



# **802.11n Wireless ADSL 2/2+ Router**

**ADN-4100**

---

---

**User's Manual**

---

---

## **Copyright**

Copyright© 2010 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## **Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

### **FCC Caution**

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

### **Federal Communication Commission (FCC) Radiation Exposure Statement**

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

### **R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

---

## WEEE Regulation



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## Energy Saving Note of the Device

This power required device does not support Standby mode operation.

For energy saving, please remove the power cable or push the power button to OFF position to disconnect the device from the power circuit.

Without removing power cable or Power off, the device will still consuming power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

## Revision

User's Manual for 802.11n Wireless ADSL 2/2+ Router

Model: ADN-4100

Rev: 1.0 (Sep. 2010)

Part No. EM-ADN4100\_v1

---

# Contents

1	Overview .....	1
1.1	Safety Precautions .....	1
1.2	LEDs and Interfaces .....	2
1.3	System Requirements .....	4
1.4	Features .....	4
2	Hardware Installation .....	6
3	Web Configuration .....	8
3.1	Accessing the Device .....	8
3.2	General Configuration .....	9
3.2.1	Wizard .....	10
3.2.2	Internet Setup .....	16
3.2.3	Wireless Setup .....	19
3.2.4	Local Network .....	27
3.2.5	Time and Date .....	31
3.2.6	Logout .....	32
3.3	Advanced Configuration .....	32
3.3.1	Advanced Wireless .....	32
3.3.2	Port Forwarding .....	40
3.3.3	DMZ .....	42
3.3.4	Parental Control .....	43
3.3.5	Filtering Options .....	47
3.3.6	QoS Config .....	52
3.3.7	Firewall Settings .....	56
3.3.8	DNS .....	57
3.3.9	Dynamic DNS .....	58
3.3.10	Network Tools .....	60
3.3.11	Routing .....	75
3.3.12	Schedules .....	79
3.3.13	Logout .....	80
3.4	Management .....	80
3.4.1	System .....	80
3.4.2	Firmware Update .....	82
3.4.3	Access Controls .....	83
3.4.4	Diagnostics .....	87

---

3.4.5	Log Configuration .....	87
3.4.6	Logout.....	88
3.5	Status.....	89
3.5.1	Device Information.....	89
3.5.2	Wireless Clients .....	91
3.5.3	DHCP Clients.....	91
3.5.4	Logs .....	91
3.5.5	Statistics.....	92
3.5.6	Route information .....	94
3.5.7	Logout.....	94

---

# 1 Overview

The ADN-4100 supports multiple line modes. It provides four 10/100Base-TX Ethernet interfaces at the user end. The device provides high speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net cafes and office users. It provides high performance access to the Internet, downstream up to 24 Mbps and upstream up to 1 Mbps.

The device supports WLAN access. It can connect to the Internet through a WLAN AP or WLAN device. It complies with IEEE 802.11, 802.11b/g/n specifications, WEP, WPA, and WPA2 security specifications.

## 1.1 Safety Precautions

Refer to the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use volume labels to mark the type of power.
- Use the power adapter packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace the power cords at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place the device on an unstable surface or support.

## 1.2 LEDs and Interfaces

### Front Panel

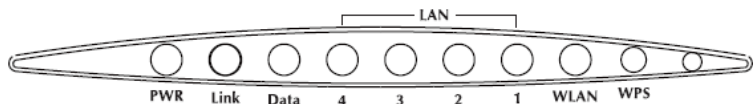


Figure 1 Front panel

The following table describes the LEDs of the device.

LED	Color	Status	Description
PWR	Green	On	The device is powered on and the initialization is normal.
		Off	The power is off.
	Red	On	The device is self-testing or self-testing is failed.
Link	Green	Slow Blinks	No signal is detected.
		Fast Blinks	The device is handshaking with the physical layer of the office.
		On	The device is connected to the physical layer of the office.
Data	Green	On	The Internet connection is normal in the routing mode (for example: PPP dial-up is successful), and no Internet data is being transmitted.
		Blinks	Internet data is being transmitted in the routing mode.
		Off	The device is in the bridge mode.
	Red	On	The Internet connection fails after successful synchronization in the routing mode (for example: PPP dial-up is failed).
LAN4-1	Green	On	The LAN connection is normal.
		Blinks	Data is being transmitted through the LAN interface, or the Internet data is being



LED	Color	Status	Description
			transmitted in the bridge mode.
		Off	The LAN connection is not established.
WLAN	Green	On	The WLAN connection has been activated.
		Blinks	Data is being transmitted through the WLAN interface.
		Off	The WLAN connection is not activated.
WPS	Green	Blinks	WPS is activated and the device is waiting for negotiation with the clients.
		Off	WPS is not activated.

## Rear Panel

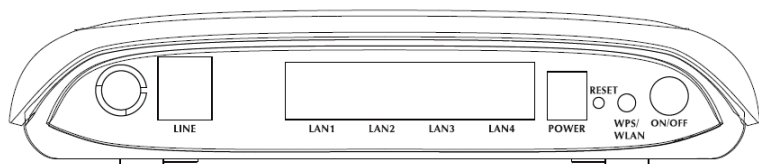


Figure 2 Rear panel

The following table describes the interfaces and buttons of the device.

Interface/Button	Description
LINE	RJ-11 interface, for connecting the interface of the telephone set through the telephone cable.
LAN1, LAN2, LAN3, LAN4	RJ-45 interface, for connecting the Ethernet interface of a computer or an Ethernet device.
POWER	Power interface, for connecting the interface of the power adapter.
RESET	Restore to factory defaults. To restore factory defaults, keep the device powered on, push a paper clip into the hole to press the button for over 3 seconds and then release.
WPS/ WLAN	<ul style="list-style-type: none"> <li>Press the button and hold it for 1 second, to enable WLAN.</li> <li>Press the button and hold it for 1 second to 3</li> </ul>

Interface/Button	Description
	seconds, it does not take effect. <ul style="list-style-type: none"> <li>● Press the button and hold it for 3 or more than 3 seconds, to initialize WPS negotiation.</li> </ul>
ON/OFF	Power switch, power on or off the device.

### 1.3 System Requirements

Recommended system requirements are as follows:

- A 10Base-T/100Base-TX Ethernet card is installed on your PC.
- A hub or switch is available for connecting one Ethernet interface on the device and several PCs.
- Operating system: Windows XP, Windows 2000, Windows ME, or Windows 98SE.
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

### 1.4 Features

The device supports the following features:

- IEEE802.11b/g/n
- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- 1483 Bridged, 1483 Routed, and MER access
- Multiple PVCs (up to eight) that can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Binding of ports with PVCs
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAPT
- Static routing
- Firmware upgrade through Web or TFTP

- 
- Restore to the factory defaults
  - DNS
  - Virtual server
  - DMZ
  - Three-level user accounts
  - Web user interface
  - Telnet CLI
  - System status displaying
  - PPP session PAP, CHAP, and MS-CHAP
  - IP filter
  - IP QoS
  - Remote access control
  - Line connection status test
  - Remote management through telnet or HTTP
  - Backup and restoration of configuration file
  - Ethernet interface supports crossover detection, auto-correction and polarity correction
  - UPnP
  - PPTP VPN
  - IPSec VPN

---

## 2 Hardware Installation

**Step 1** Connect the **LINE** interface of the device and the **Modem** interface of the splitter with a telephone cable. Connect the phone set to the **Phone** interface of the splitter through a telephone cable. Connect the input cable to the **Line** interface of the splitter.

The splitter has three interfaces:

- **Line:** Connect to a wall phone interface (RJ-11 jack).
- **Modem:** Connect to the **LINE** interface of the device.
- **Phone:** Connect to a telephone set.

**Step 2** Connect the **LAN** interface of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).



**Note:**

Use the twisted-pair cable to connect the hub or switch.

**Step 3** Insert one end of the power adapter to the wall outlet and connect the other end to the **POWER** interface of the device.

Connection 1: Figure 3 shows the connection of the device, PC, splitter, and telephone sets, when no telephone set is placed before the splitter. This type of connection is recommended.

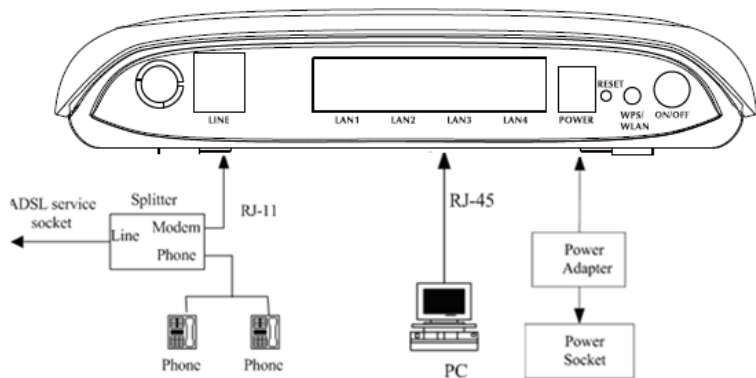


Figure 3 Connection diagram (without a telephone set before the splitter)

Connection 2: Figure 4 shows the connection of the device, PC, splitter, and telephone sets, when a telephone set is placed before the splitter.

As illustrated in the following figure, the splitter is installed close to the device:

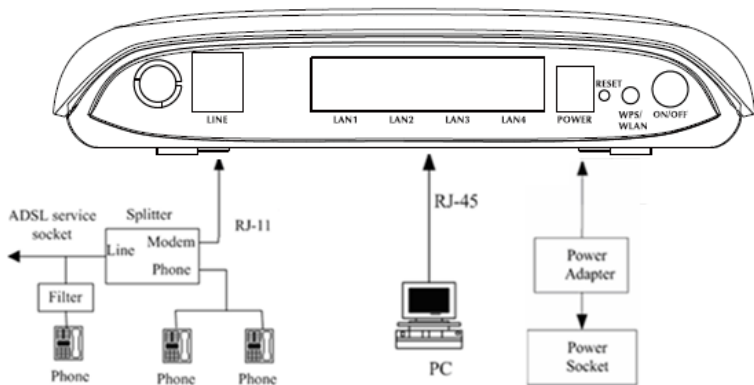


Figure 4 Connection diagram (with a telephone set before the splitter)



**Note:**

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure 4. Do not use a splitter to replace the filter.

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, failure of Internet access, or slow connection speed. If you need to add a telephone set before the splitter, you must add a microfilter before the telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

---

## 3 Web Configuration

This chapter describes how to configure the device by using the Web-based configuration utility.

### 3.1 Accessing the Device

The following describes how to access the device for the first time in detail.

**Step 1** Open the Internet Explorer (IE) browser and enter <http://192.168.1.1> in the address bar.

**Step 2** The **LOGIN** page as shown in the following figure appears:



The screenshot shows the login interface for PLANET Networking & Communication. The background is blue with a globe icon and the text 'PLANET Networking & Communication'. The main content area is white and contains the following elements:

- Title: **Input username and password**
- UserName: A dropdown menu with 'admin' selected.
- Password: A text input field with six dots representing the password.
- Login: A button labeled 'Login'.

In this page, enter the user name and the password. Then, click login.

- The user name and the password of the super user are **admin** and **admin** respectively.
- The user name and the password of the normal user are **user** and **user** respectively.

If you log in as the super user successfully, the page as shown in the following figure appears:

**PLANET** Networking & Communication **802.11n ADSL 2/2+ Router** Welcome admin, Logout

Setup Advanced Management Status Help

Setup  
Wizard  
Internet Setup  
Wireless  
Local Network  
Time and Date  
Logout

SETTING UP YOUR INTERNET

There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.

Please make sure you have your ISP connection settings first if you choose manual setup.

INTERNET CONNECTION WIZARD

You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

If the login information is incorrect, the page as shown in the following figure appears:



Click **OK** to log in again.



**Note:**

In the LAN, you can use either of the following two levels of user accounts (displayed in the user name/password format) to access the device:  
**admin/admin** and **user/user**.

In the WAN, you can use one of the following three levels of user accounts (displayed in the user name/password format) to access the device:  
**admin/admin**, **user/user**, and **support/support**.

## 3.2 General Configuration

## 3.2.1 Wizard

**Wizard** helps you to fast and accurately configure Internet connection and other important parameters. The following sections describe these various configuration parameters.

When subscribing to a broadband service, be aware of the Internet connection mode. The physical WAN device can be Ethernet, DSL, or both. Technical information about properties of Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, and the protocol, such as PPPoA or PPPoE, that you use to communicate on the Internet.

**Step 1** Choose **Setup > Wizard**. The page as shown in the following figure appears:

The screenshot shows the web interface for a Planet 802.11n ADSL 2/2+ Router. At the top, there is a navigation bar with the Planet logo and the text "802.11n ADSL 2/2+ Router". On the right side of the navigation bar, it says "Welcome admin, Logout". Below the navigation bar are five tabs: "Setup", "Advanced", "Management", "Status", and "Help". The "Setup" tab is selected and highlighted in blue. On the left side, there is a vertical menu with the following items: "Setup", "Wizard", "Internet Setup", "Wireless", "Local Network", "Time and Date", and "Logout". The "Wizard" item is highlighted in blue. The main content area is titled "SETTING UP YOUR INTERNET" and contains the following text: "There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection." Below this text, it says "Please make sure you have your ISP connection settings first if you choose manual setup." There is a horizontal line below this text. Below the line, the section is titled "INTERNET CONNECTION WIZARD" and contains the text: "You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin." Below this text is a button labeled "Setup Wizard". At the bottom of the main content area, there is a note: "Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router."

**Step 2** Click **Setup Wizard**. The page as shown in the following figure appears:



## WELCOME TO SETUP WIZARD

This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.

- **Step 1:** Set Time and Date
- **Step 2 :** Setup Internet Connection
- **Step 3:** Configure Wireless Network
- **Step 4:** Completed and Quit

There are four steps to configure the device. Click **Next** to continue.

### Step 3 Set the time and date. Then, click **Next**.

#### STEP 1: SET TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

#### TIME SETTING

**Automatically synchronize with Internet time servers**

1st NTP time server :

2nd NTP time server :

#### TIME CONFIGURATION

Time Zone:

**Enable Daylight Saving**

Daylight Saving Start :  Year  Mon  Day  Hour  Min  Sec

Daylight Saving End :  Year  Mon  Day  Hour  Min  Sec

### Step 4 Configure the Internet connection.

Select the protocol and the encapsulation mode. Set the VPI and the VCI.

If the **Protocol** is set to **PPPoE** or **PPPoA**, the page as shown in the following figure appears:

**STEP 2: SETUP INTERNET CONNECTION**

---

Please select your ISP (Internet Service Provider) from the list below.

Protocol :

Encapsulation Mode:

VPI :  (0-255)

VCI :  (32-65535)

Encapsulation Mode:

---

**PPPOE/PPPOA**

---

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue

Username:

Password :

Confirm Password :

You need to enter the user name and password for PPPoE or PPPoA dialup.

If the **Protocol** is set to **Dynamic IP**, the page as shown in the following figure appears:

**STEP 2: SETUP INTERNET CONNECTION**

---

Please select your ISP (Internet Service Provider) from the list below.

Protocol :

Encapsulation Mode:

VPI :  (0-255)

VCI :  (32-65535)

Encapsulation Mode:

---

---

If the **Protocol** is set to **Static IP**, the page as shown in the following figure appears:

**STEP 2: SETUP INTERNET CONNECTION**

---

Please select your ISP (Internet Service Provider) from the list below.

**Protocol:**

**Encapsulation Mode:**

**VPI:**  (0-255)

**VCI:**  (32-65535)

**Encapsulation Mode:**

---

**STATIC IP**

---

You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.

The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.

Click Next to continue.

**IP Address:**

**Subnet Mask:**

**Default Gateway:**

**Primary DNS Server:**

You need to enter the information of the IP address, subnet mask, and gateway.

If the **Protocol** is set to **Bridge**, the page as shown in the following figure appears:

## STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol: Bridge  
Encapsulation Mode: LLC  
VPI: 0 (0-255)  
VCI: 35 (32-65535)  
Encapsulation Mode: Scan

Back Next Cancel

If you click **Scan**, the system automatically searches the available PVCs.

## STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol: Bridge  
Encapsulation Mode: LLC  
VPI: 0 (0-255)  
VCI: 35 (32-65535)  
Encapsulation Mode: Scan scan pvc0/43 ...

Back Next Cancel

After the searching is complete, the result appears next to the **Scan** button.

## STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol: Bridge  
Encapsulation Mode: LLC  
VPI: 0 (0-255)  
VCI: 35 (32-65535)  
Encapsulation Mode: Scan no fitable pvc

Back Next Cancel

After setting, click **Next**.

**Step 5** Configure the wireless network. Enter the information and click **Next**.

**STEP 3: CONFIGURE WIRELESS NETWORK**

---

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.

**Enable Your Wireless Network :**

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

**Wireless Network Name (SSID) :**

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.

**Visibility Status :**  Visible  Invisible

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

<i>None</i>	<i>Security Level</i>		<i>Best</i>
<input checked="" type="radio"/> None	<input type="radio"/> WEP	<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK

**Security Mode:**None  
Select this option if you do not want to activate any security features.

---

**Step 6** View the configuration information of the device. To modify the information, click **Back**. To effect the configuration, click **Next**.

#### STEP 4: COMPLETED AND RESTART

Setup complete. Click "Back" to review or modify settings.

If your Internet connection does not work, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

#### SETUP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	1
NTP Server 1:	
NTP Server 2:	
Time Zone:	+00:00
Daylight Saving Time :	0
VPI / VCI :	0/35
Protocol :	Bridge
Connection Type :	LLC
Wireless Network Name (SSID) :	ADN-4100
Visibility Status :	0
Encryption :	None
Pre-Shared Key :	
WEP Key:	



#### Note:

In each step of the Wizard page, you can click **Back** to review or modify the previous settings or click **Cancel** to exit the wizard.

### 3.2.2 Internet Setup

Choose **Setup > Internet Setup**. The page as shown in the following figure appears:

## INTERNET SETUP

Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

## WAN SETUP

VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action
---------	---------	-------	--------------	----------	-------	--------	-----------------	--------

In this page, you can configure the WAN interface of the device.  
Click **Add** and the page as shown in the following figure appears:

## INTERNET SETUP

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

### ATM PVC CONFIGURATION

VPI :  (0-255)  
VCI :  (32-65535)  
Service Category : UBR With PCR   
Peak Cell Rate :  (cells/s)  
Sustainable Cell Rate :  (cells/s)  
Maximum Burst Size :  (cells)

### CONNECTION TYPE

Protocol :  Bridging   
Encapsulation Mode: LLC   
802.1Q VLAN ID :  (0=disable, 1 - 4094)

### NETWORK ADDRESS TRANSLATION SETTINGS

Enable Bridge Service :   
Service Category :

The following table describes the parameters in this page.

Field	Description
-------	-------------

Field	Description
<b>ATM PVC CONFIGURATION</b>	
VPI	Virtual Path Identifier (VPI) is the virtual path between two points in an ATM network. Its value range is from 0 to 255.
VCI	Virtual Channel Identifier (VCI) is the virtual channel between two points in an ATM network. Its value range is from 32 to 65535 (0 to 31 is reserved for local management of ATM traffic).
Service Category	Select <b>UBR with PCR</b> , <b>UBR without PCR</b> , <b>CBR</b> , <b>Non Realtime VBR</b> , or <b>Realtime VBR</b> from the drop-down list.
Peak Cell Rate	Set the maximum transmission rate of the cell in ATM transmission.
Sustainable Cell Rate	Set the minimum transmission rate of the cell in ATM transmission.
Maximum Burst Size	Set the maximum burst size of the cell in ATM transmission.
<b>CONNECTION TYPE</b>	
Protocol	Select <b>PPP over ATM (PPPoA)</b> , <b>PPP over Ethernet (PPPoE)</b> , <b>MAC Encryption Routing (MER)</b> , <b>IP over ATM (IPoA)</b> , or <b>Bridging</b> from the drop-down list.
Encapsulation Mode	Select <b>LLC</b> or <b>VCMUX</b> from the drop-down list. Usually, you can select <b>LLC</b> .
802.1Q VLAN ID	If you enter a value, packets from the interface is tagged with the set 802.1q VLAN ID. Its value range is 0-4094, while <b>0</b> indicates to disable this function.
<b>NETWORK ADDRESS TRANSLATION SETTINGS</b>	
Enable Bridge Service	Select or deselect the check box to enable or disable the WAN connection.
Service Category	The name to identify the WAN connection. You need not modify it.

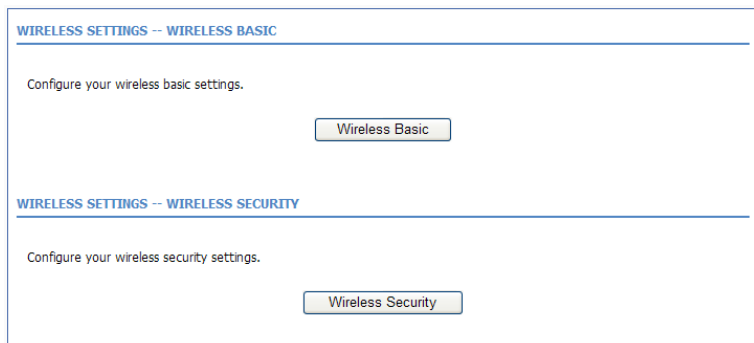


---

### 3.2.3 Wireless Setup

This section describes the wireless LAN and some basic configuration. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points that bridge network traffic to a wired LAN.

Choose **Setup > Wireless**. The **WIRELESS SETTINGS** page as shown in the following figure appears:



#### 3.2.3.1 Wireless Basics

In the **WIRELESS SETTINGS** page, click **Wireless Basic**. The page as shown in the following figure appears:

## WIRELESS BASIC

Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

### WIRELESS NETWORK SETTINGS

Enable Wireless:

Enable MultiAP Isolation:

Wireless Network Name (SSID):

Visibility Status:  Visible  Invisible

Channel:

Channel Number:

802.11 Mode:

Band Width:

Please take note of your SSID as you will need to duplicate the same settings to your wireless devices and PC.

In this page, you can configure the parameters of wireless LAN clients that may connect to the device.

The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select or deselect the check box to enable or disable the wireless function.
Enable MultiAP Isolation	Select or deselect the check box to enable or disable multiAP isolation. If this function is enabled, clients of different SSIDs cannot access each other.
Wireless Network Name (SSID)	Network name. It can contain up to 32 characters. It can consist of letters, numerals, and/or underlines.
Visibility Status	<ul style="list-style-type: none"><li>● <b>Visible</b> indicates that the device broadcasts the SSID.</li><li>● <b>Invisible</b> indicates that the device does not broadcast the SSID.</li></ul>
Channel	You can select from the drop-down list: <b>FCC(1-11)</b> , <b>ETSI(1-13)</b> , <b>JP(1-14)</b>
Channel Number	Select the wireless channel used by the device from the drop-down list. You can select <b>Auto Scan</b> or a

Field	Description
	value from <b>CH1—CH13</b> . <b>Auto Scan</b> is recommended.
802.11 Mode	Select the 802.11 mode of the device from the drop-down list. The device supports 802.11b, 802.11g, 802.11n, 802.11b/g, 802.11n/g, and 802.11b/g/n.
Band Width	You can set the bandwidth only in the 802.11n mode. You can set the bandwidth of the device to <b>20M</b> or <b>40M</b> .

Click **Apply** to save the settings.

### 3.2.3.2 Wireless Security

In the **WIRELESS SETTINGS** page, click **Wireless Security**. The page as shown in the following figure appears:

**WIRELESS SECURITY**

---

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

---

**WIRELESS SECURITY MODE**

---

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and the wired network. This device provides the following encryption modes: **None**, **WEP**, **Auto (WPA or WPA2)**, **WPA2 Only**, and **WPA Only**.

### WEP

If the **Security Mode** is set to **WEP**, the page as shown in the following figure appears:

## WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

### WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

### WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length :

Choose WEP Key:

WEP Key1:

WEP Key2:

WEP Key3:

WEP Key4:

Authentication :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

The following table describes the parameters in this page.

Field	Description
WEP Key Length	You can select <b>64 bits</b> or <b>128 bits</b> from the drop-down list. <ul style="list-style-type: none"><li>● If you select <b>64 bits</b>, you need to enter 10 hexadecimal numbers or 5 characters.</li></ul>

Field	Description
	<ul style="list-style-type: none"> <li>● If you select <b>128 bits</b>, you need to enter 26 hexadecimal numbers or 13 characters.</li> </ul>
Choose WEP Key	Select the WEP key from the drop-down list. Its value range is 1—4.
WEP Keys 1—4	Set the 64 bits or 128 bits key, in the format of Hex or ASCII.
Authentication	Select the authentication mode from the drop-down list. You can select <b>Open</b> or <b>Share Key</b> .

Click **Apply** to save the settings.

### **Auto (WPA or WPA2)**

If the **Security Mode** is set to **Auto (WPA or WPA2)**, the page as shown in the following figure appears:

## WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

### WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

### WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

### PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

The following table describes the parameters in this page.

Field	Description
WPA Mode	You can select <b>Auto (WPA or WPA2)-PSK</b> or <b>Auto (WPA or WPA2)-Enterprise</b> from the drop-down list.
Group Key Update Interval	Set the interval for updating the key.
Pre-Shared Key	Set the preshared key to identify the workstation.

If the **WPA Mode** is set to **Auto (WPA or WPA2)-Enterprise**, the page as shown in the following figure appears:

### WIRELESS SECURITY

---

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

---

### WIRELESS SECURITY MODE

---

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

**Security Mode :**  ▼

---

### WPA

---

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

**WPA Mode :**  ▼

**Group Key Update Interval :**

---

### EAP (802.1X)

---

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

**RADIUS server IP Address :**

**RADIUS server Port :**

**RADIUS server Shared Secret :**

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

You need to enter the IP address, port, shared key of the RADIUS server. Click **Apply** to save the settings.

## WPA2 Only

If the **Security Mode** is set to **WPA2 only**, the page as shown in the following figure appears:

### WIRELESS SECURITY

---

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

---

### WIRELESS SECURITY MODE

---

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

**Security Mode :**

---

### WPA

---

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

**WPA Mode :**

**Group Key Update Interval :**

---

### PRE-SHARED KEY

---

**Pre-Shared Key :**

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Parameters in this page are similar to those in the page for **Auto (WPA or WPA2)**.

Click **Apply** to save the settings.

## WPA Only

If the **Security Mode** is set to **WPA only**, the page as shown in the following figure appears:



## WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

### WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

### WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

### PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Parameters in this page are similar to those in the page for **Auto (WPA or WPA2)**.

Click **Apply** to save the settings.

## 3.2.4 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings of the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP in your

---

LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if the IP address of the device changes.

You can also enable the secondary LAN IP address. The primary and the secondary LAN IP addresses must be in different network segments.

Choose **Setup > Local Network**. The **LOCAL NETWORK** page as shown in the following figure appears:

## LOCAL NETWORK

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

## ROUTER SETTINGS

Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :   
Subnet Mask :   
Domain Name :

Configure the second IP Address and Subnet Mask for LAN

IP Address :   
Subnet Mask :

## DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server

DHCP IP Address Range :  to

DHCP Lease Time :  (seconds)

## DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address
--------	---------------	-------------	------------

## NUMBER OF DYNAMIC DHCP CLIENTS :1

Computer Name	MAC Address	IP Address	Expire Time
gj558d	00:11:2f:68:de:69	192.168.1.2	42844

By default, **Enable DHCP Server** is selected for the LAN interface of the device. DHCP service provides IP settings to workstations configured to automatically obtain IP settings that are connected to the device through the Ethernet port.

When the device is used for DHCP, it becomes the default gateway for DHCP client connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.

Click **Apply** to save the settings.

In the **LOCAL NETWORK** page, you can assign LAN IP addresses for specific computers according to their MAC addresses.

The screenshot shows a table titled "DHCP RESERVATIONS LIST". The table has four columns: "Status", "Computer Name", "MAC Address", and "IP Address". Below the table are three buttons: "Add", "Edit", and "Delete".

Click **Add** to add static DHCP reservation. The page as shown in the following figure appears:

The screenshot shows a form titled "ADD DHCP RESERVATION (OPTIONAL)". It contains the following fields: "Enable" with a checkbox, "Computer Name" with a text input field, "IP Address" with a text input field, and "MAC Address" with a text input field. At the bottom of the form are two buttons: "Apply" and "Cancel".

The following table describes the parameters in this page.

Field	Description
Enable	Select the check box to reserve the IP address for the designated PC with the configured MAC address.
Computer Name	Enter the computer name. It helps you to recognize the PC with the MAC address. For example, Father's Laptop.
IP Address	Enter the IP address of the computer.
MAC Address	Enter the MAC address of the computer.

Click **Apply** to save the settings.

After the DHCP reservation information is saved, the DHCP reservations list displays the information.

If the DHCP reservations list is not empty, you can select one or more items and click **Edit** or **Delete**.

The **NUMBER OF DYNAMIC DHCP CLIENTS** page displays the DHCP clients (PCs or Laptops) currently connected to the device and the detailed information of the connected computers.

**NUMBER OF DYNAMIC DHCP CLIENTS :1**

Computer Name	MAC Address	IP Address	Expire Time
g558d	00:11:2f:68:de:69	192.168.1.2	42844

### 3.2.5 Time and Date

Choose **Setup > Time and Date**. The **TIME AND DATE** page as shown in the following figure appears:

**TIME AND DATE**

---

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed

---

**TIME SETTING**

**Automatically synchronize with Internet time servers**

1st NTP time server :

2nd NTP time server :

---

**TIME CONFIGURATION**

Current Local Time: 2000-01-01 00:12:53

Time Zone:  ▼

**Enable Daylight Saving**

Daylight Saving Start: 2000 Year 04 Mon 01 Day 02 Hour 00 Min 00 Sec

Daylight Saving End: 2000 Year 09 Mon 01 Day 02 Hour 00 Min 00 Sec

In the **TIME AND DATE** page, you can configure, update, and maintain the time of the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also set daylight saving time to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.

---

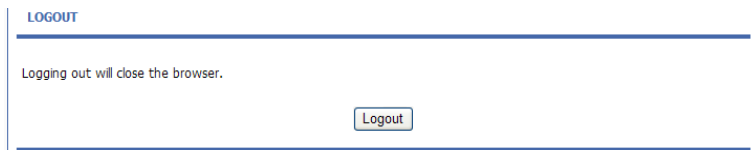
Select the appropriate time server and the time zone from the corresponding drop-down lists.

Select **Enable Daylight Saving** if necessary. Enter the correct the start and end time of the daylight saving.

Click **Apply** to save the settings.

### 3.2.6 Logout

Choose **Setup > Logout**. The page as shown in the following figure appears:



Click **Logout** to log out of the configuration page.

## 3.3 Advanced Configuration

This section contains advanced features used for network management, security and administrative tools to manage the device. You can view the status and other information of the device, to examine the performance and troubleshoot.

### 3.3.1 Advanced Wireless

This function is used to modify the standard 802.11g wireless settings. It is recommended not changing the default settings, because incorrect settings may affect the performance of the wireless performance. The default settings provide the best wireless performance in most environments.

Choose **Advanced > Advanced Wireless**. The **ADVANCED WIRELESS** page as shown in the following figure appears:

---

#### ADVANCED WIRELESS -- ADVANCED SETTINGS

---

Allows you to configure advanced features of the wireless LAN interface.

Advanced Settings

#### ADVANCED WIRELESS -- MAC FILTERING

---

Allows you to configure wireless firewall by denying or allowing designated MAC addresses.

MAC Filtering

#### ADVANCED WIRELESS -- SECURITY SETTINGS

---

Allows you to configure security features of the wireless LAN interface.

Security Settings

#### ADVANCED WIRELESS -- WPS SETTING

---

Allows you to configure wireless WPS.

WPS Setting

### 3.3.1.1 Advanced Settings

In the **ADVANCED WIRELESS** page, click **Advanced Settings**. The page as shown in the following figure appears:

## ADVANCED SETTINGS

These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. We does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

### ADVANCED WIRELESS SETTINGS

**Transmission Rate:** Auto  
**Multicast Rate:** Lower  
**Transmit Power:** 100%  
**Beacon Period:** 100 (20 ~ 1024)  
**RTS Threshold:** 2348 (0 ~ 2347)  
**Fragmentation Threshold:** 2345 (256 ~ 2346)  
**DTIM Interval:** 100 (1 ~ 255)  
**Preamble Type:** long

#### SSID

**Enable Wireless:**   
**SSID:** ADN-4100  
**Visibility Status:**  Visible  Invisible  
**User Isolation:** off  
**Disable WMM Advertise:** off  
**Max Clients:** 16 (1 ~ 32)

#### SSID-1

**Enable Wireless Guest Network:**   
**SSID:** VAP1  
**Visibility Status:**  Visible  Invisible  
**User Isolation:** off  
**Disable WMM Advertise:** off  
**Max Clients:** 16 (1 ~ 32)

#### SSID-2

**Enable Wireless Guest Network:**   
**SSID:** VAP2  
**Visibility Status:**  Visible  Invisible  
**User Isolation:** off  
**Disable WMM Advertise:** off  
**Max Clients:** 16 (1 ~ 32)

#### SSID-3

**Enable Wireless Guest Network:**   
**SSID:** VAP3  
**Visibility Status:**  Visible  Invisible  
**User Isolation:** off  
**Disable WMM Advertise:** off  
**Max Clients:** 16 (1 ~ 32)

Apply Cancel



The following table describes the parameters in this page.

Field	Description
<b>ADVANCED WIRELESS SETTINGS</b>	
Transmission Rate	Select the transmission rate of the wireless network from the drop-down list.
Multicast Rate	Select the multicast transmission rate of the wireless network from the drop-down list. You can select <b>Lower</b> or <b>Higher</b> .
Transmit Power	Select the power for data transmission from the drop-down list. You can select <b>100%</b> , <b>80%</b> , <b>60%</b> , <b>40%</b> , or <b>20%</b> .
Beacon Period	By default, the wireless beacon frame sends the data once every 100ms. Its value range is 20—1024.
RTS Threshold	The threshold of transmission request. Its value range is 0—2347 and the default value is 2346.
Fragmentation Threshold	Its value range is 256—2346 and the default value is 2345.
DTIM Interval	Data beacon proportion (transmission quantity indication). Its value range is 1—255 and the default value is 100.
Preamble Type	Select the preamble code from the drop-down list. You can select <b>long</b> or <b>short</b> .
<b>SSID</b>	
Enable Wireless	Select or deselect the check box to enable or disable the wireless function.
SSID	Set the wireless network name, that is, SSID. SSID is used to distinguish different wireless networks.
Visibility Status	Select whether to hide the AP. You can select <b>Visible</b> or <b>Invisible</b> . If you select <b>Invisible</b> , the AP is hidden and the terminal cannot obtain the SSID through passive scanning.
User Isolation	Select whether users of the AP can communicate with each other. You can select <b>Off</b> or <b>On</b> from the drop-down list. <b>On</b> indicates that computers connected to the device cannot communicate with each other.

Field	Description
Disable WMM Advertise	Select whether to disable WMM. You can select <b>Off</b> or <b>On</b> .
Max Clients	Set the maximum number of clients that can be connected to the AP at the same time. Its value range is 1—32.
<b>SSID1—3</b>	
Enable Wireless Guest Network	Select or deselect the check box to enable or disable the wireless interface.
SSID	Similar to the primary SSID, it identifies a wireless AP.

These settings are applicable only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

Click **Apply** to save the settings.

### 3.3.1.2 MAC Filtering

In the **ADVANCED WIRELESS** page, click **MAC Filtering**. The page as shown in the following figure appears:

**BLOCK MAC ADDRESS**

---

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

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC" 's MAC Address automatically displays the MAC address of the LAN device where the browser is running. To restrict another 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, open a command prompt window and type "ipconfig /all".

---

**BLOCK MAC ADDRESS**

Username	MAC	Schedule

Click **Add** and the page as shown in the following figure appears:

#### ADD SCHEDULE RULE

User Name:

Current PC's MAC Address:

Other MAC Address:

Schedule: **Always** [View Available Schedules](#)

Manual Schedule :

Day(s) :  All Week  Select Day(s)

Sun  Mon  Tue  Wed

Thu  Fri  Sat

All Day - 24 hrs

Start Time  :  (hour:minute, 24 hour time)

End Time  :  (hour:minute, 24 hour time)

The following table describes the parameters in this page.

Field	Description
User Name	Enter the name that identifies your configuration. For example, <i>kids</i> .
Current PC's MAC Address	Enter the MAC address of the computer that connects to the device.
Other MAC Address	Enter the MAC address of another device that is included in MAC filtering.
Schedule	Select the time of MAC filter from the drop-down list. You can select <b>Always</b> or <b>Never</b> .
Manual Schedule	If you select this check box, you need to manually set the time of MAC filtering.

Click **Apply** to save the settings.

### 3.3.1.3 Security Settings

In the **ADVANCED WIRELESS** page, click **Security Settings**. The page as shown in the following figure appears:

## WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

### WIRELESS SSID

Select SSID :

### WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Select the desired SSID from the drop-down list.

Select the encryption type from the **Security Mode** drop-down list. You can select **None**, **WEP**, **AUTO (WPA or WPA2)**, **WPA Only**, or **WPA2 Only**. For parameters of different encryption types, see section.3.2.3.2 Wireless Security. Click **Apply** to save the settings.

### 3.3.1.4 WPS Settings

In the **ADVANCED WIRELESS** page, click **WPS Setting**. The **WIRELESS WPS** page as shown in the following figure appears:

## WIRELESS WPS

WPS: The condition of use WPS, you can choose different auth mode in Security Setting page, and broadcast the SSID. The pin code will be saved when you press PIN button.

### WPS

Enabled :

Select SSID:

Push Button :

Input Station PIN :

WPS Session Status :

**Enabled:** The WPS service is enabled by default.



#### Note:

Ensure that the network card supports the WPS function.

You can use one of the following three methods to use WPS authentication:

- Press the **WPS** button on the side panel for 3 seconds.
- In the **WIRELESS WPS** page, click **PBC**. It has the same function of the **WPS** button on the side panel. This is an optional method on wireless clients.



#### Note:

You need a Registrar when using the PBC method in a special case in which the PIN is all zeros.

- In the **WIRELESS WPS** page, enter the **PIN** code provided by the station and click **PIN**. PIN entry is a mandatory method of setup for all WPS certified devices.



#### Note:

If you are using the PIN method, you need a Registrar, either an access point or a wireless router, to initiate the registration between a new device and an active access point or a wireless router.

## 3.3.2 Port Forwarding

This function is used to open ports in your device and re-direct data through these ports to a single PC in your network (WAN-to-LAN traffic). It allows remote users to access services in your LAN, such as FTP for file transfers or SMTP, and POP3 for e-mail. The device receives remote requests for these services at your public IP address. It uses the specified TCP or UDP protocol and port, and redirects these requests to the server on your LAN with the specified LAN IP address. Note that the specified private IP address must be within the available IP address range of the subnet where the device is in.

Choose **Advanced > Port Forwarding**. The page as shown in the following figure appears:

**PORT FORWARDING**

---

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a 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 of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

---

**PORT FORWARDING SETUP**

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Schedule Rule	Remote IP
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	-----------

Click **Add** to add a virtual server. See the following figure:

## PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a 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 of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

### PORT FORWARDING SETUP

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Schedule Rule	Remote IP
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	-----------

### PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

WAN Connection(s)

Server Name:

Select a Service:

Custom Server:

Schedule:  [View Available Schedules:](#)

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>

Select a service for a preset application or enter the name in the **Custom Server** field.

Enter an IP address in the **Server IP Address** field, to appoint the corresponding PC to receive forwarded packets.

The port table displays the ports that you want to open on the device. The **Protocol** indicates the type of protocol used by each port.

Click **Apply** to save the settings. The page as shown in the following figure appears. A virtual server is added.

**PORT FORWARDING**

---

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a 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 of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

---

**PORT FORWARDING SETUP**

	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Schedule Rule	Remote IP
<input type="checkbox"/>	AUTH	113	113	tcp	113	113	192.168.1.2	Always	

### 3.3.3 DMZ

Choose **Advanced** > **DMZ**. The page as shown in the following figure appears:



### DMZ

---

The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding 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

---

WAN Connection:

Enable DMZ:

DMZ Host IP Address

In this page, you can enable a DMZ host. In this way, access from Internet to the WAN IP address of the device is forwarded to the DMZ host and network server of the internal LAN is protected.

Click **Apply** to save the settings.

### 3.3.4 Parental Control

Choose **Advanced > Parental Control**. The **PARENTAL CONTROL** page as shown in the following figure appears:

### PARENTAL CONTROL -- BLOCK WEBSITE

---

Uses URL (i.e. www.yahoo.com) to implement filtering.

---

### PARENTAL CONTROL -- BLOCK MAC ADDRESS

---

Uses MAC address to implement filtering.

This page provides two useful tools for restricting Internet access. **Block Website** allows you to quickly create a list of websites that you wish to prevent

users from accessing. **Block MAC Address** allows you to control Internet access by clients or PCs connected to the device.

### 3.3.4.1 Block Website

In the **PARENTAL CONTROL** page, click **Block Website**. The page as shown in the following figure appears:

**BLOCK WEBSITE**

---

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

---

**BLOCK WEBSITE**

URL	Schedule
-----	----------

Click **Add**. The page as shown in the following page appears:

**ADD SCHEDULE RULE**

URL :

**Schedule** :  [View Available Schedules](#)

**Manual Schedule** :

Day(s) :  All Week  Select Day(s)

Sun  Mon  Tue  Wed

Thu  Fri  Sat

All Day - 24 hrs :

Start Time\* :  :  (hour:minute, 24 hour time)

End Time :  :  (hour:minute, 24 hour time)

Enter the website in the **URL** field. Select the time to block websites from the **Schedule** drop-down list, or select **Manual Schedule** and set the corresponding time and days.

Click **Apply** to add the website to the **BLOCK WEBSITE** table. The page as shown in the following figure appears:

**BLOCK WEBSITE**

---

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

---

**BLOCK WEBSITE**

	URL	Schedule
<input type="checkbox"/>	www.163.com	Always

### 3.3.4.2 Block MAC Address

In the **PARENTAL CONTROL** page, click **Block MAC Address**. The page as shown in the following figure appears:

**BLOCK MAC ADDRESS**

---

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

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC" 's MAC Address automatically displays the MAC address of the LAN device where the browser is running. To restrict another 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, open a command prompt window and type "ipconfig /all".

---

**BLOCK MAC ADDRESS**

Username	MAC	Schedule
----------	-----	----------

Click **Add**. The page as shown in the following figure appears:

#### ADD SCHEDULE RULE

User Name:

Current PC's MACAddress:

Other MAC Address:

Schedule:  [View Available Schedules](#)

Manual Schedule :

Day(s) :  All Week  Select Day(s)

Sun  Mon  Tue  Wed

Thu  Fri  Sat

All Day - 24 hrs

Start Time  :  (hour:minute, 24 hour time)

End Time  :  (hour:minute, 24 hour time)

The following table describes the parameters in this page.

Field	Description
User Name	Enter the name that identifies your configuration. For example, <i>kids</i> .
Current PC's MAC Address	Enter the MAC address of the computer that connects to the device.
Other MAC Address	Enter the MAC address of another device that is included in MAC filtering.
Schedule	Select the time of MAC filter from the drop-down list. You can select <b>always</b> or <b>never</b> .
Manual Schedule	If you select this check box, you need to manually set the time of MAC filtering.

Enter the use name and MAC address. Select the corresponding time and days. Then, click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS** table. The page as shown in the following figure appears:

#### BLOCK MAC ADDRESS

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

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC" 's MAC Address automatically displays the MAC address of the LAN device where the browser is running. To restrict another 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, open a command prompt window and type "ipconfig /all".

#### BLOCK MAC ADDRESS

	Username	MAC	Schedule
<input type="checkbox"/>	AB	00:11:22:33:44:55	Always

### 3.3.5 Filtering Options

Choose **Advanced > Filtering Options**. The **FILTERING OPTIONS** page as shown in the following figure appears:

#### FILTERING OPTIONS -- INBOUND IP FILTERING

Manage incoming traffic.

#### FILTERING OPTIONS -- OUTBOUND IP FILTERING

Manage outgoing traffic.

#### FILTERING OPTIONS -- BRIDGE FILTERING

Uses MAC address to implement filtering. Usefull only in bridge mode.

### 3.3.5.1 Inbound IP Filtering

In the **FILTERING OPTIONS** page, click **Inbound IP Filtering**. The **INCOMING IP FILTERING** page as shown in the following figure appears:

**INCOMING IP FILTERING**

---

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below.

Packets matched the rule will be discarded

---

**ACTIVE INBOUND FILTER**

Name	VPI/VCI	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule
------	---------	----------	----------------	-------------	---------------	------------	---------------

Click **Add** to add an inbound IP filter. The page as shown in the following figure appears:

**INCOMING IP FILTERING**

---

**Filter Name :**

**Protocol :** Any

**Source IP Type :** Any

**Source IP Address :**

**Source Subnet Mask :**

**Source Port Type :** Any

**Source Port :**  (port or port:port)

**Destination IP Type :** Any

**Destination IP Address :**

**Destination Subnet Mask :**

**Destination Port Type :** Any

**Destination Port :**  (port or port:port)

**Schedule :** Always  [View Available Schedules](#)

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**

**WWAN Interfaces :**

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port.

---

Then, click **Apply** to save the settings.



**Note:**

The settings apply only when the firewall is enabled.

The **ACTIVE INBOUND FILTER** in the **INCOMING IP FILTERING** page displays detailed information of each created inbound IP filter. Click **Delete** to delete an IP filter. Note that the **Delete** button appears only when at least one IP filter exists.

### 3.3.5.2 Outbound IP Filtering

By default, all outgoing IP traffic from the LAN is allowed. The outbound filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one criterion.

In the **FILTERING OPTIONS** page, click **Outbound IP Filtering**. The **OUTGOING IP FILTERING** page as shown in the following figure appears:

**OUTGOING IP FILTERING**

---

This 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" to save and activate the filter

**WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

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

---

**ACTIVE OUTBOUND FILTER**

Name	Protocol	Source Address	Source Port Type:	Dest. Address	Dest. Port	Schedule Rule
------	----------	----------------	-------------------	---------------	------------	---------------

Click **Add** to add an outbound IP filter. The page as shown in the following figure appears:

**OUTCOMING IP FILTERING**

Filter Name :

Protocol: Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

Source Port:  (port or port:port)

Destination IP Type: Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

Destination Port :  (port or port:port)

Schedule : Always  [View Available Schedules](#)

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port. Click **Apply** to save the settings.

The **ACTIVE OUTBOUND FILTER** in the **OUTGOING IP FILTERING** page displays detailed information of each created outbound IP filter. Click **Delete** to delete an IP filter. Note that the **Delete** button appears only when at least one IP filter exists.

### 3.3.5.3 Bridge Filtering

In the **FILTERING OPTIONS** page, click **Bridge Filtering**. The page as shown in the following figure appears:



## BRIDGE FILTER

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

**WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

### Bridge Filtering Global Policy:

- ALLOW** all packets but **DENY** those matching any of specific rules listed.  
 **DENY** all packets but **ALLOW** those matching any of specific rules listed

Apply Cancel

## DISPLAY LIST

VPI/VCI	protocol	DMAC	SMAC	DIR	TIME
Add Edit Delete					

This page is used to configure bridge parameters. In this page, you can modify the settings or view the information of the bridge and its attached ports.

Click **Add** to add a bridge filter. The page as shown in the following figure appears:

## ADD BRIDGE FILTER

Protocol Type: Click to Select ▾

Destination MAC Address:

Source MAC Address:

Frame Direction: Select ▾

Time schedule: Always ▾ [View Available Schedules](#)

WWan interface: Select all wan ▾

Apply Cancel

The following table describes the parameters in this page.

Field	Description
Protocol Type	Select the protocol type to be mapped from the drop-down list. You can select <b>PPPoE</b> , <b>IPv4</b> , <b>IPv6</b> , <b>AppleTalk</b> , <b>IPX</b> , <b>NetBEUI</b> , or <b>IGMP</b> .
Destination MAC Address	Enter the destination MAC address to be mapped.

Field	Description
Source MAC Address	Enter the source MAC address to be mapped.
Frame Direction	Select the frame direction to be mapped from the drop-down list. The device supports frame direction from LAN to WAN.
Time schedule	Select the time that you want to apply the rule from the drop-down list. You can select <b>Always</b> or <b>Never</b> .
WWan interface	Select the WAN interface to be mapped from the drop-down list.

Click **Apply** to save the settings.

### 3.3.6 QoS Config

Choose **Advanced > QoS Config**. The page as shown in the following figure appears:

**NETWORK TOOLS -- QOS INTERFACE CONFIG**

---

Allows you to config interface bandwidth control.

[QoS Interface Config](#)

**NETWORK TOOLS -- QOS QUEUE CONFIG**

---

Allows you to config queue's precedence.

[Qos Queue Config](#)

**NETWORK TOOLS -- QOS CLASSIFY CONFIGURATION**

---

Allows you to assign a classification

[QoS Classify Config](#)

### 3.3.6.1 Interface Configuration

In the **QoS CONFIG** page, click **QoS Interface Config**. The page as shown in the following figure appears:

**QOS INTERFACE CONFIG**

---

This page allows you to config interface bandwidth control, include upstream and downstream.

---

**LISTS**

	Interface Name	Schedule Algorithm	UP Stream	Down Stream	Enable
<input type="checkbox"/>	PVC:0/35	SP	unlimited	unlimited	0

Click **Edit** and the page as shown in the following figure appears:

**QOS INTERFACE CONFIG**

---

Interface:

Enable:

Schedule Algorithm: SP

Up Stream: unlimited  (Kbps)

Down Stream: unlimited  (Kbps)

In this page, you can configure the uplink bandwidth and downlink bandwidth of each interface. The uplink rate and the downlink rate are limited according to the configured bandwidth. Click **Apply** to save the settings.

### 3.3.6.2 Queue Configuration

In the **QoS CONFIG** page, click **QoS Queue Config**. The page as shown in the following figure appears:

## QOS QUEUE CONFIG

This is queue precedence configuration, the packets with high precedence will pass before medium and low precedence.

### LISTS

Queue Name	Queue Priority	UP Stream	State
------------	----------------	-----------	-------

[Add](#) [Edit](#) [Delete](#)

In this page, you can configure the priority of the queue. The device supports the following three priority levels: high, medium, low. The device handles packets of the high queue priority first, then packets of medium, and finally packets of low priority. Click **Add**. The page as shown in the following figure appears:

## QOS QUEUE CONFIG

Queue Enable:

Queue Priority: High

Associated Interface: PVC:0/35

[Apply](#) [Cancel](#)

Click **Apply** to save the settings.

### 3.3.6.3 Classification Configuration

In the **QoS CONFIG** page, click **QoS Classify Configuration**. The page as shown in the following figure appears:

## QOS CLASSIFY CONFIGURATION

This page allows you to assign a classification, the classification may assign to a queue that you can limit the bandwidth or assign precedence. the classification can also be marked such as 802.1p, dscp.

### LIST

Classification Result						
Class Name	Associated Queue	DSCP Mark	802.1P Mark	state	Details	

[Add](#) [Edit](#) [Delete](#)

This page displays the classes. Click **Add** and the page as shown in the following figure appears:

**QoS CLASSIFY CONFIGURATION**

Traffic Class Name :

Enable Classification :

**SPECIFY TRAFFIC CLASSIFICATION RULES**

Classification Type :

Physical Lan Port :

Source MAC Address :

Source MAC Mask :

Destination MAC Address :

Destination MAC Mask :

Ethernet Type :

802.1p Priority :

**SPECIFY TRAFFIC CLASSIFICATION RESULT**

Assign Classification Queue :

Mark DSCP :

Mark 802.1p Priority :

The following table describes the parameters in this page.

Field	Description
Traffic Class Name	Enter the name of the traffic class.
Enable Classification	Select or deselect the check box to enable or disable QoS classification.
<b>SPECIFY TRAFFIC CLASSIFICATION RULES</b>	
Classification Type	Select <b>L1&amp;L2</b> or <b>L3&amp;L4</b> from the drop-down list. <ul style="list-style-type: none"> <li>● <b>L1&amp;L2</b> maps to the features of layer 1 and layer 2, such as the MAC address.</li> <li>● <b>L3&amp;L4</b> maps to the features of layer 3 and layer 4, such as the IP address and the port.</li> </ul>
Physical Lan Port	Select the physical port of the packet from the drop-down list. For example, ethernet1, ethernet2,

Field	Description
	ethernet3, and ethernet4.
Source MAC Address	Enter the source MAC address of the packet.
Source MAC Mask	Use mask 000000ffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped.
Destination MAC Address	Enter the destination MAC address of the packet.
Destination MAC Mask	Use mask 000000ffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped
Ethernet Type	Select the layer 2 protocol type from the drop-down list. For example, IP protocol and IPX protocol.
802.1p Priority	Select the 802.1p priority of the packet from the drop-down list. You can select <b>no match</b> or a value in the range of 0—7. Note that this function is not supported at the moment.
<b>SPECIFIC TRAFFIC CLASSIFICATION RESULT</b>	
Assign Classification Queue	Specify the queue to which the packet belongs. You can set the queue in the classification configuration.
Mark DSCP	Attach the DSCP mark to the mapped packet.
Mark 802.1p Priority	Attach the 802.1p mark to the mapped packet.

Click **Apply** to save the settings.

### 3.3.7 Firewall Settings

A denial-of-service (DoS) attack is one of the most common network attacks and is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. It usually leads to overload of system server or core dump of the system.

Choose **Advanced > Firewall Settings**. The page as shown in the following figure appears:

**FIREWALL SETTINGS**

---

Click "Apply" button to make the changes effective immediately.

---

**FIREWALL CONFIGURATION**

---

Enable Attack Prevent

Icmp Echo

Fraggle

Echo Chargen

IP Land

Port Scan

TCP Flags: Set "SYN FIN"

TCP Flags: Set "SYN RST"

TCP Flags: Set "FIN RST"

TCP DoS :

TTCP DoS Max Rate:  (packets/second)

Click **Apply** to save the settings.

### 3.3.8 DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might be translated to `198.105.232.4`.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **Advanced > DNS**. The page as shown in the following figure appears:

**DNS**

---

Click "Apply" button to save the new configuration.

---

**DNS SERVER CONFIGURATION**

Obtain DNS server address automatically  
 Use the following DNS server addresses

Wan Connection :

Preferred DNS server :

Alternate DNS server :

The following table describes the parameters in this page.

Field	Description
Obtain DNS server address automatically	If you select this radio button, the device automatically obtains IP address of the DNS server from the ISP. You need not manually enter the IP address of the server.
Use the following DNS server addresses	If you select this radio button, you need to manually enter the IP address of the server provided by the ISP.
Wan Connection	Select the WAN interface of the DNS server to be connected from the drop-down list.
Preferred DNS server	Enter the IP address of the primary DNS server.
Alternate DNS server	Enter the IP address of the secondary DNS server. If the primary DNS server fails to work, the device tries to connect the secondary DNS server.

Click **Apply** to save the settings.

### 3.3.9 Dynamic DNS

The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of



hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers (DynDNS.org or Dlinkddns.com).

Choose **Advanced > Dynamic DNS**. The page as shown in the following page appears:

**DDNS**

---

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

---

**DDNS**

Hostname	Username	Service	Interface
----------	----------	---------	-----------

Click **Add** to add dynamic DNS. The page as shown in the following figure appears:

**ADD DYNAMIC DNS**

---

**DDNS provider:**

**Hostname:**

**Interface:**

**Username:**

**Password:**

The following table describes the parameters in this page.

Field	Description
DDNS provider	Select the DDNS provider from the drop-down list. You can select <b>DynDns.org</b> , <b>TZO</b> , or <b>GnuDIP</b> .
Hostname	Enter the host name that you register with your DDNS provider.

Field	Description
Interface	Select the interface that is used for DDNS service from the drop-down list. The IP address of the interface corresponds to the host name.
Username	Enter the user name of your DDNS account.
Password	Enter the password of your DDNS account.

Click **Apply** to save the settings.

### 3.3.10 Network Tools

Choose **Advanced > Network Tools**. The **NETWORK TOOLS** page as shown in the following figure appears:

---

#### NETWORK TOOLS -- PORT MAPPING

---

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.

Port Mapping

#### NETWORK TOOLS -- IGMP PROXY

---

Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP Proxy

#### NETWORK TOOLS -- IGMP SNOOPING

---

Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP Snooping

#### NETWORK TOOLS -- UPNP

---

Allows you to enable or disable UPnP.

Upnp

#### NETWORK TOOLS -- ADSL

---

Allows you to configure advanced settings for ADSL.

ADSL

#### NETWORK TOOLS -- SNMP

---

Network Tools -- SNMP

SNMP

#### NETWORK TOOLS -- TR-069

---

Allows you to configure TR-069 protocol.

TR-069

#### NETWORK TOOLS -- CERTIFICATES

---

Allows you to manage certificates used with TR-069.

Certificates

#### NETWORK TOOLS -- PPTP

---

Allows you to manage PPTP.

PPTP

#### NETWORK TOOLS -- IPSEC

---

Allows you to configure ipsec.

IPSEC

---

This page contains the following function items: **Port Mapping**, **IGMP Proxy**, **IGMP Snooping**, **UPnP**, **ADSL**, **SNMP**, **TR-069**, **Certificates**, **PPTP**, and **IPSEC**.

### 3.3.10.1 Port Mapping

In the **NETWORK TOOLS** page, click **Port Mapping**. The page as shown in the following figure appears:

**PORT MAPPING**

---

Port Mapping -- A maximum 5 entries can be configured

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

---

**PORT MAPPING SETUP**

	Group Name	Interfaces
<input type="checkbox"/>	Lan1	ethernet1,ethernet2,ethernet3,ethernet4,wlan0,wlan0-vap0,wlan0-vap1,...

In this page, you can bind the WAN interface and the LAN interface to the same group. Click **Add** to add port mapping. The page as shown in the following figure appears:

## ADD PORT MAPPING

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. Click "Apply" button to make the changes effective immediately.

## PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces		Available Interfaces
<div style="border: 1px solid black; height: 100px; width: 100%;"></div>	<div style="border: 1px solid gray; padding: 2px; display: inline-block; margin-bottom: 5px;">-&gt;</div> <div style="border: 1px solid gray; padding: 2px; display: inline-block;">&lt;-</div>	<div style="border: 1px solid gray; padding: 5px;"><ul style="list-style-type: none"><li>ethernet1</li><li>ethernet2</li><li>ethernet3</li><li>ethernet4</li><li>wlan0</li><li>wlan0-vap0</li><li>wlan0-vap1</li><li>wlan0-vap2</li></ul></div>

To create a mapping group, do as follows:

- Step 1** Enter the group name.
- Step 2** Select interfaces from the **Available Interfaces** list and click the **<-** arrow button to add them to the **Grouped Interfaces** list, in this way, you can create the required mapping of the ports. The group name must be unique.
- Step 3** Click **Apply** to save the settings.

### 3.3.10.2IGMP Proxy

In the **NETWORK TOOLS** page, click **IGMP Proxy**. The page as shown in the following figure appears:

### IGMP PROXY

---

IGMP proxy enables the system to issue IGMP host messages on behalf of

---

### IGMP PROXY CONFIGURATION

---

Enable IGMP Proxy

WAN Connection :

LAN Connection :

IGMP proxy enables the device to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The device serves as a proxy for its hosts after you enable the function.

Select Enable IGMP Proxy and select the desired WAN and corresponding LAN interface. Then, click **Apply** to save the settings.

### 3.3.10.3 IGMP Snooping

When IGMP snooping is enabled, only hosts that belong to the group receive the multicast packets. If a host is deleted from the group, the host cannot receive the multicast packets any more.

In the **NETWORK TOOLS** page, click **IGMP Snooping**. The page as shown in the following figure appears:

### IGMP

---

Transmission of identical content, such as multimedia, from a source to a number of recipients.

---

### IGMP SETUP

---

Enable IGMP Snooping

Click **Apply** to save the settings.

---

### 3.3.10.4 UPnP

In the **NETWORK TOOLS** page, click **Upnp**. The page as shown in the following figure appears:

UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UUPNP SETUP

Enable UPnP

WAN Connection:

LAN Connection:

Apply Cancel

In this page, you can enable universal plug and play (UPnP) and then the system serves as a daemon.

UPnP is widely applied in audio and video software. It automatically searches devices in the network. If you are concerned about UPnP security, you can disable it. Select the WAN and LAN interfaces at which you want to enable UPnP and click **Apply** to save the settings.

### 3.3.10.5 ADSL Settings

In the **NETWORK TOOLS** page, click **ADSL**. The page as shown in the following figure appears:

### ADSL SETTINGS

---

This page is used to configure the ADSL settings of your ADSL router.

---

### ADSL SETTINGS

---

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

Capability

- Bitswap Enable
- SRA Enable

In this page, you can select the ADSL modulation. Normally, you are recommended to keep the factory defaults. The device supports the following modulation types: G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+, and AnnexM. The device negotiates the modulation mode with the DSLAM.

Click **Apply** to save the settings.

### 3.3.10.6 SNMP

In the **NETWORK TOOLS** page, click **SNMP**. The page as shown in the following figure appears:



**SNMP CONFIGURATION**

---

This page is used to configure the SNMP protocol.

---

**SNMP CONFIGURATION**

**Enable SNMP Agent**

Read Community:

Set Community:

Trap Manager IP:

Trap Community:

Trap Version:

In this page, you can set the SNMP parameters. The following table describes the parameters in this page.

Field	Description
Enable SNMP Agent	Select or deselect the check box to enable or disable SNMP agent.
Read Community	Universal character to obtain the device information. It is similar to the password. The SNMP application entity can use it to directly obtain the device information.
Set Community	Universal character to modify the device configuration. It is similar to the password. The SNMP application entity can use it to directly modify the device configuration.
Trap Manager IP	Enter the address of the server that receives the trap message.
Trap Community	The field that is included in the trap message sent by the device.
Trap Version	Select the trap version from the drop-down list. You can select <b>v1</b> or <b>v2c</b> .

Click **Apply** to save the settings.

### 3.3.10.7 TR-069

In the **NETWORK TOOLS** page, click **TR-069**. The page as shown in the following figure appears:

TR-069

---

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

---

**TR-069 CLIENT -- CONFIGURATION**

Inform:  Disabled  Enabled

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

In this page, you can configure the TR-069 CPE. The following table describes the parameters in this page.

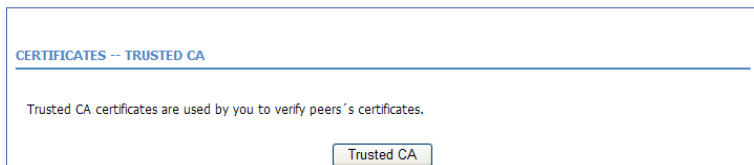
Field	Description
Inform	You can select <b>Disabled</b> or <b>Enabled</b> to disable or enable notification. <ul style="list-style-type: none"><li>● <b>Disabled</b> indicates that the device does not automatically send requests to the TR069 server.</li><li>● <b>Enabled</b> indicates that the device automatically sends a request of connection to the TR069 server. The following function items are available only when <b>Inform</b> is set to <b>Enabled</b>.</li></ul>
Inform Interval	The interval of sending a request of connection to the TR069 server from the device.
ACS URL	The path of the TR069 server to which the device sends a request.

Field	Description
ACS User Name	The user name that the devices uses to log in to the TR069 server.
ACS Password	The password that the devices uses to log in to the TR069 server.
Connection Request Authentication	Select the check box to enable authentication of connection request. If you enable the function, you need to enter the user name and password for authentication.
Connection Request User Name	The user name that the TR069 server uses to access the TR069 progress of the device.
Connection Request Password	The password that the TR069 server uses to access the TR069 progress of the device.

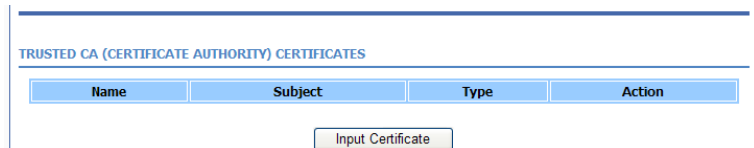
Click **Apply** to save settings.

### 3.3.10.8 Certificates

In the **NETWORK TOOLS** page, click **Certificates**. The **Certificates** page as shown in the following figure appears:



Click **Trusted CA** and the page as shown in the following figure appears:



#### Note:

Before importing a certificate, you must synchronize the system time with time server. Otherwise, the certificate fails to be imported.

Click **Input Certificate** to import a certificate. The page as shown in the following figure appears:

**TRUSTED CA CERTIFICATES**

---

Enter certificate name and paste certificate content

---

**IMPORT CA CERTIFICATE**

Certificate Name:

Certificate: 

```
-----BEGIN CERTIFICATE-----
<Import CA certificate Here>
-----END CERTIFICATE-----
```

### 3.3.10.9 PPTP

The **Point-to-Point Tunneling Protocol** (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

In the **NETWORK TOOLS** page, click **PPTP**, the page as shown in the following figure appears.

**PPTP**

---

Allows you to transmit data in safety tunnel.

---

**PPTP SETUP**

Enable PPTP

Local IP Start:

Local IP Num.:

Remote IP Start:

Remote IP Num.:

Netmask:

---

**PPTP ACCOUNT**

Username	Password
<input type="text"/>	<input type="text"/>

The following table describes the parameters in this page.

Field	Description
Local IP Start	The started IP address of the local network.
Local IP Num	The valid numbers of local IP addresses. It works together with the Local IP Start to determine the range of the local IP addresses.
Remote IP Start	The started IP address of the remote network.
Remote IP Num	The valid numbers of remote IP addresses. It works together with the Remote IP Start to determine the range of the remote IP addresses.
Netmask	It is valid for both the local network and the remote network.

Click **add**, the page as shown in the following figure appears.

#### ADD PPTP ACCOUNT

Username:   
Password:

The following table describes the parameters in this page.

Field	Description
Username	The user name that is used for dialup to connect the modem to the PPTP.
Password	The password that is used for dialup to connect the modem to the PPTP.

### 3.3.10.10 IPSEC

In the **NETWORK TOOLS** page, click **IPSEC**. The page as shown in the following figure appears.

#### IPSEC

Add,delete IPsec tunnel connections in this page.

#### IPSEC TUNNEL MODE CONNECTIONS.

Enable IPSEC

Name	Remote Gateway	Local Addresses	Remote Addresses	Interface
------	----------------	-----------------	------------------	-----------

In this page, you can add, edit and delete the IPsec tunnel connections  
Select **Enable IPSEC**, and click **Add**, the page as shown in the following figure appears.

## IPSEC

Add/delete IPsec tunnel connections in this page.

### IPSEC TUNNEL MODE CONNECTIONS.

Enable IPSEC

Name	Remote Gateway	Local Addresses	Remote Addresses	Interface
------	----------------	-----------------	------------------	-----------

### IPSEC SETTINGS

IPSec Connection Name :

Tunnel Mode :

Remote IPsec Gateway Address :

Tunnel access from local IP address :

IP Address for VPN :

IP Subnetmask :

Tunnel access from remote IP address :

IP Address for VPN :

IP Subnetmask :

Key Exchange Method :

Pre-Shared Key :

### IKE Settings

#### Phase 1

Mode :

Encryption Algorithm :

Integrity Algorithm :

Diffie-Hellman Group Key Exchange :

Key Life Time :

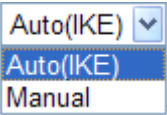
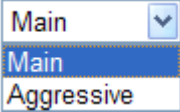
#### Phase 2

Encryption Algorithm :

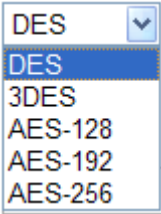
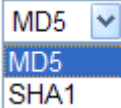
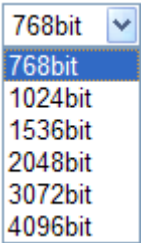
Integrity Algorithm :

Key Life Time :

Use Interface :

Field	Description
IPSec Connection Name	The connection name of the marker IPsec.
Tunnel Mode	You can select <b>ESP</b> or <b>AH</b> .
Remote IPsec Gateway Address	The IP or domain name of the Remote IPsec Gateway.
Tunnel access from local IP address	You can select <b>Subnet</b> or <b>Single Address</b> . If you select <b>Single Address</b> , it allows only one PC from local to connect remote hosts with IPSEC mode. You must enter the IP address of the PC in fourth item. If you select <b>subnet</b> , it allows more than one PC from local to connect remote hosts with IPSEC mode.
IP Address for VPN	If you select <b>Single Address</b> , it is the IP address of the PC. If you choose <b>Subnet</b> , it is the subnet address.
IP Subnetmask	Enter the subnetmask for IP.
Tunnel access from remote IP address	You can select <b>Subnet</b> or <b>Single Address</b> .
Key Exchange Method	You can select from the drop-down list. 
Pre-Shared Key	Enter the pre-shared key.
<b>IKE Settings</b>	
Mode	You can select from the drop-down list. 
Encryption Algorithm	You can select from the drop-down list.



Field	Description
	
Integrity Alogrithm	<p>You can select from the drop-down list.</p> 
Diffie-Hellman Group Key Exchange	<p>You can select from the drop-down list.</p> 
Key Life Time	Enter the time of key life.
Use Interface	Select the use interface

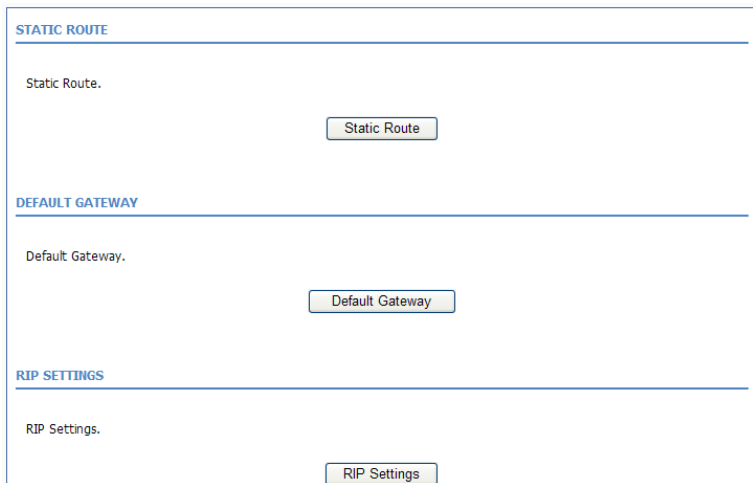
This is a dynamic page. The displays are different (some options are shown and hidden) when different types or connections are chosen.

In this page, set the parameters such as the IPSec connection name, tunnel mode, and remote IPSec gateway address.

After finishing setting, click **Apply** to save the settings.

### 3.3.11 Routing

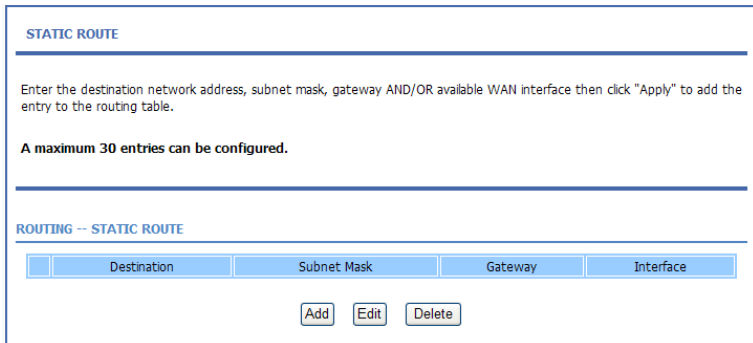
Choose **Advanced** > **Routing**. The page as shown in the following page appears:



This page contains the following function items: static route, default gateway, and RIP settings.

### 3.3.11.1 Static Route

Choose **Advanced > Routing** and click **Static Route**. The page as shown in the following figure appears:



This page displays the information of existing static routes. Click **Add** and the page as shown in the following figure appears:

#### STATIC ROUTE ADD

Destination Network Address :	<input type="text"/>
Subnet Mask:	<input type="text"/>
Use Gateway IP Address:	<input type="text"/>
Use Interface:	pppoe_0_35_0_0 ▾
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

The following table describes the parameters in this page.

Field	Description
Destination Network Address	The destination IP address of the device.
Subnet Mask	The subnet mask of the destination IP address.
Use Gateway IP Address	The gateway IP address of the device.
Use Interface	Select the interface of the static routing used by the device from the drop-down list.



#### Note:

You can enter the gateway IP address of the device in the **Use Gateway IP Address** field or set the **User Interface**, but cannot apply the two settings at the same time.

Click **Apply** to save the settings.

### 3.3.11.2 Default Gateway

Choose **Advanced > Routing** and click **Default Gateway**. The page as shown in the following figure appears:

#### DEFAULT GATEWAY

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway OR a WAN interface. Click "Apply" button to save it.

#### DEFAULT GATEWAY

- Enable Automatic Assigned Default Gateway**
- Use Gateway IP Address :**
- Use Interface:**

In this page, you can select **Enable Automatic Assigned Default Gateway**, or enter the information in the **Use Gateway IP Address** and **Use Interface** fields. Click **Apply** to save the settings.

### 3.3.11.3 RIP Settings

Choose **Advanced > Routing** and click **RIP**. The page as shown in the following figure appears:

#### RIP CONFIGURATION

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

#### RIP

Interface	VPI/VCI	Version	Operation	Enabled
pppoe_0_35_0_0	0/35	1	active	<input type="checkbox"/>
Lan1	-	1	active	<input type="checkbox"/>

In this page, you can view the interfaces on your device that use RIP and the version of the protocol used.

If you enable RIP, the device communicates with other devices using the routing information protocol (RIP).

Click **Apply** to save the settings.

### 3.3.12 Schedules

Choose **Advanced > Schedules**. The page as shown in the following figure appears:

**SCHEDULES**

Schedule allows you to create scheduling rules to be applied for your firewall.

Maximum number of schedule rules: 20

**SCHEDULE RULES**

Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	stop time
-----------	-----	-----	-----	-----	-----	-----	-----	------------	-----------

Click **Add** to add a schedule rule. The page as shown in the following figure appears:

**ADD SCHEDULE RULE**

Name :

Day(s) :  All Week  Select Day(s)

Sun  Mon  Tue  Wed  
 Thu  Fri  Sat

All Day - 24 hrs :

Start Time :  :  (hour:minute, 24 hour time)

End Time :  :  (hour:minute, 24 hour time)

The following table describes the parameters in this page.

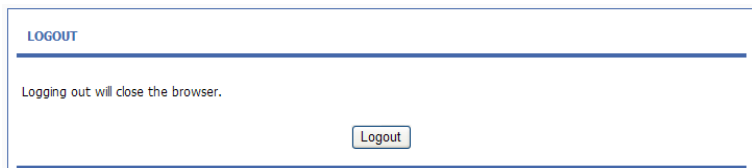
Field	Description
Name	Set the name of the schedule.
Day(s)	You can select one, more, or all of the seven days in a week.
All Day – 24 hrs	If you select the check box, the rule applies throughout the 24 hours of the day.
Start Time	Set the start time of the firewall.
End Time	Set the end time of the firewall.

---

Click **Apply** to save the settings.

### 3.3.13 Logout

Choose **Advanced** > **Logout**. The page as shown in the following figure appears:



Click **Logout** to log out of the configuration page.

## 3.4 Management

### 3.4.1 System

Choose **Management** > **System Management**. The **System** page as shown in the following figure appears:

#### SYSTEM -- REBOOT

Click the button below to reboot the router.

Reboot

#### SYSTEM -- BACKUP SETTINGS

Back up Router configurations. You may save your router configurations to a file on your PC.

Note: Please always save configuration file first before viewing it.

Backup Setting

#### SYSTEM -- UPDATE SETTINGS

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

Settings File Name:  Browse...

Update Settings

#### SYSTEM -- RESTORE DEFAULT SETTINGS

Restore Router settings to the factory defaults.

Restore Default Setting

In this page, you can restart the device, back up the current settings to a file, update the backup file, and restore the factory default settings.

The following table describes the buttons in this page.

Button	Description
Reboot	Restart the device.
Backup Setting	Specify the path to back up the current configuration in a configuration file on your computer. You can rename the configuration file.
Update Settings	Click <b>Browse...</b> to select the configuration file of device and click <b>Update Settings</b> to update the configuration

Button	Description
	of the device.
Restore Default Setting	Reset the device to default settings.



**Caution:**

**Do not turn off your device or press the Reset button when the procedure is in progress.**

### 3.4.2 Firmware Update

Choose **Management > Firmware Update**. The page as shown in the following figure appears:

**FIRMWARE UPDATE**

---

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

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

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

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

---

**FIRMWARE UPDATE**

---

Current Firmware Version: V1.0

Current Firmware Date: 2009/09/07 10:23:12

Select File:

Clear Config:

In this page, you can upgrade the firmware of the device. To update the firmware, do as follows:

- Step 1** Click **Browse...** to select the file.
- Step 2** Select **Clear Config**.



---

**Step 3** Click **Update Firmware** to update the configuration file.  
The device loads the file and reboots automatically.



**Caution:**

**Do not turn off your device or press the Reset button when the procedure is in progress.**

---

### 3.4.3 Access Controls

Choose **Management > Access Controls**. The **ACCESS CONTROLS** page as shown in the following figure appears:

The screenshot shows a web interface with three sections, each separated by a horizontal line. Each section has a title, a description, and a button.

- ACCESS CONTROLS -- ACCOUNT PASSWORD**  
Manage DSL Router user accounts.  
Account Password
- ACCESS CONTROLS -- SERVICES**  
A Service Control List ("SCL") enables or disables services from being used.  
Services
- ACCESS CONTROLS -- IP ADDRESS**  
Permits access to local management services.  
IP Address

This page contains **Account Password**, **Services**, and **IP Address**.

#### 3.4.3.1 Account Password

In the **ACCESS CONTROLS** page, click **Account Password**. The page as shown in the following figure appears:

#### ACCOUNT PASSWORD

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

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics. This user name can not be used in local.

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

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

#### ACCOUNT PASSWORD

Username:  ▼

Current Password:

New Password:

Confirm Password:

#### WEB IDLE TIME OUT SETTINGS

Web Idle Time Out:  (5 ~ 30 minutes)

In this page, you can change the password and set the time for automatic logout. You are recommended to change the default password to ensure the security of your network. Ensure that you remember the new password or write it down and keep it in a safe location for future reference. If you forget the password, you need to reset the device to the factory default settings. In that case, all configuration settings of the device are lost.

The following table describes the parameters in this page.

Field	Description
<b>ACCOUNT PASSWORD</b>	
Username	Select a user name from the drop-down list to access the device. You can select <b>admin</b> , <b>user</b> , or <b>support</b> .
Current Password	Enter the password of the user.
New Password	Enter the new password.
Confirm Password	Enter the new password again for confirmation.
<b>WEB IDLE TIME OUT SETTINGS</b>	

Field	Description
Web Idle Time Out	Set the time after which the system automatically exits the configuration page. Its value range is 5—30 minutes.

Click **Apply** to apply the settings.

### 3.4.3.2 Services

In the **ACCESS CONTROLS** page, click **Services**. The page as shown in the following figure appears:

**SERVICES**

---

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

---

**ACCESS CONTROL -- SERVICES**

WAN pppoe\_0\_35\_0\_0

Service	LAN	WAN	WAN Access Destination Port
FTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="21"/>
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="80"/>
ICMP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
TELNET	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="23"/>
TFTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="69"/>

In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled at port 23, the remote host can access the device by telnet through port 23.

Select the management services that you want to enable or disable at the LAN or WAN interface and click **Apply** to apply the settings.



**Caution:**

**If you disable the HTTP service, you cannot access the configuration page of the device any more.**

### 3.4.3.3 IP Address

In the **ACCESS CONTROLS** page, click **IP Address**. The page as shown in the following figure appears:

**IP ADDRESS**

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

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

---

**ACCESS CONTROL -- IP ADDRESSES**

Enable Access Control Mode

IP
----

In this page, you can configure the IP address in the access control list (ACL). If ACL is enabled, only devices of the specified IP addresses can access the device.

Select **Enable Access Control Mode** to enable ACL.



**Note:**

If you enable ACL, ensure that the IP address of the host is in the ACL list.

Click **Add**. The page as shown in the following figure appears:

**IP ADDRESS**

IP Address :

Enter the IP address of the desired device in the **IP Address** field and click **Apply** to apply the settings.

## 3.4.4 Diagnostics

Choose **Management > Diagnosis**. The page as shown in the following figure appears:

**DIAGNOSTICS**

---

The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection:

In this page, you can test the connection status of the device. Click **Return Diagnostic Test** to run diagnostics. The page as shown in the following figure appears:

**TEST THE CONNECTION TO YOUR LOCAL NETWORK**

Test your LAN 1 Connection	Pass
Test your LAN 2 Connection	Fail
Test your LAN 3 Connection	Fail
Test your LAN 4 Connection	Fail
Test your Wireless Connection	Pass

**TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER**

Test ADSL Synchronization	Fail
Test ATM OAM F5 Segment Loopback	Fail
Test ATM OAM F5 End-to-end Loopback	Fail
Test ATM OAM F4 Segment Loopback	Fail
Test ATM OAM F4 End-to-end Loopback	Fail

**TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER**

Ping Default Gateway	Fail
Ping Primary Domain Name Server	Fail

## 3.4.5 Log Configuration

Choose **Management > Log Configuration**. The **SYSTEM LOG** page as shown in the following figure appears:

**SYSTEM LOG**

---

if the log mode is enabled, the system will begin to log all the selected events. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.

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

Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"

---

**SYSTEM LOG -- CONFIGURATION**

---

Enable Log

Mode: Local

Server IP Address :

Server UDP Port:

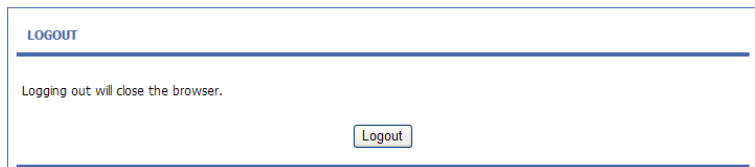
In this page, you can enable the log function. You can set **Mode** to **Local**, **Remote**, or **Both**. **Local** indicates to save the log in the local computer. **Remote** indicates to send the log to the remote log server. **Both** indicates to save the log in the local computer and the remote log server.

To log the events, do as follows:

- Step 1** Select **Enable Log**.
- Step 2** Select a mode from the drop-down list.  
If you select **Remote** or **Both**, enter the IP address and port number of the server.
- Step 3** Click **Apply** to apply the settings.
- Step 4** Click **View System Log** to view the detail information of the system log.

### 3.4.6 Logout

Choose **Management > Logout**. The page as shown in the following figure appears:



Click **Logout** to log out of the configuration page.

## 3.5 Status

In the **Status** page, you can view the system information and monitor the performance of the device.

### 3.5.1 Device Information

Choose **Status > Device Info**. The page as shown in the following figure appears:

#### DEVICE INFO

This information reflects the current status of your WAN connection.

#### SYSTEM INFO

Modem Name :	ADN-4100
Time and Date :	2000-01-01 00:11:00
Firmware Version :	V1.0

#### WINTERNET INFO

Internet Connection Status:

Internet Connection Status:	Disconnected
Default Gateway:	
Preferred Dns Server:	
Alternate Dns Server:	
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0

Enabled WAN Connections :					
VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address
0/35	pppoe_0_35_0_0	PPPOE	Disable	Disable	

#### WIRELESS INFO

select wireless :

MAC Address:	00:30:4f:78:3f:06
Status:	Enable
Network Name (SSID):	ADN-4100
Visibility:	Visible
Security Mode:	None

#### LOCAL NETWORK INFO

MAC Address:	00:30:4f:78:3f:05
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable

The page displays the summary of the device status, including the system information, WAN connection information, wireless information, and local network information.



## 3.5.2 Wireless Clients

Choose **Status > Wireless Clients**. The page as shown in the following page appears:

**WIRELESS CLIENTS**

---

This page shows authenticated wireless stations and their status.

---

**WIRELESS -- AUTHENTICATED STATIONS**

Mac	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

The page displays authenticated wireless stations and their statuses.

## 3.5.3 DHCP Clients

Choose **Status > DHCP Clients**. The page as shown in the following page appears:

**DHCP CLIENTS**

---

This information reflects the current DHCP client of your modem.

---

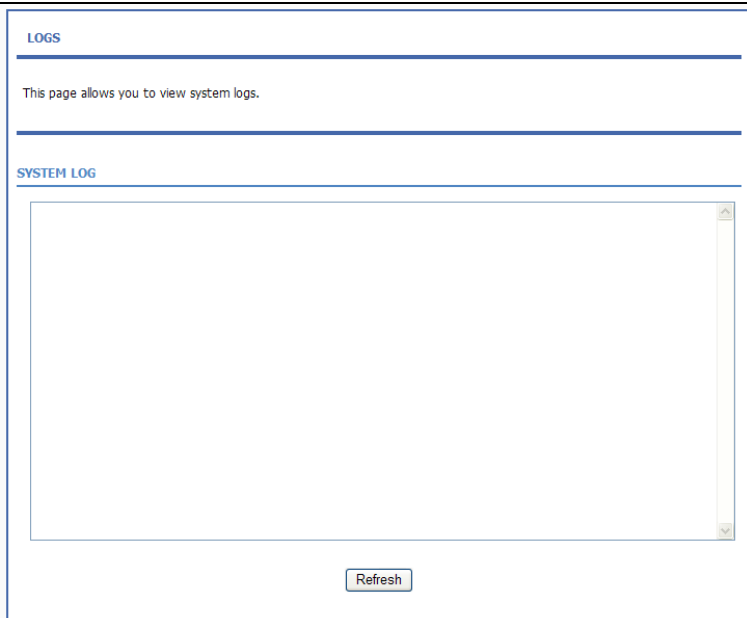
**DHCP LEASES**

Hostname	MAC Address	IP Address	Expires In
gj558d	00:11:2f:68:de:69	192.168.1.2	42554

This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address, and expiration time of the IP address.

## 3.5.4 Logs

Choose **Status > Logs**. The page as shown in the following figure appears:



This page displays the system log. Click **Refresh** to refresh the system log shown in the box.

### 3.5.5 Statistics

Choose **Status > Statistics**. The page as shown in the following figure appears:

#### DEVICE INFO

This information reflects the current status of your DSL connection.

#### LOCAL NETWORK & WIRELESS

interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN1	123200	1278	0	0	185783	576	0	0
ADN-4100	2197004	85637	0	0	2197004	5914	0	0

#### INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoe_0_35_0_0	0/35	PPPOE								

#### ADSL

Mode:	0	
Type:	0	
Line Coding:	Enable	
Status:	ACTIVATING.	
	<b>Downstream</b>	<b>Upstream</b>
SNR Margin (dB):	0.0	0.0
Attenuation (dB):	04	0.0
Output Power (dBm):	0.0	0.0
Attainable Rate (Kbps):	0	0
Rate (Kbps):	0	0
D (interleave depth):	0	0
Delay (msec):	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total ES:	0	0

This page displays the statistics information of the network and data transmission. The information helps technicians to identify whether the device is functioning properly. The information does not affect the functions of the device.

### 3.5.6 Route information

Choose **Status > Route Info**. The page as shown in the following figure appears:

**ROUTE INFO**

---

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

---

**DEVICE INFO -- ROUTE**

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br1

The table displays destination routes commonly accessed by the network.

### 3.5.7 Logout

Choose **Status > Logout**. The page as shown in the following figure appears:

**LOGOUT**

---

Logging out will close the browser.

---

Click **Logout** to log out of the configuration page.

## EC Declaration of Conformity

For the following equipment:

\*Type of Product : 802.11n Wireless ADSL 2/2+ 4-Port Router (Annex A/B)  
\*Model Number : ADN-4100A / ADN-4100B  
\* Produced by:  
Manufacturer's Name : **Planet Technology Corp.**  
Manufacturer's Address : 10F, No. 96, Minquan Rd., Xindian Dist.,  
New Taipei City 231, Taiwan, R.O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 1999/5/EC R&TTE. For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328 V1.7.1	(2006-10)
EN 301 489-1 V1.8.1	(2008-04)
EN 301 489-17 V2.1.1	(2009-05)
EN 55022	(2006 + A1: 2007, Class B)
EN 61000-3-2	(2006 + A1: 2009 + A2: 2009)
EN 61000-3-3	(2008)
EN 61000-4-2	(2009)
EN 61000-4-3	(2006 + A1: 2008)
EN 61000-4-4	(2004)
EN 61000-4-5	(2006)
EN 61000-4-6	(2009)
EN 61000-4-11	(2004)
EN 60950-1	(2006 + A11: 2009)
EN 50385	(2002)

Responsible for marking this declaration if the:

Manufacturer     Authorized representative established within the EU

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F, No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan, R.O.C.**


Person responsible for making this declaration

Name, Surname **Jonas Yang**

Position / Title : **Product Manager**

Taiwan  
Place

28<sup>th</sup>, Jan., 2011  
Date

  
Jonas  
Legal Signature

### **PLANET TECHNOLOGY CORPORATION**