PLANET
Networking & Communication

User's Manual

802.11n Wireless
ADSL 2/2+ Router

ADN-4101

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-4101

Rev: 1.0 (Apr. 2011)

Part No. EM-ADN4101_v1

Contents

1   Overview

The ADN-4101 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

1.2 LEDs and Interfaces

Front Panel
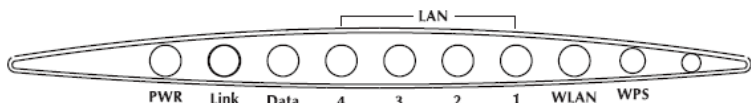
Figure 1 Front panel

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 transmitted in the bridge mode.

LED	Color	Status	Description
		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
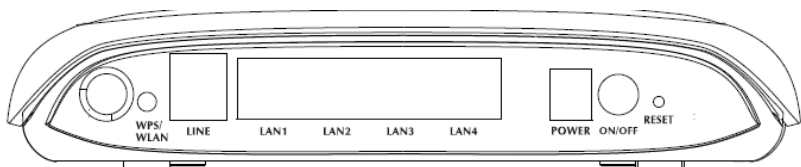
Figure 2 Rear panel

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	● Press the button and hold it for 1 second, to enable WLAN. ● Press the button and hold it for 1 second to 3 seconds, it does not take effect.

Interface/Button	Description
	● Press the button and hold it for 3 or more than 3 seconds, to initialize WPS negotiation.
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 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

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).

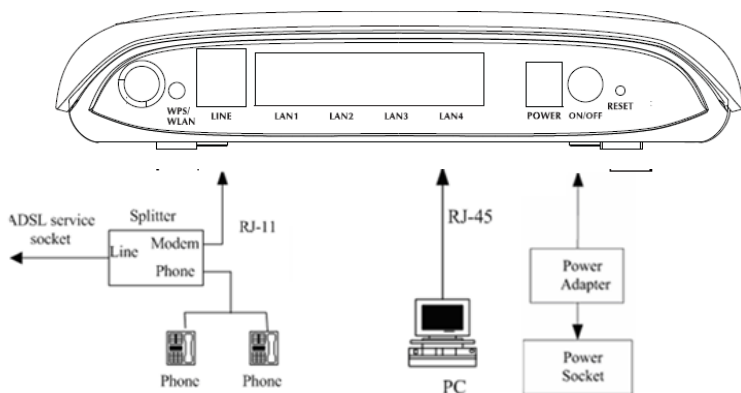📖 **Note:**

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 set, when no telephone set is placed before the splitter. This type of connection is recommended.

6

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 set, when a telephone set is placed before the splitter.

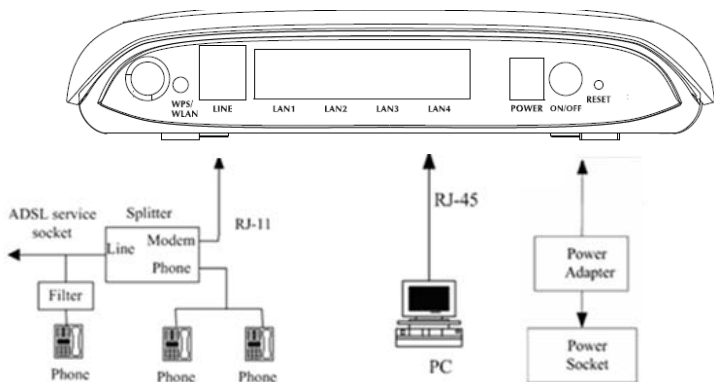As illustrated in the following figure, the splitter is installed close to the device:

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:

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 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 Internect 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:

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

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 : 192.168.2.10

2nd NTP time server : 192.168.2.100

TIME CONFIGURATION

Time Zone : (GMT) Greenwhich Mean Time: Dublin, Lisbon, London, Casablanca

☐ **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

[Back] [Next] [Cancel]

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:

11

STEP 2: SETUP INTERNET CONNECTION

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

Protocol : PPPoE

Encapsulation Mode: LLC

VPI : 8 (0-255)

VCI : 35 (32-65535)

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 :

[Back] [Next] [Cancel]

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 : Dynamic IP

Encapsulation Mode: LLC

VPI : 8 (0-255)

VCI : 35 (32-65535)

[Back] [Next] [Cancel]

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 : Static IP

Encapsulation Mode: LLC

VPI : 8 (0-255)

VCI : 35 (32-65535)

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 :

Back   Next   Cancel

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 : 8 (0-255)

VCI : 35 (32-65535)

Back   Next   Cancel

After setting, click **Next**.

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

13

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) : ADN-4101

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.

None	Security Level	Best
⊙ None	○ WEP	○ WPA-PSK	○ WPA2-PSK

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

[Back] [Next] [Cancel]

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

14

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 :	192.168.2.10
NTP Server 2 :	192.168.2.100
Time Zone :	GMT
Daylight Saving Time :	0
VPI / VCI :	8/35
Protocol :	Bridge
Connection Type :	LLC
Wireless Network Name (SSID) :	ADN-4101
Visibility Status :	1
Encryption :	Basic
Pre-Shared Key :	
WEP Key :	**********

Back   Apply   Cancel

📖 **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:

15

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

Add Edit Delete

In this page, you can configure the WAN interface of the device.

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

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

ATM PVC CONFIGURATION

VPI : [0] (0-255)

VCI : [35] (32-65535)

Service Category : [UBR With PCR]

Peak Cell Rate : [0] (cells/s)

Sustainable Cell Rate : [0] (cells/s)

Maximum Burst Size : [0] (cells)

CONNECTION TYPE

Protocol : [Bridging]

Encapsulation Mode : [LLC]

802.1Q VLAN ID : [0] (0 = disable, 1 - 4094)

Protocol Type : [IPv4]

NETWORK ADDRESS TRANSLATION SETTINGS

Apply Cancel

The following table describes the parameters in this page.

| Field	Description
ATM PVC CONFIGURATION	
VPI	Virtual Path Identifier (VPI) is the virtual path between two points in an ATM network. Its value range is from 0 to 255.

16

Field	Description
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 **UBR with PCR**, **UBR without PCR**, **CBR**, **Non Realtime VBR**, or **Realtime VBR** 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.
CONNECTION TYPE	
Protocol	Select **PPP over ATM (PPPoA)**, **PPP over Ethernet (PPPoE)**, **MAC Encryption Routing (MER)**, **IP over ATM (IPoA)**, or **Bridging** from the drop-down list.
Encapsulation Mode	Select **LLC** or **VCMUX** from the drop-down list. Usually, you can select **LLC**.
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 **0** indicates to disable this function.
NETWORK ADDRESS TRANSLATION SETTINGS	
Enable NAT	Select or deselect the check box to enable or disable the NAT connection.
NAT Type	Select Symmetric Nat or Full cone Nat from the drop-down list
Enable WAN Service	Select or deselect the check box to enable or disable the WAN connection.
Service Name	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 pear-to-pear 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:
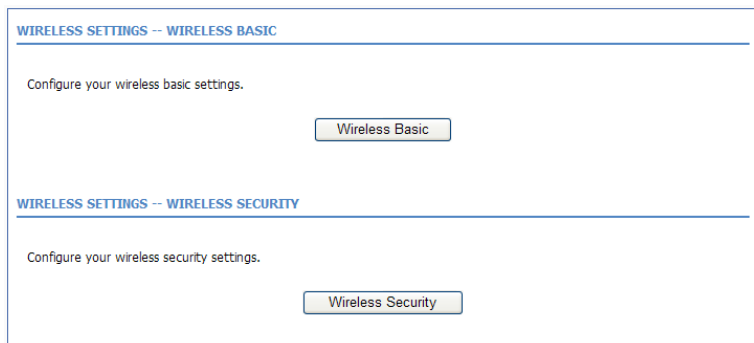
3.2.3.1 Wireless Basics

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) :	ADN-4101
Visibility Status :	⦿ Visible ○ Invisible
Channel Standard:	ETSI(1-13) ▾
Control Sideband:	Upper ▾
Wireless Channel :	Auto Scan ▾
802.11 Mode :	802.11b/g/n ▾
Band Width :	20M/40M ▾

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

Apply   Cancel

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	● **Visible** indicates that the device broadcasts the SSID. ● **Invisible** indicates that the device does not broadcast the SSID.
Channel Standard	You can select from the drop-down list: **FCC(1-11)**, **ETS(1-13)**, **JP(1-14)**
Control Sideband	You can select **Upper or Lower** from the list

19

Field	Description
Wireless Channel	Select the wireless channel used by the device from the drop-down list. You can select **Auto Scan** or a value from **CH1**—**CH13**. **Auto Scan** 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 **20M** or **40M**.

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 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:

The following table describes the parameters in this page.

Field	Description
WEP Key Length	You can select **64 bits** or **128 bits** from the drop-down list.

Field	Description
	● If you select **64 bits**, you need to enter 10 hexadecimal numbers or 5 characters. ● If you select **128 bits**, you need to enter 26 hexadecimal numbers or 13 characters.
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 **Open** or **Share Key**.

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 : Auto(WPA or WPA2)

WPA Encryption : AES

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 : Auto(WPA or WPA2)-PSK

Group Key Update Interval : 100

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.

Apply   Cancel

The following table describes the parameters in this page.

Field	Description
WPA Mode	You can select **Auto (WPA or WPA2)-PSK** or **Auto (WPA or WPA2)-Enterprise** from the drop-down list.
WPA Encryption	You can select **AES** or **TKIP+AES** 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:

23

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 : Auto(WPA or WPA2)-Enterprise

Group Key Update Interval : 100

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 : 192.168.1.1

RADIUS server Port : 2801

RADIUS server Shared Secret : testradiuskey

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

Apply   Cancel

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 : WPA2 only

WPA Encryption : AES

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 : WPA2-PSK

Group Key Update Interval : 100

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.

Apply   Cancel

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 only

WPA Encryption : TKIP+AES

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 : WPA-PSK

Group Key Update Interval : 100

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.

Apply   Cancel

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 : `192.168.1.1`
Subnet Mask : `255.255.255.0`
Domain Name : `ADN-4101`

☐ Configure the second IP Address and Subnet Mask for LAN
IP Address :
Subnet Mask :

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. You can also make DHCP server just acting on the specific port, by default, those ports are selected.

If your DHCP server doesn't belong to the same segment with your pc, but you need to assign IP address from DHCP server, you must uncheck the **Enable**

DHCP Server and selected the **Enable DHCP Relay** to set the DHCP Relay IP address.And you can also set the perferrde and alternate DNS server.

Click **Apply** to save the settings.

In the **DHCP CLIENT CLASS LIST** page, you can set a IP address range for some specification device. The page as shown in the following figure appears:

DHCP CLIENT CLASS LIST

	Client Class	Min Address	Max Address	DNS Address

Add Edit Delete

ADD DHCP CLIENT CLASS(OPTIONAL)

Client Class Name : [_____]

Min IP Address : [_____]

Max IP Address : [_____]

DNS Address : [_____]

Apply Cancel

The following table describes the parameters in this page.

Field	Description
Client Class Name	Enter the Client Class name
Min IP Address	The IP Address for minimun
Max IP Address	The IP Address for maxmun
DNS Address	Enter the DNS Address with the client class

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

DHCP RESERVATIONS LIST

	Status	Computer Name	MAC Address	IP Address

Add Edit Delete

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

ADD DHCP RESERVATION (OPTIONAL)

Enable : ☐

Computer Name : [_____]

IP Address : [_____]

MAC Address : [_____]

Apply Cancel

The following table describes the parameters in this page.

29

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
gj558d	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 : 192.168.2.10

2nd NTP time server : 192.168.2.100

TIME CONFIGURATION

Current Local Time: 2010-10-10 00:05:09

Time Zone: (GMT) Greenwich Mean Time: Dublin, Lisbon, London; Casablanca ▾

☐ **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

[Apply] [Cancel]

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 ~ 1000)

RTS Threshold : 2346   (256 ~ 2346)

Fragmentation Threshold : 2345   (256 ~ 2346)

DTIM Interval : 100   (1 ~ 255)

Preamble Type : long

SSID

Enable Wireless : ☑

Wireless Network Name (SSID) : ADN-4101

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16   (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : ☐

Guest SSID : VAP1

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16   (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network : ☐

Guest SSID : VAP2

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16   (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable Wireless Guest Network : ☐

Guest SSID : VAP3

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16   (1 ~ 32)

Apply   Cancel

The following table describes the parameters in this page.

Field	Description
ADVANCED WIRELESS SETTINGS	
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 **Lower** or **Higher**.
Transmit Power	Select the power for data transmission from the drop-down list. You can select **100%**, **80%**, **60%**, **40%**, or **20%**.
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 **long** or **short**.
SSID	
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 **Visible** or **Invisible**. If you select **Invisible**, 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 **Off** or **On** from the drop-down list. **On** indicates that computers connected to the device cannot communicate with each other.

Field	Description
WMM Advertise	Select whether toenable WMM. You can select **Off** or **On**.
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.
SSID1—3	
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:

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

MAC ADDRESS

MAC Address : [   ] (xx:xx:xx:xx:xx:xx)

Apply   Cancel

The following table describes the parameters in this page.

Field	Description
MAC Address	Enter the MAC address of another device that is included in 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 : [ADN-4101 ▼]

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 : [None ▼]

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

Apply   Cancel

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.

37

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 :	☑
SSID :	ADN-4101
Select Mode :	Enrollee ▾
Configuration State :	Configured ▾
Push Button :	PBC
Input Station PIN :	[ ] PIN
WPS Session Status :	

Apply   Cancel

Enabled: The WPS service is enabled by default.

📖 **Note:**

Ensure that the network card supports the WPS function.

Field	Description
Select Mode	Select **Enrollee** or **Registrar** from the drop-down list.
Configuration State	Select **Configured** or **unconfigured** from the drop-down list.
Input Station PIN	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.

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

● Press the **WPS** button on the side panel for 3 seconds.

38

● 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.

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:

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

PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

WAN Connection(s) [pppoe_0_35_0_0 ▼]

Server Name:

◉ Select a Service: [click to select ▼]

○ Custom Server: [_____]

Schedule: [always ▼] View Available Schedules:

Server IP Address: [192.168.1]

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

[Apply] [Cancel]

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 80 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	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
☐	AUTH	pppoe_0_...	113/113	tcp	113/113	192.168.1.2	Always	

Add   Edit   Delete

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 "ApplyS" to activate the DMZ host.

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

DMZ HOST

WAN Connection: pppoe_0_35_0_0 ▾

Enable DMZ: ☐

DMZ Host IP Address [ ]

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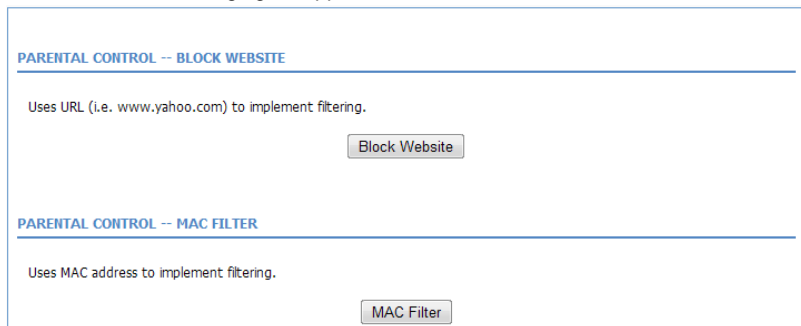
In this page, you can enable a DMZ host. In this way, access from Internet to the WAN IP address of the device is forwarded to the DMZ host and network server of the internal LAN is protected.
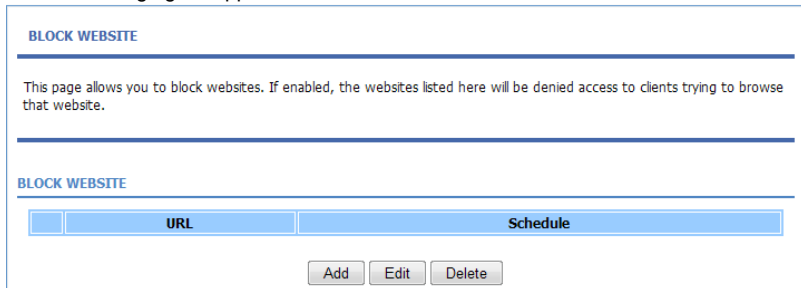Click **Apply** to save the settings.

3.3.4 Parental Control

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

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. **MAC Filter** 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:

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

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:

3.3.4.2   MAC Filter

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

BLOCK MAC ADDRESS

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".

Mac Filtering Global Policy:

⦿ **BLACK_LIST** --Allow all packets but **DENY** those matching any of specific rules listed
○ **WHITE_LIST** --Deny all packets but **ALLOW** those matching any of specific rules listed

[Apply] [Cancel]

BLOCK MAC ADDRESS--BLACKLIST

	Username	MAC	Schedule

[Add] [Edit] [Delete]

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

ADD SCHEDULE RULE

User Name:	
○ **Current PC´s MACAddress:**	00:22:b0:68:de:69
⦿ **Other MAC Address :**	
⦿ **Schedule:**	Allways ▾ View Available Schedules
○ **Manual Schedule :**	
Day(s) :	○ All Week ⦿ Select Day(s)
	☐ Sun ☐ Mon ☐ Tue ☐ Wed
	☐ Thu ☐ Fri ☐ Sat
All Day - 24 hrs	☐
art Time	☐ : ☐ (hour:minute, 24 hour time)
End Time	☐ : ☐ (hour:minute, 24 hour time)

[Apply] [Cancel]

The following table describes the parameters in this page.

Field	Description
User Name	Enter the name that identifies your configuration. For example, *kids*.
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.

Field	Description
Schedule	Select the time of MAC filter from the drop-down list. You can select **always** or **never**.
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:

3.3.5   Filtering Options

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

FILTERING OPTIONS -- IP FILTERING

Uses IP address to implement filtering.

[IP Filtering]

FILTERING OPTIONS -- BRIDGE FILTERING

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

[Bridge Filtering]

3.3.5.1   IP Filtering

In the **Fitering Options** page, click **IP Filtering**. The **FIREWALL** page as shown in the following figure appears:

IP FILTER

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

FIREWALL

Name	Interface	Type	Default action	Bytes	Pkts

[Add Filter] [Edit Filter] [Delete Filter]

RULE

Enabled	Protocol	Action	RejectType	IcmpType	OrigIP/ Mask	OrigPort	DestIP/ Mask	DestPort	Bytes	Pkts

[Add Rule] [Edit Rule] [Delete Rule]

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

Field	Description
Name	Enter the name that identifies your configuration.
Interface	Select **LAN** or the other connection from the drop-down list.
Type	Select the **In , Out or Both** from the drop-down list.
Default action	Select the **Permit or Drop** from the drop-down list.
Default Chain	Select the **Local , Forward or Both** from the drop-down list.

After set the firewall info finish, click **Add Rule** to add an IP filter rule.The page as shown in the following figure appears:

IP FILTER

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

RULE

Enabled	Protocol	Action	RejectType	IcmpType	OrigIP/ Mask	OrigPort	DestIP/ Mask	DestPort	Bytes	Pkts

[Add Rule] [Edit Rule] [Delete Rule]

RULE INFO

Notes:
1.When Protocol is 'ICMP',one of IcmpType to be selected;
2.When Action is 'Reject',one of RejectType to be selected;
3.Only when Protocol is 'TCP',may RejectType select 'tcp-reset';

Enabled:	☐
Protocol:	▼
Action:	Permit ▼
RejectType:	▼
IcmpType:	▼
origIPAddress:	
origMask:	
origStartPort:	0
origEndPort:	0
destIPAddress:	
destMask:	
destStartPort:	0
destEndPort:	0

[Apply] [Cancel]

Check the **Enabled** 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.

48

3.3.5.2   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: [   ] (xx:xx:xx:xx:xx:xx)
Source MAC Address: [   ] (xx:xx:xx:xx:xx:xx)
Frame Direction: WAN=>LAN ▾
Time schedule: always ▾   View Available Schedules
Wan interface: select all interface ▾

[Apply] [Cancel]

The following table describes the parameters in this page.

Field	Description
Protocol Type	Select the protocol type to be mapped from the

Field	Description
	drop-down list. You can select **PPPoE**, **IPv4**, **IPv6**, **AppleTalk**, **IPX**, **NetBEUI**, or **IGMP**.
Destination MAC Address	Enter the destination MAC address to be mapped.
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** and **WAN to LAN.**
Time schedule	Select the time that you want to apply the rule from the drop-down list. You can select **Always** or **Never**.
Wan interface	Select the WAN interface to be mapped from the drop-down list.

Click **Apply** to save the settings.

3.3.6   QoS Configuration

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

3.3.6.1   QoS Global Option

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

In this page, you can select or deselect the check box to enable or disable the Queuing Operation.

3.3.6.2   Queue Configuration

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

In this page, you can configure the upstream bandwidth and downstream bandwidth of each interface. The uplink rate and the downlink rate are limited according to the configured bandwidth.You also can set the priority of the queue.

The device supports the following four priority levels: 1,2,3,4. Click **Submit** to save the settings.

3.3.6.3   Classification Configuration

In the **QoS Configuration** page, click **QoS Classification Configuration**. Click **Add** and the page as shown in the following figure appears:

The following table describes the parameters in this page.

Field	Description
Classify Type	You can select **Upstream Flow Classify** or **Downstream Flow Classify**
Enable	Select or deselect the check box to enable or disable

Field	Description
	QoS classification.
SPECIFY TRAFFIC CLASSIFICATION RULES	
Input Interface	Select the physical port of the packet from the drop-down list. For example, ethernet1, ethernet2, ethernet3, and ethernet4.
Source MAC Address	Enter the source MAC address of the packet.
Source MAC Mask	Use mask 000000ffffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped.
802.1P	Select the 802.1p priority of the packet from the drop-down list. You can select **Not match** or a value in the range of 0—7. Note that this function is not supported at the moment.
Source IPv4 Address	Enter the Source IP address of the packet.
Source subnet mask	Enter the Source subnet mask of the packet.
Destination IPv4 Address	Enter the destination IP address of the packet.
Destination subnet mask	Enter the destination subnet mask of the packet.
Ethernet Type	Select the layer 2 protocol type from the drop-down list. For example, IP protocol and IPX protocol.
DSCP check	You can use this feature to differentiate the complex data type from the drop-down list.
Protocol Type	Select the protocol on this column.
Source port range	Enter the source port range of the packet.
Destination port range	Enter the destination port range of the packet.
CLASSIFY MATCH RESULT	
Classify Queue	Specify the queue to which the packet belongs. You can set the queue in the classification configuration.
DSCP Mark	Attach the DSCP mark to the mapped packet.
Cos Mark	Attach the 802.1p mark to the mapped packet.

Click **Submit** 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:

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:

The following table describes the parameters in this page.

Field	Description
Wan Connection	Select the WAN interface of the DNS server to be connected from the drop-down list.
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.
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 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 (DyndDNS.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

Add Edit Delete

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

ADD DYNAMIC DNS

DDNS provider: DynDNS.org

Hostname:

Interface: pppoe_0_35_0_0

Username:

Password:

Apply Cancel

The following table describes the parameters in this page.

56

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

PPTP

[PPTP]

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

3.3.11 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
☐	Lan1	ethernet1,ethernet2,ethernet3,ethernet4,wlan0,wlan0-vap0,wlan0-vap1,...

[Add] [Edit] [Delete]

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

	[->] [<-]	ethernet1 ethernet2 ethernet3 ethernet4 wlan0 wlan0-vap0 wlan0-vap1 wlan0-vap2

[Apply] [Cancel]

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.

3.3.11.1   IGMP Proxy

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

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 click **Apply** to save the settings.

3.3.11.2   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.

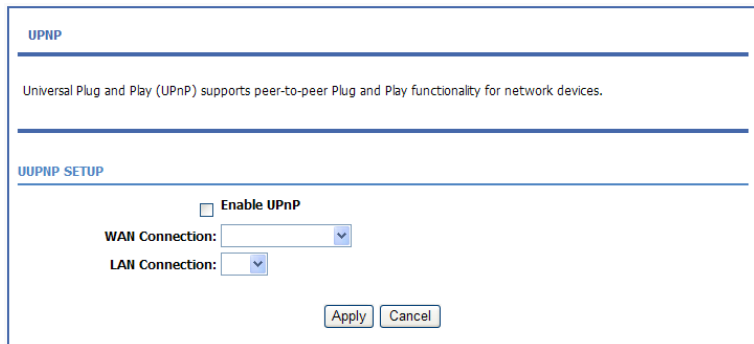In the **NETWORK TOOLS** page, click **IGMP Snooping**. The page as shown in the following figure appears:

Click **Apply** to save the settings.

3.3.11.3   UPnP

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

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.

3.3.11.4 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. You need to disable DSL before you change the ADSL mode.

ADSL SETTINGS

☑ **Enable DSL**

☑ **G.Dmt Enabled**
☐ **G.Lite Enabled**
☐ **T1.413 Enabled**
☑ **ADSL2 Enabled**
☑ **AnnexL Enabled**
☑ **ADSL2+ Enabled**
☐ **AnnexM Enabled**
Capability
☑ **Bitswap Enable**
☐ **SRA Enable**
☐ **1 bit Constellation Modulation Enable**

Apply

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.

3.3.11.5 SNMP

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

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 **v1** or **v2c**.

Click **Apply** to save the settings.

3.3.11.6　TR-069

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

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

Field	Description
TR069 Configuration	You can select **Disabled** or **Enabled** to disable or enable TR-069 configuraion.
Inform	You can select **Disabled** or **Enabled** to disable or enable notification. ● **Disabled** indicates that the device does not automatically send requests to the TR069 server. ● **Enabled** indicates that the device automatically sends a request of connection to the TR069 server. The following function items are available only when **Inform** is set to **Enabled**.

| Field	Description
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.
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.

3.3.11.7 Certificates

In the **NETWORK TOOLS** page, click **Certificates**. The **Certificates** page as shown in the following figure appears:
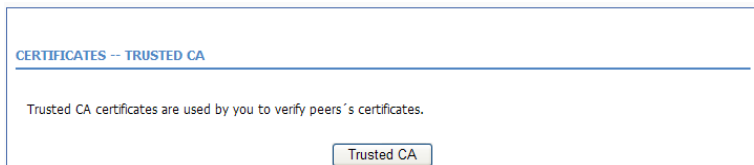
Click **Trusted CA** and the page as shown in the following figure appears:
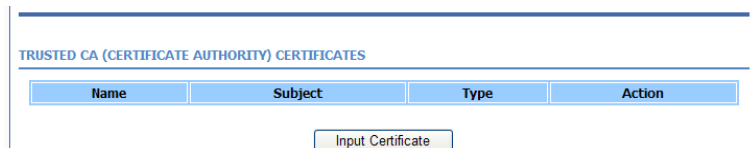
📖 **Note:**

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-----

[Back] [Apply] [Cancel]

3.3.12 Routing

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

STATIC ROUTE

Static Route.

<div align="center">[Static Route]</div>

POLICY ROUTE

Policy Route.

<div align="center">[Policy Route]</div>

DEFAULT GATEWAY

Default Gateway.

<div align="center">[Default Gateway]</div>

This page contains the following function items: **Static Route, Policy Router** and **Default Gateway**.

3.3.12.1 Static Route

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

STATIC ROUTE

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

A maximum 30 entries can be configured.

ROUTING -- STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface

<div align="center">[Add] [Edit] [Delete]</div>

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

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..**

3.3.12.2 Policy Route

Choose **Advanced** > **Routing** and click **Policy Route.** Click Add and the page as shown in the following figure appears:

In this page, you can select the interfaces on your device that use RIP 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.

3.3.12.3 Default Gateway

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

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.

3.3.13 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

Add   Edit   Delete

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)

Apply   Cancel

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.

3.3.14 NAT

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

Traditional NAT would allow hosts within a Internal network to transparently access hosts in the external network, you can select **Single IP** or **IP Range** with the Internal and External IP type and enter the Internal and External IP address to decide witch Internal IP address transparently the specify External IP address.

3.3.15 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:

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 **Browse…** to select the configuration file of device and click **Update Settings** to update the configuration 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 to locate the image file.

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:	V1.4
Current Firmware Date:	2011-05-10
Select File:	[_____] Browse...
Clear Config:	☐

Update Firmware

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:

74

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:

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

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 adresses 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

Add   Delete

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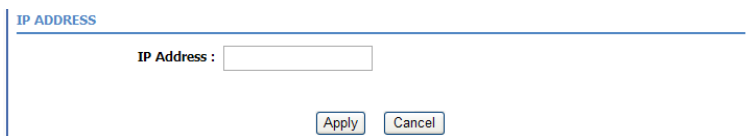
Select **Enable Access Control Mode** to enable ACL.

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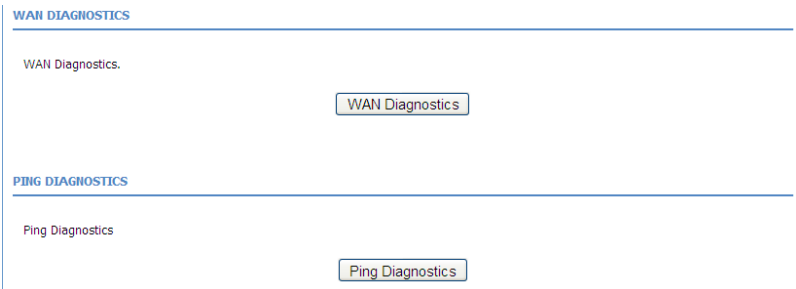
Enter the IP address of the desired device in the **IP Address** field and click **Apply** to apply the settings.

3.4.4   Diagnostics

Choose **Management** > **Diagnosis**. The page as shown in the following figure appears:
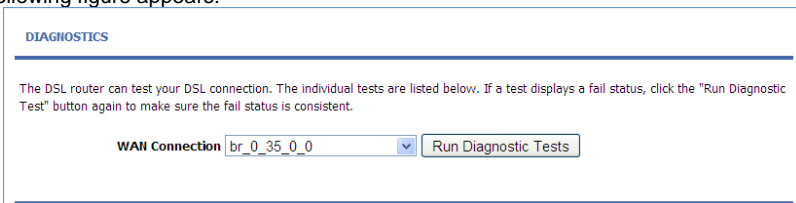
This page contains **WAN Diagonstics** and **Ping Diagnostics.**

3.4.4.1   WAN Diagnostics

In the **Diagnosis** page, click **WAN Diagnostics**. The page as shown in the following figure appears:

In this page, you can test the connection status of the device. Click **Run 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	FAIL
Test your LAN 2 Connection	FAIL
Test your LAN 3 Connection	PASS
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

3.4.4.2   Ping Diagnostics

In the **Diagnosis** page, click **Ping Diagnostics**. The page as shown in the following figure appears:

PING DIAGNOSTICS

Run Ping diagnostics.

PING CONFIGURATION

Host :	192.168.1.1
Number of Packets Repreat :	5
Timeout (ms) :	1000
Packet Size :	56
Ping Results :	

[Ping...]

In this page, you can test the IP address on the same segment connect status of the device. Click **Ping** to run diagnostics.

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 :   [   ]

[Apply] [Cancel] [View System Log] [View Firewall Log]

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** or **View Firewall 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:
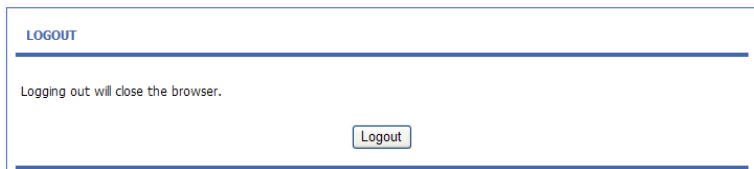
Click **Logout** to log out of the configuration page.

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-4101
Serial Number :	00304f123456
Time and Date :	2010-10-10 00:05:03
HardwareVersion :	ADN-4101
SoftwareVersion :	V1.4
Firmware Version :	V1.4
System Up Time :	00:05:58

INTERNET INFO

Internet Connection Status : pppoe_0_35_0_0_Internet ▾

Internet Connection Status:	Disconnected
Wan service type:	Internet
Default Gateway:	
Preferred DNS Server:	
Alternate DNS Server:	
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0
Data Time Counter (Second):	

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address
PVC:0/35	pppoe_0_35_0_0_Internet	PPPOE	Disable	Disable	

WIRELESS INFO

select wireless : ADN-4101 ▾

MAC Address:	00:30:4f:12:34:5f
Status:	Enable
Network Name (SSID):	ADN-4101
Visibility:	Visible
Security Mode:	Basic

LOCAL NETWORK INFO

MAC Address:	00:30:4f:12:34:56
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable

82

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

Refresh

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

Refresh

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
ADN-4101	66034626	879783	0	0	7900049	34189	0	0

INTERNET

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

ADSL

Mode:	0
Type:	0
Line Coding:	Enable
Status:	ACTIVATING.
Up Time:	

	Downstream	Upstream
SNR Margin (0.1dB):	0	0
Attenuation (0.1dB):	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
Data Counter:	0 [Clear]	0 [Clear]
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
CRC Errors:	0	0
FEC Errors:	0	0
Total ES	0	0
Total Frames	0	510

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, !-reject, G-getway, 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 **Staus** > **Logout**. The page as shown in the following figure appears:

LOGOUT

Logging out will close the browser.

Logout

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