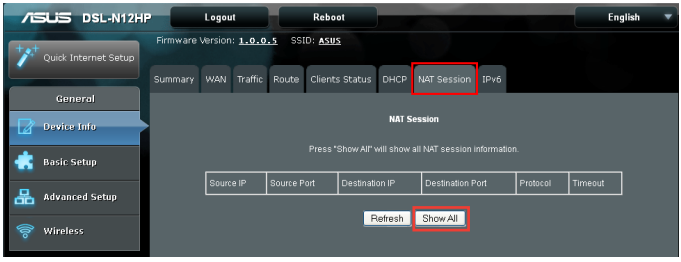


Select **DHCPv6** from the drop-down menu.

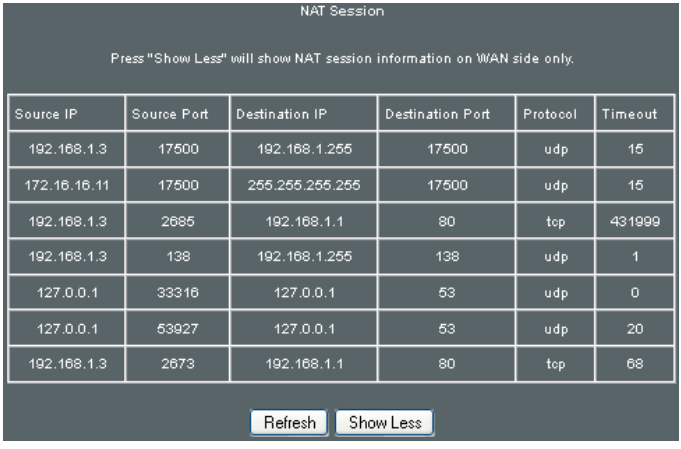
Field	Description
IPv6 Address	Shows IP address of device/host/PC
MAC Address	Shows the Ethernet MAC address of the device/host/PC
Duration	Shows leased time in hours
Expires In	Shows how much time is left for each DHCP Lease

3.1.6 NAT Session

Click the NAT Session tab to display the following.



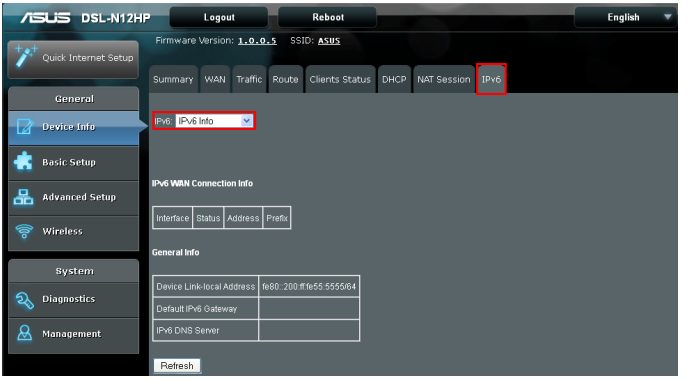
Click **Show All** to display the following.



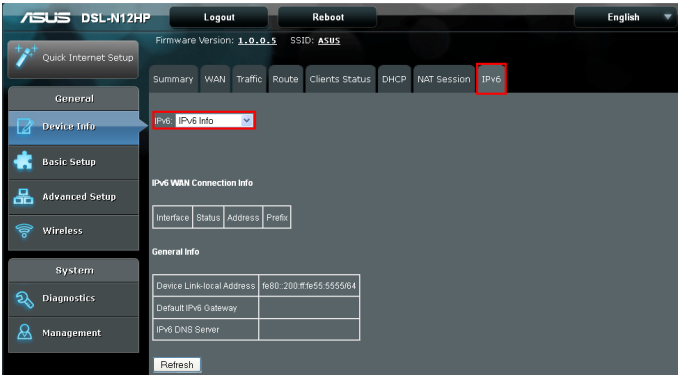
Field	Description
Source IP	The source IP from which the NAT session is established
Source Port	The source port from which the NAT session is established
Destination IP	The IP which the NAT session was connected to
Destination Port	The port which the NAT session was connected to
Protocol	The Protocol used in establishing the particular NAT session
Timeout	The time remaining for the TCP/UDP connection to be active

3.1.7 IPv6

Click the IPv6 tab to display the following.



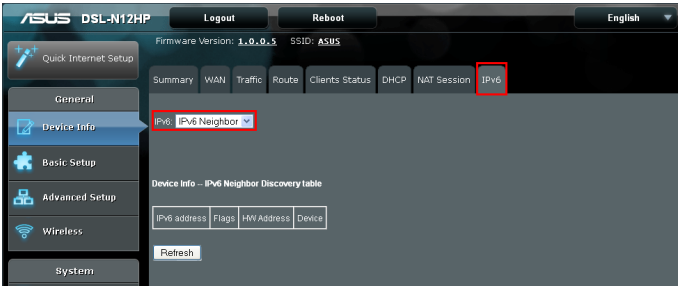
IPv6 Info



Select **IPv6 Info** from the drop-down menu.

Field	Description
Interface	WAN interface with IPv6 enabled
Status	Connection status of the WAN interface
Address	IPv6 Address of the WAN interface
Prefix	Prefix received/configured on the WAN interface
Device Link-local Address	The CPE's LAN Address
Default IPv6 Gateway	The default WAN IPv6 gateway
IPv6 DNS Server	The IPv6 DNS servers received from the WAN interface / configured manually

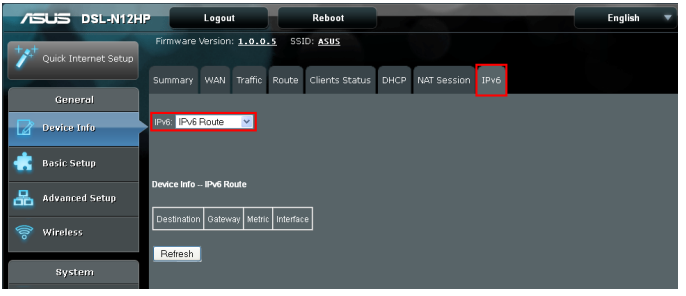
IPv6 Neighbor



Select **IPv6 Neighbor** from the drop-down menu.

Field	Description
IPv6 Address	Ipv6 address of the device(s) found
Flags	Status of the neighbor device
HW Address	MAC address of the neighbor device
Device	Interface from which the device is located

IPv6 Route



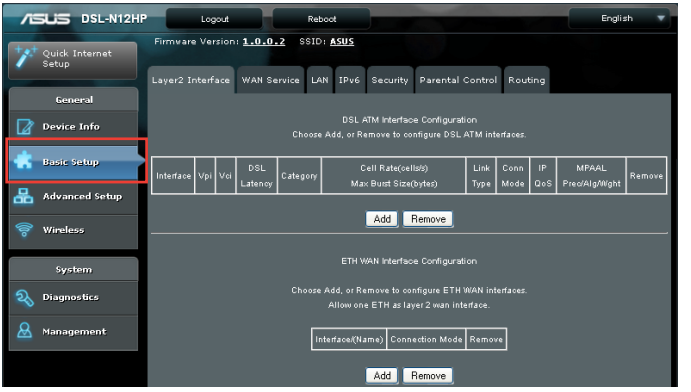
Select **IPv6 Route** from the drop-down menu.

Field	Description
Destination	Destination IP Address
Gateway	Gateway address used for destination IP
Metric	Metric specified for gateway
Interface	Interface used for destination IP

3.2 Basic Setup

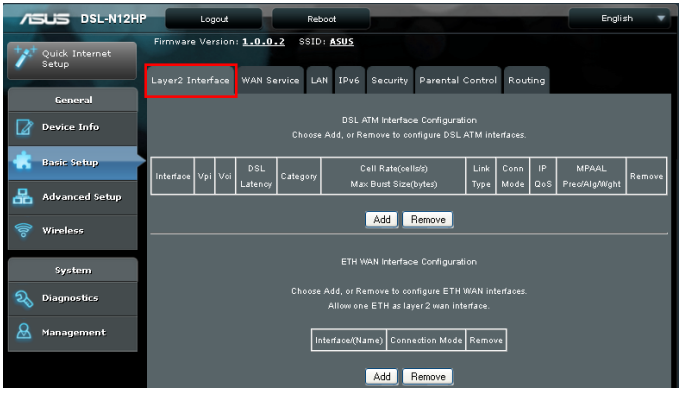
You can reach this page by clicking on the **Basic Setup** icon located on the left side of the screen.

This will bring you to the following screen.



3.2.1 Layer 2 Interface

Add or remove ATM and ETH WAN interface connections here.



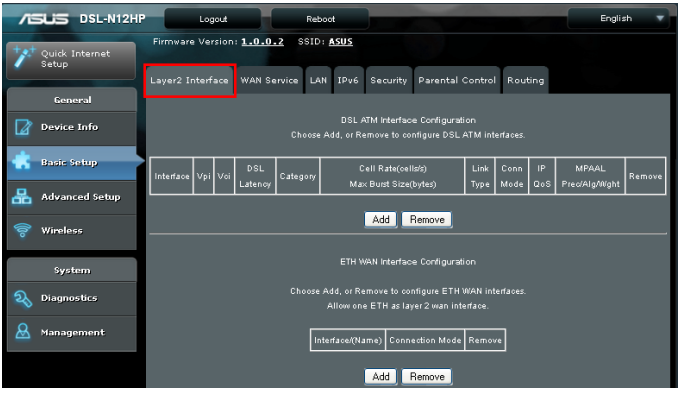
Click **Add** to create a new ATM interface (see **Appendix E - Connection Setup**).

NOTE: Up to 8 ATM interfaces can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click **Remove**.

3.2.1 Layer 2 Interface

Add or remove ATM and ETH WAN interface connections here.



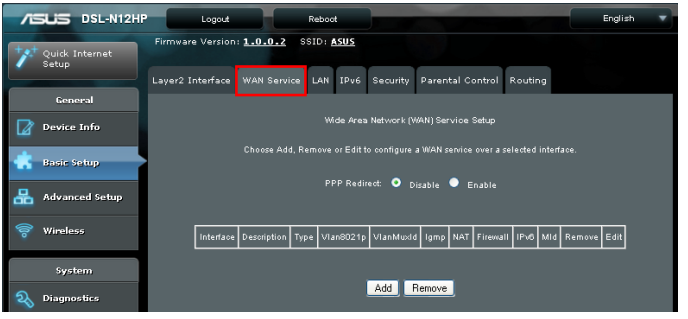
Click **Add** to create a new ATM interface (see **Appendix E - Connection Setup**).

NOTE: Up to 8 ATM interfaces can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click **Remove**.

3.2.2 WAN Service Setup

This screen allows for the configuration of WAN interfaces. Click the WAN Service tab to display the following.



Click **Add** to create a new connection. For connections on ATM or ETH WAN interfaces see **Appendix E - Connection Setup**.

To remove a connection, select its Remove column radio button and click **Remove**.

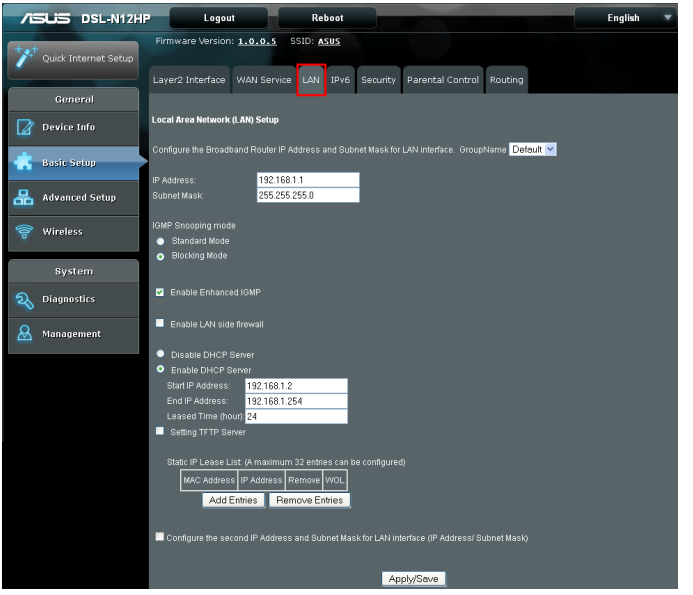
Field	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
Igmp	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows the WAN IPv6 address
MLD	Shows Multicast Listener Discovery (MLD) status
Remove	Select interfaces to remove

NOTES:

- ETH and ATM service connections cannot coexist. In Default Mode, up to 8 WAN connections can be configured; while VLAN Mux Connection Mode supports up to 16 WAN connections.
- Up to 16 PVC profiles can be configured and saved in flash memory. Also, ETH and PTM/ATM service connections cannot coexist.

3.2.3 LAN

Click the **LAN** tab to display the following.



Configure the LAN interface settings and then click **Apply/Save**.

Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

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

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

IGMP Snooping:

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.

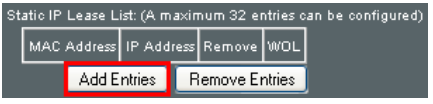
Enable Enhanced IGMP: Enable by ticking the checkbox. IGMP packets between LAN ports will be blocked.

Enable LAN side firewall: Enable by ticking the checkbox.

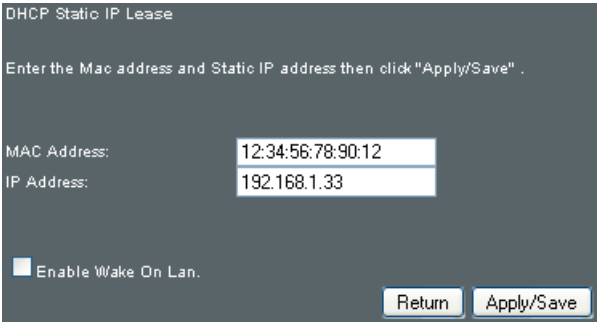
DHCP Server: To enable DHCP, select Enable DHCP server and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

Setting TFTP Server: Enable by ticking the checkbox. Then, input the TFTP server address or an IP address.

Static IP Lease List: A maximum of 32 entries can be configured.



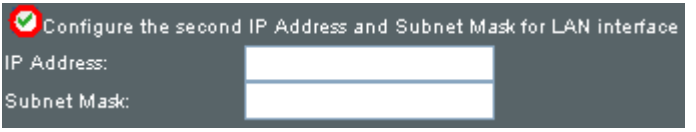
To add an entry, enter MAC address and Static IP address and then click **Apply/Save**.



To remove an entry, tick the corresponding checkbox in the Remove column and then click **Remove Entries**.

2ND LAN INTERFACE

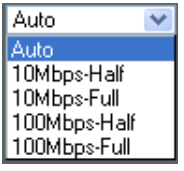
To configure a secondary IP address, tick the checkbox outlined (in RED) below.



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

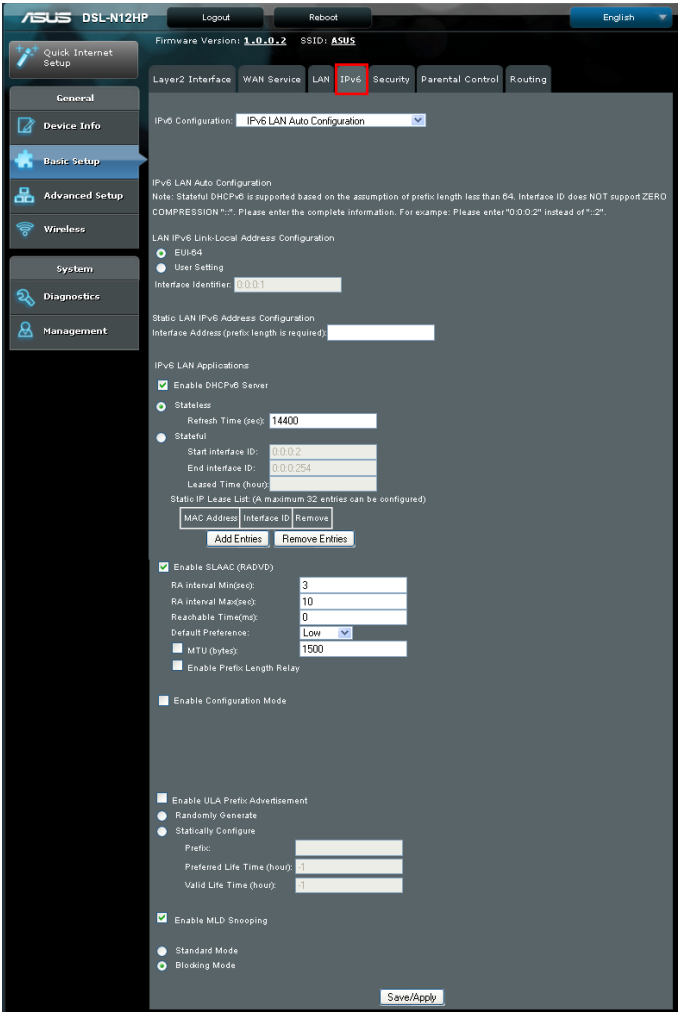
Subnet Mask: Enter the secondary subnet mask for the LAN port.

Ethernet Media Type:



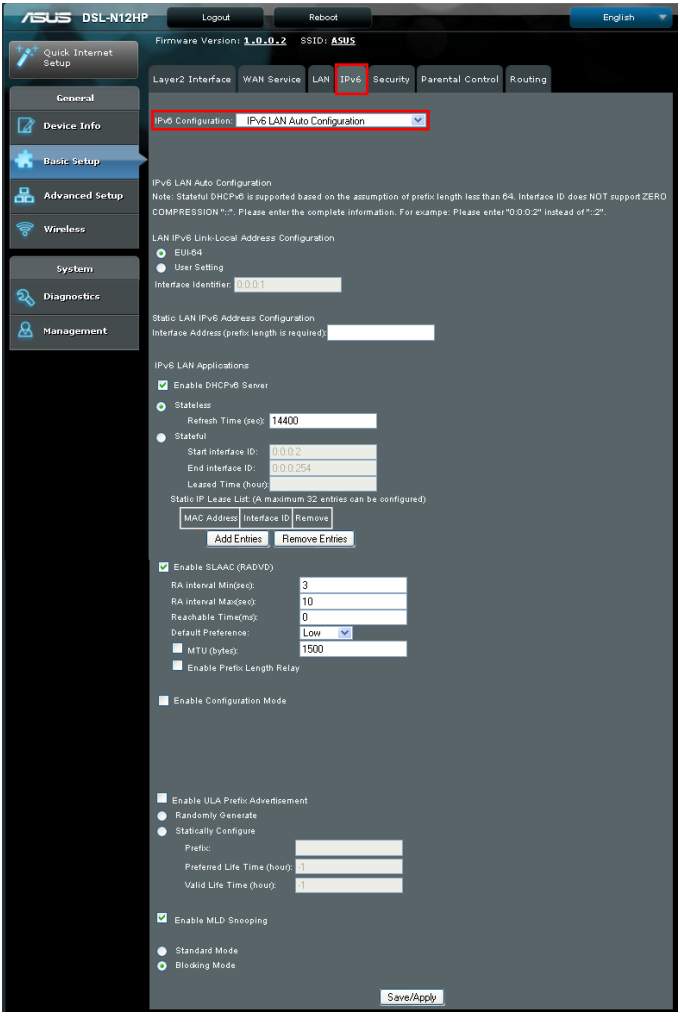
3.2.4 IPv6

Click the **IPv6** tab to display the following.



LAN IPv6 Auto Configuration

Select **IPv6 LAN Auto Configuration** from the drop-down menu.



Configure the LAN interface settings and then click **Save/Apply**.

Consult the field descriptions below for more details.

LAN IPv6 Link-Local Address Configuration

Field	Description
EUI-64	Use EUI-64 algorithm to calculate link-local address from MAC address
User Setting	Use the Interface Identifier field to define a link-local address

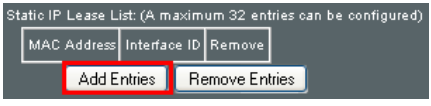
Static LAN IPv6 Address Configuration

Field	Description
Interface Address (prefix length is required):	Configure static LAN IPv6 address and subnet prefix length

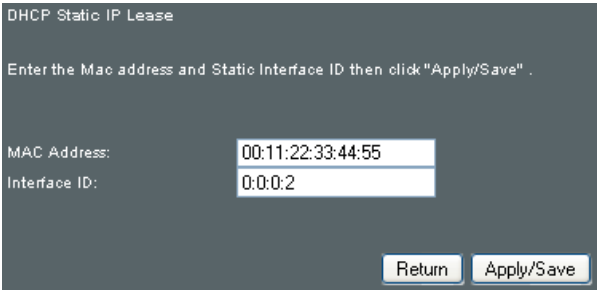
IPv6 LAN Applications

Field	Description
Stateless	Use stateless configuration
Refresh Time (sec):	The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6
Stateful	Use stateful configuration
Start interface ID:	Start of interface ID to be assigned to dhcpv6 client
End interface ID:	End of interface ID to be assigned to dhcpv6 client
Leased Time (hour):	Lease time for dhcpv6 client to use the assigned IP address

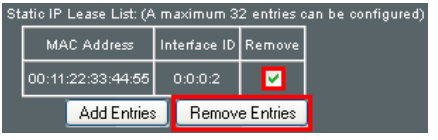
Static IP Lease List: A maximum of 32 entries can be configured.



To add an entry, enter MAC address and Interface ID and then click **Apply/Save**.



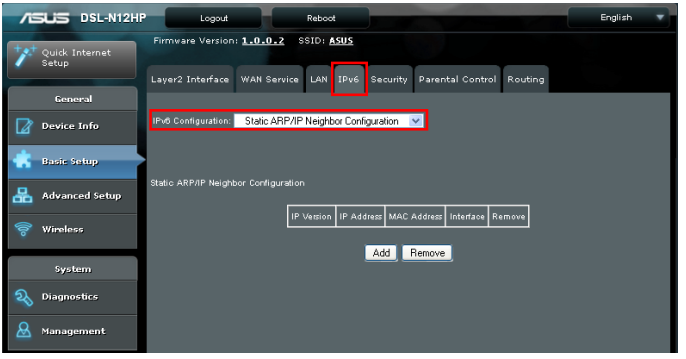
To remove an entry, tick the corresponding checkbox in the Remove column and then click **Remove Entries**.



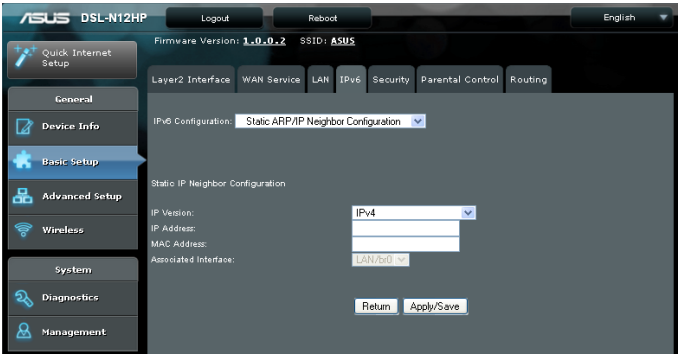
Field	Description
Enable RADVD	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation
Default Preference:	Preference level associated with the default router
MTU (bytes):	MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value
Enable Prefix Length Relay	Use prefix length receive from WAN interface
Enable Configuration Mode	Manually configure prefix, prefix length, preferred lifetime and valid lifetime used in router advertisement
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure Prefix	Specify the prefix to be used
Statically Configure	The prefix to be used
Preferred Life Time (hour)	The preferred life time for this prefix
Valid Life Time (hour)	The valid life time for this prefix
Enable MLD Snooping	Enable/disable IPv6 multicast forward to LAN ports
Standard Mode	In standard mode, IPv6 multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if MLD snooping is enabled
Blocking Mode	In blocking mode, IPv6 multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group

Static ARP/IP Neighbor Configuration

Select **Static ARP/IP Neighbor Configuration** from the drop-down menu.



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



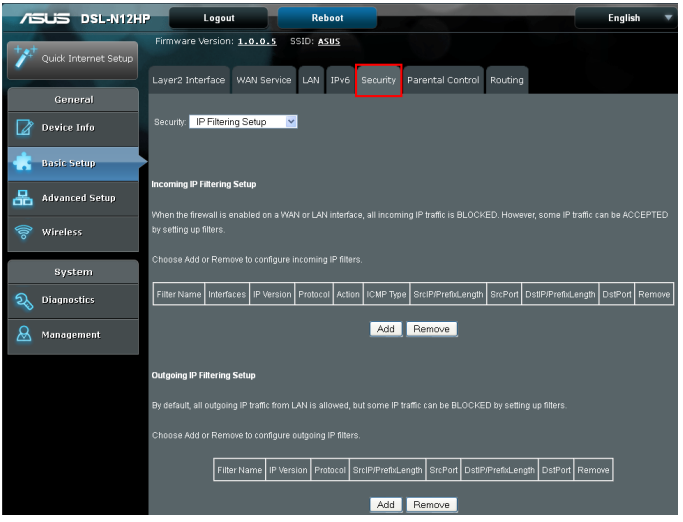
Click **Apply/Save** to apply and save the settings.

Field	Description
IP Version	The IP version used for the neighbor device
IP Address	Define the IP Address for the neighbor device
MAC Address	The MAC Address of the neighbor device
Associated Interface	The interface where the neighbor device is located

3.2.5 Security

To display this function, you must enable the firewall feature in WAN Setup. For detailed descriptions, with examples, please consult **Appendix A - Firewall**.

Click the Security tab to display the following.

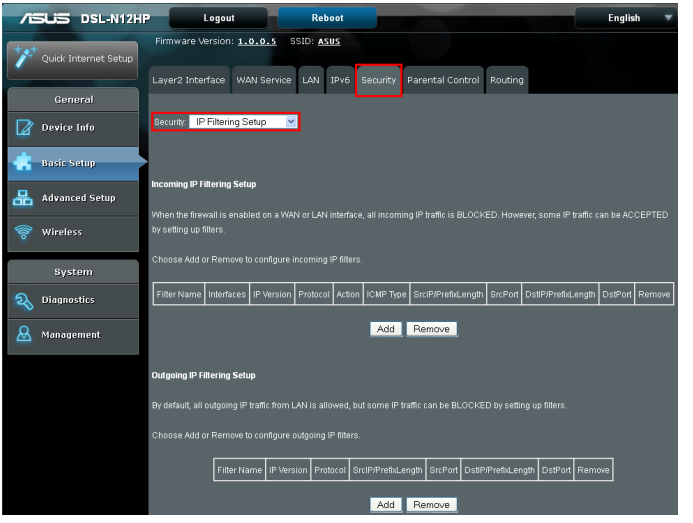


IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/ Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

NOTE: This function is not available when in bridge mode. Instead, MAC Filtering performs a similar function.

Select **IP Filtering Setup** from the drop-down menu.

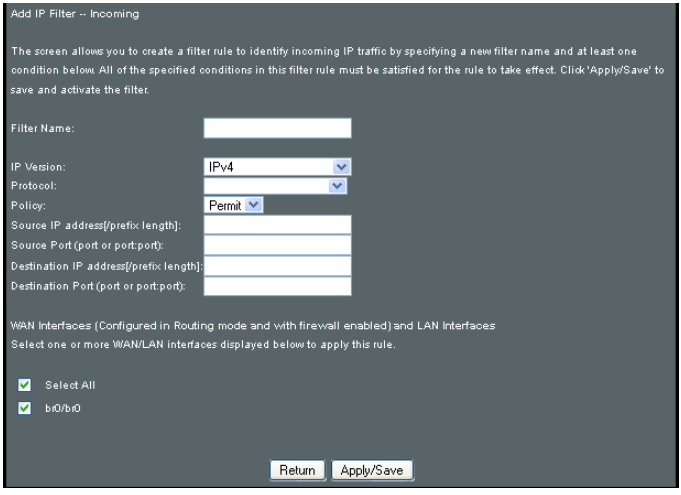


INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.

To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.



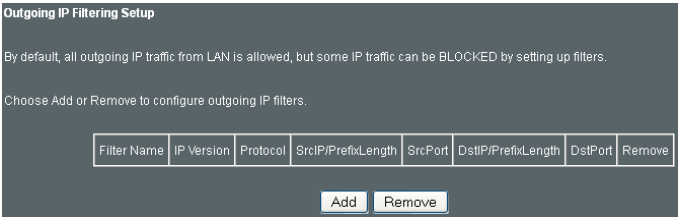
Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	Select from the drop down menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Policy	Permit/Drop packets specified by the firewall rule.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

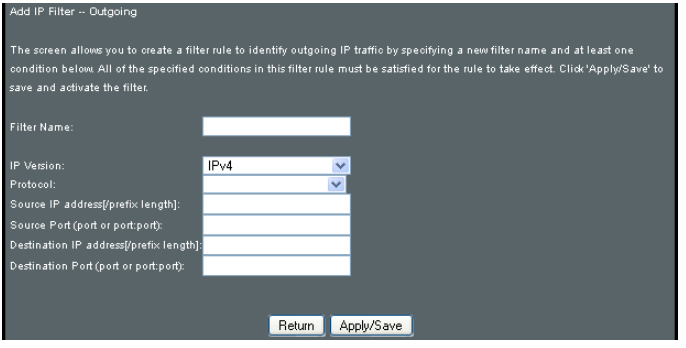
OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.



To add a filter (to block some outgoing IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.



Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	Select from the drop down menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

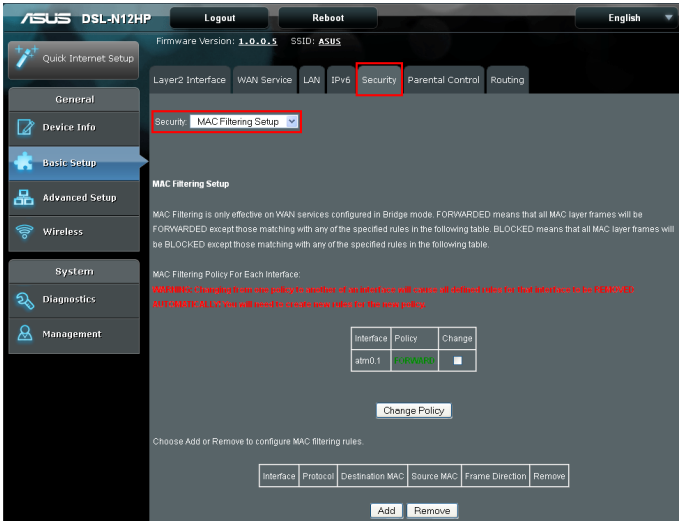
MAC Filtering

NOTE: This option is only available in bridge mode. Other modes use IP Filtering to perform a similar function.

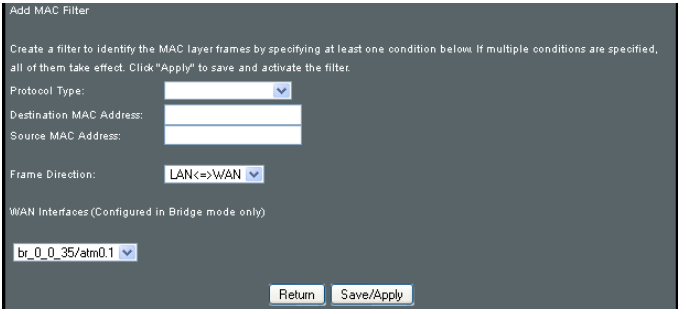
Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the DSL-N12HP can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. FORWARDED means that all MAC layer frames will be FORWARDED except those matching the MAC filter rules. BLOCKED means that all MAC layer frames will be BLOCKED except those matching the MAC filter rules. The default MAC Filtering Global policy is FORWARDED. It can be changed by clicking the Change Policy button.

Select **MAC Filtering Setup** from the drop-down menu.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save/Apply** to save and activate the filter rule.



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

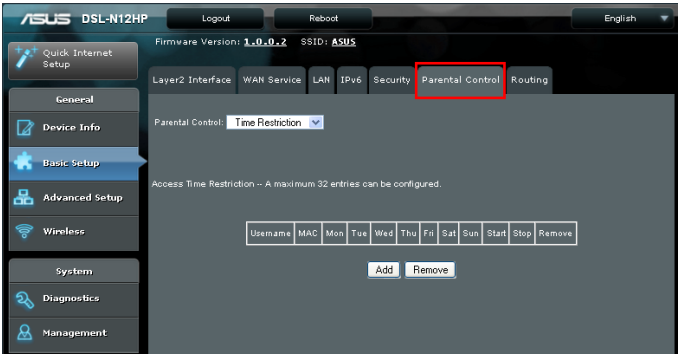
Consult the table below for detailed field descriptions.

Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface

3.2.6 Parental Control

This selection provides WAN access control functionality.

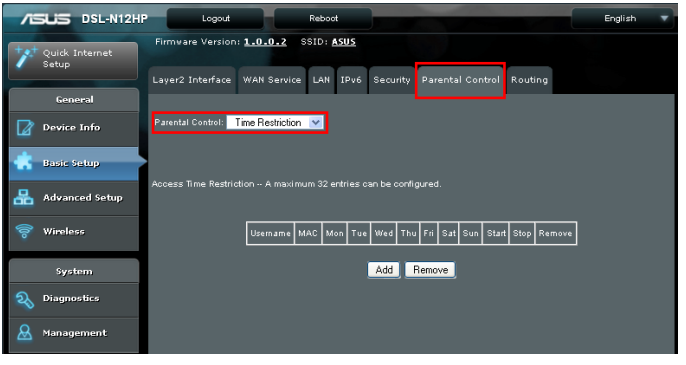
Click on the Parental Control tab to display the following.



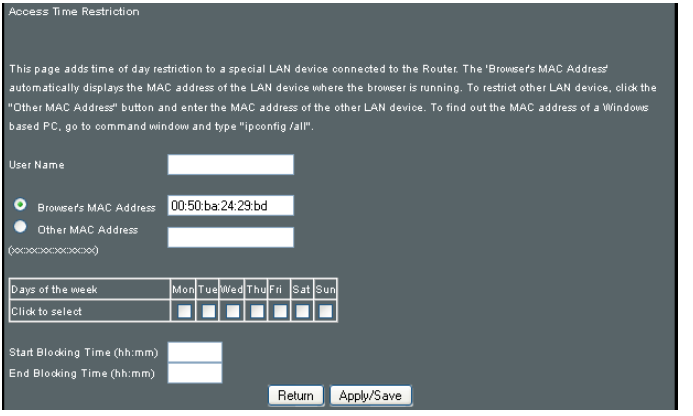
Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section Internet Time, so that the scheduled times match your local time.

Select **Time Restriction** from the drop-down menu.



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



See below for field descriptions.

User Name: A user-defined label for this restriction.

Browser's MAC Address: MAC address of the PC running the browser.

Other MAC Address: MAC address of another LAN device.

Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

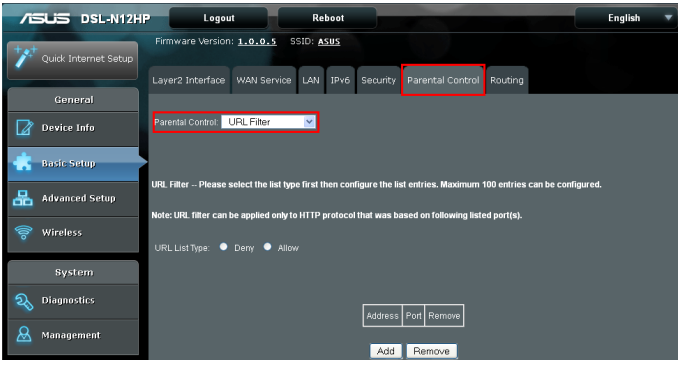
End Blocking Time: The time the restrictions end.

Click **Apply/Save** to add a time restriction.

URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL address and port number.

Select **URL Filter** from the drop-down menu.

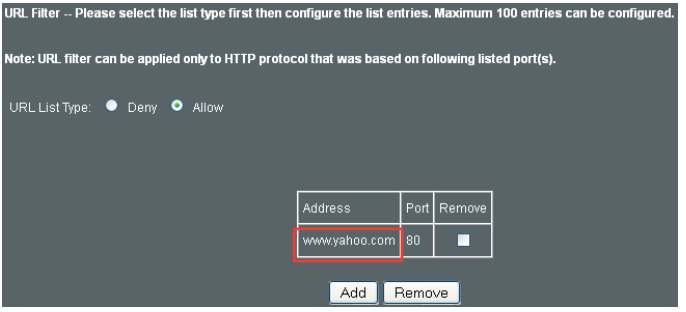


Select the **Deny** radio button to deny access to the websites listed.

Select the **Allow** radio button to restrict access to only those listed websites.

Then click **Add** to display the following screen.

Enter the URL address and port number then click **Apply/Save** to add the entry to the URL filter. URL Addresses begin with "www", as shown in this example.



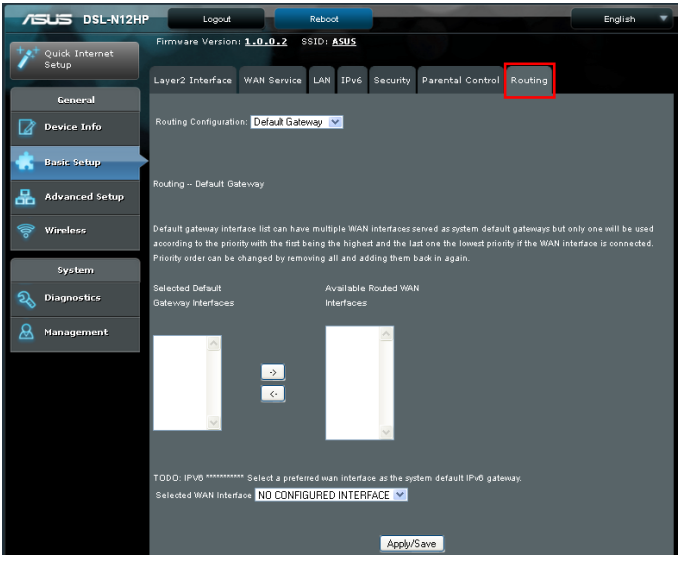
A maximum of 100 entries can be added to the URL Filter list.

3.2.7 Routing

The following routing functions are accessed from this menu: Default Gateway, Static Route, Policy Routing, RIP and IPv6 Static Route.

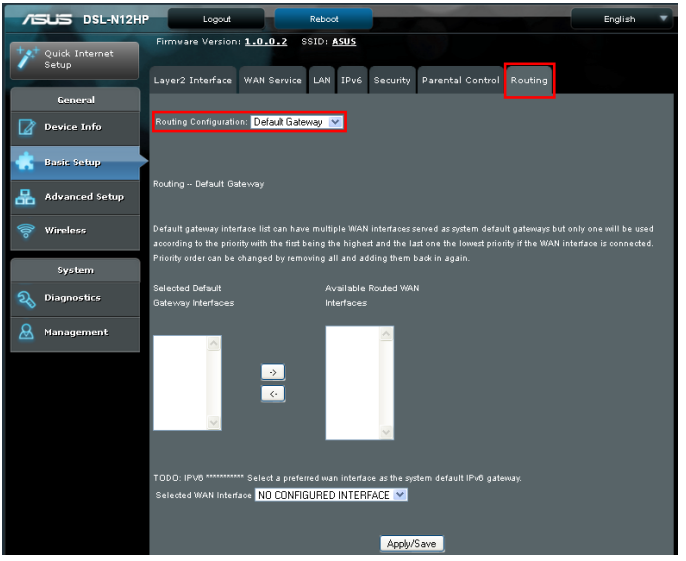
NOTE: In bridge mode, the RIP menu option is hidden while the other menu options are shown but ineffective.

Click the Routing tab to display the following.



Default Gateway

Select Default Gateway from the drop-down menu.



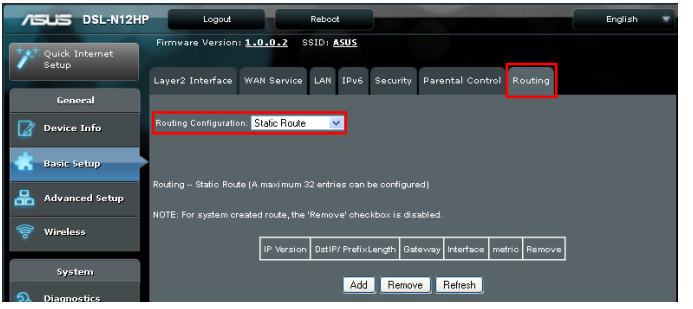
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Static Route

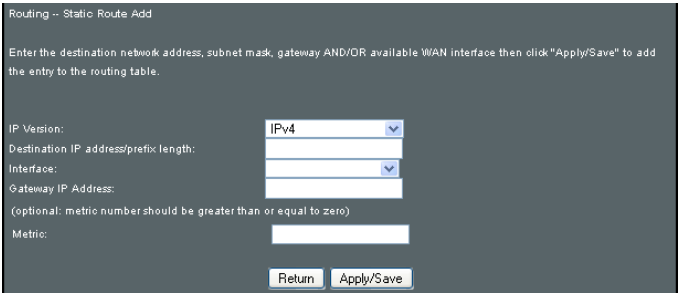
This option allows for the configuration of static routes by destination IP.

Click **Add** to create a static route or click **Remove** to delete a static route.

Select **Static Route** from the drop-down menu.



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



IP Version: Select the IP version to be IPv4.

Destination IP address/prefix length: Enter the destination IP address.

Interface: select the proper interface for the rule.

Gateway IP Address: The next-hop IP address.

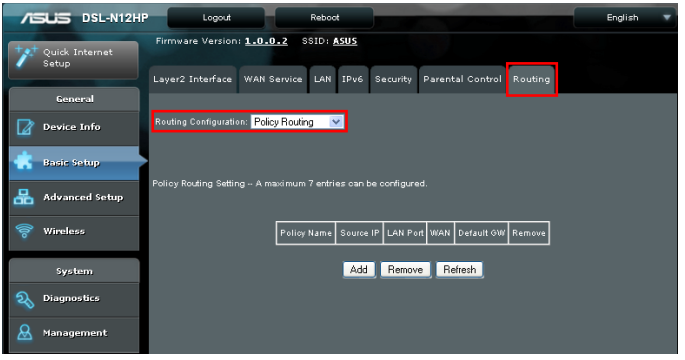
Metric: The metric value of routing.

After completing the settings, click **Apply/Save** to add the entry to the routing table.

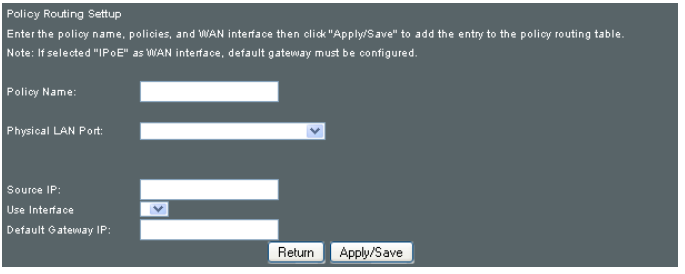
Policy Routing

This option allows for the configuration of static routes by policy.

Select **Policy Routing** from the drop-down menu.



Click **Remove** to delete an entry. Click **Add** to display the following.

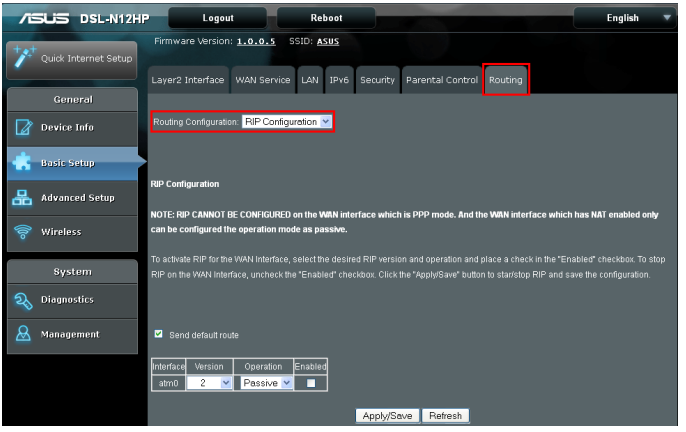


Complete the form and click **Apply/Save** to create a policy.

Field	Description
Policy Name	Name of the route policy
Physical LAN Port	Specify the port to use this route policy
Source IP	IP Address to be routed
Use Interface	Interface that traffic will be directed to
Default Gateway IP	IP Address of the default gateway

RIP Configuration

Select **RIP Configuration** from the drop-down menu.



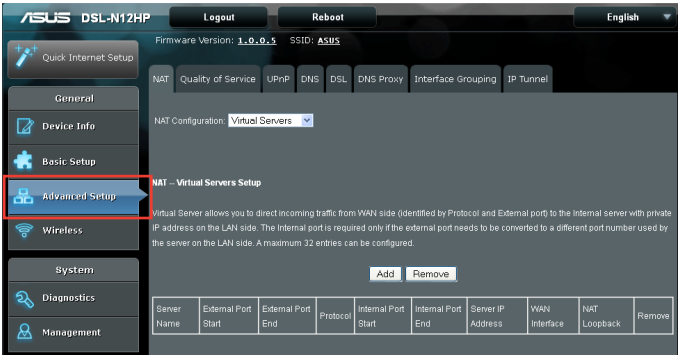
To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the "Enabled" checkbox. To stop RIP on the WAN Interface, uncheck the "Enabled" checkbox.

Click **Apply/Save** to start/stop RIP and save the configuration.

3.3 Advanced Setup

You can reach this page by clicking on the Advanced Setup icon located on the left side of the screen.

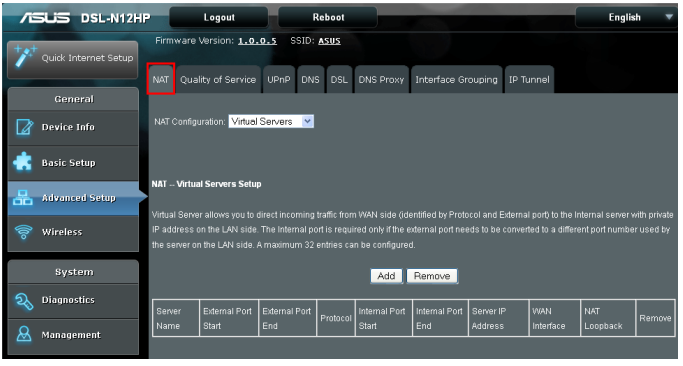
This will bring you to the following screen.



3.3.1 NAT

NOTE: To display this option, NAT must be enabled in at least one PVC. NAT is not an available option in Bridge mode.

Click the NAT tab to display the following.

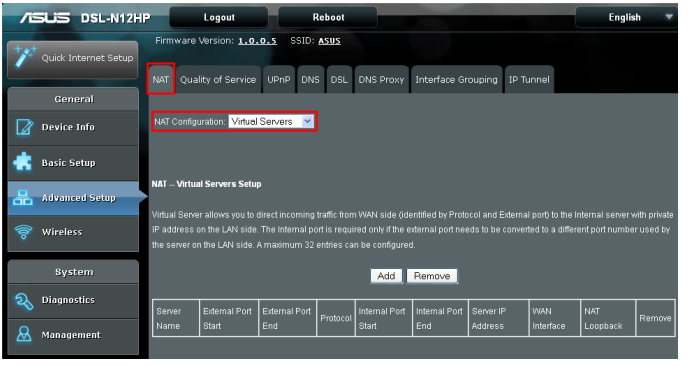


Virtual Servers

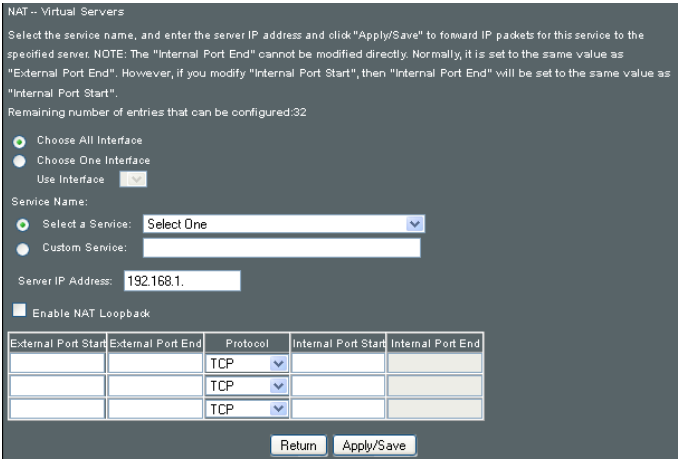
Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server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

A maximum of 32 entries can be configured.

Select **Virtual Servers** from the drop-down menu.



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



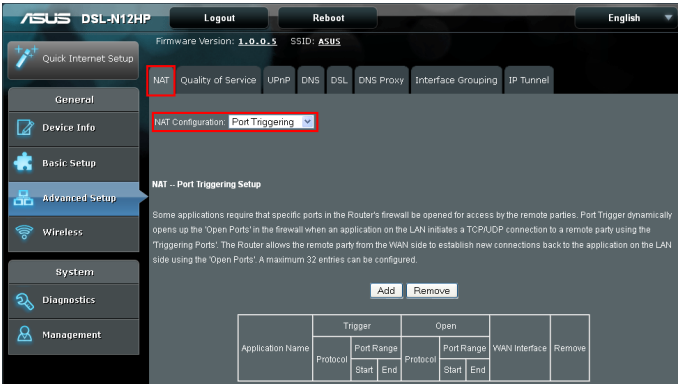
Consult the table below for field and header descriptions.

Field	Description
Use Interface	Select a WAN interface from the drop-down box.
Select a Service	User should select the service from the list.
Custom Service	User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
Enable NAT Loopback	Allows local machines to access virtual server via WAN IP Address
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	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.

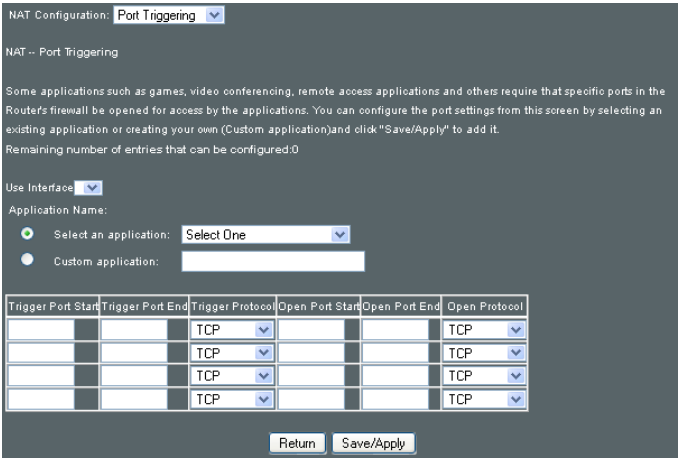
Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port Triggers dynamically '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.

Select **Port Triggering** from the drop-down menu.



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



Click **Save/Apply** to save and apply the settings.

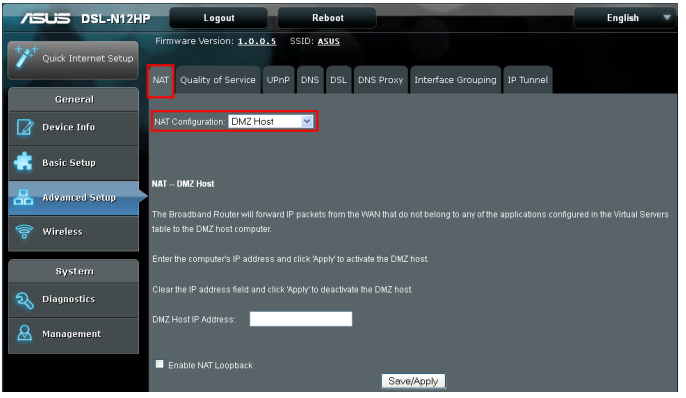
Consult the table below for field and header descriptions.

Field	Description
Use Interface	Select a WAN interface from the drop-down box.
Select an Application	User should select the application from the list.
Custom Application	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	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	TCP, TCP/UDP, or UDP.

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.

Select **DMZ Host** from the drop-down menu.



Click **Save/Apply** to save and apply the settings.

To Activate the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

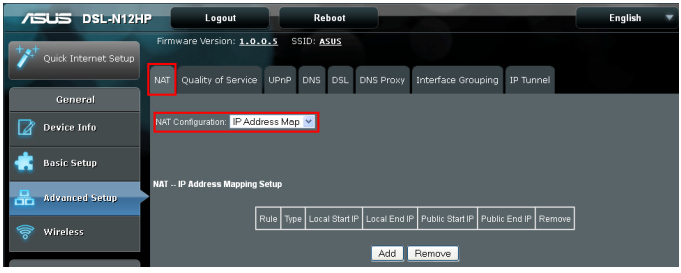
To Deactivate the DMZ host, clear the IP address field and click **Save/Apply**.

Enable NAT Loopback allows PC on the LAN side to access servers in the LAN network via the router's WAN IP.

IP Address Map

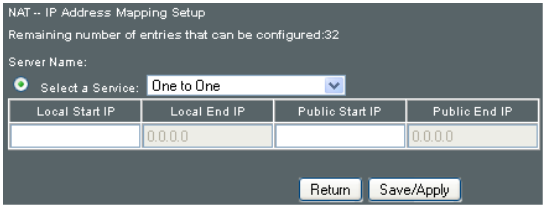
Mapping Local IP (LAN IP) to some specified Public IP (WAN IP).

Select **IP Address Map** from the drop-down menu.



Field	Description
Rule	The number of the rule
Type	Mapping type from local to public.
Local Start IP	The beginning of the local IP
Local End IP	The ending of the local IP
Public Start IP	The beginning of the public IP
Public End IP	The ending of the public IP
Remove	Remove this rule

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



Select a Service, then click the **Save/Apply** button.

One to One: mapping one local IP to a specific public IP

Many to one: mapping a range of local IP to a specific public IP

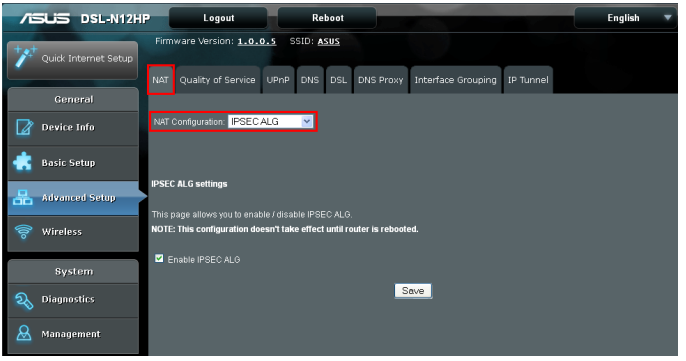
Many to many(Overload): mapping a range of local IP to a different range of public IP

Many to many(No Overload): mapping a range of local IP to a same range of public IP

IPSEC ALG

IPSEC ALG provides multiple VPN passthrough connection support, allowing different clients on LAN side to establish a secured IP Connection to the WAN server.

Select **IPSEC ALG** from the drop-down menu.

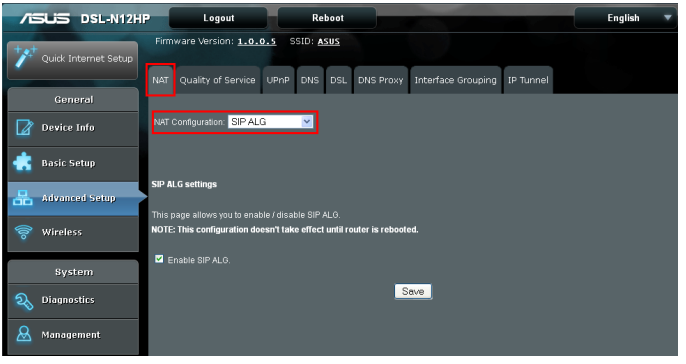


To enable IPSEC ALG, tick the checkbox and click **Save**.

SIP ALG

This page allows you to enable / disable SIP ALG.

Select **SIP ALG** from the drop-down menu.

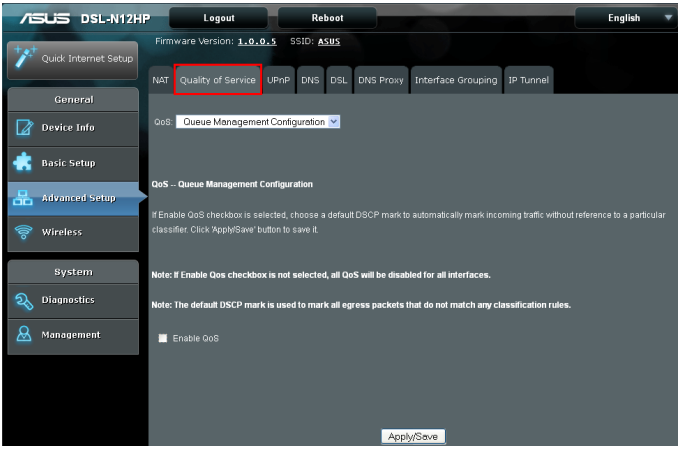


To enable SIP ALG, tick the checkbox and click **Save**.

3.3.2 Quality of Service (QoS)

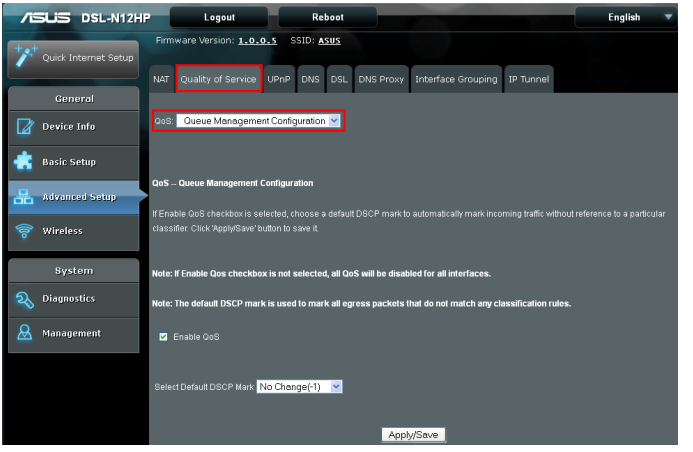
NOTE: QoS must be enabled in at least one PVC to display this option. (See **Appendix E - Connection Setup** for detailed PVC setup instructions).

Click the QoS tab to display the following.



Queue Management Configuration

Select **QoS Queue Setup** from the drop-down menu.



To Enable QoS tick the checkbox and select a Default DSCP Mark.

Click **Apply/Save** to activate QoS.

QoS and DSCP Mark are defined as follows:

Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

QoS Queue Setup

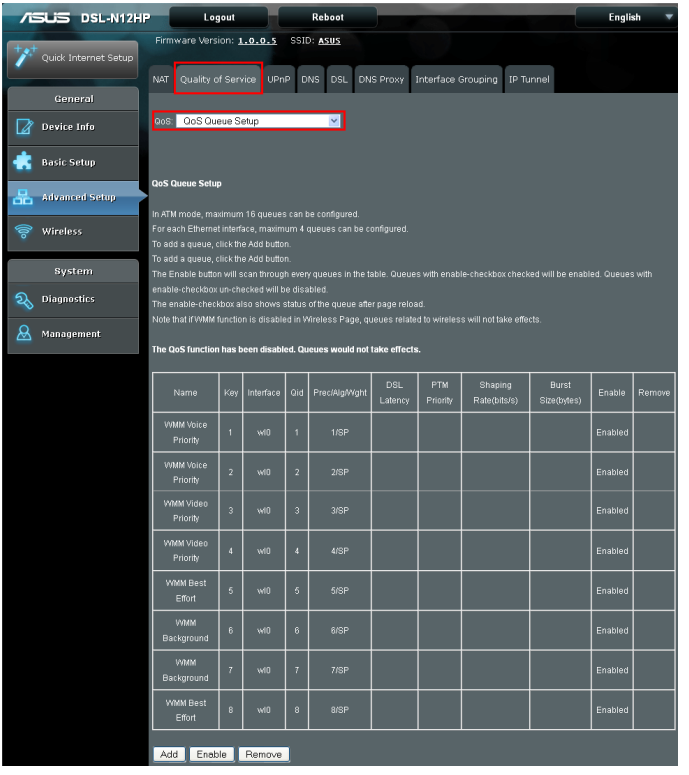
Configure queues with different priorities to be used for QoS setup.

In ATM mode, maximum 16 queues can be configured.

In PTM mode, maximum 8 queues can be configured.

For each Ethernet interface, maximum 3 queues can be configured.

Select **QoS Queue Setup** from the drop-down menu.



To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes (for user created queues), then click the **Remove** button.

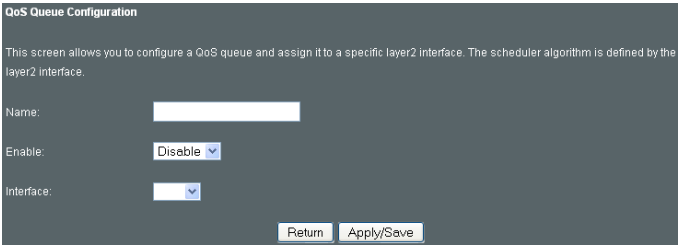
The **Enable** button will scan through every queue in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effect. This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button.

Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.

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



Click **Apply/Save** to apply and save the settings.

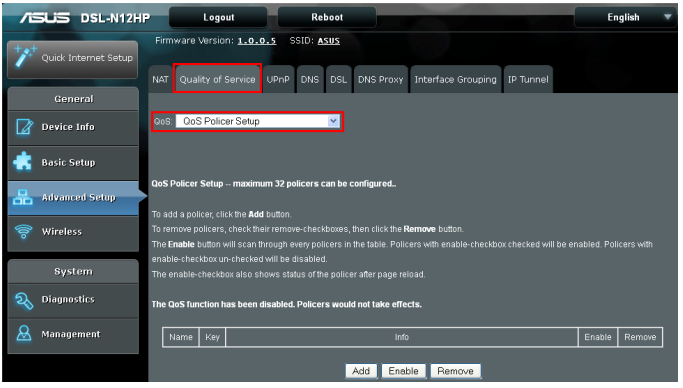
Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

Interface: Assign the entry to a specific network interface (QoS enabled).

QoS Policer Setup

Select **QoS Policer Setup** from the drop-down menu.

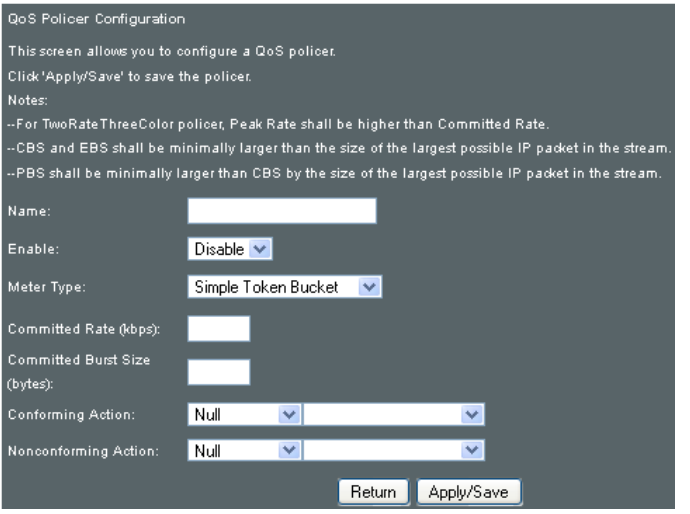


To remove policers, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the policer after page reload.

To add a policer, click the **Add** button.



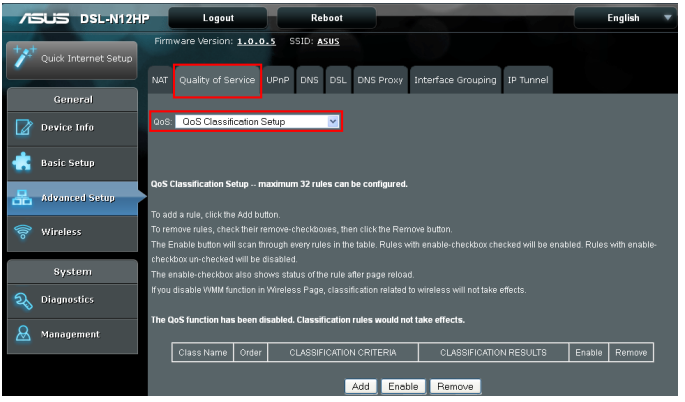
Click **Apply/Save** to save the policer.

Field	Description
Name	Name of this policer rule
Enable	Enable/Disable this policer rule
Meter Type	Meter type used for this policer rule
Committed Rate (kbps)	Defines the rate allowed for committed packets
Committed Burst Size (bytes)	Maximum amount of packets that can be processed by this policer
Conforming Action	Defines action to be taken if packets match this policer
Nonconforming Action	Defines actions to be taken if packets do not match this policer

QoS Classification Setup

The network traffic classes are listed in the following table.

Select **QoS Classification Setup** from the drop-down menu.



Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

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

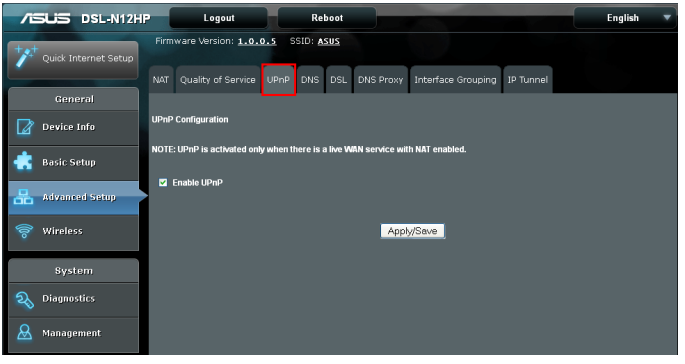
Click **Apply/Save** to save and activate the rule.

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.

Field	Description
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
Specify Class Queue	Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.
Specify Class Policer	Packets classified into a policer will be marked based on the conforming action of the policer
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7.
Set Rate Limit	The data transmission rate limit in kbps.

3.3.3 UPnP

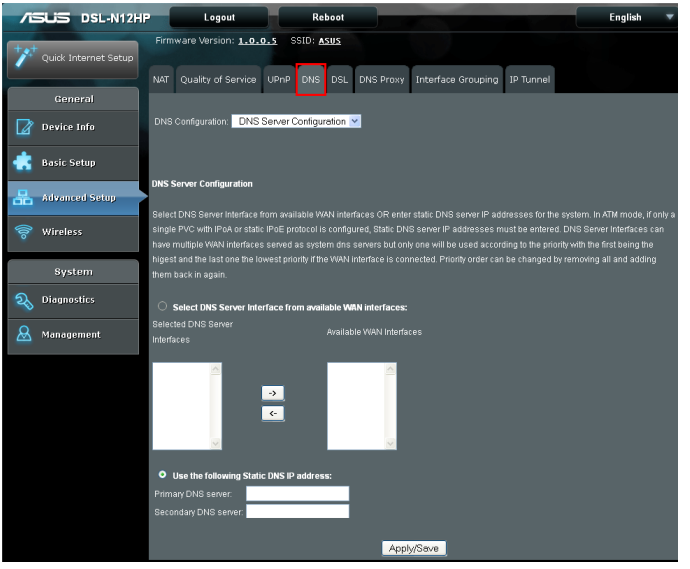
Click the UPnP tab to display the following.



Select the checkbox and click **Apply/Save** to enable UPnP.

3.3.4 DNS

Click the DNS tab to display the following.

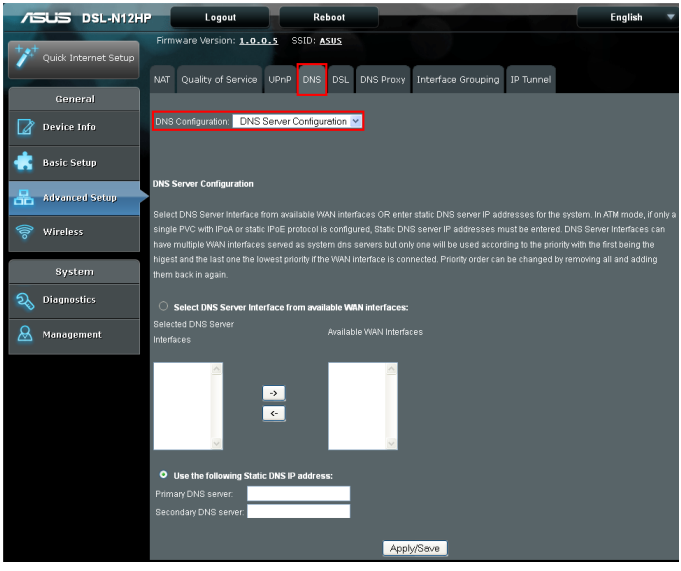


DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select **DNS Server Configuration** from the drop-down menu.



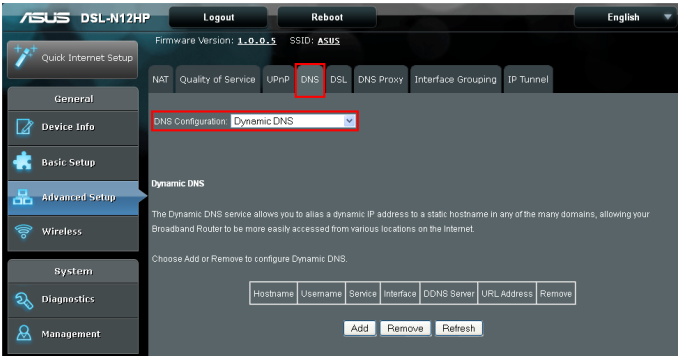
Click **Apply/Save** to save the new configuration.

NOTE: You must reboot the router to make the new configuration effective.

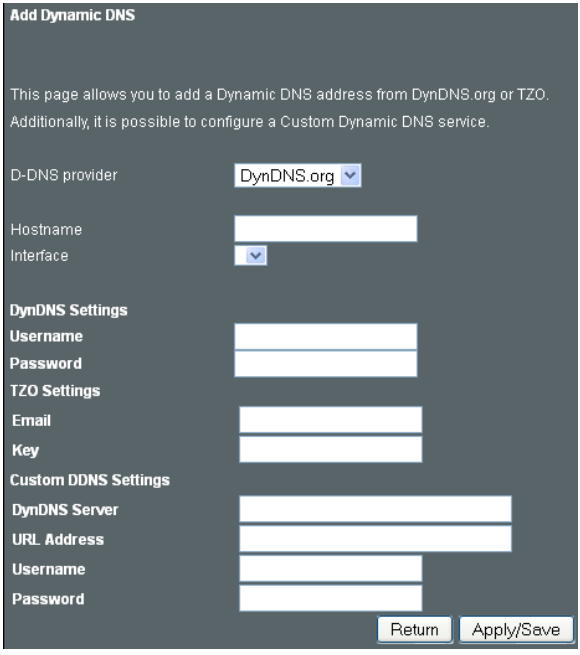
Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the DSL-N12HP to be more easily accessed from various locations on the Internet.

Select **Dynamic DNS** from the drop-down menu.



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



Click **Apply/Save** to save your settings.

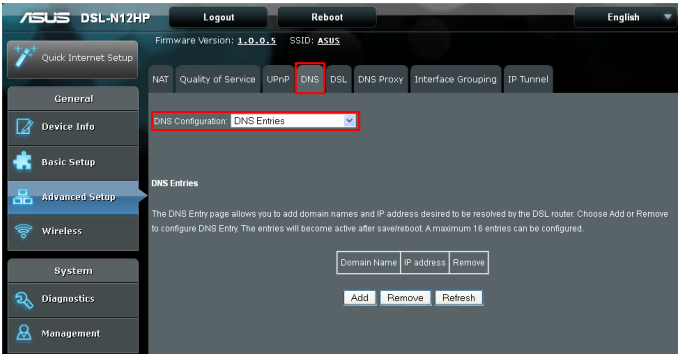
Consult the table below for field descriptions.

Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server
Email	Enter mail server for DDNS
Key	Enter an account level key which can be used to update DNS hosts instead of our HTTP-based DNS update API
DynDNS Server	Enter dynamic DNS server
URL Address	Dynamic DNS server URL
Username	Dynamic DNS server name
Password	Dynamic DNS server password

DNS Entries

The DNS Entry page allows you to add domain names and IP address desired to be resolved by the DSL router.

Select **Dynamic DNS** from the drop-down menu.



Choose **Add** or **Remove** to configure DNS Entry. The entries will become active after save/reboot.

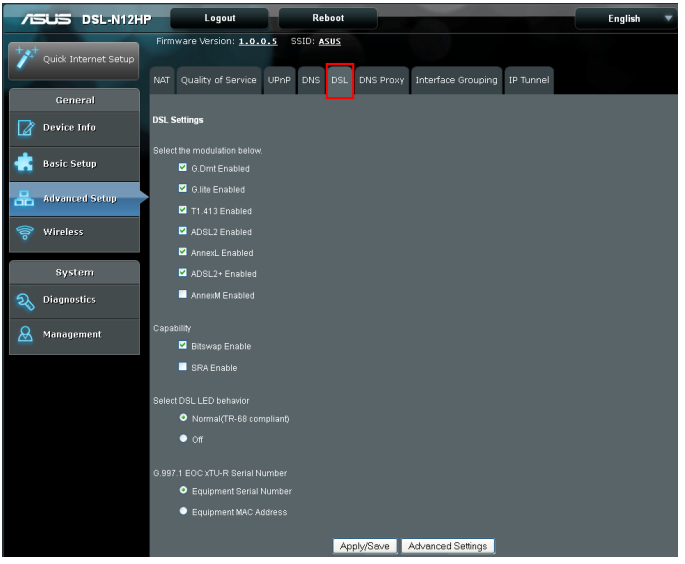
Enter the domain name and IP address that needs to be resolved locally, and click the **Add Entry** button.

3.3.5 DSL

The DSL Settings screen allows for the selection of DSL modulation modes.

For optimum performance, the modes selected should match those of your ISP.

Click the DSL tab to display the following.

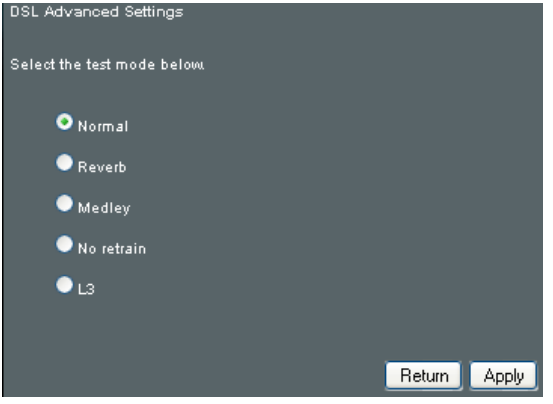


DSL Mode	Data Transmission Rate - Mbps (Megabits per second)	
G.Dmt	Downstream: 12 Mbps	Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps	Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps	Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps	Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates	
ADSL2+	Downstream: 24 Mbps	Upstream: 1.0 Mbps
AnnexM	Downstream: 24 Mbps	Upstream: 3.5 Mbps

Options	Description
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)
Select DSL LED behavior	Normal (TR-68 compliant): Select this option for DSL LED to operate normally (See section **1.3 Your ADSL modem router**)
	Off:DSL LED will always be OFF
G997.1 EOC xTU-R Serial Number	Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages

Advanced DSL Settings

Click **Advanced Settings** to reveal additional options.



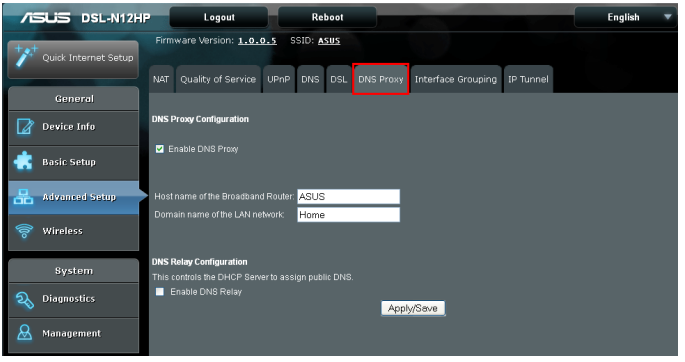
On this screen you select the required test mode, then click the **Apply** button.

Field	Description
Normal	DSL line signal is detected and sent normally
Reverb	DSL line signal is sent continuously in reverb mode
Medley	DSL line signal is sent continuously in medley mode
No Retrain	DSL line signal will always be on even when DSL line is unplugged
L3	DSL line is set in L3 power mode

3.3.6 DNS Proxy

DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and the PC can access route with "ASUS.Home".

Click the DNS Proxy tab to display the following.



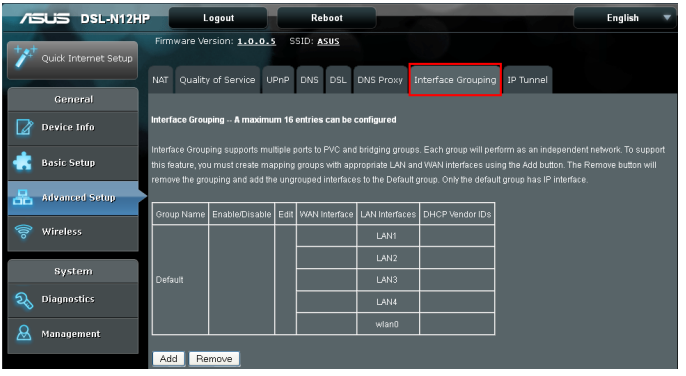
Click **Apply/Save** to implement new configuration settings.

3.3.7 Interface Grouping

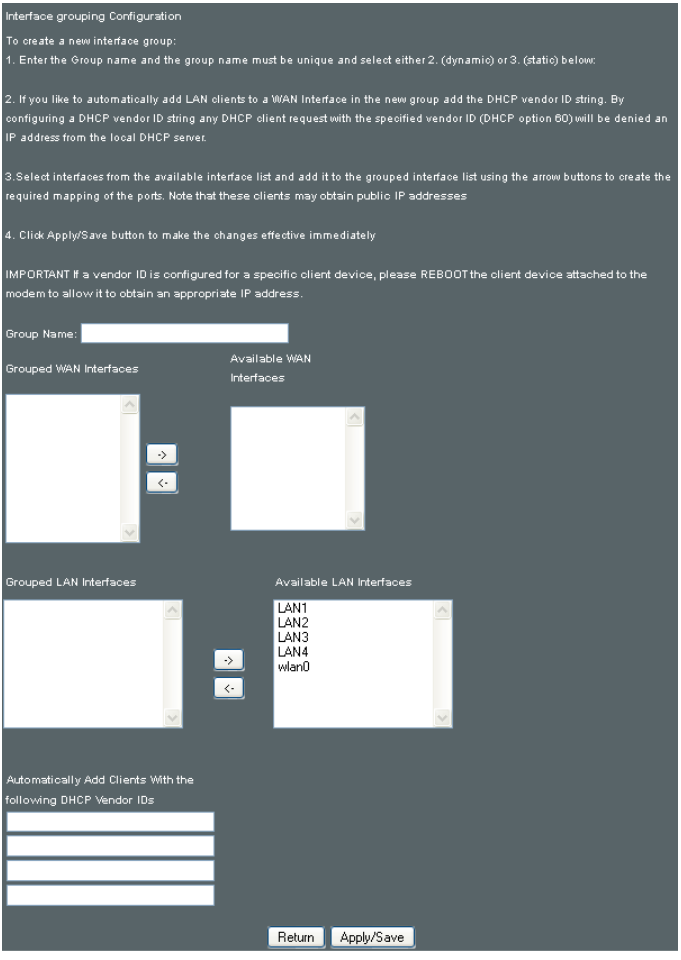
Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

The Remove button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

Click the Interface Grouping tab to display the following.



To add an Interface Group, click **Add**. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown onscreen.



Click **Apply/Save** to implement new configuration settings.

Automatically Add Clients With Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces 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 Interface Grouping is enabled.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are LAN1, LAN2, LAN3, and LAN4.

The Interface Grouping configuration will be:

1. Default: LAN1, LAN2, LAN3, and LAN4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

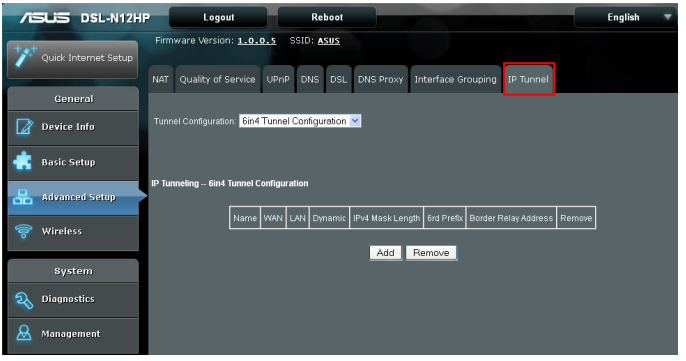
If the onboard DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

If a set-top box is connected to ETH1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: LAN2, LAN3, and LAN4
2. Video: nas_0_36, nas_0_37, nas_0_38, and LAN1

3.3.7 IP Tunnel

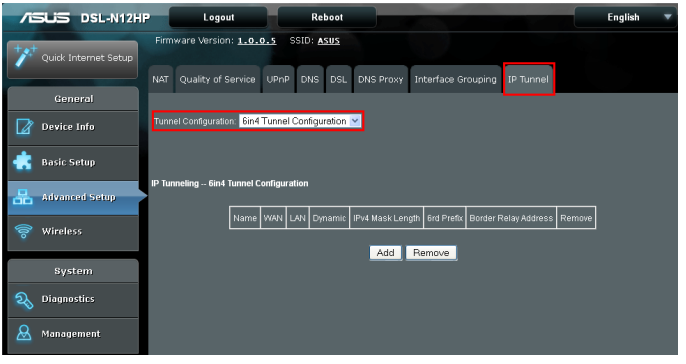
Click on the IP Tunnel tab to display the following.



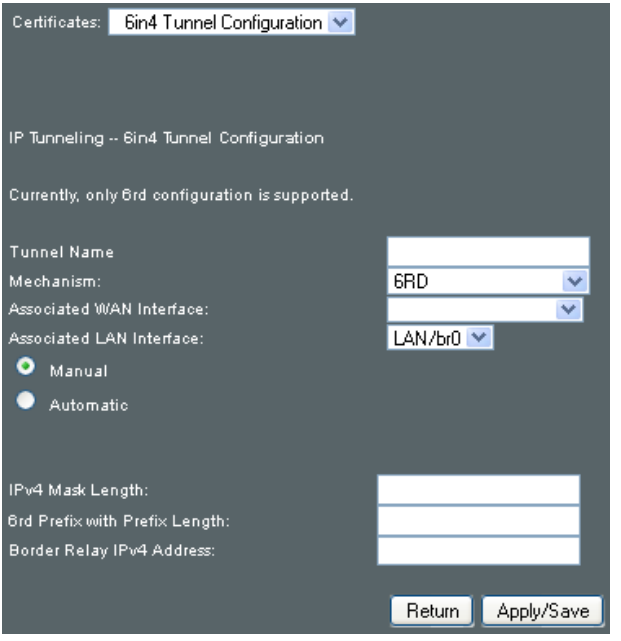
IPv6inIPv4

Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.

Select **6in4 Tunnel Configuration** from the drop-down menu.



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



Click **Apply/Save** to implement new configuration settings.

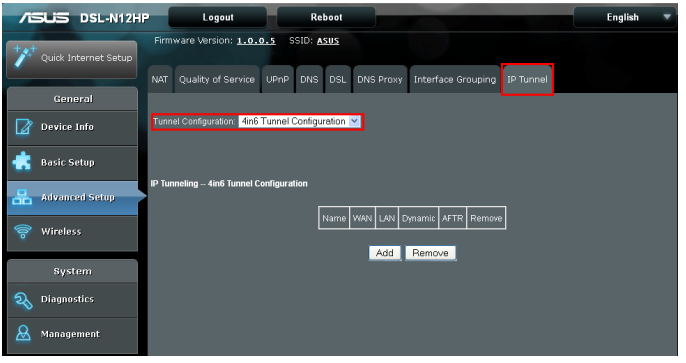
Click **Return** to go back to the previous page.

Field	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling/ manual for point-to-point tunneling
IPv4 Mask Length	The subnet mask length used for the IPv4 interface
6rd Prefix with Prefix Length	Prefix and prefix length used for the IPv6 interface
Border Relay IPv4 Address	Input the IPv4 address of the other device

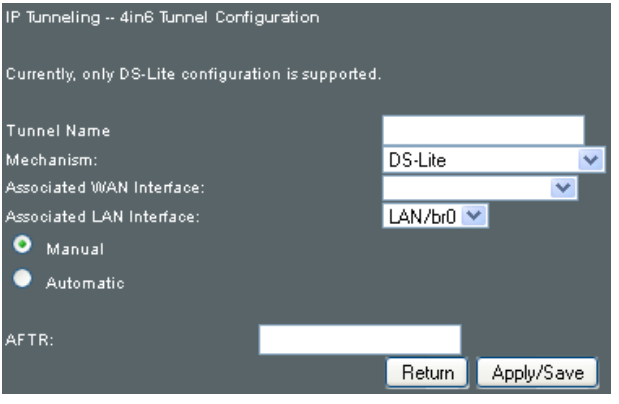
IPv4inIPv6

Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.

Select **4in6 Tunnel Configuration** from the drop-down menu.



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



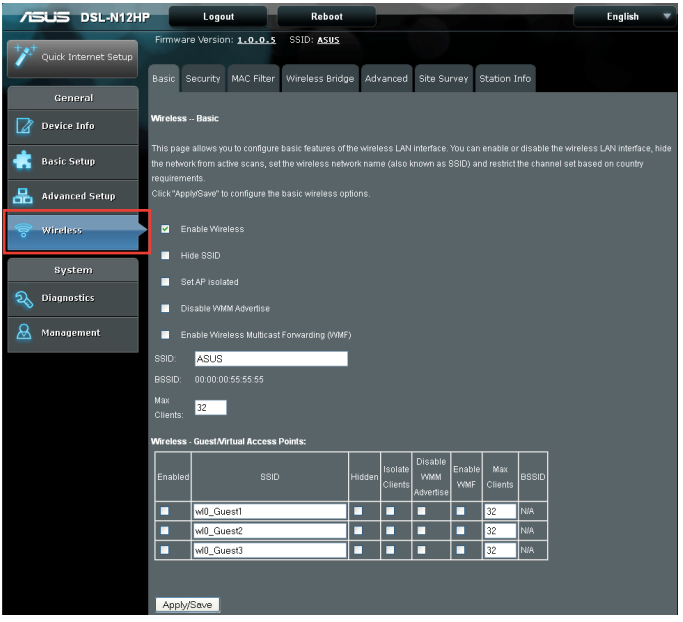
Click **Apply/Save** to implement new configuration settings.

Click **Return** to go back to the previous page.

Field	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling/ manual for point-to-point tunneling
AFTR	Address of Address Family Translation Router

3.4 Wireless

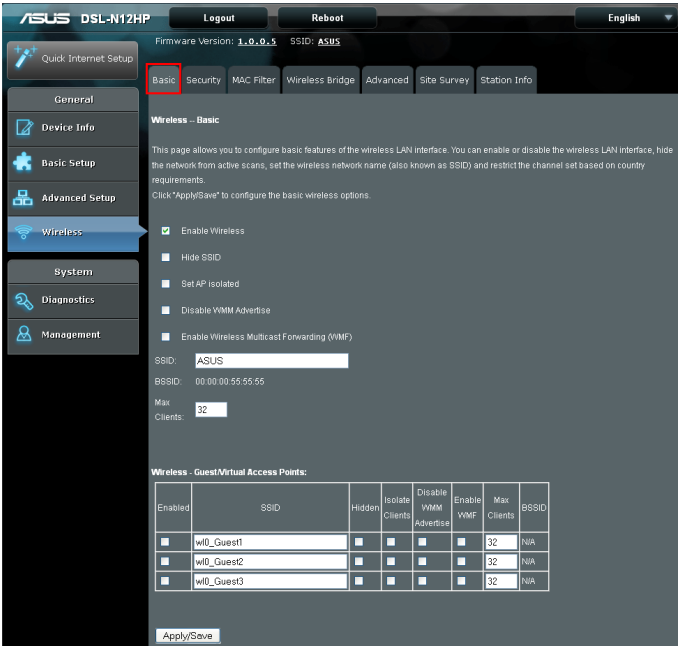
You can reach this page by clicking the Wireless icon located on the left side of the screen.



3.4.1 Basic

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, 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 the Basic tab to display the following.



Click **Apply/Save** to apply the selected wireless options.

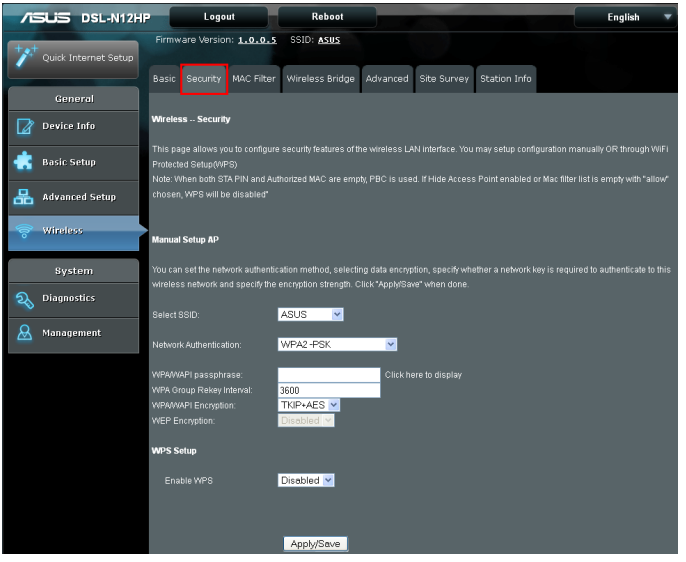
Consult the table below for descriptions of these options.

Field	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide SSID	Select the checkbox to enable this function.
Set AP isolated	Select the checkbox to enable this function.
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).
Enable Wireless Multicast Forwarding	Select the checkbox to enable this function.
SSID [1-32 characters]	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.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media 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. Local regulations limit 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 checkboxes in the Enabled column. To hide a Guest SSID, select its checkbox in the Hidden column. Do the same for Isolate Clients and Disable WMM Advertise. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for Enable WMF, Max Clients and BSSID, consult the matching entries in this table. **NOTE**: Remote wireless hosts cannot scan Guest SSIDs.

3.4.2 Security

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.

Click the Security tab to display the following.



Please see **Appendix F** for WPS setup instructions.

Click **Apply/Save** to implement new configuration settings.

WIRELESS SECURITY

Setup requires that the user configure these settings using the Web GUI (see the table below).

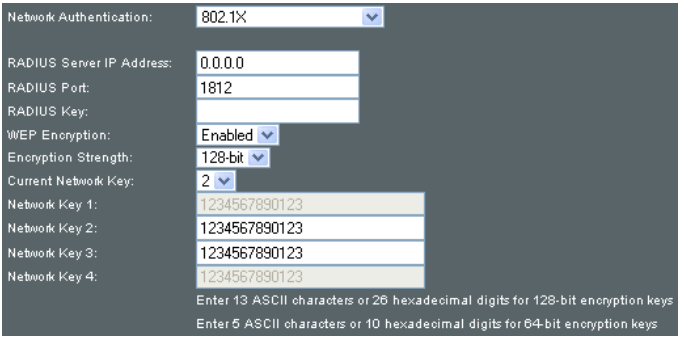
Select SSID

Select the wireless network name from the drop-down menu. 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 client will not be granted access.

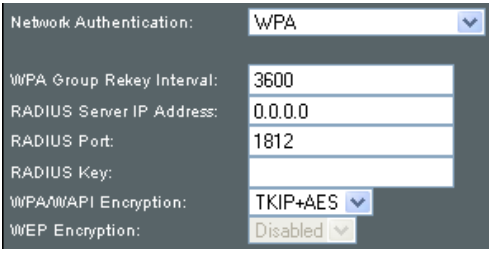
Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

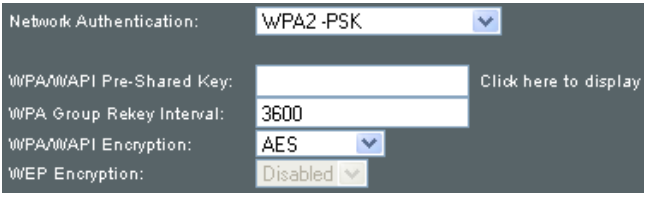
Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.



The settings for WPA authentication are shown below.



The settings for WPA2-PSK authentication are shown next.



WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

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.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

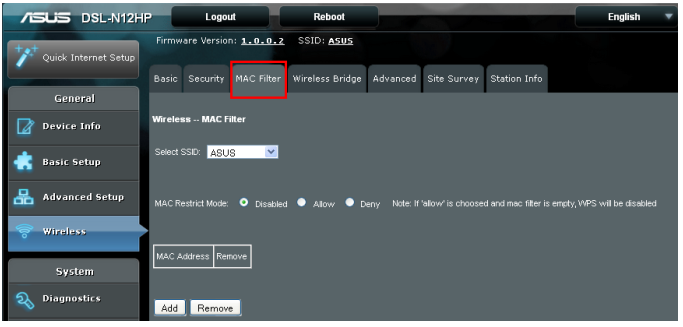
Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

3.4.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses.

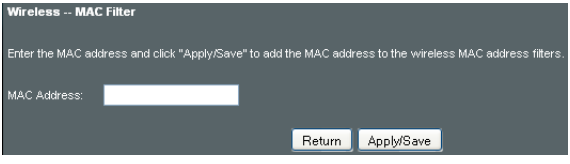
Click the MAC Filter tab to display the following.



To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the MAC Address table below and click the **Remove** button.

Option	Description
Select SSID	Select the wireless network name from the drop-down box. 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.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: ¬Rejects access for the specified MAC addresses.
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.

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

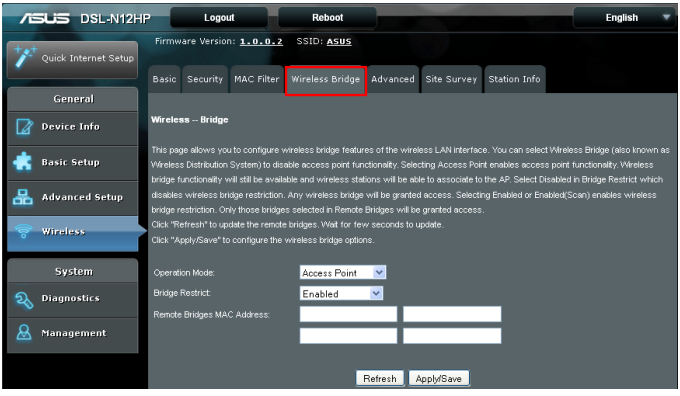


Enter the MAC address in the box provided and click **Apply/Save**.

3.4.4 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the Wi-Fi interface. See the table beneath for detailed explanations of the various options.

Click the Wireless Bridge tab to display the following.



Click **Apply/Save** to implement new configuration settings.

Feature	Description
AP Mode	Selecting Wireless Bridge (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

3.4.5 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 the Wireless Bridge tab to display the following.

Click **Apply/Save** to set new advanced wireless options.

Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. 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)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20MHz or 40MHz bandwidth. 40MHz bandwidth uses two adjacent 20MHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40MHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g client's access to the router.
RIFS Advertisement	One of several draft-n features designed to improve efficiency. Provides a shorter delay between OFDM transmissions than in802.11a or g.
OBSS Co-Existence	Co-existence between 20 MHZ AND 40 MHZ overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
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 for multicast packet transmit rate (1-54 Mbps)

Field	Description
Basic Rate	Setting for basic transmission 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) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs 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 in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. 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).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress TM Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
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.

3.4.6 Site Survey

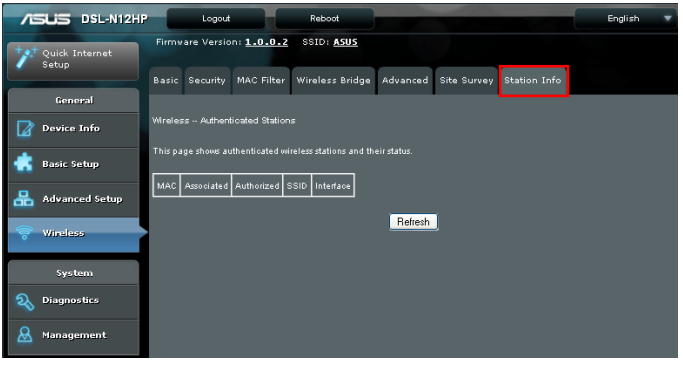
The graph displays wireless APs found in your neighborhood by channel.

Click the Site Survey tab to display the following.

3.4.7 Station Info

This page shows authenticated wireless stations and their status. Click the Refresh button to update the list of stations in the WLAN.

Click the Station Info tab to display the following.



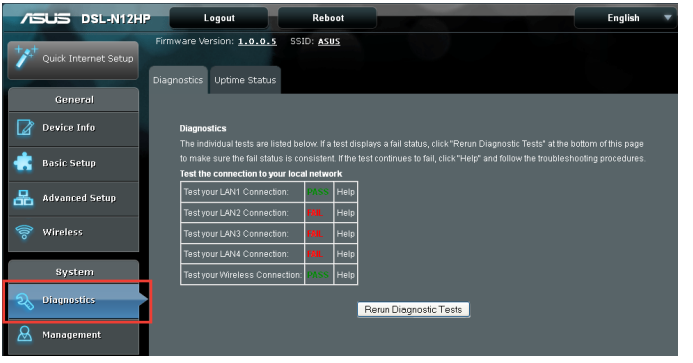
Consult the table below for descriptions of each column heading.

Field	Description
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.

4 Configuring the System settings

4.1 Diagnostics

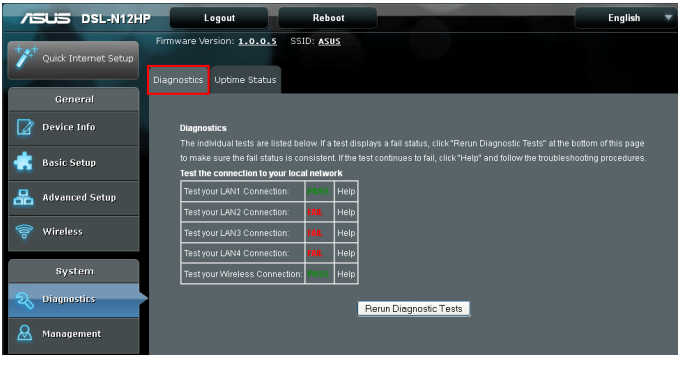
You can reach this page by clicking on the Diagnostics icon located on the left side of the screen.



4.1.1 Individual Tests

The first Diagnostics screen is a dashboard that shows overall connection status.

Click the Diagnostics tab to display the following.

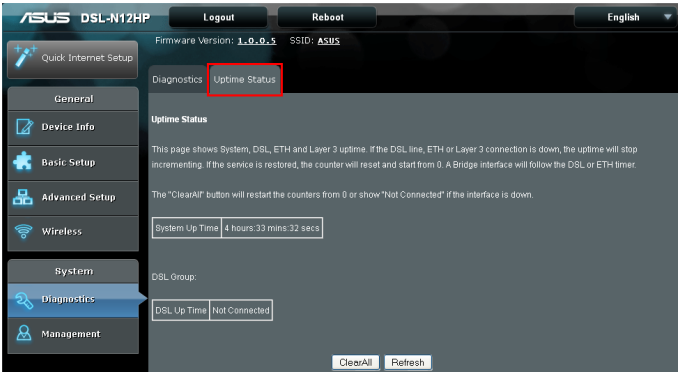


If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

4.1.2 Uptime Status

This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.

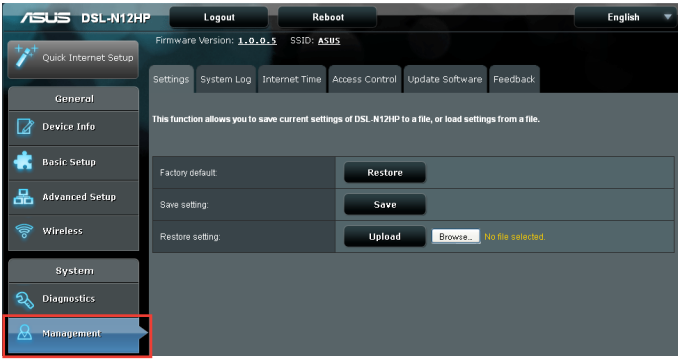
Click the Uptime Status tab to display the following.



The **ClearAll** button will restart the counters from 0 or show **Not Connected** if the interface is down.

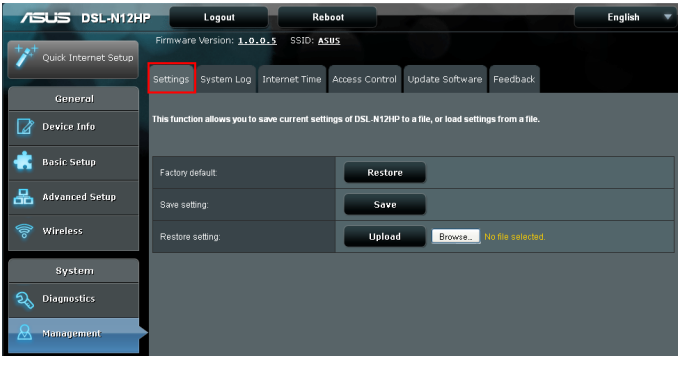
4.2 Management

You can reach this page by clicking on the Management icon located on the left side of the screen.



4.2.1 Settings

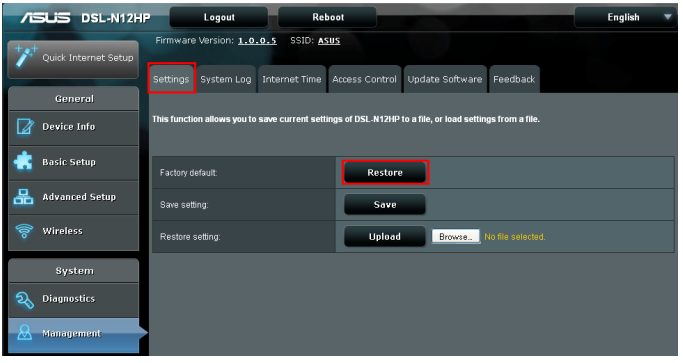
Click on the Settings tab to display the following.



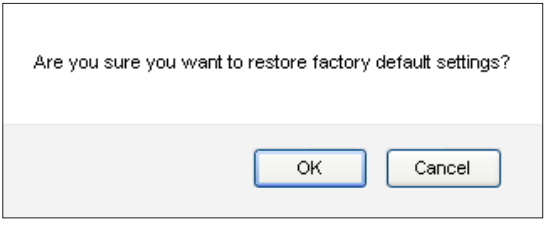
This includes Restore Default, Save Setting, and Restore Setting screens.

Restore Default

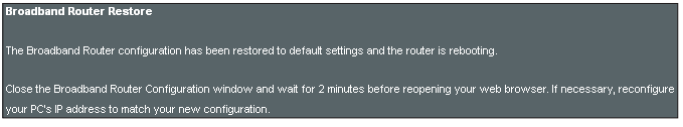
Click the Restore button to restore factory default settings.



After clicking **Restore**, the following window appears.



Click **OK** to display the following.

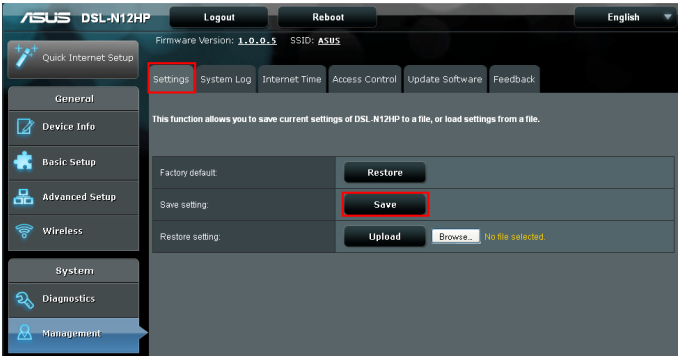


Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

NOTE: This entry has the same effect as the Reset button. The DSL-N12HP board hardware and the boot loader support the reset to default. If the Reset button is continuously pressed for more than 10 seconds, the boot loader will erase the configuration data saved in flash memory.

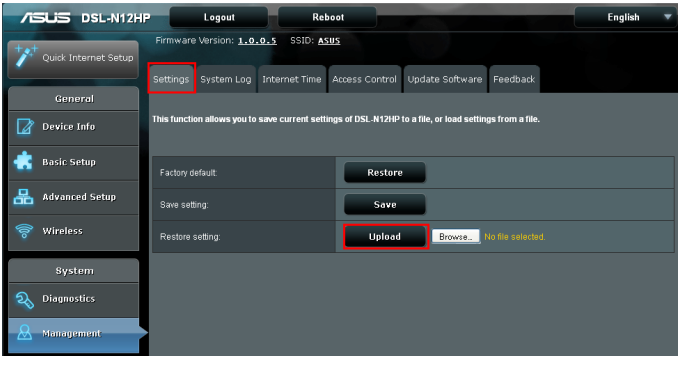
Save Setting

To save the current configuration to a file on your PC, click the Save button. You will be prompted for backup file location. This file can later be used to recover settings on the Restore Setting screen, as described below.



Upload Setting

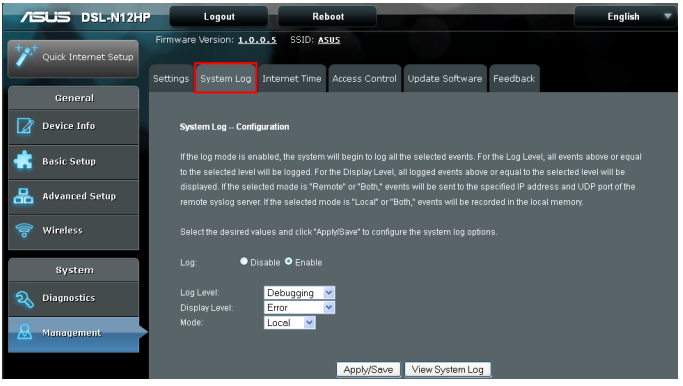
This option recovers configuration files previously saved using Save Setting. Press the **Browse…** button to search for the file, then click the **Upload** button to restore settings.



4.2.2 System Log

This function allows a system log to be kept and viewed upon request.

Click the System Log tab to display the following.



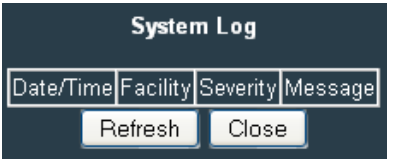
Select the desired values and click **Apply/Save** to configure the system log options.

Consult the table below for detailed descriptions of each system log option.

Field	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, select the Enable radio button and then click Apply/Save.

Field	Description
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 DSL-N12HP 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 log levels are defined as follows: • 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 window 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 system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log 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.

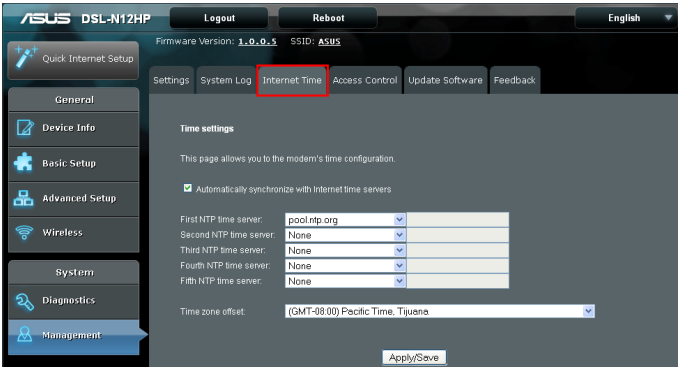
Click **View System Log**. The results are displayed as follows.



4.2.3 Internet Time

This option automatically synchronizes the router time with Internet timeservers.

Click the Internet Time tab to display the following.

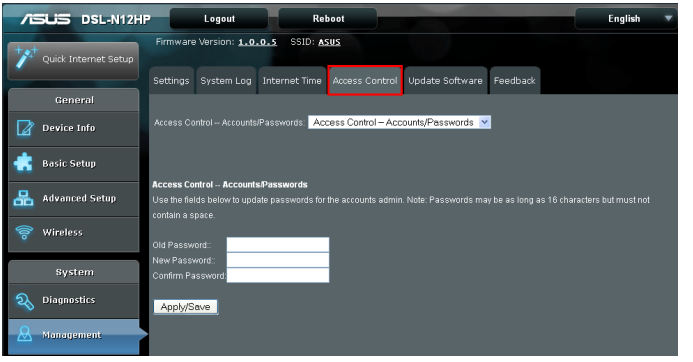


To enable time synchronization, tick the corresponding checkbox, choose your preferred time server(s), select the correct time zone offset, and click **Apply/Save**.

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

4.2.4 Access Control

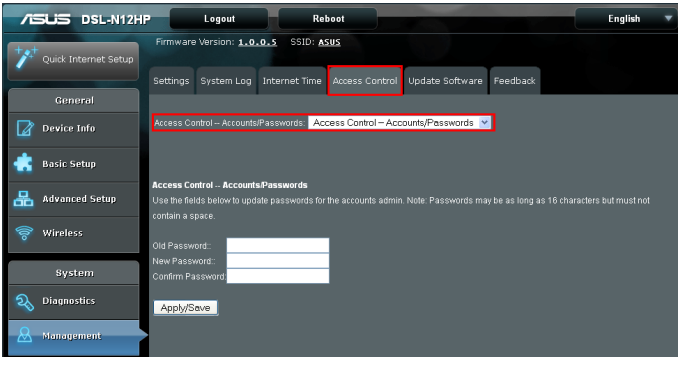
Click the Access Control tab to display the following.



Passwords

This screen is used to configure the user account access passwords for the device.

Select **Access Control - Accounts/Passwords** from the drop-down menu.



Use the fields to update passwords for the accounts administration.

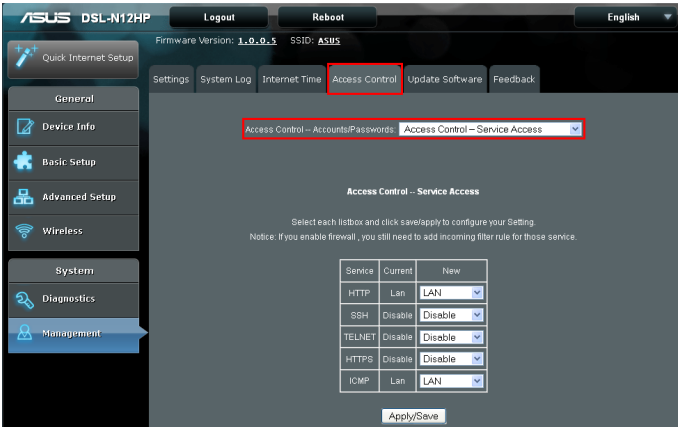
NOTE: Passwords may be as long as 16 characters but must not contain a space.

Click **Apply/Save** to apply and save the settings.

Service Access

The Services option limits or opens the access services over the LAN or WAN.

Select **Access Control – Service Access** from the drop-down menu.

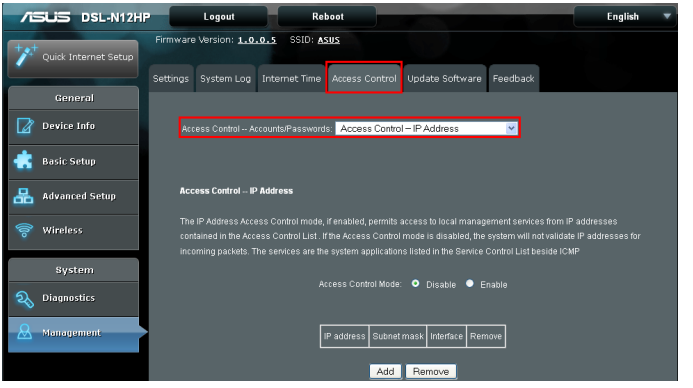


These access services available are: HTTP, SSH, TELNET, HTTPS and ICMP. Enable a service by selecting its drop-down list box. Click **Apply/Save** to activate.

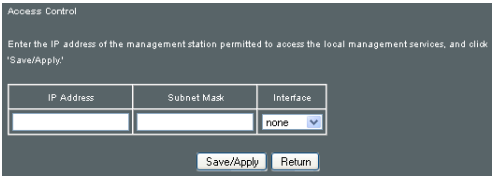
IP Address

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 beside ICMP.

Select **Access Control - IP Address** from the drop-down menu.



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



Configure the address and subnet of the management station permitted to access the local management services, and click **Save/Apply**.

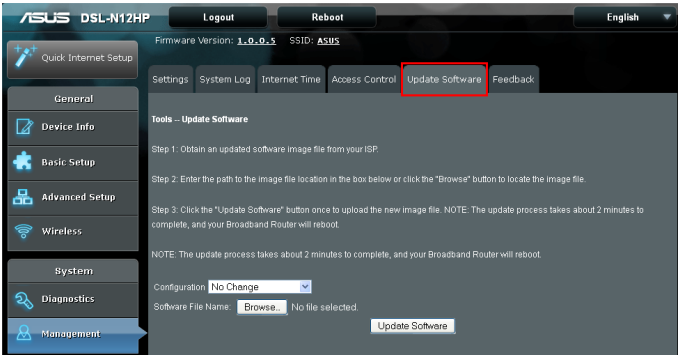
IP Address – IP address of the management station.

Subnet Mask – Subnet address for the management station.

Interface – Access permission for the specified address, allowing the address to access the local management service from none/lan/wan/lan&wan interfaces.

4.2.5 Update Software

This option allows for firmware upgrades from a locally stored file. Click the Update Software tab to display the following.



1. Obtain an updated software image file from your ISP.
2. Select the configuration from the drop-down menu.

Configuration options:

No change – upgrade software directly.

Erase current config – If the router has save_default configuration, this option will erase the current configuration and restore to save_default configuration after software upgrade.

Erase All – Router will be restored to factory default configuration after software upgrade.

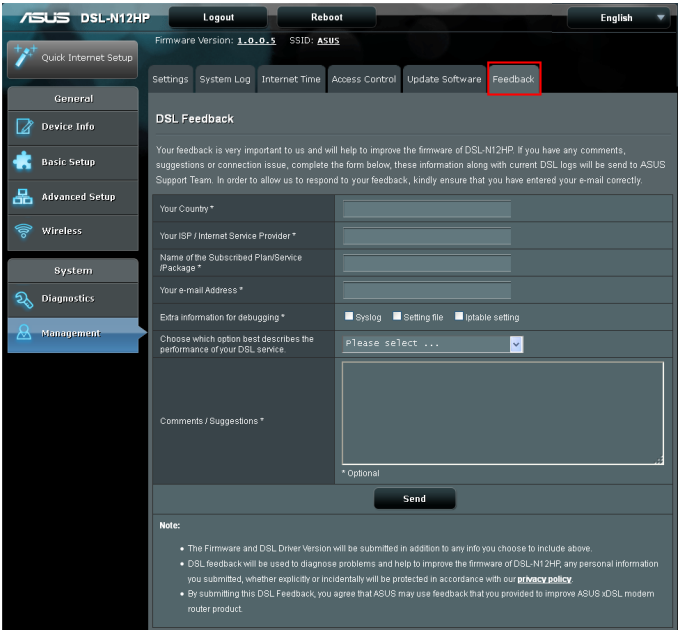
3. Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
4. Click the Update Software button once to upload and install the file.

NOTE: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the Software Version on the Device Information screen with the firmware version installed, to confirm the installation was successful.

4.2.6Feedback

Your feedback is very important to us and will help to improve the firmware of DSL-N12HP. If you have any comments, suggestions or connection issue, complete the form below, these information along with current DSL logs will be send to ASUS Support Team. In order to allow us to respond to your feedback, kindly ensure that you have entered your e-mail correctly.

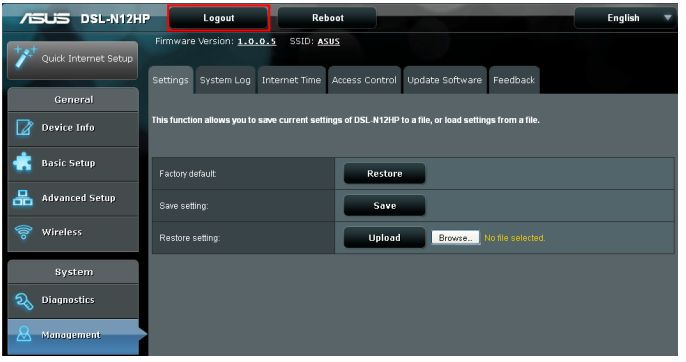
Click the Feedback tab to display the following.



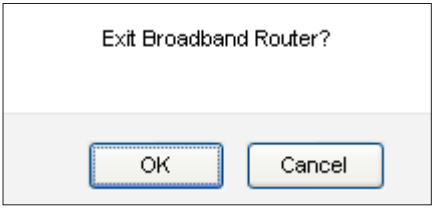
Upon completing the form, click **Send** to submit.

5 Logout & Reboot

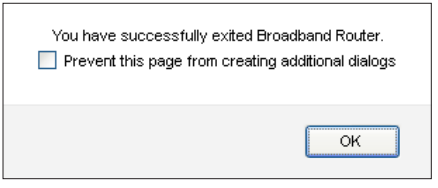
To log out from the device simply click the Logout button at the top of your screen.



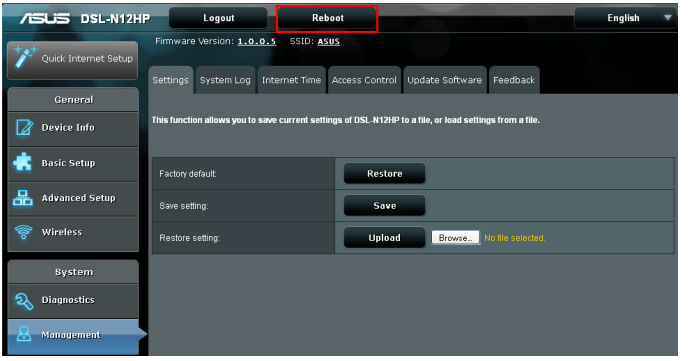
When the following window pops up, click the **OK** button to exit the router.



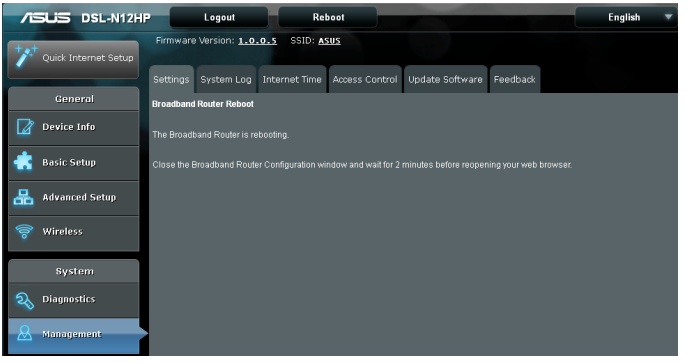
Upon successful exit, the following message will be displayed.



To reboot the device simply click the Reboot button at the top of your screen.



While rebooting, the following message will be displayed.



Appendix A - 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 device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER

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**.

OUTGOING IP FILTER

Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

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

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

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

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

INCOMING IP FILTER

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

Example 1:	Filter Name:	In_Filter1
	Protocol:	TCP
	Policy:	Allow
	Source IP Address:	210.168.219.45
	Source Subnet Mask:	255.255.0.0
	Source Port:	80
	Dest. IP Address:	NA
	Dest. Subnet Mask:	NA
	Dest. Port:	NA

	Selected WAN interface:	br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:	Filter Name:	In_Filter2
	Protocol:	UDP
	Policy:	Allow
	Source IP Address:	210.168.219.45
	Source Subnet Mask:	255.255.0.0
	Source Port:	5060:6060
	Dest. IP Address:	192.168.1.45
	Dest. Sub. Mask:	255.255.255.0
	Dest. Port:	6060:7070
	Selected WAN interface:	br0

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet 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 FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in Bridge mode. After a Bridge mode connection is created, navigate to **Advanced Setup** > **Security** > **MAC Filtering** in the Web GUI.

Example 1:	Global Policy:	Forwarded
	Protocol Type:	PPPoE
	Dest. MAC Address:	00:12:34:56:78:90
	Source MAC Address:	NA

	Src. Interface:	eth1
	Dest. Interface:	eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:	Global Policy:	Blocked
	Protocol Type:	PPPoE
	Dest. MAC Address:	00:12:34:56:78:90
	Source MAC Address:	00:34:12:78:90:56
	Src. Interface:	eth1
	Dest. Interface:	eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. 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 DSL-N12HP , as per chosen days of the week and the chosen times.

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

With this rule, a LAN device with MAC Address of 00:25:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix B - Pin Assignments

ETHERNET Ports (RJ45)

ETHERNET LAN Ports (10/100Base-T)

Table 1

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

Signals for ETHERNET WAN port (10/1001000Base-T)

Table 2

Pin	Signal name	Signal definition
1	TRD+(0)	Transmit/Receive data 0 (positive lead)
2	TRD-(0)	Transmit/Receive data 0 (negative lead)
3	TRD+(1)	Transmit/Receive data 1 (positive lead)
4	TRD+(2)	Transmit/Receive data 2 (positive lead)
5	TRD-(2)	Transmit/Receive data 2 (negative lead)
6	TRD-(1)	Transmit/Receive data 1 (negative lead)
7	TRD+(3)	Transmit/Receive data 3 (positive lead)
8	TRD-(3)	Transmit/Receive data 3 (negative lead)

DSL Port

Table 3

Pin	Signal definition
1	LINE2 TIP
2	LINE1 TIP
3	LINE1 RING
4	LINE2 RING

Appendix C – Specifications

Hardware Interface

- RJ-11 X 1 for ADSL
- RJ-45 X 4 for LAN (10/100 Base-T auto-sense)
- WPS/Wi-Fi Button X 1
- On/Off Button X 1
- Reset Button X 1
- Wi-Fi Antenna X 2

WAN Interface

- Downstream up to 12M for ADSL, 24 Mbps for ADSL2+; Upstream up to 1.3 Mbps,
- ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, Annex A/L/M

LAN Interface

- Standard IEEE 802.3, IEEE 802.3u
- Support MDI/MDX
- 10/100 Base T Auto-sense

Wireless Interface

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
- WDS/WEP/WPA/WPA2

Management

- Remote upgrade
- TFTP/FTP upgrade
- Telnet remote access support
- Support Web based configuration
- Support for backup & restore configuration to/from PC

Networking Protocols

- RFC 2684 VC-MUX, LLC/SNAP encapsulations for bridged or routed packet
- RFC 2364 PPP over AAL5
- IPoA, PPPoA, PPPoE, Multiple PPPoE sessions on single PVC, PPPoE pass-through
- PPPoE filtering of on-PPPoE packets between WAN and LAN
- Transparent bridging between all LAN and WAN interfaces
- 802.1p/802.1q VLAN support
- Spanning Tree Algorithm
- IGMP Proxy V1/V2/V3, IGMP Snooping V1/V2/V3, Fast leave
- Static route, RIP v1/v2, ARP, RARP, SNTP
- DHCP Server/Client/Relay,
- DNS Proxy/Relay, Dynamic DNS,
- UPnP IGD v1.0
- IPv6 subset

Security Functions

- PAP, CHAP, Packet and MAC address filtering, SSH
- VPN termination
- Three level login including local admin, local user and remote technical support access

QoS

- Packet level QoS classification rules,
- Priority queuing using ATM/PTM TX queues,
- IP TOS/Precedence,
- 802.1p marking,
- DiffServ DSCP marking
- Src/dest MAC addresses classification

Firewall/Filtering

- Stateful Inspection Firewall
- Stateless Packet Filter
- Denial of Service (DOS): ARP attacks, Ping attacks, Ping of Death, LAND,SYNC, Smurf, Unreachable, Teardrop
- TCP/IP/Port/interface filtering rules Support both incoming and outgoing filtering

NAT/NAPT

- Support Port Triggering and Port forwarding
- Symmetric port-overloading NAT, Full-Cone NAT
- Dynamic NAPT (NAPT N-to-1)
- Support DMZ host
- Virtual Server (Port forwarding)
- VPN Passthrough (PPTP, L2TP, IPSec)

Application Passthrough

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

NOTE: Specifications are subject to change without notice.

Appendix D - SSH Client

Unlike Microsoft Windows, Linux OS has a ssh client included. For Windows users, there is a public domain one called "putty" that can be downloaded from here: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the ssh client you must first enable SSH access for the LAN or WAN from the **Management** > **Access Control** > **Services** menu in the Web GUI.

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

For WAN access, type: ssh -l support ***WAN IP address***

To access the router using the Windows "putty" ssh client

For LAN access, type: putty -ssh -l root 192.168.1.1

For WAN access, type: putty -ssh -l support ***WAN IP address***

NOTE: The ***WAN IP address*** can be found on the Device Info > WAN screen.

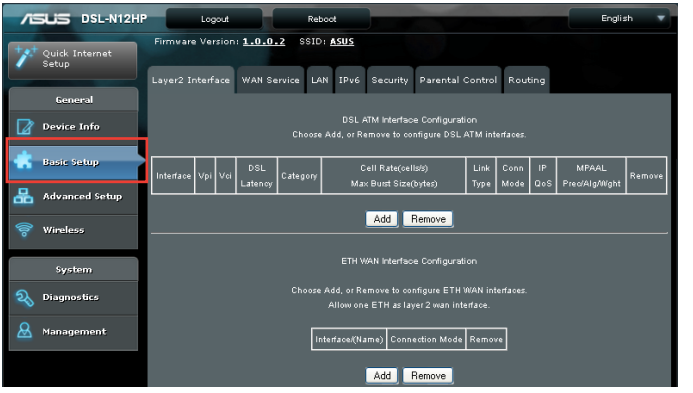
Appendix E - Connection Setup

Creating a WAN connection is a two-stage process.

1 - Setup a Layer 2 Interface (ATM or Ethernet WAN).

2 - Add a WAN connection to the Layer 2 Interface.

You can reach this page by clicking on the Basic Setup icon located on the left side of the screen.



The following sections describe each stage in turn.

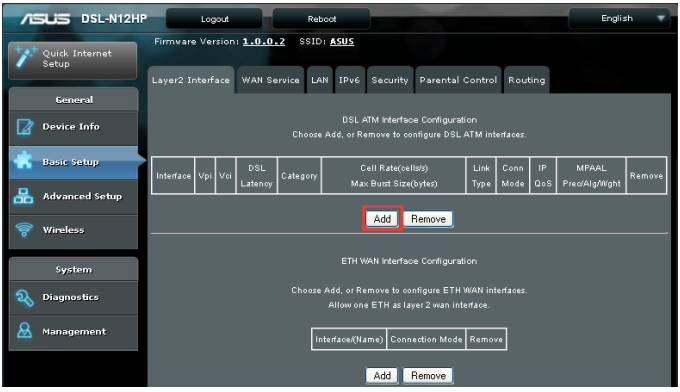
E1 Layer 2 Interfaces

Every layer2 interface operates in Multi-Service Connection (VLAN MUX) mode, which supports multiple connections over a single interface. Note that PPPoA and IPoA connection types are not supported for Ethernet WAN interfaces. After adding WAN connections to an interface, you must also create an Interface Group to connect LAN/WAN interfaces.

E1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE: The DSL-N12HP supports up to 16 ATM interfaces.



1. Click **Add** to create a new ATM interface.

NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the Remove button.

This table is provided here for ease of reference.

Field	Description
Interface	WAN interface name.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} > portID = 0 {Path1} > port ID = 1 {Path0&1} > port ID = 4
Category	ATM service category
Max Burst Size	The maximum allowable burst size of cells that can be transmitted contiguously on the VBR service connection
Link Type	Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA.
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection
IP QoS	Quality of Service (QoS) status
MPAAL	QoS Scheduler algorithm and queue weight defined for the connection
Remove	Select items for removal

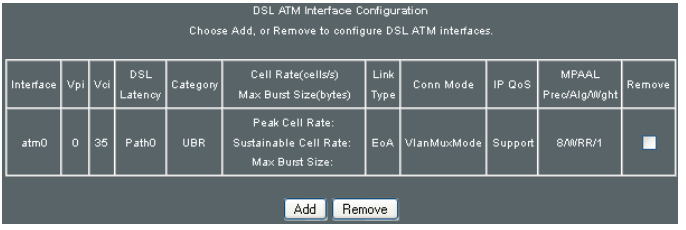
There are many settings here including: VPI/VCI, DSL Link Type, Encapsulation Mode, Service Category, Connection Mode and Quality of Service.

Here are the available encapsulations for each xDSL Link Type:

- EoA- LLC/SNAP-BRIDGING, VC/MUX
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- IPoA- LLC/SNAP-ROUTING, VC MUX

2. Click **Apply/Save** to confirm your choices.

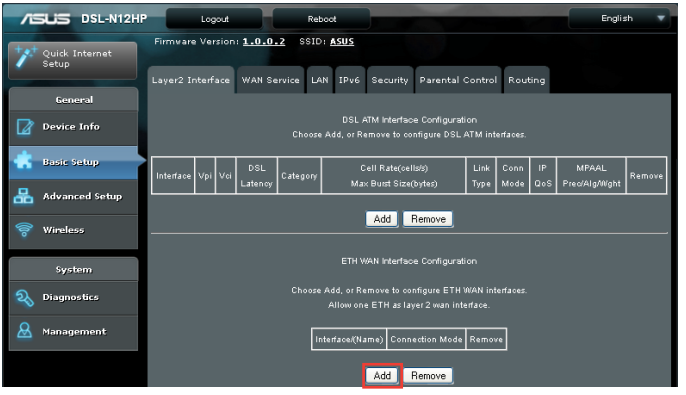
On the next screen, check that the ATM interface is added to the list. For example, an ATM interface on PVC 0/35 in Default Mode with an EoA Link type is shown below.



To add a WAN connection go to section **E2 WAN Connections**.

E1.2 ETHERNET WAN Interfaces

Follow these procedures to configure an Ethernet WAN interface.



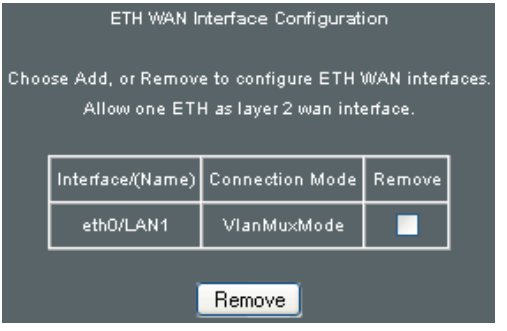
1. Click **Add** to create an Ethernet WAN interface.

This table is provided here for ease of reference.

Field	Description
Interface/ (Name)	WAN interface name.
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface.
Remove	Select interfaces to remove.

2. Select an Ethernet port and Click **Apply/Save** to confirm your choices.

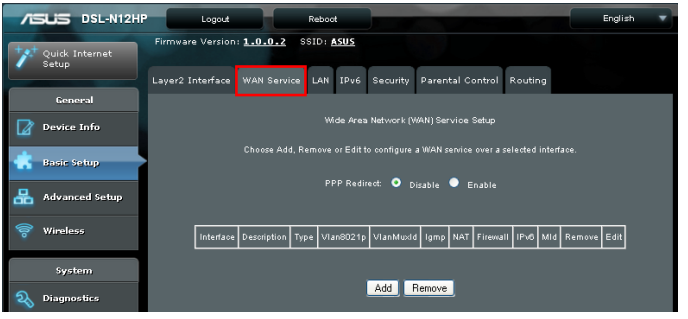
On the next screen, check that the ETHERNET interface is added to the list.



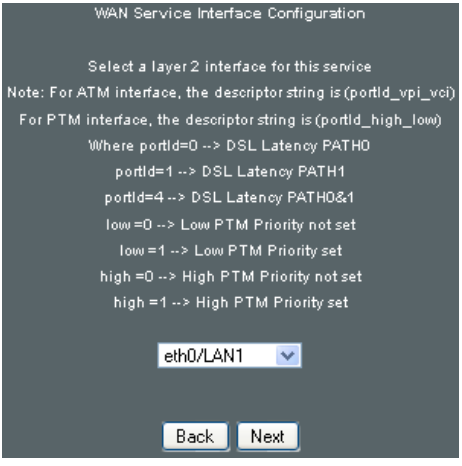
E2 WAN Connections

The DSL-N12HP supports one WAN connection for each interface, up to a maximum of 16 connections.

1. Click the **WAN Service** tab to display the following.

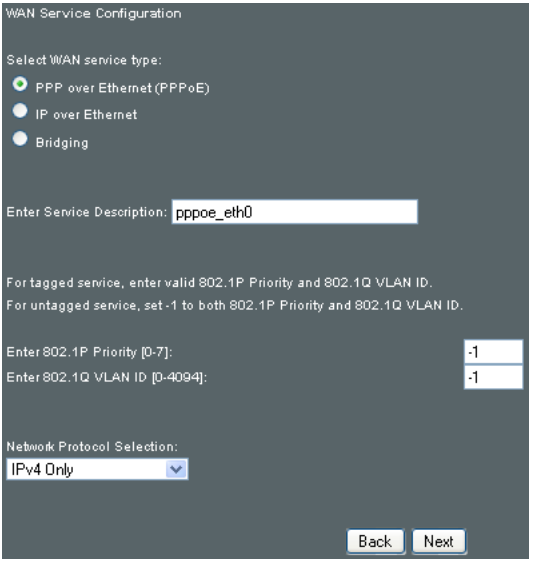


2. Click the **Add** button to create a WAN connection. The following screen will display.



3. Choose a layer 2 interface from the drop-down box and click **Next**.

   The WAN Service Configuration screen will display as shown below.



NOTE: The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the Back button and select a different layer 2 interface.

4. For VLAN Mux Connections only, you must enter Priority & VLAN ID tags.

5. You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) For PPP over ETHERNET (PPPoE), go to page 134.

(2) For IP over ETHERNET (IPoE), go to page 139.

(3) For Bridging, go to page 144.

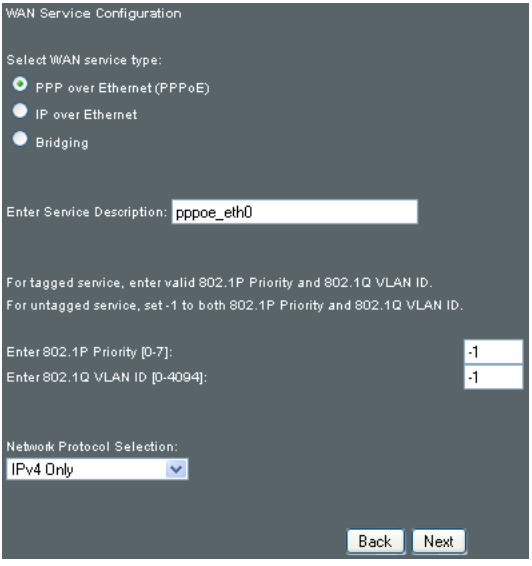
(4) For PPP over ATM (PPPoA), go to page 145.

(5) For IP over ATM (IPoA), go to page 149.

The subsections that follow continue the WAN service setup procedure.

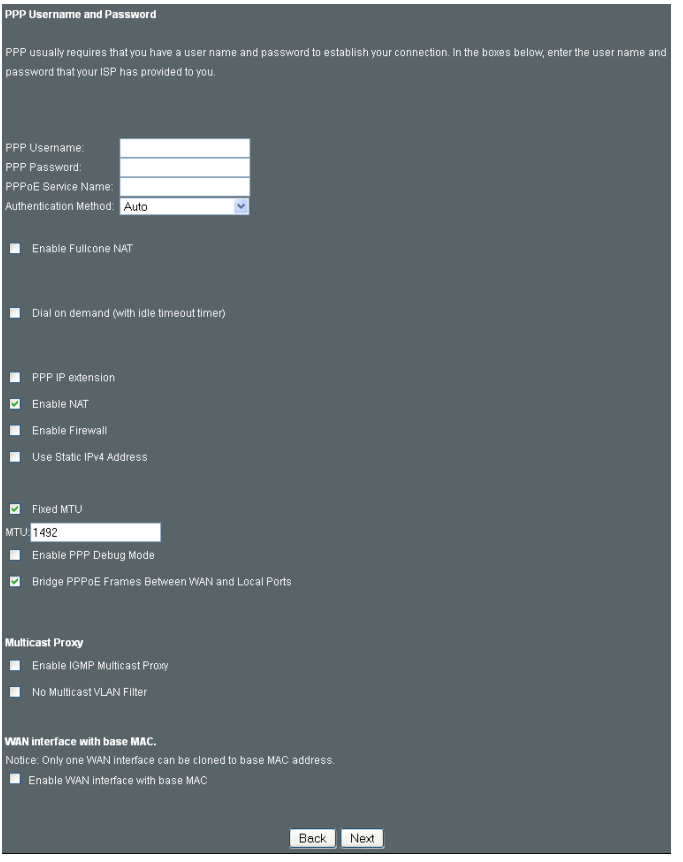
E2.1 PPP over ETHERNET (PPPoE)

1. Select the PPP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox at the bottom of this screen.



2. On the next screen, enter the PPP settings as provided by your ISP.

   Click **Next** to continue or click **Back** to return to the previous step.



The settings shown above are described below.

PPP SETTINGS

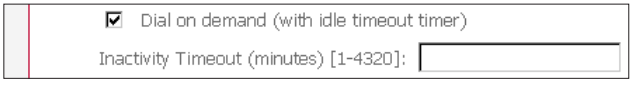
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

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.

DIAL ON DEMAND

The DSL-N12HP can be configured to disconnect if there is no activity for a period of time by selecting the Dial on demand checkbox. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



PPP IP EXTENSION

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

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- 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 device has only a single IP address to assign to a LAN device.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, 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 not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox. If selected, enter the static IP address in the **IPv4 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section **2.2 IP configuration**.

FIXED MTU

Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS

(This option is hidden when PPP IP Extension is enabled)

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running

PPPoE clients, otherwise disable it. The DSL-N12HP supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE IGMP MULTICAST PROXY

Tick the checkbox to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

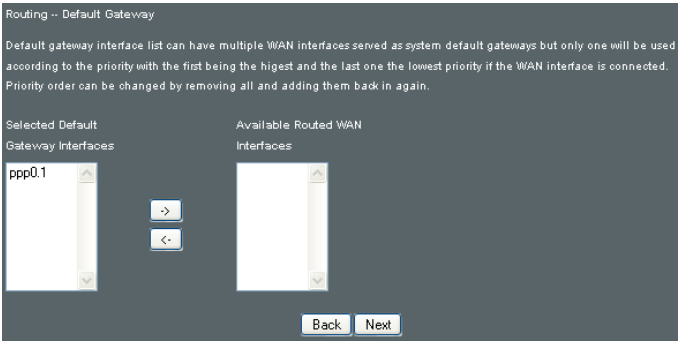
NO MULTICAST VLAN FILTER

Tick the checkbox to Enable/Disable multicast VLAN filter.

Enable WAN interface with base MAC

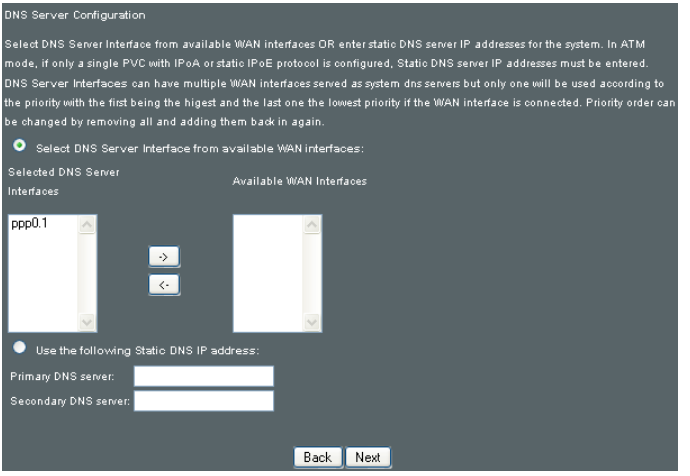
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

3. Choose an interface to be the default gateway.



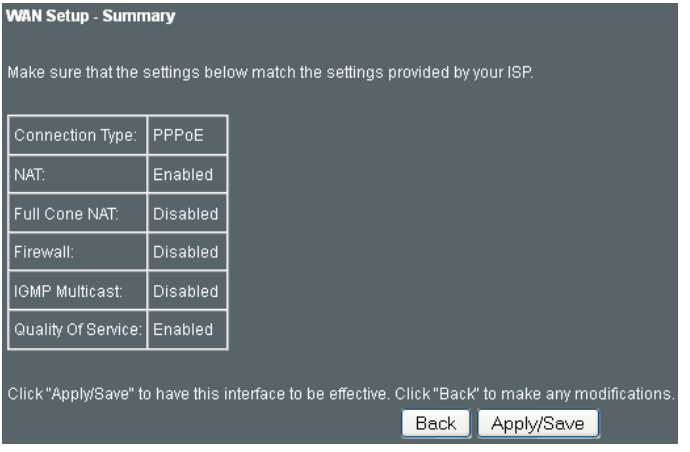
Click **Next** to continue or click **Back** to return to the previous step.

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



Click **Next** to continue or click **Back** to return to the previous step.

4. The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

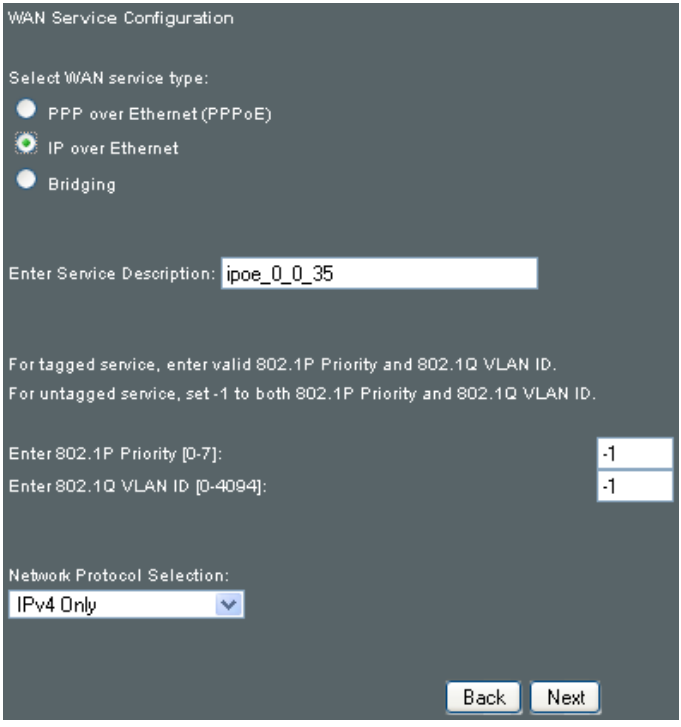


After clicking **Apply/Save**, the new service should appear on the main screen.

To activate it, you must click the **Reboot** button at the top of the screen to reboot.

E2.2 IP over ETHERNET (IPoE)

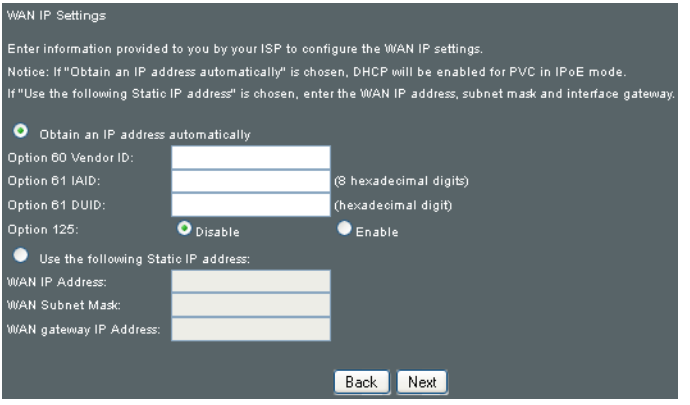
1. Select the **IP over Ethernet** radio button and click **Next**.



NOTE: For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

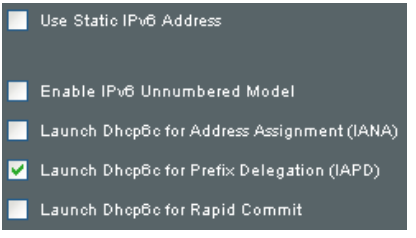
2. The WAN IP settings screen provides access to the DHCP server settings.

   You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can instead use the Static IP address method to assign WAN IP address, Subnet Mask and Default Gateway manually.



Click **Next** to continue or click **Back** to return to the previous step.

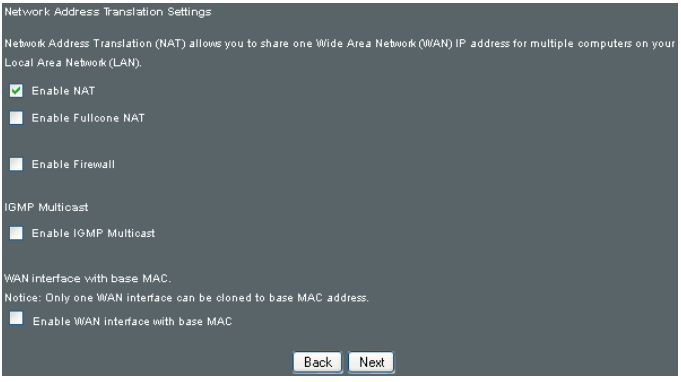
If IPv6 is enabled, the following will also be shown.



Enter information provided to you by your ISP to configure the WAN IPv6 settings.

If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

3. This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox. Click **Next** to continue or click **Back** to return to the previous step.



ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, 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 not be selected, so as to free up system resources for improved performance.

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 this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST

Tick the checkbox to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

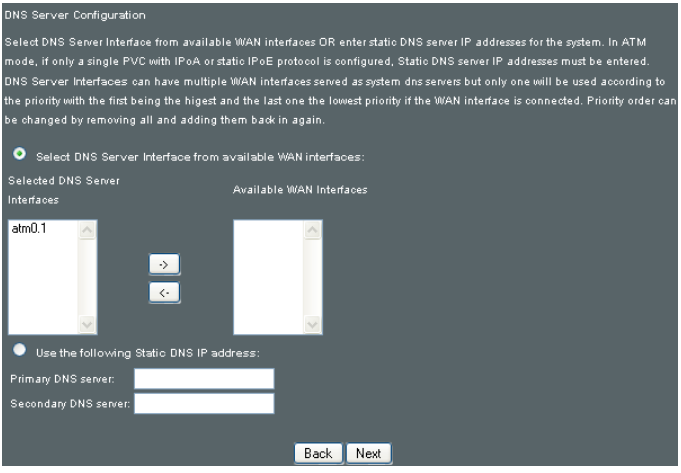
Enable WAN interface with base MAC

Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

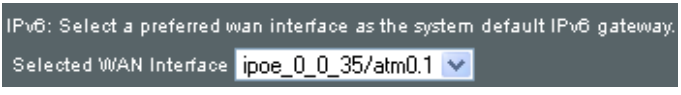
4. To choose an interface to be the default gateway.

Click **Next** to continue or click **Back** to return to the previous step.

5. Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



If IPv6 is enabled, the following will also be shown.



IPv6: Select a preferred wan interface as the system default IPv6 gateway.

Click **Next** to continue or click **Back** to return to the previous step.

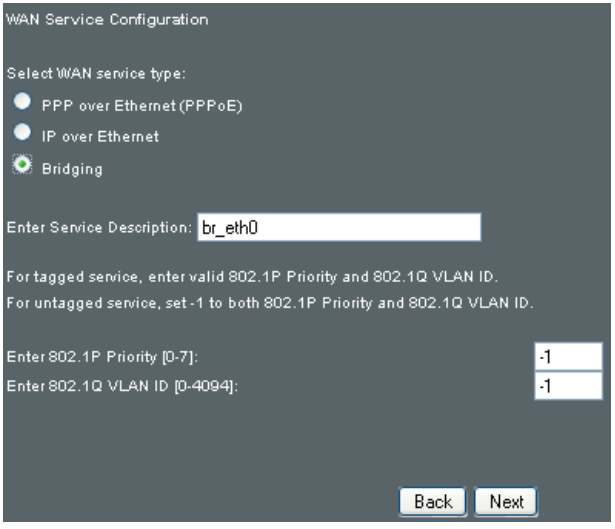
6. The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

After clicking **Apply/Save**, the new service should appear on the main screen.

To activate it, you must click the **Reboot** button at the top of the screen to reboot.

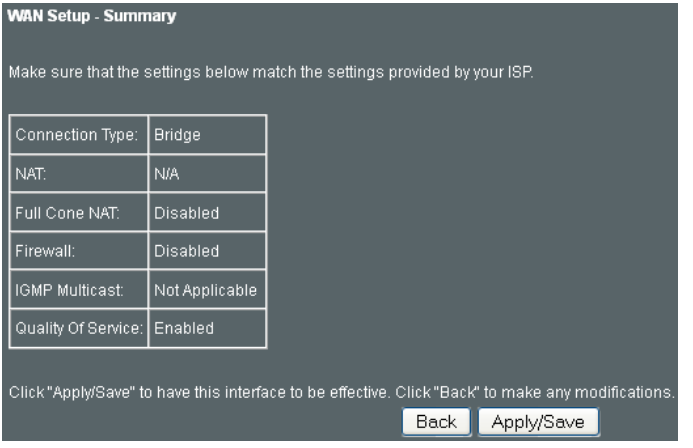
E2.3 Bridging

1. Select the **Bridging** radio button and click **Next**.



NOTE: For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

2. The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to return to the previous screen.

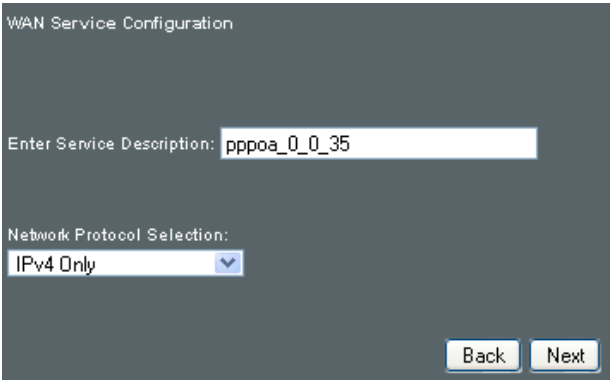


After clicking **Apply/Save**, the new service should appear on the main screen.

To activate it, you must click the **Reboot** button at the top of the screen to reboot.

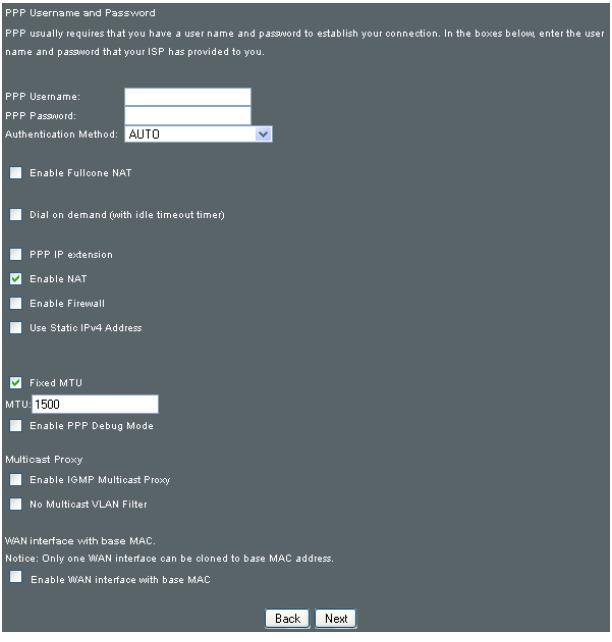
NOTE: If this bridge connection is your only WAN service, the DSL-N12HP will be inaccessible for remote management or technical support from the WAN.

E2.4 PPP over ATM (PPPoA)



1. Click **Next** to continue.
2. On the next screen, enter the PPP settings as provided by your ISP.

   Click **Next** to continue or click **Back** to return to the previous step.



PPP SETTINGS

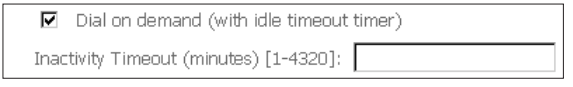
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

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.

DIAL ON DEMAND

The DSL-N12HP can be configured to disconnect if there is no activity for a period of time by selecting the Dial on demand checkbox. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



PPP IP EXTENSION

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

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN

ports, unless the packet is addressed to the device's LAN IP address.

- 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 device has only a single IP address to assign to a LAN device.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, 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 not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox. If selected, enter the static IP address in the IP Address field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in section **2.2 IP Configuration**.

Fixed MTU

Fixed Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

ENABLE IGMP MULTICAST PROXY

Tick the checkbox to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

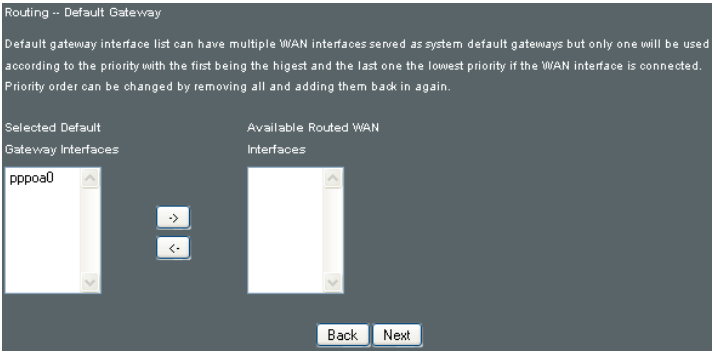
NO MULTICAST VLAN FILTER

Tick the checkbox to Enable/Disable multicast VLAN filter.

Enable WAN interface with base MAC

Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

3. Choose an interface to be the default gateway.

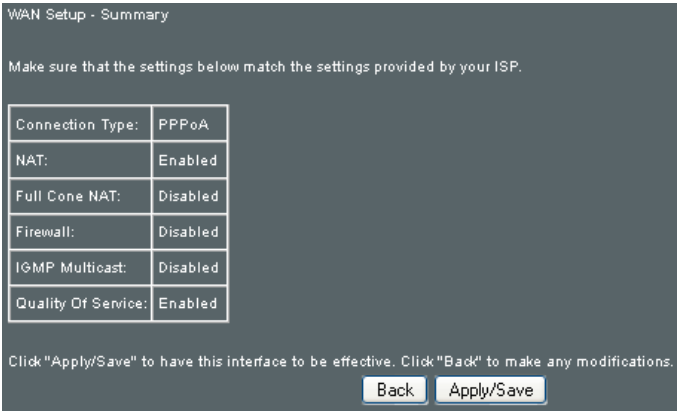


Click **Next** to continue or click **Back** to return to the previous step.

4. Choose an interface to be the default gateway.

Click **Next** to continue or click **Back** to return to the previous step.

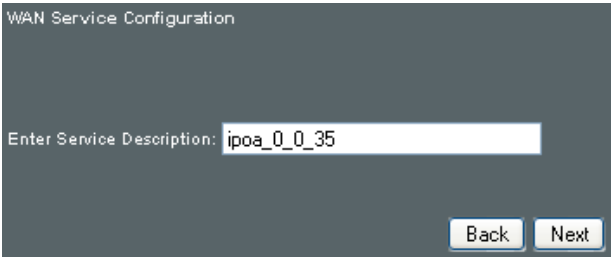
5. The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



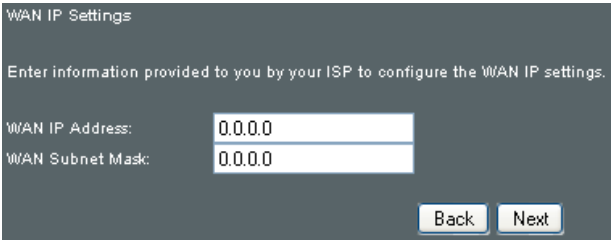
After clicking **Apply/Save**, the new service should appear on the main screen.

To activate it, you must click the **Reboot** button at the top of the screen to reboot.

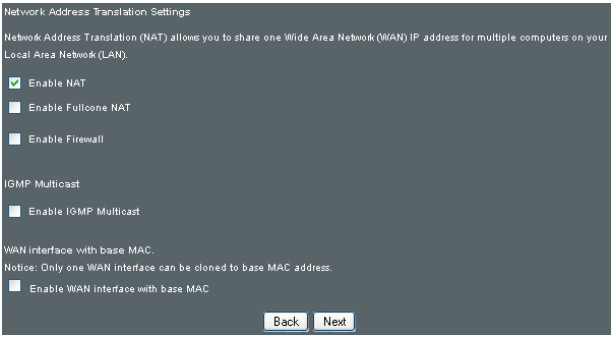
E2.5 IP over ATM (IPoA)



1. Click **Next** to continue.
2. Enter the WAN IP settings provided by your ISP. Click **Next** to continue.



3. This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox. Click **Next** to continue or click **Back** to return to the previous step.



ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, 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 not be selected, so as to free up system resources for improved performance.

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 this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox should not be selected so as to free up system resources for better performance.

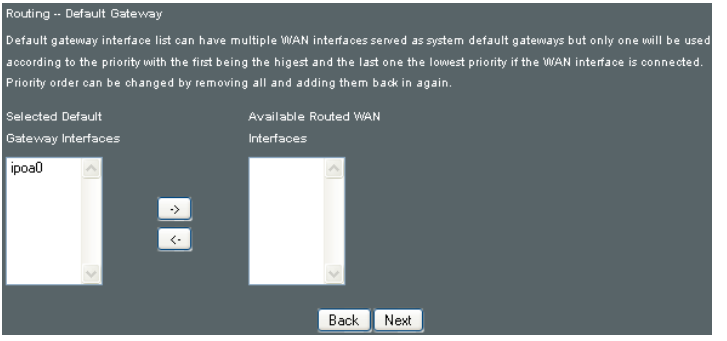
ENABLE IGMP MULTICAST

Tick the checkbox to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

Enable WAN interface with base MAC

Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

4. Choose an interface to be the default gateway.

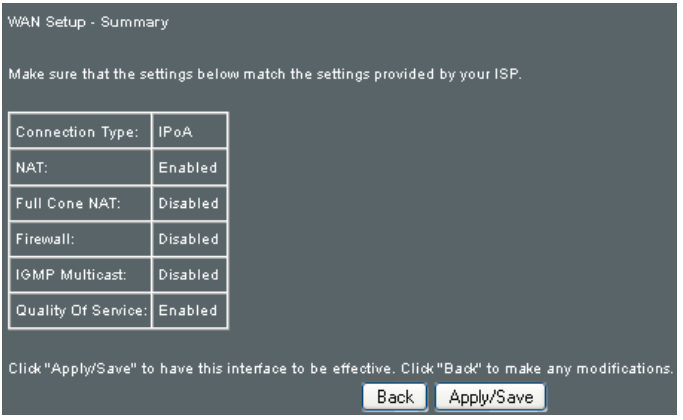


Click **Next** to continue or click **Back** to return to the previous step.

5. Choose an interface to be the default gateway.

Click **Next** to continue or click **Back** to return to the previous step.

6. The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



After clicking **Apply/Save**, the new service should appear on the main screen.

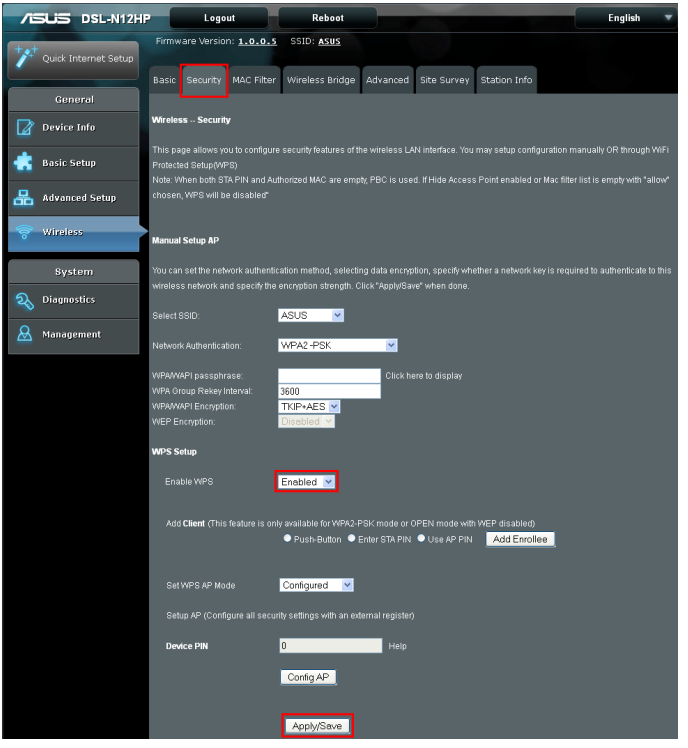
To activate it, you must click the **Reboot** button at the top of the screen to reboot.

Appendix F - WPS OPERATION

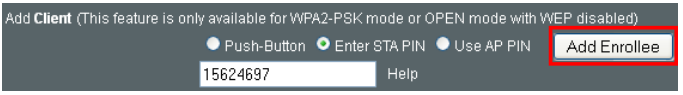
This section shows the basic AP WPS Operation procedure.

F1 Add Enrollee with Pin Method

1. Click on the Wireless tab on the left side of your screen. Then, click on the Security tab to display the following.



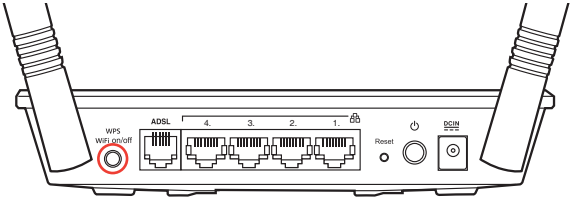
2. Select **Enabled** from the Enable WPS drop-down menu. Click the **Apply/Save** button at the bottom of the screen.



3. When the screen refreshes select the Radio button **Enter STA Pin**.
4. Input Pin from Enrollee Station (15624697 in this example)
5. Click **Add Enrollee**.
6. Operate Station to start WPS Adding Enrollee.

F2 Add Enrollee with PBC Method

1. Press the WPS/Wi-Fi button on the back panel of the router to activate WPS PBC operation.



2. Operate Station (your dongle for example) to start WPS Adding Enrollee.
3. Press more than 5 seconds to trigger WPS.

Appendix G

Notices

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to http://csr.asus.com/english/Takeback.htm for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

http://csr.asus.com/english/index.aspx

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

IMPORTANT! This device within the 5.15 ~ 5.25 GHz is restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

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

Prohibition of Co-location

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

Safety Information

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna.

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements – Article 3

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 & EN 301 893 have been conducted. These are considered relevant and sufficient.

Operate the device in 5150-5250 MHz frequency band for indoor use only.

CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Canada, Industry Canada (IC) Notices

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

The radiated output power of the ASUS Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has been evaluated for and shown compliant with the IC Specific Absorption Rate ("SAR") limits when installed in specific host products operated in portable exposure conditions (antennas are less than 20 centimeters of a person's body).

This device has been certified for use in Canada. Status of the listing in the Industry Canada's REL (Radio Equipment List) can be found at the following web address: http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng

Additional Canadian information on RF exposure also can be found at the following web: http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes

canadiennes ICES-003 et RSS-210.

Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent a ecter son fonctionnement.

NCC 警語

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. We include a copy of the GPL with every CD shipped with our product. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The

act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute

the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to

be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide

range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

For Turkey only

Authorised distributors in Turkey:

BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.

Tel. No.: +90 212 3311000

Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10 AYAZAGA/ISTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.

Tel. No.: +90 212 3567070

Address: CEMAL SURURI CD. HALIM MERIC IS MERKEZI No: 15/C D:5-6 34394 MECIDIYEKOY/ ISTANBUL

KOYUNCU ELEKTRONiK BiLGi iSLEM SiST. SAN. VE DIS TIC. A.S.

Tel. No.: +90 216 5288888

Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZi, SANCAKTEPE ISTANBUL

AEEE Yönetmeliğine Uygundur.

ASUS Contact Information

ASUSTeK COMPUTER INC. (Asia Pacific)

Address	15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Website	www.asus.com.tw

Technical Support

Telephone	+886228943447
Support Fax	+886228907698
Online support	support.asus.com

ASUS COMPUTER INTERNATIONAL (America)

Address	800 Corporate Way, Fremont, CA 94539, USA
Telephone	+15107393777
Fax	+15106084555
Website	usa.asus.com
Online support	support.asus.com

ASUS COMPUTER GmbH (Germany and Austria)

Address	Harkort Str. 21-23, D-40880 Ratingen, Germany
Support Fax	+49-2102-959931
Website	asus.com/de
Online contact	eu-rma.asus.com/sales

Technical Support

Telephone (Component)	+49-2102-5789555
Telephone Germany (System/Notebook/Eee/LCD)	+49-2102-5789557
Telephone Austria (System/Notebook/Eee/LCD)	+43-820-240513
Support Fax	+49-2102-959911
Online support	support.asus.com

Networks Global Hotline Information

Region	Country	Hotline Number	Service Hours
Europe	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri
	France	0033-170949400	09:00-18:00 Mon-Fri
	Germany	0049-1805010920 0049-1805010923 (component support) 0049-2102959911 (Fax)	09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
	Hungary	0036-15054561	09:00-17:30 Mon-Fri
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Austria	0043-820240513	09:00-18:00 Mon-Fri
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri
	Belgium	0032-78150231	09:00-17:00 Mon-Fri
	Norway	0047-2316-2682	09:00-18:00 Mon-Fri
	Sweden	0046-858769407	09:00-18:00 Mon-Fri
	Finland	00358-969379690	10:00-19:00 Mon-Fri
	Denmark	0045-38322943	09:00-18:00 Mon-Fri
	Poland	0048-225718040	08:30-17:30 Mon-Fri
	Spain	0034-902889688	09:00-18:00 Mon-Fri
	Portugal	00351-707500310	09:00-18:00 Mon-Fri
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri
	Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri
	Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri
	Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri
	United Kingdom	0044-1442265548	09:00-17:00 Mon-Fri
	Ireland	0035-31890719918	09:00-17:00 Mon-Fri
	Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri
	Ukraine	0038-0445457727	09:00-18:00 Mon-Fri

Networks Global Hotline Information

Region	Country	Hotline Numbers	Service Hours
Asia-Pacific	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
		0081-570783886 (Non-Toll Free)	09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717 1800-8525201	09:00-18:00 Mon-Fri
	Singapore	0065-64157917	11:00-19:00 Mon-Fri
		0065-67203835	11:00-19:00 Mon-Fri
		(Repair Status Only)	11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India India(WL/NW)	1800-2090365	09:00-18:00 Mon-Sat 09:00-21:00 Mon-Sun
	Indonesia	0062-2129495000 500128 (Local Only)	09:30-17:00 Mon-Fri 9:30 – 12:00 Sat
	Vietnam	1900-555581	08:00-12:00 13:30-17:30 Mon-Sat
	Hong Kong	00852-35824770	10:00-19:00 Mon-Sat
Americas	USA Canada	1-812-282-2787	8:30-12:00 EST Mon-Fri 9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri 08:00-15:00 CST Sat

Networks Global Hotline Information

Region	Country	Hotline Numbers	Service Hours
Middle East + Africa	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
	UAE	00971-42958941	09:00-18:00 Sun-Thu
	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800	08:00-17:00 Sun-Thu
		*9770/00972-35598555	08:30-17:30 Sun-Thu
Balkan Countries	Romania	0040-213301786	09:00-18:30 Mon-Fri
	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
	Bulgaria	00359-70014411	09:30-18:30 Mon-Fri
		00359-29889170	09:30-18:00 Mon-Fri
	Croatia	00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
	Slovenia	00368-59045400 00368-59045401	08:00-16:00 Mon-Fri
	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

NOTE: For more information, visit the ASUS support site at:
http://support.asus.com

Manufacturer:	**ASUSTeK Computer Inc.**	
	Tel:	+886-2-2894-3447
	Address:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Authorised representative in Europe:	**ASUS Computer GmbH**	
	Address:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY