

Communicate via *Micro network*



Micronet[®]
Making Communication Easier

User's Manual

11N ADSL2+ Modem Router

Model No.: SP3367NL



Table of Contents

1.	Introduction.....	2
1.1	Package Contents.....	2
1.2	Key Features.....	2
1.3	Safety Information.....	3
2.	Physical Description.....	5
2.1	Back Panel.....	5
2.2	Front Panel.....	6
2.3	Hardware Connection.....	7
3.	System and Network Setup.....	8
3.1	Build Network Connection.....	8
3.2	Connecting to Web-Based Management.....	9
3.3	Router' s IP Address.....	13
4.	Web-Based Management UI.....	16
4.1	Fast internet access.....	16
4.2	Wireless.....	20
4.3	Advanced Setup.....	28
5.	Management.....	70
5.1	System log.....	70
5.2	SNMP Agent.....	71
5.3	TR-069 client.....	72
5.4	Internet Time.....	74
5.5	Access Control.....	75
5.6	Backup.....	76
5.7	Update.....	77
5.8	Restore default.....	77
5.9	Update Software.....	79
5.10	Reboot.....	79

Certifications

FCC

This equipment has been tested and found to comply with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received. Include interference that may cause undesired operation.

CE

This equipment is in compliance with the requirements of the following regulations: EN 55022: CLASS B.

RoHS

All contents of this package, including products, packing materials and documentation comply with RoHS.



1. Introduction

Micronet SP3367NL/SP3367NE, 11N ADSL2+ Modem Router, delivers highly reliable and scalable network environment. The model has incorporated both modem and router functions into a single unit with wireless support. It is compliant with IEEE 802.11 N and backward compatible with IEEE 802.11b/g. The wireless connection can be optimized up to high-speed data rate of 300Mbps for multimedia applications. The modem router allows multiple network devices to share the single Internet connection via ADSL. Sustain network security via router's in-built firewall and DMZ functions.

1.1 Package Contents

Prior to the installation of the device, please verify the following items are in the package:

- 1 x 11N ADSL2+ Modem Router
- 1 x Quick Installation Guide
- 1 x Product CD
- 1 x Voice Splitter
- 1 x Power Adapter

1.2 Key Features

- ADSL2/2+ Compliance
 - Support downstream rates of up to 24Mbps and upstream rates of up to 1Mbps.
 - Compliant to ITU-T G.992.1 (G.dmt), G.992.2 (G.lite), G.992.3 (ADSL2), G.992.4 (splitterless ADSL2), G.992.5 (ADSL2+) for Annex A, B. (Annex A and B are supported in different H/W platform)
 - Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.994.1 and G.996.1 (for ISDN only); G.991.1;G.lite (G992.2)).
 - Multiple Protocols over AAL5 (RFC 1483/2684).
 - PPP over AAL5 (RFC 2364).

- PPP over Ethernet (RFC 2516).
- Support 802.11n Wireless Access Point
 - Complies with IEEE 802.11n, IEEE 802.11g and IEEE 802.11b standards.
 - Farther coverage, less dead spaces and higher throughput with MIMO technology.
 - High data rate – up to 300Mbps network speed.
 - Supports 64-bit/128-bit WEP, WPA-PSK and WPA2-PSK wireless security functions.
 - Supports WPS (WiFi Protected Setup) to easy connect wireless network without configuring the security.
 - Support Auto Channel Selection.
 - Supports MAC address filtering.
 - Supports WDS
- Router Advance Functions
 - NAT (Network Address Translation) IP Sharing
 - Virtual Server
 - DMZ
 - SPI Anti-DOS Firewall
 - DHCP Server and Client
 - ACL (Access Control)
 - IP/MAC/Application/URL Filter
 - UPnP (Universal Plug and Play)
 - Dynamic DNS

1.3 Safety Information

In order to keep the safety of users, please follow the following safety instructions:

- This router is designed for indoor use only.
- Do not put this router at or near hot or humid places. Also, do not leave this router in the car in summer.
- Do not pull any connected cable with force and disconnect it from the router.

- If users want to place this router at high places, please make sure the router is firmly secured. Falling from high places would damage the router and its accessories, and in such cases, the warranty will be void.
- Accessories of this router, like antenna and power supply, are danger to small children under 3 years old. They may put the small parts in their nose or month and it could cause serious damage to them.
- The router will become hot when being used for long time (This is normal and is not a malfunction). Do not put this router on paper, cloth or other flammable materials.
- There's no user-serviceable part inside the router. If users found the router is not working properly, please contact the authorized dealer of purchase. Do not disassemble the router, otherwise warranty will be void.
- If the router falls into water when it's powered on, do not use hands to pick it up. Switch the electrical power off before doing anything, or contact an experienced technician for help.
- If users smell something strange, or even see some smoke coming out from the router or power supply, remove the power supply or switch the electrical power off immediately, and call authorized for help.

2. Physical Description

2.1 Back Panel



Parameter	Description
ON/OFF	Power Switch. Press it in to turn on the power and press it out to turn off the power.
WPS/Reset	Hold and press it for 1 seconds to connect WPS, and 7 seconds to bring all settings back to factory defaults.
Power Jack	Please plug the power adapter attached with the ADSL Router to the power jack. The power adapter is 9VDC, 1A.
LAN	LAN network cable interface. It is used to connect Hub, Switch, or computer in a LAN. (LAN2 port can also be used to connect IPTV Set-top box to enable watching TV and online surfing at the same time. When the access way is changed into community broadband, LAN4 can be used as the wireless Router's WAN port.)
ADSL	Connect the supplied RJ-11 telephone line to this port and your ADSL/telephone network.

Note:

Please use the supplied power adapter, for use of an unmatched power adapter may damage the device.

2.2 Front Panel

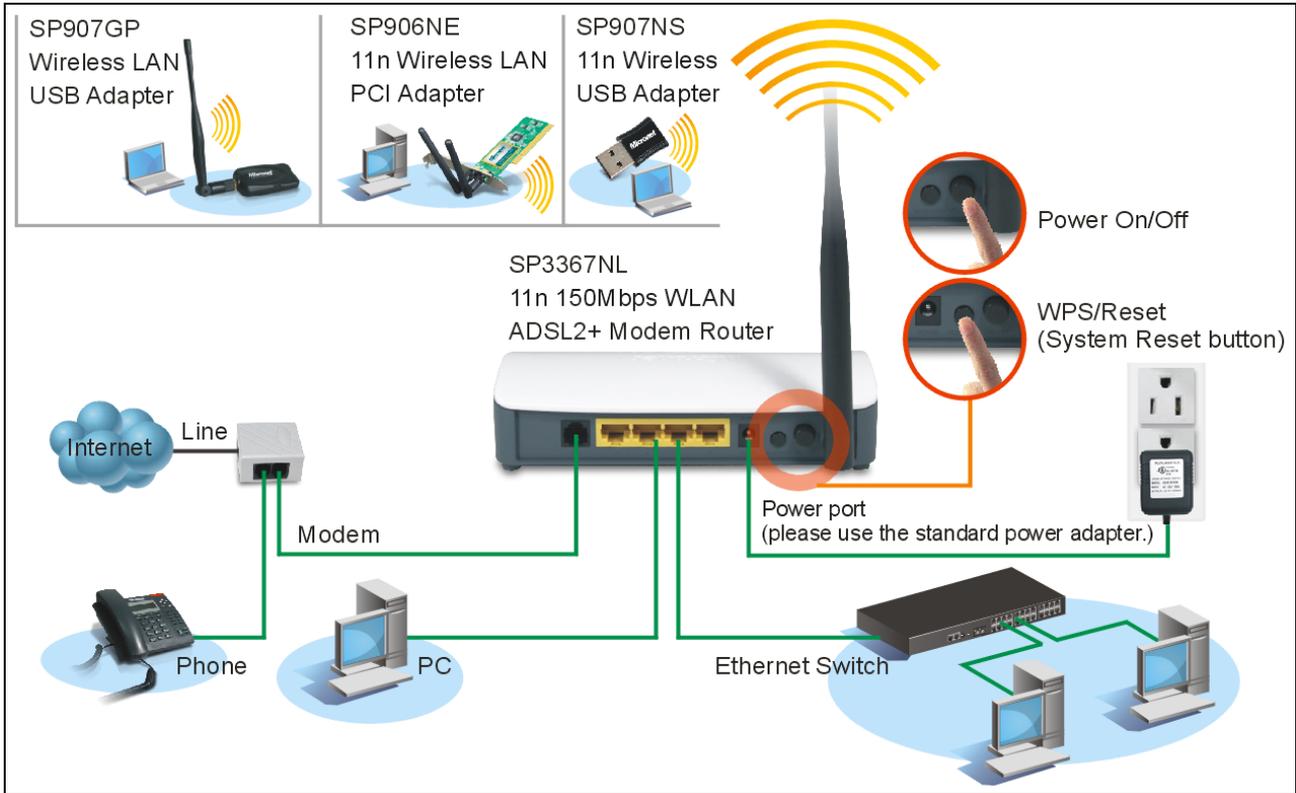


LED	Color	Status	Description
Power	Green	Always On	The device has power
		OFF	The device has no power or power adapter is damaged
SYS	Green	Always On	Connected to Internet
		Flashing	Packets are being transferred through ADSL Link
WLAN	Green	Flashing	Packets are being transferred
		Off	Wireless is disabled
ADSL	Green	Slow Flashing	ADSL Link has not been established
		Fast Flashing	ADSL Link is being established
		Always On	ADSL Link has already been established
LAN 1/2/3/4	Green	Off	Unconnected
		Flashing	Packets are being transferred

		Always On	The router has been connected to the computer
WPS	Green	ON	Terminal WPS is successfully connected and the LED lights off in 5 minutes
		Flashing	WLAN terminal is connecting WPS
		Off	No WLAN terminal WPS connection is present or terminal WPS connection exceeds 5 minutes

2.3 Hardware Connection

Follow the diagram below to connect your network devices when using DSL uplink access mode (through telephone line).

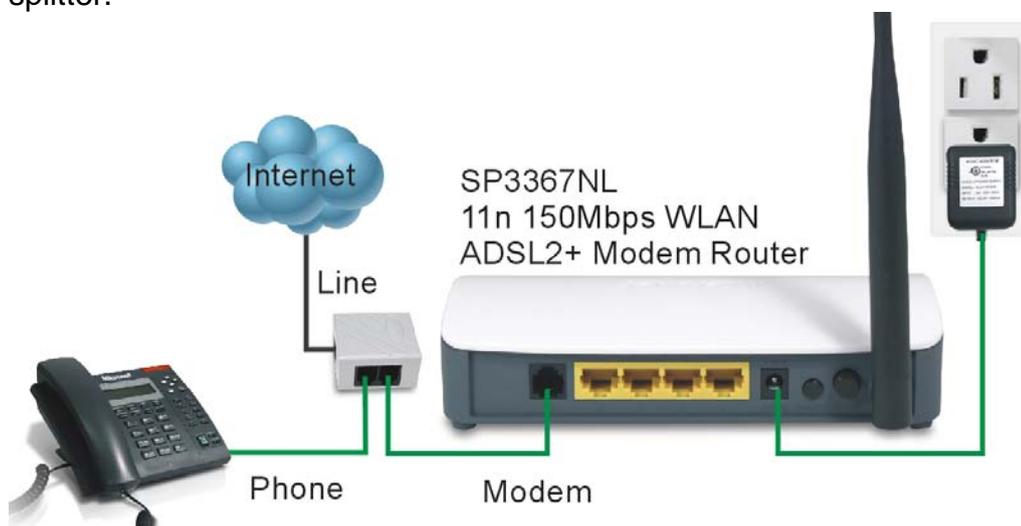


3. System and Network Setup

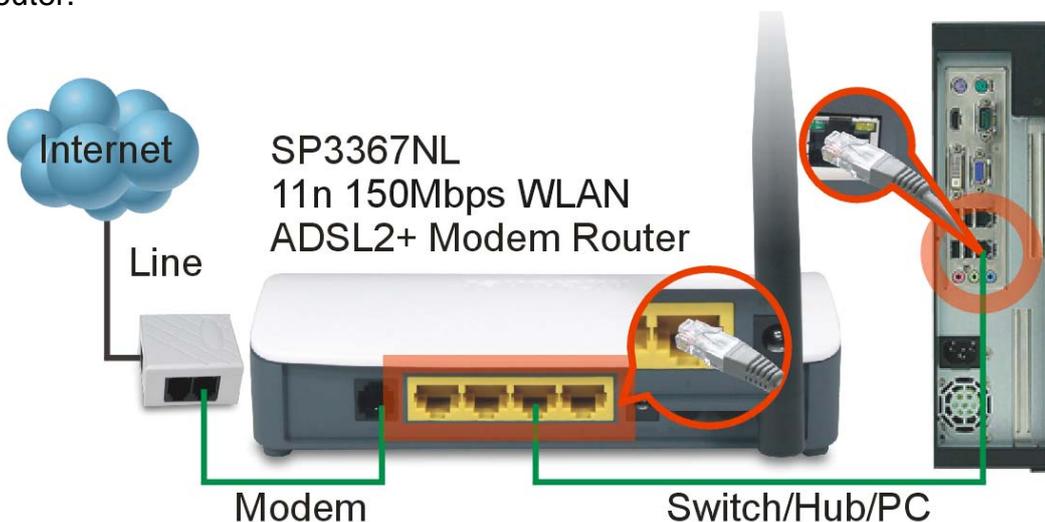
3.1 Build Network Connection

Please follow the following instruction to build the network connection between the new wireless router and other network computers and devices:

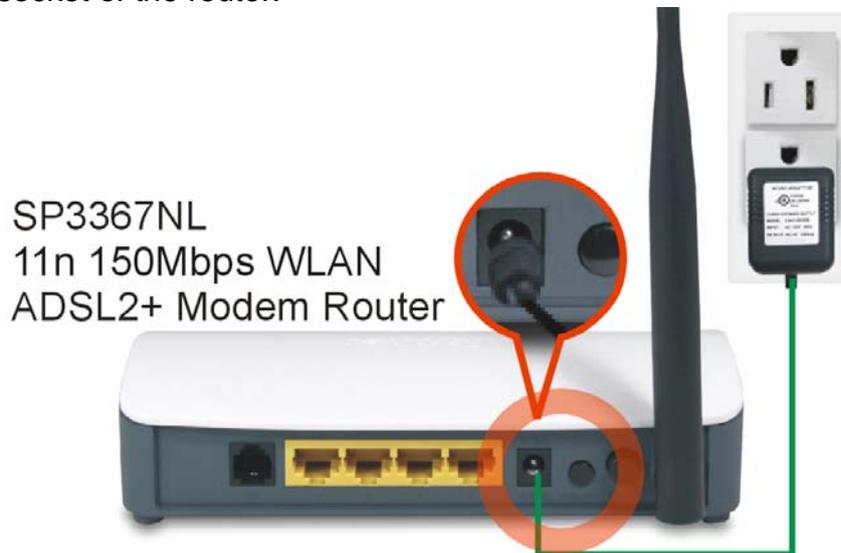
1. Connect the ADSL port of modem router by telephone cable (RJ-11) to an outlet or splitter.



2. Connect all computers, network devices (network-enabled consumer devices other than computers, like game console, or switch / hub) to the LAN port of the router.



3. Connect the A/C power adapter to the wall socket, and then connect it to the 'Power' socket of the router.



4. The ADSL LED will be ON if the router is connected to the ADSL cable and receives the ADSL signals successfully. If the LED is blinking, please contact with your ISP (Internet Service Provider) to check the problem.

3.2 Connecting to Web-Based Management

After the network connection is established, the next step is to setup the router with proper network parameters for the user's network environment.

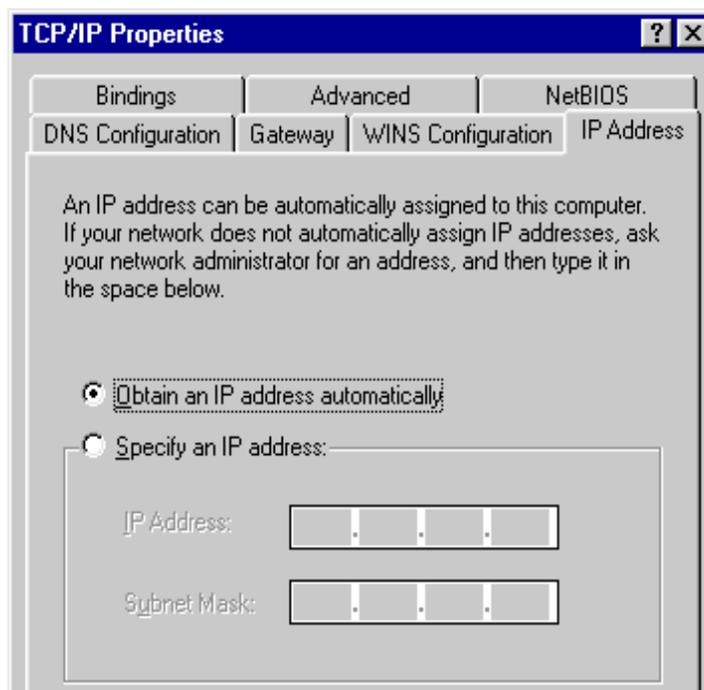
Before connecting to the router and start configuration procedures, user's computer must be able to get an IP address automatically (use dynamic IP address). If the PC is set to 'static IP address', then follow instructions below to reconfigure it to 'dynamic IP address'.

IP Address Configuration

a) Windows 95/98/Me

1. Click the Start button and select **<Settings>**, then click **<Control Panel>**. The Control Panel window will appear.
2. Double-click on **<Network>** icon. The Network window will appear.

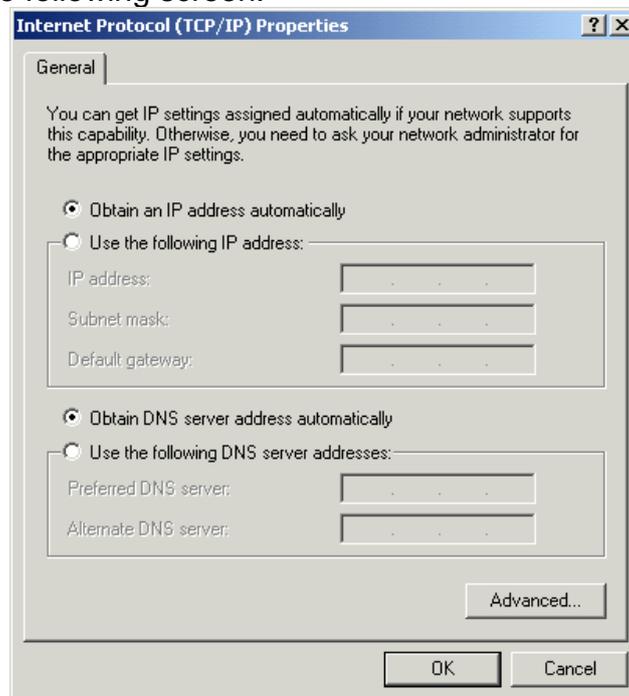
3. Check the list of Network Components. If TCP/IP is not installed, click the **<Add>** button to install it. If TCP/IP is installed, go to step 6.
4. In the Network Component Type dialog box, select **<Protocol>** and click **<Add>** button.
5. In the Select Network Protocol dialog box, select **<Microsoft>** and **<TCP/IP>** then click the **<OK>** button to start installing the TCP/IP protocol. Windows CD may be needed to complete the installation.
6. After installing TCP/IP, go back to the Network dialog box. Select **<TCP/IP>** from the list of Network Components and then click the **<Properties>** button.
7. Check each of the tabs and verify the following settings:
 - Bindings: Check Client for Microsoft Networks and File and printer sharing for Microsoft Networks.
 - Gateway: All fields are blank.
 - DNS Configuration: Select Disable DNS.
 - WINS Configuration: Select Disable WINS Resolution.
 - IP Address: Select Obtain IP address automatically.



8. Reboot the PC. PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
9. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.
10. Proceed to Web-based User Interface once IP address is correctly configured.

b) Windows 2000

1. Click the **<Start>** button and select **<Settings>**, then click **<Control Panel>**. The Control Panel window will appear.
2. Double-click **<Network and Dial-up Connections>** icon. In the Network and Dial-up Connection window, double-click on **<Local Area Connection>** icon. The Local Area Connection window will appear.
3. In the Local Area Connection window, click the **<Properties>** button.
4. Check the list of Network Components. Users should see Internet Protocol [TCP/IP] on the list. Select it and click the **<Properties>** button.
5. In the Internet Protocol (TCP/IP) Properties window, select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>** as shown on the following screen.

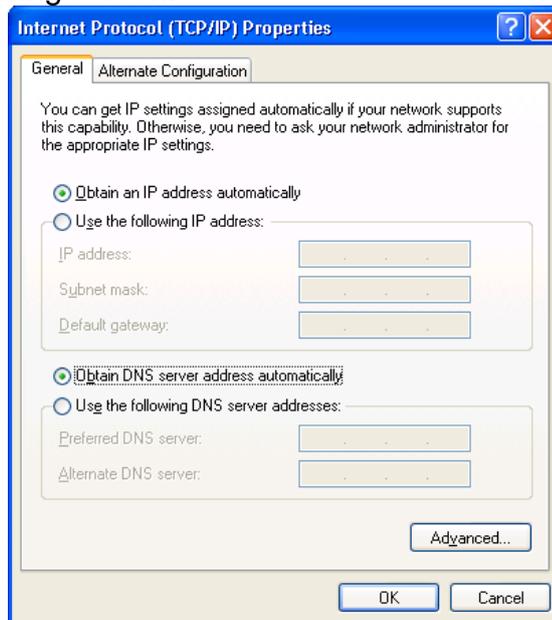


6. Click **<OK>** to confirm the setting. The PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
7. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.
8. Proceed to Web-based User Interface once IP address is correctly configured.

c) Windows XP

1. Click the **<Start>** button and select **<Settings>**, then click **<Network Connections>**. The Network connections window will appear.

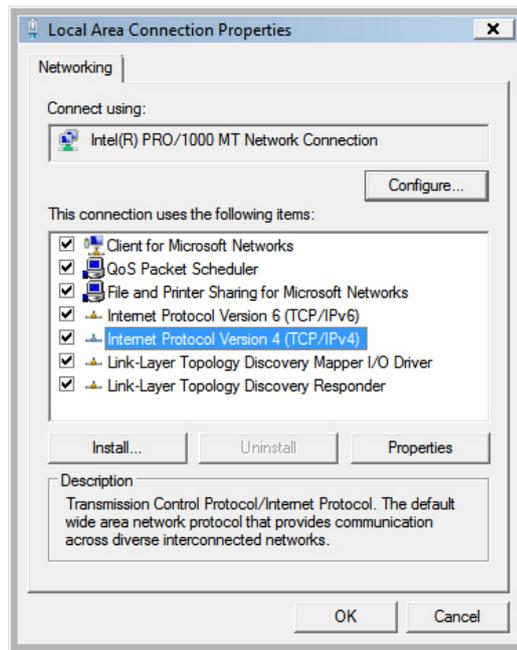
2. Double-click **<Local Area Connection>** icon. The Local Area Connection window will appear.
3. Check the list of Network Components. Users should see Internet Protocol [TCP/IP] on the list. Select it and click the **<Properties>** button.
4. In the Internet Protocol (TCP/IP) Properties window, select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>** as shown on the following screen.



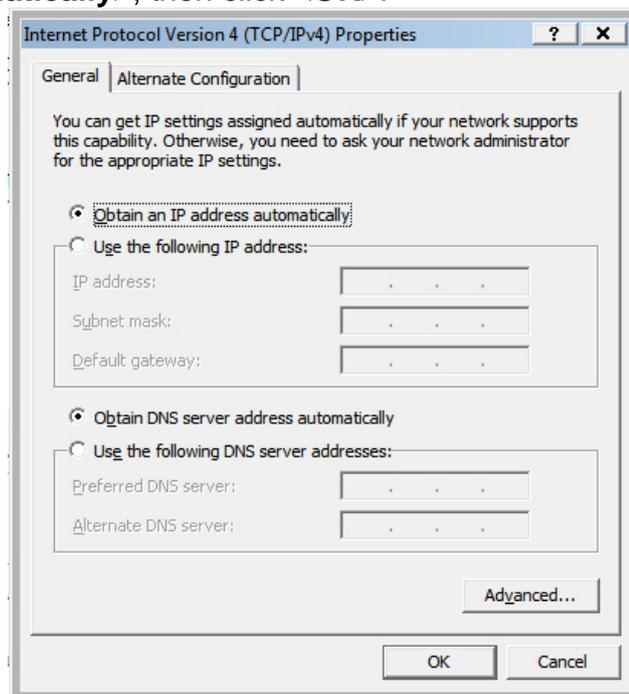
5. Click **<OK>** to confirm the setting. PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
6. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.

d) Windows Vista

1. Click **<Start>** button, then click control panel. Click **<View Network Status and Tasks>**, then click **<Manage Network Connections>**. Right-click **<Local Area Network>**, then select **<Properties>**. Local Area Connection Properties window will appear, select **<Internet Protocol Version 4 (TCP / IPv4)>** and click **<Properties>**.



2. Select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>**, then click **<OK>**.

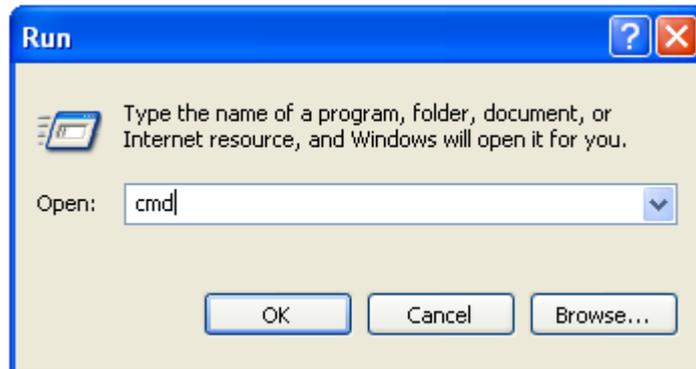


3.3 Router's IP Address

1. After the IP address setup is complete, please click **<Start>** then **<Run>** at the bottom lower corner of the desktop.



2. Enter 'cmd' command and click <OK>.



3. Input 'ipconfig', then press 'Enter' key. Please check the IP address followed by 'Default Gateway' (In this example, the IP address of router is 192.168.1.1, please note that this value may be different).

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

4. Web-Based Management UI

4.1 Fast internet access

In previous section, we have explained how to log on to the router and in the following; we are going to illustrate how to configure the router quickly to let your PC access Internet.

Micronet SP3367NL

11n 150Mbps WLAN ADSL2+ Modem Router

Version No.:Ver1.0

[Advanced Settings](#)



 Line connected

Status

Connect Status : **Disconnect**

Network

VPI/VCI Settings: (VPI/VCI:0/35)

PPPOE User Name:

PPPOE Password:

Wireless

Key:

Password:

Now check whether you have the screen below, if not, please re-log on to the router's management interface.

Micronet SP3367NL

11n 150Mbps WLAN ADSL2+ Modem Router

Version No.:Ver1.0

[Advanced Settings](#)



 Line connected

Status

Connect Status : **Disconnect**

Network

VPI/VCI Settings: (VPI/VCI:0/35)

PPPOE User Name:

PPPOE Password:

Wireless

Key:

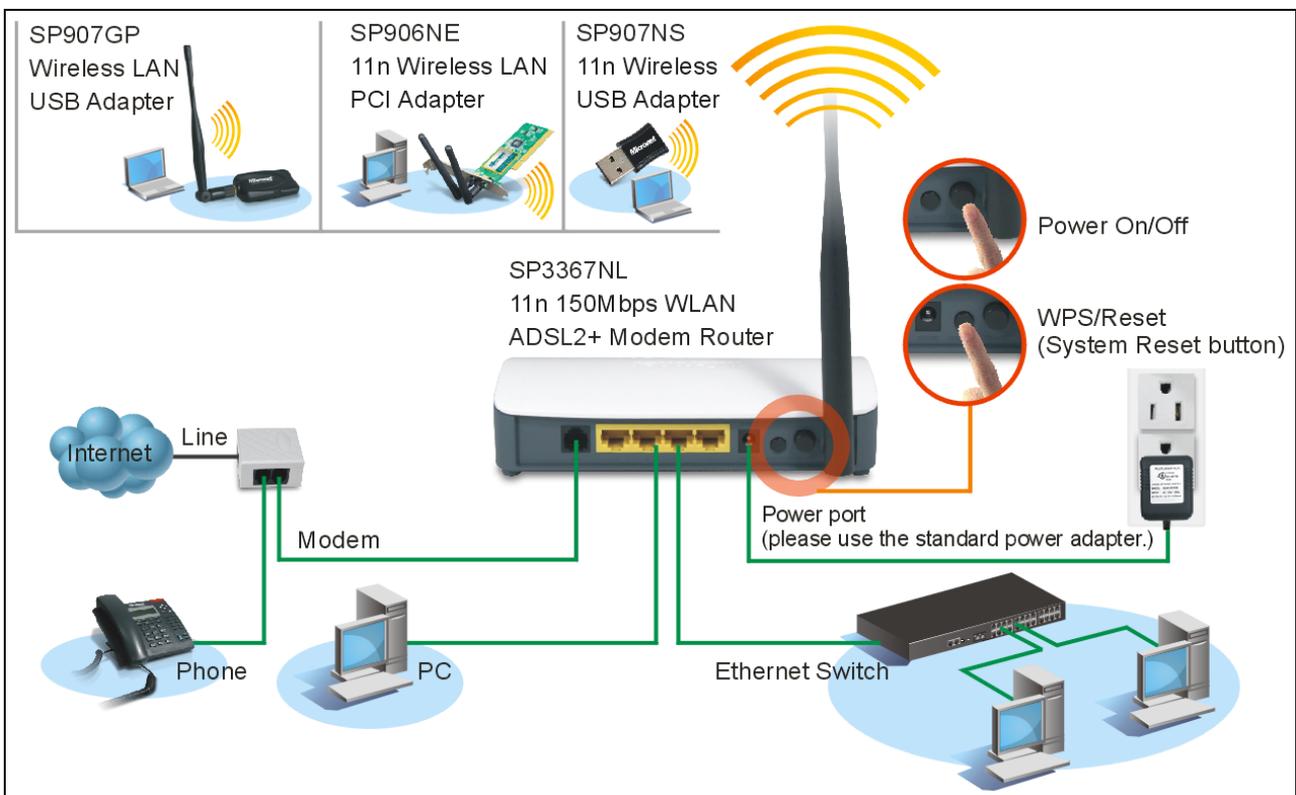
Password:

Have you noticed the option of “ Network” ----“ Access Mode” . There are two modes available:

DSL Uplink: Select this mode, if you are using a telephone line to directly connect to router’ s DSL port and then connect the router to your PC (Internet---telephone line—router---network cable---PC).

Ethernet Uplink: Select this mode, if you are using a network cable to directly connect to router and then connect the router to your PC (Internet---network cable—router---network cable---PC).

Diagram of DSL Uplink mode (Internet access through telephone line) is shown below:



For Internet access via DSL uplink mode (through telephone line), there are 4 options available under “ Network” : 1. Country, 2. Area, 3. PPPOE User name, 4. PPPOE Password.



Line connected

Status

Connect Status : **Disconnect**

Network

VPI/VCI Settings: (VPI/VCI:0/35)

PPPOE User Name:

PPPOE Password:

Wireless

Key:

Password:

Country: Select your country.

Area : This option is mainly for distinguishing various areas and operators that have different VPI/VCI values. To make it convenient for its users, this device has integrated some main VPI/VCI values. You only need to select your area and operator and the router will automatically offer a correspondingly matched VPI/VCI value of your local area.

PPPOE User name: the user name provided by your ISP; used together with password to authenticate the user.

PPPOE Password: the password provided by your ISP; used together with user name to authenticate the user.

For example: User A obtains a user name and a pass word, which are respectively sz123456789@163.gd and micronet24689, from **New Zealand/Slingshot Telecom** for ADSL broadband, so he/she needs to input the parameters as below:

Network

VPI/VCI Settings: (VPI/VCI:0/100)

PPPOE User Name:

PPPOE Password:

Note: For the sake of security, password input on Web UI is shown in encryption code.

Wireless function is supported by this product, so you still have to configure wireless parameters. Please read the following:

Easy-to-install-----Wireless network configuration (as shown below)

Wireless

Key:

Password:

There are 2 options to configure for the wireless part:

SSID: It indicates the name of wireless network and can be modified (it can be letters, or underline). You can also keep the default name unchanged.

Key : It allows you to enter a password; only the users who know your password can be connected to your wireless network.

For example: if you want to set the wireless SSID as Wireless_40D371 and password as micronet24689, follow the configurations as shown in the figure below:

Wireless

Key:

Password:

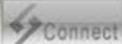
And then click “ OK” to save the settings. Congratulations! You can access Internet now when the following screen appears as below (the Status displays “ Connected” .)

Launch a web browser, enter www.Micronet.com.tw in the address field and Internet access will be successful.

Now, try to use a wireless network adapter to search “ Wireless_40D371” :

First, click  (network adapter connection icon) to search wireless signals as shown in the figure below:

SSID	Wireless mode	Channel	Strength	Encryption
Wireless_40D371	11n/11g/11b	1		—
Guest	11n/11g/11b	1		
MN_demo_base	11n/11g/11b	9		
unixtar-3	11g/11b	1		
Office_916GN	11n/11g/11b	6		

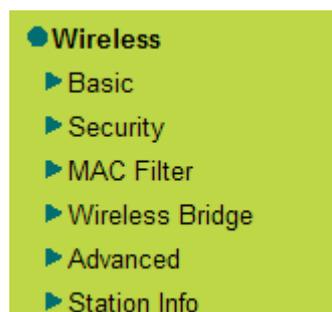
Then click “ Wireless_40D371” select “ Connect” to go to the dialogue box below:



Enter the key: micronet24689 and click “ OK” ; system will automatically connects with your wireless network in a while.

4.2 Wireless

Wireless function includes “ Basic” , “ Security” , “ MAC Filter” , “ Wireless Bridge” and “ Station Info” .



4.2.1 Basic Setting

Wireless Basic Setting

Enable Wireless	<input checked="" type="checkbox"/>
Wireless Mode	b/g/n Mixed Mode
SSID	SP3367NL <input type="checkbox"/> Hide SSID
BSSID	00:11:3B:29:CD:29
Max Clients	8 (Max:16)
Channel	Auto
Bandwidth	<input type="radio"/> 20MHz <input checked="" type="radio"/> 40MHz

Apply

- ✧ Enable Wireless: check/uncheck to enable/disable the wireless function.

Wireless Mode:

- ✧ **b/g/n Mixed Mode:** By default, system is in this mode. So your network adapter can connect to this router' s wireless network no matter which standard it complies with: 802.11b, 802.11g or 802.11n. (Different wireless network standards have different maximum transmission rates : 802.11b mode is at 11Mbps , 802.11g mode at 54 Mbps and 802.11n mode at 150Mbps. And devices that adopts 2T2R can reach up to 300Mbps).
- ✧ **b/g Mixed Mode:** If this mode is selected, then wireless adapters in use must support 802.11b or 802.11g mode.
- ✧ **g Mode :** If this mode is selected, then wireless adapters in use must support 802.11g mode.
- ✧ **SSID:** the name of wireless network. It can divide a wireless LAN into several sub-networks that requires different identity authentication, and allows itself to be scanned by other wireless devices through broadcast. The name displayed in “ View available wireless networks” under Windows is a SSID.
- ✧ **Hide SSID:** If you don' t want wireless network to be searched by other users via SSID name, then you' d better prohibit SSID broadcast. As a result, your wireless network will not appear in the searched wireless network list but it is still available, you

only need to manually add it to the list.

BSSID : BSS is a special Ad-hoc LAN application. A wireless network consists of, at least, an AP that is connected to wired network and several wireless work stations, which is called BSS (Basic Service Set).

A group of PCs with the same BBS name can establish a group, and this BBS name is called BSSID. In a small wireless LAN environment, there is only one AP and all clients share the same BSSID which is usually the MAC address of the AP.

- ✧ **Max Clients:** The max number of wireless clients that are allowed to be connected to the wireless network, 16 by default. You can modify it manually (The Max number is 16).
- ✧ **Channel:** wireless signal needs to be transferred through a certain channel. If two transmission signals are using the same channel, then mutual interference will be caused to decrease communication efficiency. There are 13 channels (1 to 13) for your option. Thus, to avoid interferences, you are recommended to choose the channel that is different from that of another SSID. If you select “ Auto” , then system will automatically choose a channel with relatively less interference for your wireless network.
- ✧ **Bandwidth:** The bandwidth here refers to wireless signal' s frequency width which only functions in b/g/n Mixed wireless mode. The max wireless rate is 150Mbps in 20MHZ and 300Mbps in 40MHZ.

4.2.2 Security Setting

WPS Setup

This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured

Enable WPS	<input checked="" type="checkbox"/>
Setup AP	<input type="radio"/> Push Button <input checked="" type="radio"/> PIN
Device PIN	<input type="text"/>
	<input type="button" value="Add enrollee"/>
Device WPS Status	Configured
Device PIN Code	42484004
	<input type="button" value="Unconfigure WPS"/>

- ✧ **Channel bandwidth:** works in 11n mode only. 802.11n supports 20MHz and 20MHz/40MHz channels. Previous standard adopts the 20MHz bandwidth while 802.11n adopts 20MHz/40MHz bandwidth. The usable channel bandwidth provided by 40MHz channel is over two times that of two 802.11 carry-over channels. 802.11n standard supports 20MHz and 40MHz channels, and the 40MHz channel combined by two adjoining and carry-over 20MHz channels is the widest channel. Certainly you can use the 20MHz channel instead according to your needs.
- ✧ **WPS Setup:** Wi-Fi protected setting (WPS) can create encrypted connection between wireless network clients and the router simply and quickly. Without selecting an encryption mode and configuring a key, you only need to enter the correct PIN code or select the “ Push Button” (press the WPS button on the router’ s back panel) to easily configure WPS instructions for operation are described below:
- ✧ **Push Button:** Press the WPS button for about 1 second and the WPS LED will keep flashing for about 2 minutes, which indicates the function is enabled. During this time, wireless client can enable WPS/PBC for authentication negotiation; if negotiation succeeds, then the WPS LED keeps “ always on” . A wireless client is successfully connected.
- ✧ **PIN:** To use PIN, you must know wireless client’ s PIN code and input it in its text box, then save this configuration. Meanwhile, use the same PIN code in the client for connection.

Enable WPS: check/uncheck to enable/disable the WPS function. It is enabled by default.

Note: The WPS feature only functions with wireless network available.

Network Authentication: To secure your wireless network, system provides several authentication modes:

Open: you can select “ no encryption” or WEP (64 bits/128 bits) as encryption algorithm.

Shared: You can select WEP 64 bits/ WEP 128 bits as encryption algorithm.

WPA-PSK: You can select AES, TKIP or TKIP+AES as encryption algorithm.

WPA2-PSK: you can select AES, TKIP or TKIP+AES as encryption algorithm.

Mixed WPA/ WPA2-PSK: you can select AES, TKIP or TKIP+AES as encryption algorithm.

4.2.3 MAC Filter

MAC address filter can allow or refuse specific clients to access your wireless network, see the screen below:

Wireless - MAC Filter

SSID: SP3367NL_LAN1_10M

MAC Restrict Mode: Disabled Allow Deny

MAC Address	Remove
-------------	--------

Save Add Remove

“ **Disabled**” : Select it to disable MAC filter function.

“ **Allow**” : only allows clients in the MAC address list to access your wireless network.

“ **Deny**” : only prohibits clients in the MAC address list from accessing your wireless network.

Add: to add a MAC address, click the “ Add” button.

To delete an added MAC address, first check the “ Remove” box behind the MAC address in list and then click the “ Remove” button.

Example 1: If you want to allow the PC with MAC address of 00:1A:3D:9C:BB:23 only to access your wireless network, then follow the instructions below:

Click the “ Add” button in the above screen to enter the page below and enter the MAC address 00:1A:3D:9C:BB:23 in the text box as shown in the below figure:

Wireless -- MAC Filter

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

MAC Address: (AA:BB:CC:DD:EE:FF)

Apply/Save

And then click the " Apply/Save" button on the above screen to save the parameter. Select " Allow" on the page below:

Wireless -- MAC Filter

SSID:

MAC Restrict Mode: Disabled Allow Deny

MAC Address	Remove
11:22:33:44:55:66	<input type="checkbox"/>

Save Add Remove

Example 2: If you want to prohibit the PC with MAC address of 00:c2:a5:67:d4:23 only from accessing your wireless network, then follow the instructions below:

1. Enter the Wireless--MAC filter page and click the " Add" button to enter the page below and enter the MAC address 00:11:3B:67:d4:23 in the text box as shown in the below figure:

Wireless -- MAC Filter

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

MAC Address: (AA:BB:CC:DD:EE:FF)

Apply/Save

- And then click the " Apply/Save" button on the above screen to save the paramter.
2. Select " Deny" on the page below:

Wireless -- MAC Filter

SSID:

MAC Restrict Mode: Disabled Allow Deny

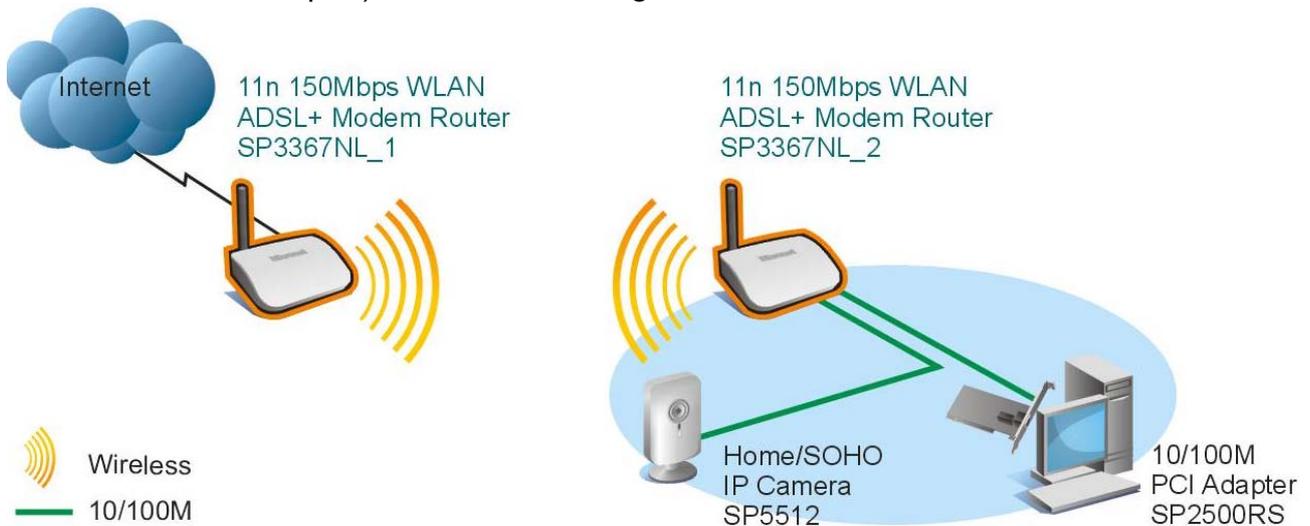
MAC Address	Remove
11:22:33:44:55:66	<input type="checkbox"/>

4.2.4 Wireless Bridge

Wireless Distribution System is used to extend the existing wireless signal coverage.

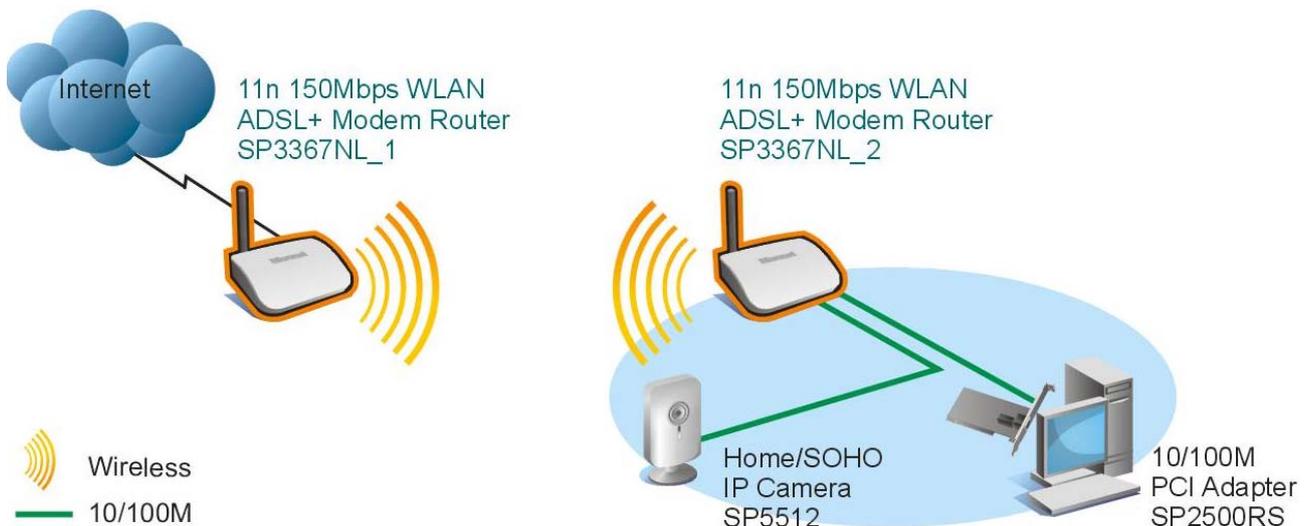
Wireless bridge includes 2 modes:

1. Access point (Once it is selected, the AP function will be enabled while wireless bridge function will be reserved. And wireless base station will establish bridge with the AP in the meantime. Namely, you can establish communication with wireless base station through a wireless network adapter) as shown in the figure below:



In the above figure, 2 SP3367NLs are used to enlarge wireless signal coverage. SP3367NL-2 is configured as a wireless access point to establish a wireless bridge with SP3367NL-1. In the meantime, the AP function reserved in SP3367NL-2 enables PC3 and PC4 to communicate with SP3367NL-2 and access Internet through wireless network adapters.

2. Wireless bridge (Here in this mode, wireless is used as pure bridge only with no more AP function to connect and communicate with remote devices. Namely, your PC can only be connected to the device via wired media instead of communicating with the device through wireless network adapter.) see the figure below:



In the above figure, 2 SP3367NLs are used to enlarge wireless signal coverage. SP3367NL-2 is configured as a wireless bridge to establish a wireless bridge with SP3367NL-1. SP3367NL-2, here, does not have the AP function, thus, PC3 and PC4 can communicate with SP3367NL-2 and access Internet only through wired network adapters instead of wireless ones.

Note: To use wireless bridge, you must disable wireless encryption.

Bridge Restrict : There are 3 options available: Enabled, Enabled (Scan) and Disabled.

Enabled: Select it to enable wireless bridge function. You need to know the MAC address of a remote bridge and enter it manually. 4 MAC addresses of remote bridges can be saved to simultaneously establish bridges with 4 APs.

Enabled (Scan): Select it to enable the wireless bridge function. In the meantime, system will automatically scan MAC addresses of available wireless devices. See the figure below:

Model No. SP3367NL
11n 150Mbps WLAN ADSL2+ Modem Router
Version No.: Ver1.0

Wireless -- Bridge

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

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

You only need to check the wireless network that you want to bridge with and click the “ Apply/Save” button. And system will automatically establish wireless bridge with the remote device for you.

Disabled: To disable wireless bridge function, select this option.

Note:

To use the wireless bridge function, both devices must support the function. Besides, SSID, channel, encryption method and key of one device must be set to the same value of its link partner' s.

4.2.5 Station Info

This page shows authenticated wireless stations and their status.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Refresh

4.3 Advanced Setup

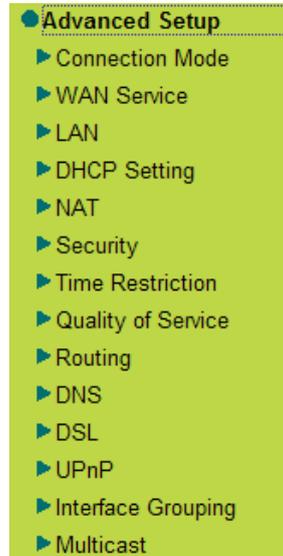
Enter the setup wizard screen below and then click “ Advanced Settings” on the upper right corner as shown in the below:

After you enter the advanced settings screen, you can set the advanced settings for the router to satisfy your requirements. There are seven main menus on this screen: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Exit and Back to wizard as shown in the below picture.

4.3.1 Advanced Setup

Advanced Setup: Consists of 14 submenus including Connection Mode/ WAN Service/LAN/DHCP Setting/NAT/Security/Time Restriction/Quality of

Service/Routing/DNS/DSL/UPnP/ Interface Grouping and Multicast as shown in the figure below:



4.3.2 Connection mode

Connection Mode

This router supports two connection modes: DSL mode and Ethernet mode. Select DSL mode, if you access Internet through telephone line and Ethernet mode through network cable. By default, system is in DSL mode.

Mode Select

Mode Select:

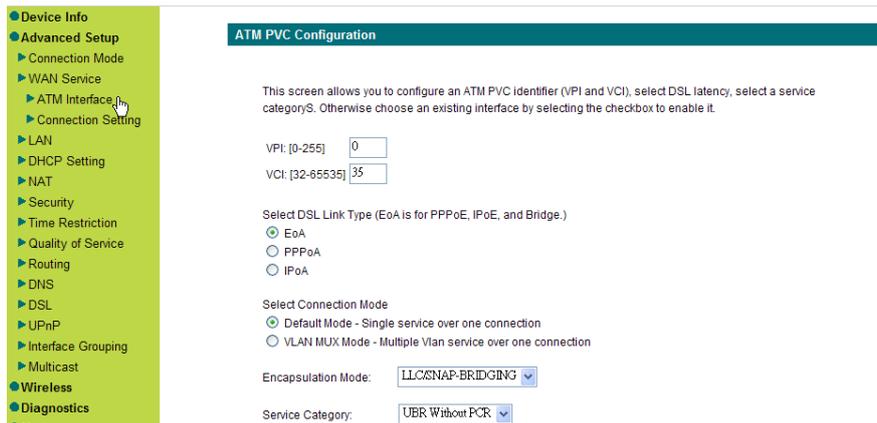
- DSL Mode
- Ethernet Mode

Apply

To enter the connection mode interface, click “ Advanced Setup” ---“ Connection Mode” . Select a proper connection mode and then click the “ Apply” button.

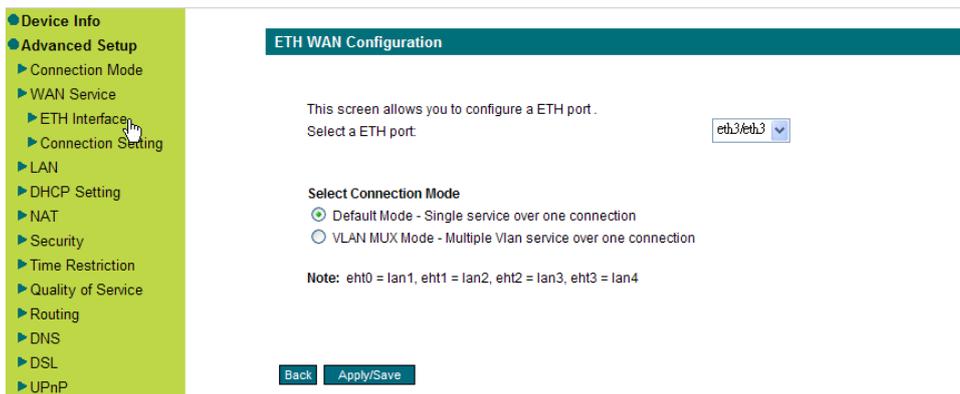
1. In DSL mode, you are required to configure parameters for ATM interface.

To enter the ATM Interface page, click “ Advanced Setup” ---“ Connection Mode” (Select DSL mode and click “ Apply”)--- “ WAN Service” ---ATM Interface. And then click “ Add” to configure the relevant parameters.



On this page, you can configure VPI and VCI values (consult your local ISP if you are not clear). For other options, keep the defaults and click the “ Apply/Save” button.

2. In Ethernet modes, you are required to configure parameters for Ethernet interface. To enter the ETH Interface page, click “ Advanced Setup” ---“ Connection Mode” (Select Ethernet mode and click “ Apply”) --- “ WAN Service” ---“ ETH Interface” . And then click the “ Add” button to configure relevant parameters.



The Ethernet interface configured on this page is used as a WAN port. You can select only one LAN interface to function as a WAN port. Once you finish, click the “ Apply/Save” button.

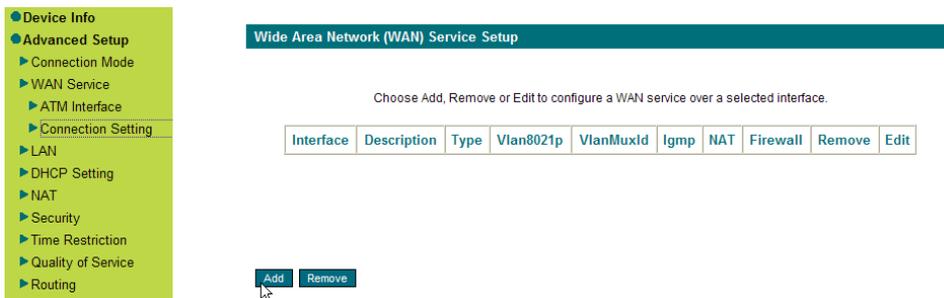
4.3.3 WAN service

WAN Configuration in DSL Mode

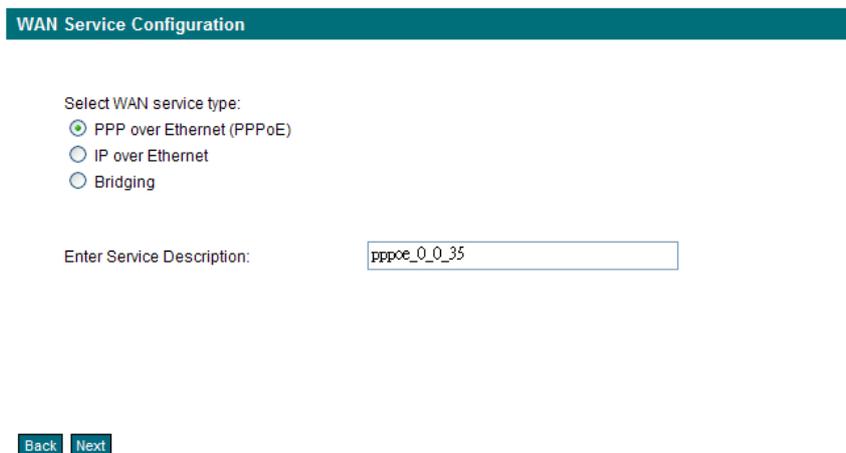
-PPP over Ethernet (PPPoE)

Click “ Advanced Setup” —“ Connection mode” (Select DSL mode and click “ Apply”)---“ WAN Service” ---“ ATM Interface” (refer to 4.3 for configuring the ATM

interface)---“ Connection Setting” to enter WAN service setup interface (page1) and then click the “ Add” button there to select a WAN service type on page 2.

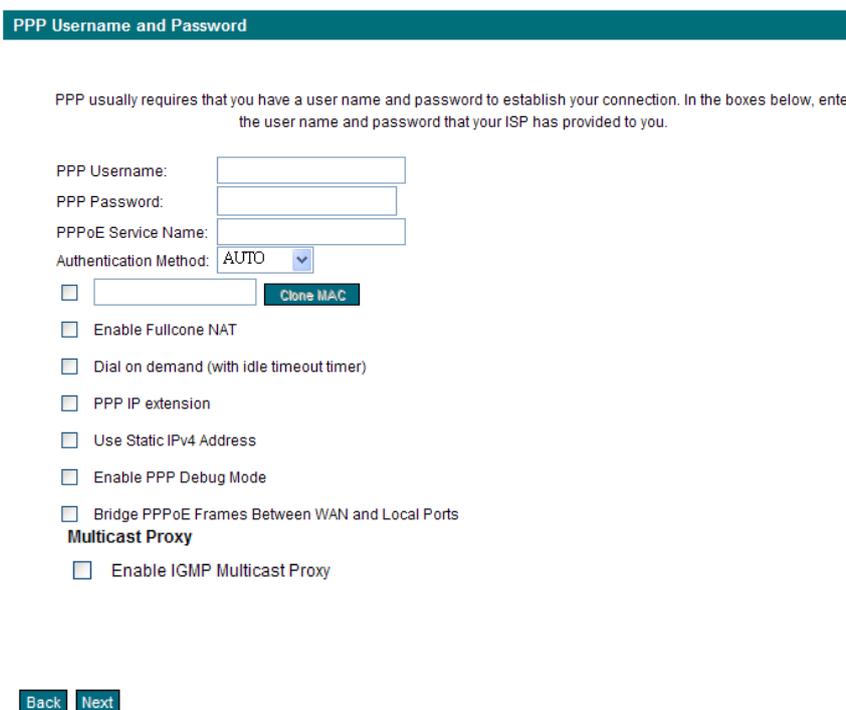


Page 1



Page 2

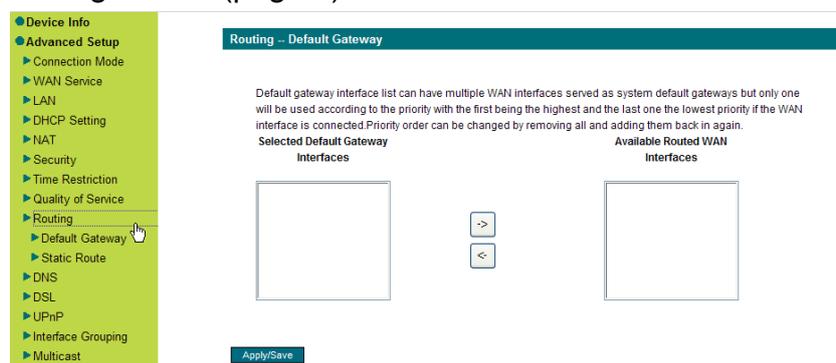
Select PPP over Ethernet (PPPoE), modify the service description if necessary and then click “ Next” on page 2 to enter the page below (page 3):



Page 3

- ✧ **PPP User Name:** User name for PPPoE dialup. It is provided by your ISP.
- ✧ **PPP Password:** The password provided by your ISP for PPPoE dialup.
- ✧ **PPPoE Service Name:** it is provided by your ISP. Do not fill it in if you don't have it; otherwise PPPoE dialup may fail.
- ✧ **Authentication Method:** it is used by ISP to verify its clients during PPPoE dialup. Select “ Auto” if you are not sure about it.
- ✧ **Clone MAC :** This feature clones the MAC address of the PC that is currently entering the router's management page to work as the WAN MAC address of the router.
- ✧ **Dial on Demand:** Automatically connects or disconnects Internet according to the use of the network. It is recommended when your ISP limits network use time.
- ✧ **PPP IP extension:** The IP addresses of all packets including management packets that egress WAN port will be converted to the WAN port's IP address once this feature is enabled.
- ✧ **Enable PPP Debug Mode:** This feature can be enabled only when supported by your ISP.
- ✧ **Bridge PPPoE Frames Between WAN and Local Ports :** PPPoE dialup frame initiated by LAN port will directly egress WAN port without being modified if this feature is enabled.
- ✧ **Multicast Proxy:** Router enables multicast proxy server if this feature is enabled.

Enter the PPP user name and PPP Password provided by your ISP. For other options, keep the default values if you are not clear about them, and then click the “ Next” button to display the following screen (page 4):



Page 4

This page allows you to configure the gateway address for WAN connection. We recommend you to keep the default values and click the “ Next” button on page 4 to enter the following page (page 5):

Routing -- Default Gateway

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.

Selected Default Gateway Interfaces

ppp0

Available Routed WAN Interfaces

[Back](#) [Next](#)

page 5

This page allows you to configure the DNS server's IP address for the WAN port. We recommend you to keep the default values if you are not clear about it and click the " Next" button (on page 5) to enter the following page (page 6):

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 Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp0

Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

[Back](#) [Next](#)

WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

Page 6

This page displays the configuration information. After confirmation, please click " Apply/Save" to save it.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

You can access Internet once PPPoE dialup succeeds.

4.3.4 IP over Ethernet

When your ISP provides you an IP address or tells you that you only need to configure your PC to obtain an IP address automatically to access Internet, you need to select IP over Ethernet as the WAN service type.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Modify the service description if necessary and then click the “ Next” button:

WAN IP Settings

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

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

[Back](#) [Next](#)

- ✧ Use the following Static IP address: select this feature if your ISP provides you an IP address.
- ✧ WAN IP Address: the IP address provided by your ISP for accessing Internet.
- ✧ WAN Subnet Mask: the subnet mask address provided by your ISP for accessing Internet.
- ✧ WAN gateway IP Address: the gateway IP address provided by your ISP for accessing Internet.

Enter the IP/ subnet mask/gateway IP address provided by your ISP or select " Obtain an IP address automatically" and click the " Next" button (on page 1) to enter page 2 below:

WAN IP Settings

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

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

[Back](#) [Next](#)

Page 1

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

- Enable NAT
- Enable Fullcone NAT
- Enable Firewall
- Enable IGMP Multicast

[Back](#) [Next](#)

Page 2

We recommend you to keep the default settings unchanged and click the “ Next” button (on page 2) to enter the screen (page 3) below:

Routing -- Default Gateway

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.

Selected Default Gateway Interfaces

ppp0



Available Routed WAN Interfaces

[Back](#) [Next](#)

page 3

This page allows you to configure the gateway address for WAN connection. We recommend you to keep the default values and click the “ Next” button (on page 3) to enter the following page (page 4):

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 Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp0



Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

[Back](#) [Next](#)

Page 4

This page allows you to configure the DNS server's IP address for the WAN port. We recommend you to keep the default values if you are not clear about it and click the "Next" button (on page 4) to enter the following page (page 5):

WAN Setup - Summary

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

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

page 5

This page displays the configuration information. After confirmation, please click "Apply/Save" to save it.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
atm0	ipoe_0_0_35	IPoE	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>	Edit

[Remove](#)

You can access Internet once the configured connection succeeds.

4.3.5 Bridging

If you want to use your PC or other devices to execute dialup or you don't want to share your broadband service with other users, you can first configure your router's WAN service type as bridging and then use your PC or other devices for dialup connection.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

[Back](#) [Next](#)

Modify the service description if necessary and then click “Next”.

WAN Setup - Summary

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

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable

Click “Apply/Save” to have this interface to be effective. Click “Back” to make any modifications.

[Back](#) [Apply/Save](#)

This page displays the configuration information. After confirmation, please click “Apply/Save” to save it.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
atm0	br_0_0_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

[Remove](#)

After successful configurations, use your PC or other devices to dialup and then you can access Internet.

Note: When you need to configure several WAN connections (multiple PVCs), first configure the needed number of ATM interfaces and then follow the above corresponding configuration procedures.

4.4.6 WAN Configuration in Ethernet Mode

In Ethernet mode, system supports PPP over Ethernet (PPPoE), PPP over ATM (PPPoA) and IP over Ethernet IPoE.

-PPP over Ethernet (PPPoE)

Click “ Advanced Setup” — “ WAN Service” – “ Connection Setting” to enter WAN service setup interface (page 1) and then click the “ Add” button to go to page 2 and select a proper WAN service type.



Page 1



Page 2

Select PPP over Ethernet (PPPoE) on page 1, modify the service description if necessary and then click “ Next” to enter page 2:



Page 1

PPP Username and Password

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

Page 2

- ✧ PPP User Name: User name for PPPoE dialup. It is provided by your ISP.
- ✧ PPP Password: The password provided by your ISP for PPPoE dialup.
- ✧ PPPoE Service Name: it is provided by your ISP. Do not fill it in if you don't have it; otherwise PPPoE dialup may fail
- ✧ Authentication Method: it is used by ISP to verify its clients during PPPoE dialup. Select " Auto" if you are not sure about it.
- ✧ Clone MAC : This feature clones the MAC address of the PC that is currently entering the router's management page to work as the WAN MAC address of the router. Configure it when your ISP requires a fixed MAC for your Internet access.
- ✧ Dial on Demand: Automatically connects or disconnects Internet according to the use of the network. It is recommended when your ISP limits network use time. This feature can help you to save the Internet fee.
- ✧ PPP IP extension: The IP addresses of all packets including management packets that egress WAN port will be converted to the WAN port's IP address once this feature is enabled.
- ✧ Enable PPP Debug Mode: This feature can be enabled only when supported by your ISP.
- ✧ Bridge PPPoE Frames Between WAN and Local Ports : PPPoE dialup frame initiated by LAN port will directly egress WAN port without being modified if this feature is

enabled.

- ✧ Multicast Proxy: Router enables multicast proxy server if this feature is enabled.

Enter the PPP user name and PPP Password provided by your ISP. For other options, keep the default values if you are not clear about them, and then click the “ Next” button to display the following screen:

Routing -- Default Gateway

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.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
<input type="text" value="ppp0"/>	<input type="button" value="->"/> <input type="button" value="<-"/>	<input type="text"/>

This page allows you to configure the gateway address for the WAN connection. We recommend you to keep the default values and click the “ Next” button to enter the following page:

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 Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
<input type="text" value="ppp0"/>	<input type="button" value="->"/> <input type="button" value="<-"/>	<input type="text"/>

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

This page allows you to configure the DNS server's IP address for the WAN port. We recommend you to keep the default values if you are not clear about it and click the "Next" button to enter the following page:

WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

This page displays the configuration information. After confirmation, please click "Apply/Save" to save it.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
ppp0	pppoe_eth3	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>	Edit

[Remove](#)

You can access Internet once PPPoE dialup succeeds.

4.3.7 IP over Ethernet

When your ISP provides you an IP address or tells you that you only need to configure your PC to obtain an IP address automatically to access Internet, you need to select IP over Ethernet (I PoE) as the WAN service type.

- Device Info
- **Advanced Setup**
 - ▶ Connection Mode
 - ▶ WAN Service
 - ▶ ETH Interface
 - ▶ Connection Setting
 - ▶ LAN
 - ▶ DHCP Setting
 - ▶ NAT
 - ▶ Security
 - ▶ Time Restriction
 - ▶ Quality of Service
 - ▶ Routing
 - ▶ DNS
 - ▶ DSL
 - ▶ UPnP

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Enter Service Description:

[Back](#) [Next](#)

Modify the service description if necessary and then click the "Next" button:

WAN IP Settings

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

Obtain an IP address automatically
 Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

Back Next

- ✧ **Obtain an IP address automatically:** WAN port will automatically obtain an IP address for accessing Internet from the ISP, if this feature is selected.
- ✧ **Use the following Static IP address:** select this feature if your ISP provides you an IP address.
- ✧ **WAN IP Address:** the IP address provided by your ISP for accessing Internet.
- ✧ **WAN Subnet Mask:** the subnet mask address provided by your ISP for accessing Internet.
- ✧ **WAN gateway IP Address:** the gateway IP address provided by your ISP for accessing Internet.

Enter the IP/ subnet mask/gateway IP address provided by your ISP or select " Obtain an IP address automatically" and click the " Next" button on page 1 to enter page 2:

WAN IP Settings

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

Obtain an IP address automatically
 Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

Back Next

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

- Enable NAT
- Enable Fullcone NAT
- Enable Firewall
- Enable IGMP Multicast

[Back](#) [Next](#)

Page 2

We recommend you to keep the default settings unchanged and click the “ Next” button on page 2 to enter the page 3 below:

Routing – Default Gateway

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.

Selected Default Gateway Interfaces

eth3



Available Routed WAN Interfaces

[Back](#) [Next](#)

Page 3

The page 3 allows you to configure the gateway address for WAN connection. We recommend you to keep the default values and click the “ Next” button on page 3 to enter the following page (Page 4):

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 Interface from available WAN interfaces:

Selected DNS Server Interfaces: eth3

Available WAN Interfaces:

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Page 4

This page allows you to configure the DNS server's IP address for the WAN port. We recommend you to keep the default values if you are not clear about it and click the "Next" button on page 4 to enter the following page:

WAN Setup - Summary

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

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

This page displays the configuration information. After confirmation, please click "Apply/Save" to save it.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
eth3	ipoe_eth3	IPoE	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

You can access Internet once the configured connection succeeds.

4.3.8 LAN

You can change the IP address of the LAN port to match the requirement of the practical network environment.

To enter the screen below, click “ Advanced Setup” ----“ LAN” .

Local Area Network (LAN) Setup

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

IP Address:

Subnet Mask:

Enable IGMP Snooping

Apply/Save

- ✧ IP Address: It is the Router’ s LAN IP address. The default IP address is 192.168.1.1.
- ✧ Subnet Mask: It is the Router’ s LAN subnet mask. You can modify it according to your needs.
- ✧ Enable IGMP Snooping: Check/uncheck to enable/disable the IGMP Snooping.

Note:

If you have changed the LAN IP address, then you must re-configure your PC’ s IP address to log on to the router’ s Web-based management interface, and the default gateway of all computers that connect to the router’ s LAN ports have to be set to the new IP address for normal Internet access.

4.3.9 DHCP setting

-DHCP Server

This router enables DHCP server function by default. DHCP refers to Dynamic Host Control Protocol. With an internal DHCP server, the Router can automatically configure the IP addresses, subnet mask, gateway and DNS server, etc for the computers that connect to the router’ s LAN ports and are configured to obtain an IP address automatically.

Therefore it reduces the inconvenience and trouble in manually configuring IP address and other network parameters for multiple computers in LAN.

DHCP Settings - DHCP Server

Disable DHCP Server
 Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Apply/Save

- ✧ Enable/ Disable DHCP Server: Click the corresponding button to enable/ disable the DHCP Server.
- ✧ Start IP: The point from which DHCP server starts IP address distribution.
- ✧ End IP: The point where DHCP server ends IP address distribution.
- ✧ Lease Time: It indicates the valid time of the dynamic IP address which is distributed to the client' s host computer by DHCP server. During this time, the server will not distribute the IP address to any other host computer.

Note:

To use the Router' s DHCP server function, you must set the TCP/IP protocol of the computers in LAN to “ Obtain an IP address automatically” .

-DHCP client

This page displays DHCP client' s information such as host name, MAC address, IP address, and lease time.

Device Info -- DHCP Leases

DHCP Leases			
Hostname	MAC Address	IP Address	Expires In

- ✧ **Hostname:** The name of a PC or a network device that has successfully obtained an IP address from the DHCP server.
- ✧ **MAC Address:** The MAC address of a PC or a network device that has successfully obtained an IP address from the DHCP server.
- ✧ **IP Address:** The IP address distributed by DHCP server.

✧ **Expires In:** This item displays the leftover lease time.

4.3.10 NAT

- Virtual Server

When you create a server such as a Web server, FTP server or game server in your router's LAN side, you can let Internet users access the created server through the router's WAN IP address by configuring virtual server.

NAT -- Virtual Server

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

[Add](#) [Remove](#)

To enter virtual server interface, click “ NAT” -> “ Virtual Server” . And then click the “ Add” button to add rules for accessing the server.

NAT -- Virtual Servers

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

Remaining number of entries that can be configured: 32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		

- ✧ **Use Interface:** It indicates which WAN connection the configured rules are to be applied to. When there is only one configured WAN connection available, system will select it automatically.
- ✧ **Service Name:** There are two options available: (1) Select a Service: allows you to select an existing service from the drop-down list box. (2) Custom Service: allows you

to define a service yourself.

- ✧ **Server IP Address:** The IP address of the server created on LAN side.
- ✧ **External Port Start/ External Port End:** The port range through which Internet users access the router' s LAN side server.
- ✧ **Protocol:** There are 3 options: TCP, UDP and TCP/UDP. We recommend you to select TCP/UDP if you are not sure about which protocol to choose.
- ✧ **Internal Port Start/ Internal Port End:** The port range used by the created server on router' s LAN side.

Note: When UPNP function is enabled on the router and on some application programs on the computer that is connected to the router' s LAN port, the virtual server page will display: UPNP interface is being used.

For example: You have created 2 servers on the router' s LAN side: (1) FTP server (Port: 2100) for transferring files is at the IP address of 192.168.1.100 (2) Web server (port: 80) is at the IP address of 192.168.1.110. And you want your Internet friends to access your FTP and Web servers respectively via port: 2100 and port: 80. For configurations, follow the instructions below:

1. Configuring FTP server:

Click “ NAT” -> “ Virtual Server” to enter the virtual server interface. And then click the “ Add” button to configure the following page (refer to the parameters that are configured on the page):

Use Interface:	pppoe_0_0_35/ppp0			
Service Name:	Web Server (HTTP)			
<input type="radio"/> Select a Service:	Web Server (HTTP)			
<input checked="" type="radio"/> Custom Service:	FTP			
Server IP Address:	192.168.1.100			
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
2100	2100	TCP	2100	2100
		TCP		

2. Configuring Web server

Use Interface: pppoe_0_0_35/ppp0

Service Name:

Select a Service: Web Server (HTTP)

Custom Service:

Server IP Address: 192.168.1.110

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
80	80	TCP	80	80
		TCP		

The screen appears as below after the above configuration is finished:

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
FTP	2100	2100	TCP	2100	2100	192.168.1.100	ppp0	<input type="checkbox"/>
Web Server (HTTP)	80	80	TCP	80	80	192.168.1.110	ppp0	<input type="checkbox"/>

Supposing that the IP address of PPP0 is 183.37.227.201, then the Internet user only needs to enter ftp : //183.37.227.201 : 2100 or http : //183.37.227.201 in Web browser address field to respectively access your FTP or Web server.



- Port Triggering

Some application programs or network business (such as network game, video conference, etc) can not work with simple NAT router due to the isolation caused by router' s built-in firewall. Therefore, proper configuration is needed. When application program initiates a connection toward the triggering port, all correspondingly open ports will be enabled to implement successful connection and service.

NAT -- Port Triggering

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

Remaining number of entries that can be configured: 32

Use Interface: ▼

Application Name:

Select an application: ▼

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼

Save/Apply

Click " Advanced Setup " --- " NAT " ---" Port Triggering " to enter the port triggering interface and then click the " Add " button to add rules.

NAT -- Port Triggering

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

Remaining number of entries that can be configured: 32

Use Interface: ▼

Application Name:

Select an application: ▼

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼

Save/Apply

- ✧ **Use Interface:** It indicates which WAN connection the configured rules are to be applied to. When there is only one configured WAN connection available, system will select it automatically.
- ✧ **Application Name:** There are two options available:
 - (1) **Select an application:** allows you to select an existing application from the drop-down list box.
 - (2) **Custom application:** allows you to define an application yourself.
- ✧ **Trigger Port Start/ Trigger Port End:** The port range for application programs to initiate connections.
- ✧ **Trigger Protocol:** There are 3 options: TCP, UDP and TCP/UDP. We recommend you to select TCP/UDP if you are not sure about which protocol to choose.
- ✧ **Open Port Start/ Open Port End:** the port range that will be automatically enabled by the built-in firewall when connections initiated by application programs succeed.

For example: You have created a server on router' s LAN side that can automatically download material from Internet (via port: 9090) and share its data with other users. And you want Internet users to download data from your server (via port: 9999). For configurations, follow the instructions below:

To enter the port triggering interface, click “ Advanced Setup” --- “ NAT” ---“ Port Triggering” , and then click the “ Add” button to configure the page below (Refer to the parameters configured on the page below):

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

Remaining number of entries that can be configured: 32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
9090	9090	TCP	9999	9999	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

When your server initiates a connection toward the server on Internet via port: 9090, the router' s firewall will automatically open port: 9999 to let Internet users access your server to download data via this port: 9999.

-DMZ Host

Once a PC on a LAN is set as a DMZ host, it can implement network communication with Internet without limit.

NAT -- DMZ Host

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

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

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

DMZ Host IP Address:

Save/Apply

✧ DMZ Host IP Address: the IP address of a PC to be set as a DMZ host. DMZ host must be connected to the router's LAN port.

Note: The router's firewall can not have effect on the DMZ host once it is enabled. So network security problem may occur. Thus we recommend you to enable this function only when necessary and delete the corresponding settings as soon as you are not using it. For example: If you want the PC at the IP address of 192.168.1.100 from your router's LAN side to be shared by Internet users for data and other resources. For configurations, follow the instructions below:

Click "Advanced Setup" ---- "NAT" --- "DMZ Host" to configure the page below:

NAT -- DMZ Host

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

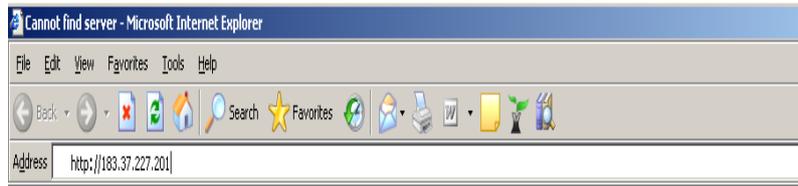
Enter the computer's IP address and click 'Apply' to activate the DMZ host.

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

DMZ Host IP Address:

Save/Apply

Supposing that the router's WAN IP address is 183.37.227.201, then the Internet user only needs to enter http : //183.37.227.201 in Web browser address field to access your Web server.



4.3.11 Security

-IP Filter

IP filter function can block LAN PCs from communicating with Internet PCs by preventing specific IP addresses from accessing external network through router via specific a port number or range.

Outgoing IP Filtering Setup

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

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

[Add](#) [Remove](#)

- 1) Click “ Advanced Setup” → “ Security” → “ IP Filtering” to display the page above and then click the “ Add” button to enter the page below to add filtering rules.

Add IP Filter -- Outgoing

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

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

[Apply/Save](#)

Filter Name: Enter the defined filtering name.

IP Version: Only IPv4 is provided.

Protocol: TCP/UDP; TCP; UDP; ICMP available for your option.

Source IP address [/prefix length]: Enter the LAN IP address to be filtered.

Source Port (port or port: port): The port number or range used by LAN PCs in accessing the Internet.

Destinations IP address [/prefix length]: The external network IP address to be accessed by LAN PC.

Destination Port: The port number or range used by LAN PCs in accessing external network.

Note:

- ✧ Packets filtered in this function are transferred from LAN to WAN.
- ✧ If you are not familiar with all parameters to be configured, you can just configure some of them and keep the left unchanged. And the filtering function can also be implemented.

For example:

If you want to filter the PC at the IP address of 192.168.1.200 and make it unable to access Internet. Then follow the instructions below:

First, click “ Advanced Setup” → “ Security” → “ IP Filtering” to enter the IP filtering setup page and then click the “ Add” button to enter the page below to configure needed parameters as below:

Add IP Filter -- Outgoing

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

Filter Name:

IP Version: IPv4

Protocol: TCP/UDP

Source IP address/prefix length:

Source Port (port or port:port):

Destination IP address/prefix length:

Destination Port (port or port:port):

Apply/Save

And then click the “ Apply/Save” button to save your setting.

Note:

- ✧ Principle of using “ IP Filter” function to prohibit BT download: when you use BT software to download data, it needs to send request for connecting “ seed” server, and when this request passes the router, the router’ s IP Filter function will hold it up and ignore the request so that BT fails to connect the server and download will be aborted.

- ✧ The ports that BT “ seed” server frequently uses are in the range of 6900-8100 such as 6969 , 8000 and 7373. So we can block this port range by creating proper rules to stop BT software from connecting the server. However, some Non-BT “ seed” servers are also using port 8080, thus, in order not to affect other servers, we must divide the port range of 6900-8100 to be blocked into 2 groups: 6900-8079 and 8081-8100 .
- ✧ The protocols that BT uses are TCP/UDP, so we need to block both of them.

-URL Filter

URL filter function blocks all LAN PCs from accessing specific domain names on Internet. It rejects all requests to access the specific domains.

URL Filter Add

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

URL Address:

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

Apply/Save

For example: If you want to prevent all LAN PCs from accessing www.sina.com.cn, then follow the instructions below:

Click “ Advanced Setup” —“ Security” —“ URL Filter” to the page above and then click the “ Add” there to enter the page below to configure needed parameters:

URL Filter Add

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

URL Address:

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

Apply/Save

URL Address: Enter the domain name that rejects LAN PCs access.

Port Number: The port used by Web server, 80 by default.

Then click the “ Apply/Save” button to save your settings. And all LAN PCs can not access www.micronet.info.

Note: After you have added the URL filter rule, if you previously accessed this URL, then you need to reboot the router and delete your PC' s cache to activate the function. However, you can access the deleted URL without rebooting the router after you delete a filter rule.

-Time Restriction

This function can restrict PCs or other network devices that are connected to the router' s LAN ports to a specific Internet access time.

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

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
----------	-----	-----	-----	-----	-----	-----	-----	-----	-------	------	--------

[Add](#) [Remove](#)

For example: If you want the PC at the MAC address of aa:bb:cc:dd:ee:ff to access Internet on Saturday and Sunday only, then follow the instructions below: Click “ Advanced Setup” —“ Security” —“ Time Restriction” to enter the screen above and then click the “ Add” button there to enter the screen below to configure needed parameters:

Access Time Restriction

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

User Name

Browser's MAC Address

 Other MAC Address

(xxxxxxxxxxxx)

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

[Apply/Save](#)

- ❖ **User Name:** Enter the defined user name by you.
- ❖ **Browser's MAC Address:** The MAC address of the PC that is currently accessing the router' s management interface; it is automatically added by system.
- ❖ **Other MAC Address:** The MAC address whose Internet access time you want to

restrict. Enter it manually.

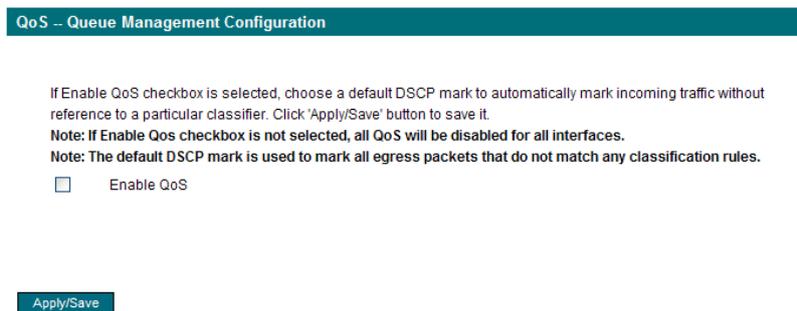
- ✧ **Start Blocking Time (hh:mm) / End Blocking Time (hh:mm):** The time range during which Internet access is blocked.

After configuration is finished, click the “ Apply/Save” button and the MAC address of aa:bb:cc:dd:ee:ff can only access Internet on Saturday and Sunday.

4.3.12 Quality of Service

Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Select the "Advanced Setup → Quality of Service" menu to enter the following screen.



Select the “ Enable QoS” Checkbox, and select Default DSCP Mark Value, then, Click 'Save/Apply' to save and activate the rule.

Queue Configuration

Click “ Advanced Setup” -> “ Quality of Service” -> “ Queue config” to display the configured QoS rule.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	Enable	Remove
WMM Voice Priority	1	wi0	SP	1			Enabled	
WMM Voice Priority	2	wi0	SP	2			Enabled	
WMM Video Priority	3	wi0	SP	3			Enabled	
WMM Video Priority	4	wi0	SP	4			Enabled	
WMM Best Effort	5	wi0	SP	5			Enabled	
WMM Background	6	wi0	SP	6			Enabled	

Click “ Add” to enter the following screen to add rules.

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.
Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others
 Click 'Apply/Save' to save and activate the queue.

Name:	<input type="text" value="QoS"/>
Enable:	<input type="button" value="Enable"/>
Interface:	<input type="text" value="eth0"/>
Precedence:	<input type="text" value="1"/>

Name: The name of the configured rule.

Enable: Enable/Disable the rule.

Interface: The interface that needs to configure priority. **Precedence:** Set a priority for the selected interface.

Click “ Save/Apply” to save the settings.

4.3.13 Routing

Default Gateway

Gateway is the path for sending packets when your computer is communicating with computers on other networks. When there are multiple WAN connections, the gateway must be specified, otherwise, your computer may not be able to communicate with computers on other networks. When there' s only one WAN connection, just keep the default settings.

Click “ Advanced Setup” -> “ Routing” -> “ Default Gateway” to enter the screen below.

Routing -- Default Gateway

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.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
eth3	<input type="button" value="→"/> <input type="button" value="←"/>	

Available Routed WAN Interfaces : Current existed WAN connection.

Selected Default Gateway Interfaces : WAN connection has already been selected as the gateway.

Select the WAN connection that you want to set as the gateway and click “ Apply/Save” to save the settings. The settings will be effective after the system reboot.

Static Route

Static Route is a special route. When you use proper static routing in networks, you can reduce routing selection problems and the forwarding rate of the data packets. IP address, subnet mask and gateway can be set to specify a routing item. Destination IP address and subnet mask can be used to specify an object network/ host. Then the Router will send the packets to the specific object network/ host.

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

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
------------	---------------------	---------	-----------	--------	--------

[Add](#) [Remove](#)

Click “ Add” to enter the screen below.

Routing -- Static Route Add

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

IP Version:	<input type="text" value="IPv4"/>
Destination IP address /prefix length:	<input type="text"/>
Interface:	<input type="text"/>
Gateway IP Address:	<input type="text"/>
(optional: metric number should be greater than or equal to zero)	
Metric:	<input type="text"/>

Apply/Save

Click “ Apply/Save” to display the current configured static route information.

- ✧ IP version: It is used to indicate that the IP belongs to IPv4.
- ✧ Destination IP address/prefix length: to identify the destination IP address or network that the data is sending to. Prefix length together with the destination IP address are used to identify the destination network.
- ✧ Interface: the interface the data is sending to
- ✧ Gateway IP address: the IP address of the router or host the data packets are sending to.
- ✧ Metric: the number of the routers that the data packets go through (optional).
- ✧ Apply /Save : Complete the settings.

Note:

- ✧ Destination IP address can not be at the same net segment with the IP addresses of the router' s WAN or LAN port.
- ✧ We recommend using the default settings if there' s no special requirement, for inappropriate or incorrect route setting would cause network malfunction.

4.3.14 DNS

-DNS server

DNS server is used to map the domain name and it can be automatically obtained when you connect to the ISP or it can also be manually configured.

DNS Server Configuration

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Apply/Save

After entering the DNS server IP address, click “ Apply/Save” to save the settings.

Note:

- ✧ After saving the settings, you need to reboot the router to bring the new configuration into effect.
- ✧ Please keep the default settings if there' s no special requirement for incorrect DNS settings will cause the LAN computer to be unable to access the Internet via the domain name.

4.3.15 DNS

If your server is set up on the router' s LAN side, and the router' s WAN IP address is changeable. When users on the Internet want to visit the server via the domain name, but the domain name can not be translated as the router' s WAN IP, which will cause visit failure. However, DDNS will request the corresponding ISP to update the domain name and IP address when WAN IP is changed. When the WAN IP address is updated, users on the Internet can still successfully visit the server.

This router supports three DDNS providers: www.dyndns.org, www.3322.org, www.tzo.com

Select “ Advanced Setup” ->“ DNS” -> “ Dynamic DNS” , and click the “ Add” button to add a rule.

This page allows you to add a Dynamic DNS address from DynDNS.org ,3322 or TZO.

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text" value="DDNS@DynDNS.org"/>
Interface	<input type="text" value="pppoe_0_0_35/ppp0"/>
DynDNS Settings	
Username	<input type="text" value="DDNS"/>
Password	<input type="password" value="•••••"/>

Dynamic DNS Provider: Select your DDNS provider.

Hostname: The domain name registered at the corresponding DDNS website.

Interface: WAN connection interface

Username: Enter the username that you use to register from the DDNS provider

Password: Enter the password that you use to register from the DDNS provider

Click “ Apply/Save” to save the settings.

4.3.16 DSL

To be applicable for different environments, DSL advanced setting screen provides multiple ASDL modulation modes for users to choose from.

DSL Settings

Select the modulation below.

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

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Apply/Save

Advanced Settings

Click the checkbox to enable corresponding modulation modes, and then click “ Apply/Save” to complete the settings.

Note: If you are not familiar with the ADSL modulation modes, please use the default settings.

4.3.17 UPnP

With UPnP (Universal Plug and Play) function, the host in LAN can request the Router to carry specific port forwarding, thus the external host can access the internal host for resources. For example, the MSN Messenger under Windows XP and Windows Me can utilize UPnP in video and audio communication, thus the function restricted by NAT can restore its normal use. Enable UPnP to help support applications that would not otherwise work behind a Router. Both UPnP Internet Gateway Device and NAT Traversal are supported.

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

Enable UPnP

Apply/Save

Select “ Enable UPnP” and then click “ Apply/Save” to save the settings.

 Note:

1. Because the security of current UPnP version has not been guaranteed, please close it when you don' t need it.
2. Only the application programs that support UPnP protocol can use this function. MSN Messenger may need to be supported by Operating Systems such as Windows XP/ ME.
3. UPnP function needs the support from Operating Systems such as Windows XP/ME.

4.3.18 Interface Grouping

If your ADSL line supports multi-WAN connection(there are multiple groups of PPPOE or other access modes),and you wish some LAN ports of your router(or the wireless network) to solely share one of the WAN ports, then you may fulfill this function by configuring the interface grouping.

Interface Grouping -- A maximum 16 entries can be configured

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

Note: After add a group of interface, please reboot you router manually.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		eth3	eth0	
			eth1	
			eth2	
			wlan0	

[Add](#) [Remove](#)

- ✧ **Group Name** : The name of the configuration rule.
- ✧ **WAN Interface used in the grouping:** WAN connection that needs to be grouped.
- ✧ **Available LAN Interfaces:** Interfaces that can be grouped.
- ✧ **Grouped LAN Interfaces:** LAN interface that needs to connect with specified WAN interface.

Example:

Your ADSL line supports two groups of PVC; the PVC that used to transmit network data is ppp0 and the PVC that used to transmit IPTV data is atm1. and you wish your router' s LAN2 port is particularly used for IPTV and the IPTV data will not be sent to other ports.

The configurations are as follows:

Configure two groups of PVC: ppp0 and atm1 (for the configuration steps, please refer to the chapter for WAN configuration).

Click “ Advanced Setup” -> “ Interface Grouping” to enter the screen below, and click “ Add” to configure the IPTV grouping parameters.

Interface Grouping -- A maximum 16 entries can be configured

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

Note: After add a group of interface, please reboot you router manually.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		eth3	eth0	
			eth1	
			eth2	
			wlan0	

Click “ Save/Apply” to save the settings.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			eth0	
			eth2	
			wlan0	
			eth3	
IPTV	<input type="checkbox"/>	ppp0	eth1	

Note:

After completing the settings, reboot the router to bring the router settings into effect.

After setting the interface grouping, the gateway IP address the default grouping uses is 192.168.1.1, and then the second grouping uses 192.168.1.1 as the gateway IP address, and the others follow by analogy.

4.3.19 Multicast

IGMP Configuration

Click “ Advanced Setup” -> “ Multicast” to enter the IGMP Configuration screen.

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="3"/>
Query Interval(s):	<input type="text" value="125"/>
Query Response Interval(s):	<input type="text" value="10"/>
Last Member Query Interval(s):	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="25"/>
Maximum Multicast Data Sources for IGMPv3 : (1 - 24):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="25"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:	<input checked="" type="checkbox"/>

[Apply/Save](#)

You can configure IGMP parameters on this screen, if you are not clear about the IGMP, we recommend using the default configuration.

If you want to modify the configured parameters, please make sure whether the router's IGMP feature is enabled.

4.3.20 Diagnostics

Through the Diagnostics function, you can check connection status of the router's interfaces. When a connection is successfully established, its status displays a "PASS", otherwise it displays a "FAIL" click ". To enter the page below, click the "Diagnostics" tab on the left navigation menu column:

ipoe_eth3 Diagnostics

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

Test the connection to your local network

Test your eth0 Connection:	PASS	Help
Test your eth1 Connection:	FAIL	Help
Test your eth2 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your Internet service provider

Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

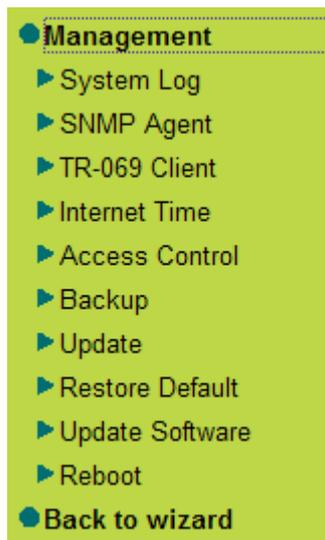
Test

Test With OAM F4

If you are not clear about the test result, please click "Help" for mor details.

5. Management

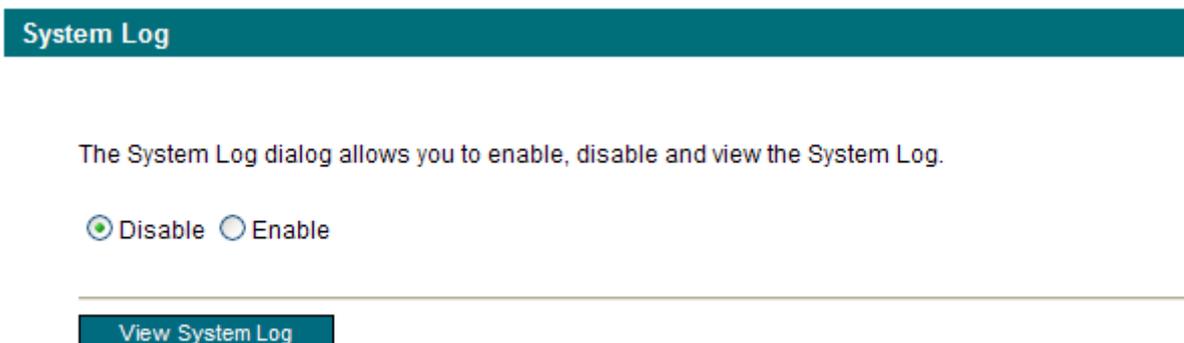
Management settings include: system log, TR-069 client, Internet time, access control, backup, update, restore default , update software and reboot, as shown in the picture below.



5.1 System log

System log records the running status of SP3367NL, such as ADSL dial-up procedure and data packets records and so on. To view the log, please follow the steps below.

1. Click “ System Log” to enter the “ System Log” screen and click the radio button before “ Enable” (Note: The function is disabled by system default).



2. Click “ View System Log” and you can check the logs on the appearing screen.

System Log

Date/Time	Facility	Severity	Message
Jan 1 01:06:28	syslog	emerg	BCM96345 started: BusyBox v1.00 (2011.08.17-03:29+0000)
Jan 1 01:06:28	user	notice	kernel: klogd started: BusyBox v1.00 (2011.08.17-03:29+0000)
Jan 1 01:06:28	user	notice	kernel: Linux version 2.6.30 (root@linux-ivan) (gcc version 4.4.2 (Buildroot 2010.02-git)) #1 Wed Aug 17 11:26:27 CST 2011
Jan 1 01:06:28	user	notice	kernel: Kernel command line: root=31:0 ro noinitrd console=ttyS0,115200
Jan 1 01:06:28	user	crit	kernel: eth0 Link UP 100 mbps full duplex
Jan 1 01:06:28	user	crit	kernel: eth2 Link UP 100 mbps full duplex

[Refresh](#) [Close](#)

5.2 SNMP Agent

SNMP - Configuration

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

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

SNMP Agent	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Read Community:	<input type="text" value="public"/>
Set Community:	<input type="text" value="private"/>
System Name:	<input type="text" value="Broadcom"/>
System Location:	<input type="text" value="unknown"/>
System Contact:	<input type="text" value="unknown"/>
Trap Manager IP:	<input type="text" value="0.0.0.0"/>

[Save/Apply](#)

Read Community

Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

Set Community

Specify the password for the incoming Set requests from the management station.

Trap Manager IP

Specify the IP address of the station to send the SNMP traps to.

5.3 TR-069 client

TR-069 client is used to implement remote centralized management over the SP3367NL from the Internet (Note: to use this function, there must be a remote centralized manager), the configuration steps are as follows:

1. Click “ TR-069 client” to enter the “ TR-069 client – Configuration” screen.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Apply/Save

GetRPCMethods

2. Click “ Enable” to open the function. The default is disabled.

Disable Enable
 Inform Interval:
 ACS URL:
 ACS User Name:
 ACS Password:
 WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable
 Connection Request Authentication
 Connection Request User Name:
 Connection Request Password:
 Connection Request URL:

3. Enter the Inform Interval which is 300, ACS URL (the domain name of the Auto-Configure Server), ACS User name, ACS Password and WAN Interface used by TR-069 client as the picture below.

Disable Enable
 Inform Interval:
 ACS URL:
 ACS User Name:
 ACS Password:
 WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable
 Connection Request Authentication
 Connection Request User Name:
 Connection Request Password:
 Connection Request URL:

4. Disable “ Display SOAP messages on serial console” , and uncheck “ Connection Request Authentication” , then click” Apply/Save” .

Disable Enable
 Inform Interval:
 ACS URL:
 ACS User Name:
 ACS Password:
 WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable
 Connection Request Authentication
 Connection Request User Name:
 Connection Request Password:
 Connection Request URL:

5.4 Internet Time

Internet time synchronization is used to update the router's system time so that the router's system time accords with the Internet time. The default setting selects "Automatically synchronize with Internet time servers", as shown in the picture below.

Time settings

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

Automatically synchronize with Internet time servers

First NTP time server:
 Second NTP time server:
 Third NTP time server:
 Fourth NTP time server:
 Fifth NTP time server:

Time zone offset:

Note: NTP time server is used to update the time. Select “ Time zone offset” as the time zone where you are.

5.5 Access Control

This screen allows you to change the device’ s login password which is admin by default.

1. Click “ Access Control” to enter the “ Access Control-Passwords” screen.

Access Control -- Passwords

Access to your broadband router is controlled through user accounts: admin

- The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.
- Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords.
Note: Password cannot contain a space.

User Name:	<input type="text" value="admin"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

Apply/Save

2. Enter the router’ s current login password in the old password textbox.
3. Enter the password you wish to set in the new password and confirm password textboxes.
4. After clicking Apply/Save, the login dialog will pop up.
5. Enter the new password you have set to re-enter the router’ s setup wizard screen.

Micronet SP3367NL
11n 150Mbps WLAN ADSL2+ Modem Router
Version No.:Ver1.0

Advanced
Settings



Line connected

Status Connect Status : Disconnect

Network VPI/VCI Settings: (VPI/VCI)

PPPOE User Name:

PPPOE Password:

Wireless Key:

Password:

ok

5.6 Backup

With backup settings, you can back up your router' s configuration. The steps are as follows:

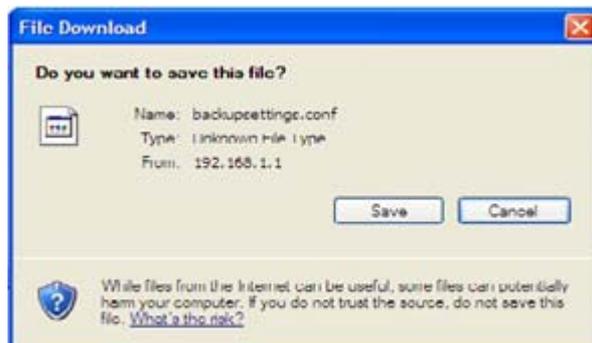
1. Click “ Backup” to enter the “ Settings—Backup” screen.

Backup

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

Backup Settings

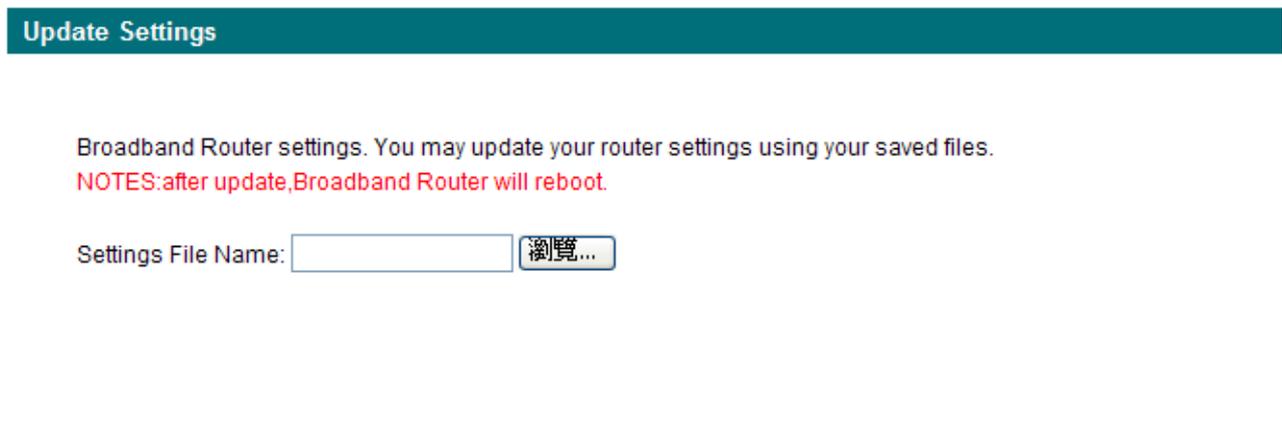
2. Click the “ Backup settings” button, and click “ Save” on the appearing “ File Download” dialog to export the router' s configuration file.



5.7 Update

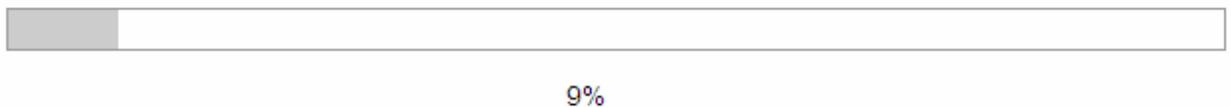
This function enables you to import the previous backup file with ease. The steps are as follows:

1. Click the “ Update” menu to display the “ Tools—Update Settings” screen.



2. Click “ Browse” to select the file you want to import.
3. Click “ Update settings” to import the configuration and the device will reboot.

Uploading is in progress. The Broadband Router will reboot upon completion. This process will take about 2 minutes,and then it will automatically renew the web page



5.8 Restore default

If you have made some illegal operation on the device, you will be unable to access the Internet. This feature enables you to restore the device to factory default settings.

1. Click “ Restore Default” to display the “ Tools -- Restore Default Settings ” screen.

Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Restore Default Settings

2. Click the Restore Default Settings button, and click “ Ok” on the appearing dialog.

Restore Default Settings



Restore Default Settings

3. After clicking “ Ok” , you will see the procedure bars.

Broadband Router Restore

The Broadband Router configuration has been restored to default settings and the router is rebooting. It will take about 1 minute. If necessary, reconfigure your PC's IP address to match your new configuration.



6%

5.9 Update Software

Update Software enables you to upgrade the device to improve its system stability. The upgrade steps are as follows:

1. Click “ Update Software” to display the “ Tools -- Update Software” screen.

Update Software

Step 1: Obtain an updated software image file from website of your product manufacturer .

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

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

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

Software File Name:

Update Software

2. Click the “ Browse” button to select the upgrade file and then click “ Update Software” .

3. After clicking the “ Update Software” , it comes to the upgrade screen. The progress takes about 2 minutes.

Uploading is in progress. The Broadband Router will reboot upon completion. This process will take about 2 minutes, and then it will automatically renew the web page



5.10 Reboot

To reboot the router, click “ Management” ----“ Reboot” to enter the page below, and then click the “ Reboot” button there.

Reboot Device

Click the button below to reboot the router.

[Reboot](#)

Exit

Select the Exit menu and click Ok on the appearing dialog to log out from the router's web-based utility.



Back to Wizard

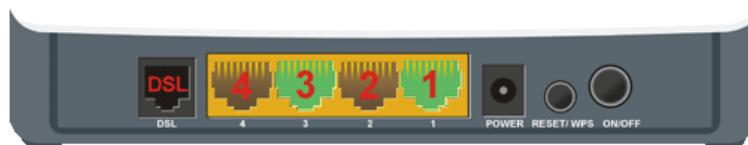
Click Back to Wizard menu, you will come back to the router's setup wizard screen as shown in the screen below:

Micronet SP3367NL

11n 150Mbps WLAN ADSL2+ Modem Router

Version No.:Ver1.0

[Advanced Settings](#)



 Line connected

Status

Connect Status : **Unconfigured**

Network

VPI/VCI Settings: (VPI/VCI:)

PPPOE User Name:

PPPOE Password:

Wireless

Key:

Password:

[ok](#)

10Base-T

It is an Ethernet standard for Local Area Network (LAN). 10Base-T uses a twisted pair cable with maximum length of 100 meters.

AAL

ATM Adaptation Layer that defines the rules governing segmentation and reassembly of data into cells. Different AAL types are suited to different traffic classes.

ADSL

Asymmetric Digital Subscriber Line, as its name showing, is an asymmetrical data transmission technology with high traffic rate downstream and low traffic rate upstream. ADSL technology satisfies the bandwidth requirement of applications, which demand “asymmetric” traffic, such as web surfing, file download and Video-on-demand (VOD).

ATM

Asynchronous Transfer Mode is a layer 2 protocol supporting high-speed asynchronous data with advanced traffic management and quality of service features.

bps

Bits per second, a standard measurement of digital transmission speeds.

Bridge

Bridge is a device that connects multiple physical networks and forward packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are: repeaters which simply forward electrical signals from one cable to the other and full-fledged routers which make routing decisions based on several criteria.

CPE

Customer Premises Equipment, such as ADSL router, USB modem.

Default Gateway (Router)

Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device

has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP

Dynamic Host Configuration Protocol, this protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address

DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as `www.Broadbandrouter.com`) and one or more IP addresses (such as `192.34.45.8`). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "`Broadbandrouter.com`" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL

Digital Line Subscriber (DSL) technology provides high-speed access over twisted copper pair for connection to the Internet, LAN interfaces, and to broadband services such as video-on-demand, distance learning, and video conferencing.

Ethernet

It is a standard for computer networks. Ethernet networks are connected by special cables and hubs or switches, and move data around at up to 10/100 million bits per second (Mbps).

FTP

File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.

Idle Timeout

Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

ISP

Internet Service Provider is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

ISP Gateway Address

The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

LAN

Local Area Network is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address

MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT

Network Address Translator is defined by RFC 1631. Enable a LAN network to use one set of IP address for internal traffic. A NAT box located where the LAN meets the Internet provides the necessary IP address translation. This helps provide a sort of firewall and allow for a wider address range to be used internally without danger of conflict. Using the router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port

Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21

SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPP

PPP is the Point-to-Point-Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoA (RFC 2364)

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol data grams over point-to-point links. This document describes the use of ATM Adaptation Layer 5 (AAL5) for framing PPP encapsulated packets.

PPPoE (RFC 2516)

This document describes how to build PPP sessions and encapsulate PPP packets over Ethernet. PPP over Ethernet (PPPoE) provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator.

Protocol

A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

PVC

Permanent Virtual Circuit, connection-oriented permanent leased line circuit between end-stations on a network over a separate ATM circuit.

RFC

Request for Comments. The document (begun in 1969) is for describing the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

RFC 1483

Multi-protocol encapsulation over AAL-5. Two encapsulation methods for carrying network interconnect traffic over ATM AAL-5. The first method allows multiplexing of multiple protocols over a single ATM virtual circuit. The protocol of a carried PDU is identified by prefixing the PDU by an IEEE 802.2 Logical Link Control (LLC) header. This method is in the following called "LLC Encapsulation". The second method does higher-layer protocol multiplexing implicitly by ATM Virtual Circuits (VCs). It is in the following called "VC Based Multiplexing".

Router

A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics."

Subnet Mask

A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP

Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

TELNET

It is the virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and act as normal terminal users of that host.

VCI

Virtual Circuit Identifier is part of the ATM cell header. A VCI is a tag indicating the channel over which a cell will travel. The VCI of a cell can be changed as it moves between switches via Signaling.

VPI

Virtual Path Identifier is part of the ATM cell header. A VPI is a pipe for a number of Virtual Circuits.

WAN

Wide Area Network is a network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI)

Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

