

HUAWEI

Aolynk DR811/DR814 ADSL2+Broadband Router
User Manual

Aolynk DR811/DR814 ADSL2+Broadband Router

User Manual

Manual Version T2-080127-20050126-C-1.00

BOM 3101A027

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. If you purchase the products from the sales agent of Huawei Technologies Co., Ltd., please contact our sales agent. If you purchase the products from Huawei Technologies Co., Ltd. directly, please feel free to contact our local office, customer care center or company headquarters.

Huawei Technologies Co., Ltd.

Address: East of Liuhe Road, Zhijiang Science Park,

Hangzhou, P. R. China

Website: <http://www.huawei-3com.com>

Email: soho@huawei-3com.com

Copyright © 2005 Huawei Technologies Co., Ltd.

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks

 , HUAWEI, C&C08, EAST8000, HONET,  , ViewPoint, INtess, ETS, DMC, TELLIN, InfoLink, Netkey, Quidway, SYNLOCK, Radium,  M900/M1800, TELESIGHT, Quidview, Musa, Airbridge, Tellwin, Inmedia, VRP, DOPRA, iTELLIN, HUAWEI OptiX, C&C08iNET, NETENGINE, OptiX, iSite, U-SYS, iMUSE, OpenEye, Lansway, SmartAX, infoX, TopEng are trademarks of Huawei Technologies Co., Ltd.

All other trademarks mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.

Table of Contents

1 Introductions	3
1.1 Product Overview.....	3
1.2 Appearance	4
1.2.1 Front View	4
1.2.2 Rear View.....	5
1.3 Features	5
1.4 Parts Check	6
2 Connecting Your Device	7
2.1 Overview.....	7
2.2 Steps	7
2.3 Finish.....	8
3 Getting Started with the Web Pages.....	9
3.1 Accessing the Web Pages.....	9
3.2 Web Page Layout	11
3.3 Commonly Used Buttons.....	12
3.4 Testing Your Setup	13
3.5 Default Device Settings.....	14
4 Web-based Management.....	15
4.1 Quick Setup	15
4.2 WAN Setting	16
4.3 DNS Relay	18
4.4 LAN Setting.....	19
4.5 DHCP	21
4.6 Route.....	22
4.7 Security Interface	25
4.8 DMZ Configuration.....	28
4.9 Security Policy	30
4.10 Trigger	31
4.11 IDS	34
4.12 SNTP	35
4.13 ZIPB	36
4.14 Password.....	38
4.15 Remote Access.....	38
4.16 Restart Router.....	39
4.17 Configuration Backup/Restore.....	40
4.18 Upgrade.....	42
4.19 Status	43

4.20 Log	45
4.21 PVC Scan	46
4.22 Save Configure	47
5 Configuring Your Computers	48
5.1 Configuring Ethernet PCs.....	48
5.1.1 Before You Begin.....	48
5.1.2 Windows® XP PCs	48
5.1.3 Windows 2000 PCs.....	49
5.1.4 Windows Me PCs.....	50
5.1.5 Windows 95, 98 PCs.....	50
5.1.6 Windows NT 4.0 Workstations	51
5.1.7 Assigning Static Internet Information to Your PCs	52
5.2 Configuring a PC Connected by USB Port.....	53
5.2.1 Connecting a Computer to the USB Port by a USB cable	53
5.2.2 Installing the USB Driver	53
5.2.3 Configuring IP Properties on PC Connected by USB Port.....	56
6 IP Addresses, Network Masks, and Subnets	57
6.1 IP Addresses	57
6.1.1 Structure of an IP Address	57
6.1.2 Network Classes.....	58
6.2 Subnet Masks	58
7 Service Configuration	60
7.1 Configuration Overview	60
7.2 PureBridge.....	61
7.3 DHCP/StaticIP	62
7.4 IPoA.....	62
7.5 PPPoA.....	63
7.6 PPPoE.....	63
8 Troubleshooting.....	65
8.1 Troubleshooting Suggestions	65
8.2 Diagnosing Problem Using IP Utilities.....	67
8.2.1 ping	67
8.2.2 nslookup	68
9 Appendix - Glossary.....	69

1 Introductions

1.1 Product Overview

DSL (Digital Subscriber Line) refers to a technology used to increase the data capacity of standard twisted-pair wires that are generally used to connect most households to the telephone network. In addition, this technology allows simultaneous voice and high-speed data transmission over a single pair of telephone wires.

ADSL (Asymmetric Digital Subscriber Line), as its name indicates, is an asymmetrical data transmission technology with higher traffic rates downstream and lower traffic rates upstream. It is suitable for Internet users because information is usually downloaded more often than uploaded, such as when surfing the web or downloading files.

The Aolynk ADSL2+ router with embedded ADSL2+ technology brings up high-speed internet access and remote connection features, which make it an ideal solution for small businesses and SOHO users.

DR811/DR814 uses the ATM over ADSL2+ technology to communicate with the central office providing the ADSL2+ service. As ATM PVC supports connections of various types such as PPPoE, PPPoA, IPoA and bridge, Aolynk DR811/DR814 delivers great networking flexibility and accommodates diversified requirements.

This type of router falls into 4 models as below.

Table 1-1 DR series of routers

Model	Difference
DR814	ADSL2+ over POTS, 4 Ethernet ports
DR814I	ADSL2+ over ISDN, 4 Ethernet ports
DR811	ADSL2+ over POTS, 1 Ethernet port
DR811I	ADSL2+ over ISDN, 1 Ethernet port

1.2 Appearance

1.2.1 Front View

The front panel contains lights called LEDs that indicate the status of the unit.



Figure 1-1 Front panel

Table 1-2 LED description

LED	Status	Description
Power	ON	Power has been switched on and is working normally
	OFF	Power is switched off or fails
Diag	-	For factory test only
Link	ON	ADSL loop is brought UP
	Blinking	Starting up
	OFF	ADSL loop is down
Act	Blinking	Data is being transmitted or received through ADSL
	OFF	No data transmission activities present on the link
USB	ON	USB connection established
	OFF	No USB cable connected
LAN1/2/3/4 (Only one for DR811)	ON	Ethernet link is up
	Blinking	Ethernet interface is transmitting or receiving data
	OFF	No link is up

1.2.2 Rear View

All cable connections to the ADSL router are made at the rear panel. A factory reset button is located here as well.

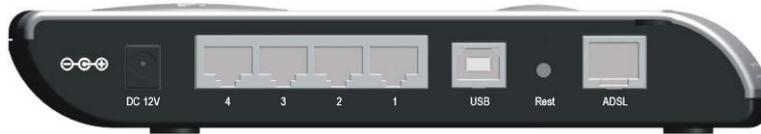


Figure 1-2 Rear panel connections

Table 1-3 Port description

Interface	Quantity	Connector	Description
Ethernet	1 (DR811) 4 (DR814)	RJ45	10/100Base-TX 10/100 Mbps auto-negotiation MDI/MDIX auto-sensing Compatible with IEEE802.3/802.3u
USB	1	Series-B Receptacle	USB 1.1
ADSL	1	RJ11	ANSI T1.413 Issue 2 ITU G.992.1 AnnexA G.dmt ITU G.992.2 G.lite ITU G.992.3 ADSL2 ITU G.992.5 ADSL2+
Reset	1	-	Restoring to factory default settings (For this purpose, you are required to hold down the button for at least 5 seconds.)

1.3 Features

The list below contains the main features of the device which make it excellent for network connections.

Features include:

- | Internal DSL modem for high-speed Internet access.
- | Data rates up to 20Mbps for downstream and 1Mbps for upstream.
- | Uses NAT to allow your entire network's PCs to connect to the Internet using only one (purchased) IP Address.
- | Supports PPPoE that enables users to seamlessly connect to ISPs via the familiar "dial-up" connection interface.

- | Built-in firewall for protecting your PCs from outside intruders.
- | Supports DHCP client to acquire either a dynamic IP Address or a fixed IP Address from the ISP.
- | Built-in DHCP server for automatically assigning and managing LAN IP addresses.
- | USB port for connecting a USB-enabled PC.
- | Zero Installation PPP Bridge (ZIPB), Network address translation (NAT), Firewall, and IP filtering functions to provide security for your LAN.
- | Network configuration through DHCP Server and DHCP Client.
- | Services including IP route and DNS configuration and IP and DSL performance monitoring.
- | Allows multiple users to access the Internet at the same time by providing maximum Internet utilization to multiple users sharing a single public IP Address.
- | Allows users on Ethernet LAN to transfer data to each other.
- | Friendly built-in web-based graphical user interface for easy configuration and management through common web browsers.

1.4 Parts Check

Please check the arrived shipment against the following packing list, making sure all the items are included and in good condition:

Table 1-4 Packing list

Interface	Quantity
Aolynk ADSL2+ Broadband Router	1
Power adaptor	1
Telephone cables	1
Ethernet cable	1
USB cable	1
Screw and anchor	2
Quick Start manual	1
Driver & Manual CD	1
Quality card	1

2 Connecting Your Device

2.1 Overview

This chapter provides basic instructions for connecting the ADSL router to a computer or LAN.

This chapter assumes that you have already established a DSL service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

When selecting a location for the ADSL router, allow ample clearance to access the connections on the rear panel. For convenience, try to place the ADSL router near your computer so you can monitor the LED indicators. Allow some space above the ADSL router for ventilation to avoid problems with overheating.

The diagram below illustrates the hardware connections. Refer to the steps that follow for specific instructions.

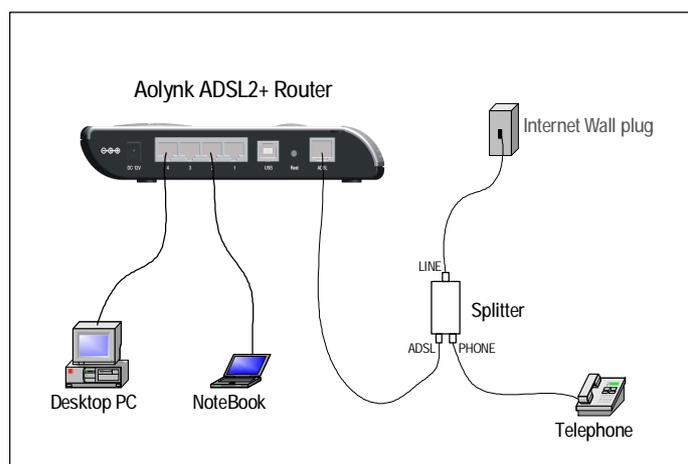


Figure 2-1 Hardware connections

2.2 Steps

- 1) Connect the DSL cable and optional telephone

Two options are available for connecting the ADSL cable:

Option 1: Connect the ADSL port (same as a regular telephone port) on the rear panel of DR811/DR814 to the wall jack of telephone line using the telephone cable.

Option 2: Connect the ADSL port on DR811/DR814 and a telephone set to a splitter, and then the splitter to the wall jack of telephone line. Thus you may place phone calls when accessing the Internet.

2) Connect the Ethernet cable

You can choose one of the following two options:

- 1 If you are connecting a LAN hub to the ADSL router, attach one end of the provided Ethernet cable to a regular hub port and the other to the one of the Ethernet ports on the device.
- 1 If you are connecting a single Ethernet computer to the ADSL router, attach it directly to the one of the Ethernet ports on the device via an Ethernet cable.

3) Attach the power connector

Connect the power adapter to the Power connector on the back of the device and plug the adapter into a wall outlet or power strip. DR811/DR814 has no power switch; so it is powered on soon after the power cable is connected to the power jacket.

4) Configure your Ethernet PCs

You must also configure the Internet properties on your Ethernet PCs. Refer to "5.1 Configuring Ethernet PCs".

5) Install USB software and connect the USB cable

Only include this step if you want users to use the USB port.

You can attach a single computer to the device using a USB cable. The USB port is useful if you have a USB-enabled PC that does not have a network interface card for attaching to your Ethernet network.

Before attaching the USB cable, you must install a USB driver on your PC and configure the computer. For complete instructions, refer to "5.2 Configuring a PC Connected by USB Port."

2.3 Finish

After setting up and configuring the device and PCs, you can log on to the device by following the instructions in "3 Getting Started with the Web Pages".

3 Getting Started with the Web Pages

The ADSL router provides a series of web pages that function as an interface for managing the device. These web pages enable you to configure the device to meet the needs of your network. You can access them through your web browser from any PC connected to the device via the LAN or USB port.

3.1 Accessing the Web Pages

To access the web pages, you need the following:

- | A PC or laptop connected to the LAN or USB port on the device.
- | A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v5.0 or Netscape v4. For the best display quality, use Internet Explorer v6, or Netscape v6.1.

1. The default IP settings for the ADSL router are as follows:

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

Before performing the above configurations on the ADSL router, first have the computer set in the same subnet with the router. To do so, first install and enable the TCP/IP protocol (refer to 5.1 Configuring Ethernet PCs), and then set an IP address and a subnet mask, for example, **192.168.1.100** and **255.255.255.0**. Make sure the IP settings place the computer in the same subnet as the router.

2. If the browser software on the computer you are using is configured to use a proxy server for Internet access, it is necessary to first disable the proxy connection.

In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:

- | In the Explorer Window, select and click on **Tools->Internet Options** to enter the **Internet Options** window.

- 1 In the **Internet Options** window, click the **Connections** tab and then click on the **LAN Settings** button.
- 1 Verify that the **Use proxy server** option is **NOT** checked. If it is checked, click in the checked box to deselect the option and then click **OK**.

3. From any of the LAN computers, open the web browser, type "<http://192.168.1.1>" in the web address (or location) box, and press [Enter]. A login screen is displayed:



Figure 3-1 Login screen

4. Enter your user name and password. The first time you log into the program, use the default user ID and password (*admin* and *admin*)

& Note:

You can change the password at any time. For the default user ID, admin, only the password can be changed. Refer to 4.14 Password.

5. Click OK. The Welcome page is displayed:

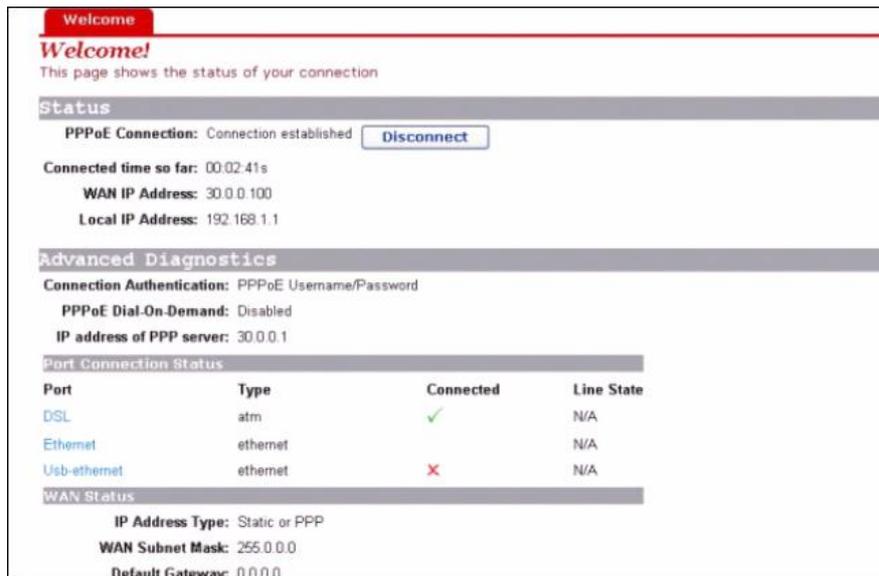


Figure 3-2 The welcome page

This is the first page that is displayed each time you log in to the web pages.

& Note:

If you receive an error message or the Welcome page is not displayed, refer to "8.1 Troubleshooting Suggestions".

3.2 Web Page Layout

The web pages provide information that allows you to configure your device. Links to configuration pages are listed in the Main Menu on the left-hand side of the screen. Click on an individual menu entry to display a page in the Main Frame, which is in the white area.

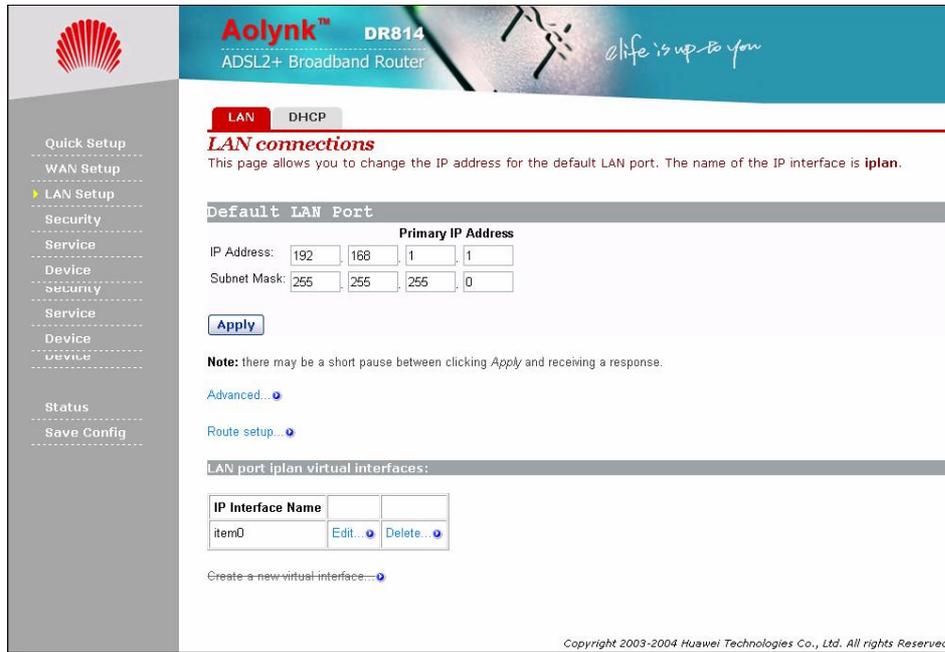
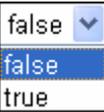


Figure 3-3 The page layout

3.3 Commonly Used Buttons

The following buttons are used throughout the web pages:

Table 3-1 Buttons in the web pages

Button	Function
  	These buttons appear at the end of a series of configuration pages. Click on these buttons to confirm and save the changes you have made.
	This button appears on configuration pages. Click on this button to restore the original settings.
	This button appears on some pop-up configuration pages. Click on this button to cancel the configurations you have made, close the page, and return to the Main Frame.
<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Radio buttons, which appear on many configuration pages. Sometimes it may be necessary to select one radio button from two or more available. You cannot select more than one radio button at a time.
	Drop-down list buttons, which appear on many configuration pages. Click to select one.

The following terms are used throughout this guide in association with these buttons:

- 1 *Click* – Position the cursor over a button, menu entry or link on the screen and click the left mouse button. This performs an action, such as displaying a new page.
- 1 *Select* – Usually used when describing which radio button to select from a list, or which entry to select from a drop-down list. Position the cursor over the entry and left-click to select it. This does not perform an action – you will also be required to click on a button, menu entry or link in order to proceed.

3.4 Testing Your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the device’s DSL connection to access the Internet.

To test the connection, connect a single Ethernet computer to the ADSL router, plug the power cable to POWER socket of the device, wait for 1 minute and then verify that the LEDs are illuminating as follows:

Table 3-2 Router LEDs

LED	Behavior
Power	Solid green to indicate that the power has been switched on. If this light is not on, check the power cable attachment.
Link	Flashing on/off while the ADSL line of the device is being activated. After about 20-30 seconds, solid green to indicate that the device is now communicating normally with the central office.
Act	Flashing on/off while data is being transmitted. Going off indicates that no data transmission happens.
LAN	Solid green to indicate that the Ethernet link is up. Flashing on/off while Ethernet interface is transmitting or receiving data.
USB	Solid green to indicate that the USB connection is operational.

If the LEDs illuminate as expected, test your Internet connection from the LAN computer (and from the USB computer, if applicable): Open your web browser, and type the URL of any external website (such as <http://www.yahoo.com>). The LED labeled ADSL Act should be blinking rapidly and may appear solid as the device connects to the site.

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. For details, refer to “4.2 WAN Setting”. If the LEDs still do not illuminate as expected, or the web page is not displayed, refer to “8.1 Troubleshooting Suggestions”, or contact your ISP for assistance.

3.5 Default Device Settings

In addition to handling the DSL connection to your ISP, the ADSL router can provide a variety of services to your network. The device is pre-configured with default settings for use with a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review these settings to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

We strongly recommend that you contact your ISP prior to changing the default configuration.

Table 3-3 Default settings

Option	Default Setting	Explanation/Instruction
DSL Port IP Address	Unnumbered interface: 0.0.0.0 Subnet mask: 0.0.0.0	This is the temporary public IP address of the WAN port on the device. It is an unnumbered interface that is replaced as soon as your ISP assigns a 'real' IP address. Refer to 7 Service Configuration.
LAN Port IP Address	Assigned static IP address: 192.168.1.1 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. Refer to 6 IP Addresses, Network Masks, and Subnets.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.2 to 192.168.1.21	The ADSL router maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in 5.1 Configuring Ethernet PCs.
NAT (Network Address Translation)	NAT enabled	Your computers' private IP addresses (refer to DHCP above) will be translated to your public IP address whenever they access the Internet. Refer to 4.7 Security Interface.
DSL mode	MultiMode	Can be configured to multiple standard DSL line modes.
Default Username: Password	admin:admin	Use this account to login web-based setup pages.

4 Web-based Management

This chapter tells you how to use the web-based configuration and management software to configure the ADSL router. It is organized basing on the order of the items in the navigation tree to describe the functions of the ADSL router and their configuration procedures.

4.1 Quick Setup

Click **Quick setup** in the Main menu to open the **Quick Start** page.

This page allows you to:

- 1 Choose the login type.
- 1 Set up authentication & login details which may be required by your ISP.

To configure **DHCP Login Options**, click the radio button labeled **No Login / DHCP**, the following page is displayed:

The screenshot shows the 'Quick Start' configuration page. At the top, there is a red header with 'Quick Start' and a sub-header 'Quick Start'. Below this, a message states: 'This page allows you to set up some authentication & login details which may be required by your ISP'. The 'Login Type' section has two radio buttons: 'No Login / DHCP' (selected) and 'PPPoE Login'. The 'DHCP Login Options' section contains several input fields: 'VPI' (0), 'VCI' (36), 'Special DHCP host name', and 'Domain Name for Clients to send with DNS Requests'. Below these fields are 'Apply' and 'Reset' buttons. At the bottom, there is a copyright notice: 'Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved'.

Figure 4-1 Quick setup page – no login

Enter VCI and VPI values as specified by your ISP; specify the **Special DHCP host name** and/or **Domain Name for Clients to send with DNS Requests**, if needed (usually not needed); then click the **Apply** button.

To configure **PPPoE Login Options**, click the radio button labeled **PPPoE Login**, the following page is displayed:

The screenshot shows a web-based configuration page titled "Quick Start". It contains the following sections:

- Quick Start**: A sub-header with a red background.
- Quick Start**: A sub-header in red text.
- This page allows you to set up some authentication & login details which may be required by your ISP**: A descriptive sentence.
- Login Type**: A section with two radio buttons: "No Login / DHCP" (unselected) and "PPPoE Login" (selected).
- PPPoE Login Setup**: A section with input fields for:
 - VPI: 0
 - VCI: 35
 - PPPoE Username: [empty]
 - PPPoE Password: [empty]
 - PPPoE Password (confirm): [empty]
- PPPoE Login Options**: A section with:
 - PPPoE Service Name: [empty]
 - Dial On Demand
 - Auto-disconnect idle time (in minutes): 0
 - Keep-Alive
 - You may need to change the following advanced option to successfully resolve host names from your ISP's name-server.*
 - Domain Name for Clients to send with DNS Requests: [empty]
- Apply** and **Reset** buttons.
- Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 4-2 Quick setup page – PPPoE

Enter VCI and VPI values as specified by your ISP, the PPPoE login authentication info and configuration, and then click the **Apply** button.

& Note:

Avoid using the same pair of VPI and VCI values for configuring DHCP and PPPoE login options.

4.2 WAN Setting

Click **WAN Setup** in the Main menu and choose the **WAN** tab in the Main Frame to open the **WAN Connection Configuration** page.

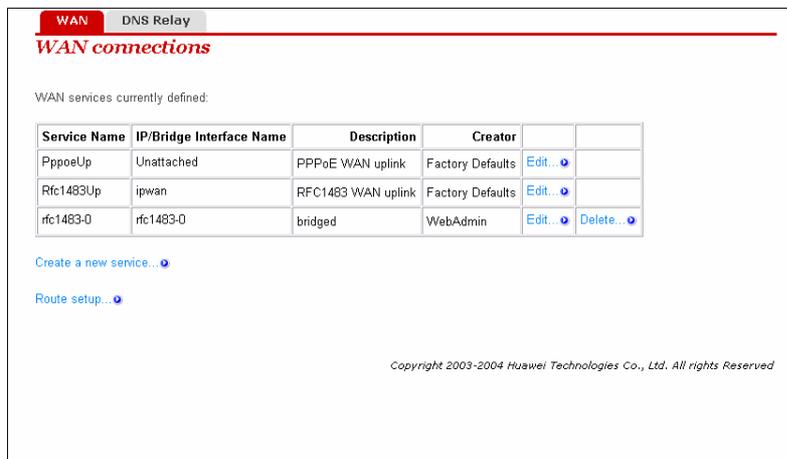


Figure 4-3 WAN setting

This page allows you to:

- | Edit an existing WAN service present in the WAN service list.
- | Delete a WAN service present in the WAN service list.
- | Add a new WAN service to the WAN service list.
- | Edit a route.

To edit a present WAN service, click the corresponding [Edit...](#) label to see the edit page as the following one. If needed, change the values of the service options then click the [Change](#) button.

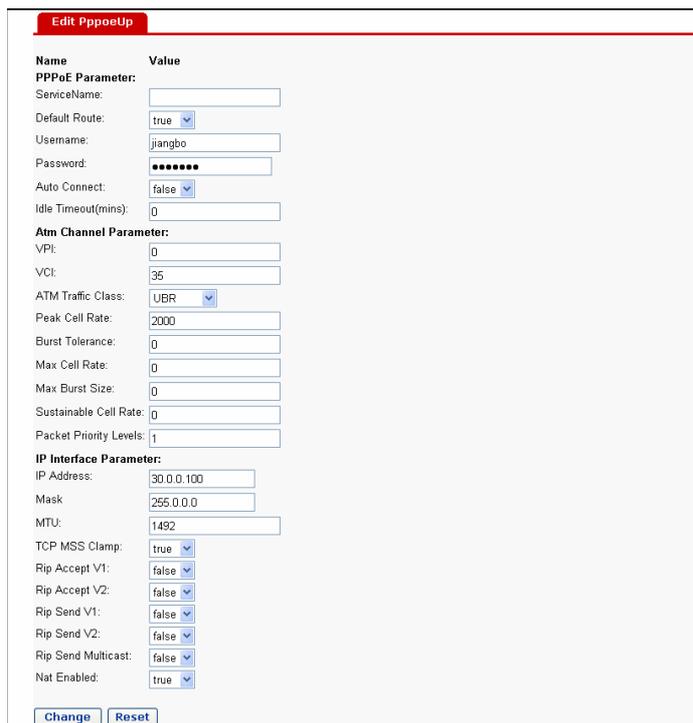


Figure 4-4 Edit WAN settings

To delete a present WAN service, click the [Delete...](#) label that corresponds to this item to open the web page **Delete WAN connection**.

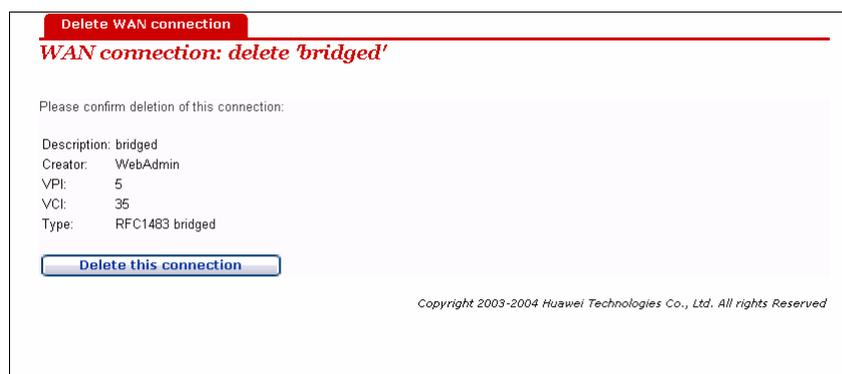


Figure 4-5 Delete WAN settings

Click the  button to delete the service.

& Note:

Only services created by the user can be edited. The first two items in the WAN service list are default services.

To add a new WAN service, click the [Create a new service...](#) label to open the web page **WAN Connection: create service**. To add a new service, refer to 7 Service Configuration.

To configure the routes, click the [Route setup...](#) label to open the route configuration page. To edit routes, refer to 4.6 Route.

4.3 DNS Relay

A DNS relay server forwards the requests received from the PCs on the LAN to the actual DNS servers. When the unit is configured as a DNS relay server, users will not need to change the DNS server IP address on their PC whenever their ISP changes DNS servers, or when the user connects to a different ISP.

Click **WAN Setup** in the Main menu and choose the **DNS Relay** tab in the Main Frame to open the DNS configuration page.

WAN **DNS Relay**

DNS Relay

This page allows you to enter a list of DNS server IP addresses that the DNS relay can forward DNS queries to.

Edit DNS server list

Use this section to edit existing DNS server addresses present in the DNS relay's list. The first address should be the Primary DNS server, the second address should be the Secondary DNS server, and so on. You cannot have more than three addresses at a time.

DNS server IP address	Hostname	Delete?
218 72 1 1		<input checked="" type="checkbox"/>

Add new DNS server

Use this section to add a new DNS server to the DNS relay's list.

New DNS server IP address:

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 4-6 DNS relay

This page allows you to:

- | Edit a DNS server address present in the DNS relay list.
- | Add a new DNS server to the DNS relay list.
- | Delete a present DSN server.

To edit a present DNS server item, modify the server's IP address and click the button.

To delete a present DNS server, check the corresponding check box and click the button.

To add a new DNS server, enter the server's IP address, and then click the button. For more details about IP address, refer to 6.1 IP Addresses.

& Note:

In DNS Server list, the first address should correspond to the Primary DNS server; the second address should correspond to the Secondary DNS server, and so on. You cannot have more than three addresses at a time.

4.4 LAN Setting

Click **LAN Setup** in the Main menu and choose the **LAN** tab in the Main Frame to open the LAN configuration page.

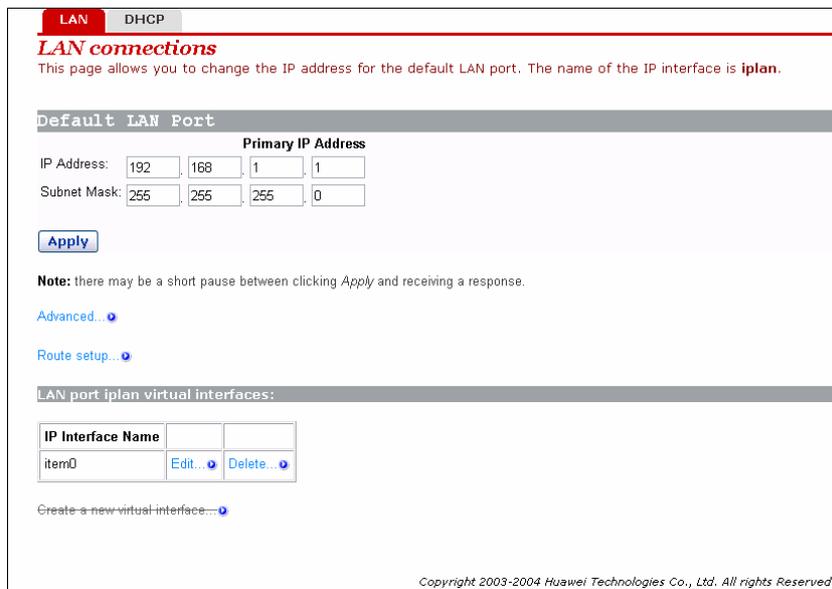


Figure 4-7 LAN setting

This page allows you to:

- | View and modify the LAN IP address and subnet mask.
- | Advanced configuration about LAN setting.
- | Edit a route.
- | Create a virtual interface.
- | Edit the current virtual interface.
- | Delete the current virtual interface.

To modify the LAN IP address and subnet mask, enter the IP address and/or subnet mask, and then click the button. For more details about IP address, refer to 6.1 IP Addresses.

To configure the advanced attributes about LAN settings, click the [Advanced...](#) label to open the web page **Edit iplan**. If needed, change the values of options, and then click the button.

Name	Value
IP Address:	<input type="text" value="192.168.1.1"/>
Mask	<input type="text" value="255.255.255.0"/>
MTU:	<input type="text" value="1500"/>
TCP MSS Clamp:	<input type="button" value="false"/>
Rip Accept V1:	<input type="button" value="false"/>
Rip Accept V2:	<input type="button" value="false"/>
Rip Send V1:	<input type="button" value="false"/>
Rip Send V2:	<input type="button" value="false"/>
Rip Send Multicast:	<input type="button" value="false"/>
Nat Enabled:	<input type="button" value="false"/>

Figure 4-8 Edit iplan interface

To configure the routes, click the [Route setup...](#) label to open the route configuration page. To edit routes, refer to 4.6 Route.

To create a new virtual interface, click **Create a new virtual interface** to enter the **Create virtual interface** page. Input an IP address for the virtual interface and/or a subnet (Note that the IP address of the virtual interface must not belong to the same subnet as that of the LAN interface), and then press **Apply** to enable it. Refer to 6.1 IP Addresses for more information about IP address. The virtual interface created here can be used for DMZ configuration. Refer to 4.8 DMZ Configuration for more information.

To edit the current virtual interface, click **<Edit...>**. Then in the new page, change the settings if necessary, and press **<change>** to confirm your changes.

To delete the current virtual interface, click **<Delete...>**. Then in the new page, click **<Delete this connection...>** to confirm your deletion.

& Note:

Only after the user has created a virtual interface can you create a new security interface in **Security Interface Configuration** page, refer to 4.7 Security Interface for more information.

4.5 DHCP

As a DHCP server, the unit maintains a pool of IP addresses and distributes them to LAN hosts whenever those hosts are switched on.

Click **LAN Setup** in the Main menu and choose the **DHCP** tab in the Main Frame to open the DHCP configuration page.

LAN DHCP

DHCP Server
This page allows editing of DHCP server subnets . You may also enable and disable the DHCP server from here.

DHCP Enable

The DHCP server is currently **enabled**

IP addresses to be available on this subnet
You need to make sure that the start and end addresses offered in this range are within the subnet of your network. Alternatively, you may check the **Use a default range** box to assign a suitable default IP address pool on this subnet.

Start of address range: 192 168 1 2
End of address range: 192 168 1 51
Use a default range:
Local domain name: local.lan

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 4-9 DHCP setting

This page allows you to:

- 1 Enable/disable the DHCP server.
- 1 Assign the DHCP server address pool.

If the DHCP server is currently disabled, you may click the button to enable it. If the DHCP server is currently enabled, you may click the button to disable it.

The DHCP server (if enabled) will use the address pool defined in this page to provide IP addresses to requesting DHCP clients. You may check the **Use the default range** box to assign a suitable default IP address pool on this subnet (recommended). If needed, you can change the DHCP address pool manually, but you must uncheck the **Use the default range** box in the meantime.

To change the DHCP address pool manually, enter the start IP address and/or end IP address, and then click the button. For more details about IP address, refer to 6.1 IP Addresses.

Enter a DNS suffix in the **Local domain name** box as needed. This option is usually used for small- to moderate-sized enterprises. Common home users do not need to set it.

4.6 Route

This option allows you to create static IP routes to destination addresses via an IP interface name or a gateway address.

To access the route configuration page, follow anyone of these steps:

- | Click **WAN Setup** in the Main menu and choose the **WAN** tab in the Main Frame to open the WAN connection configuration page, and then click the [Route setup...](#) label to open the route configuration page.
- | Click **LAN Setup** in the Main menu and choose the **LAN** tab in the Main Frame to open the LAN configuration page, and then click the [Route setup...](#) label to open the route configuration page.
- | Click **Status** in the Main menu and choose the **Status** tab in the Main Frame to open the status page, and then click the [Route setup...](#) label to open the route configuration page.

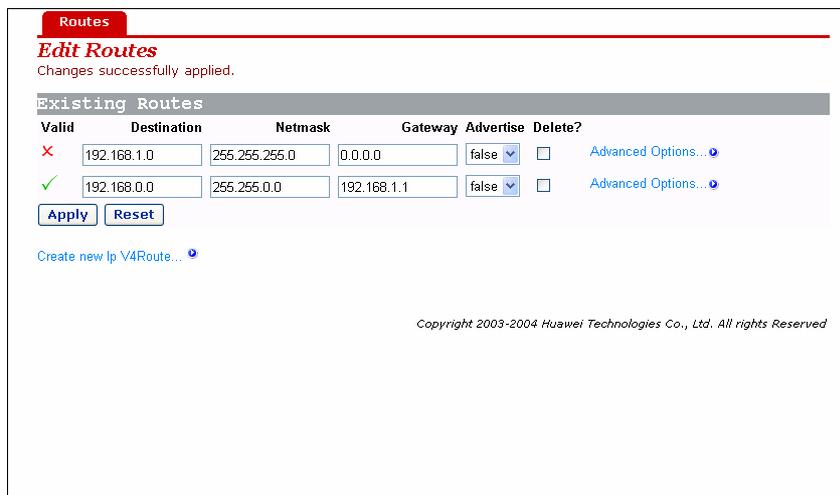


Figure 4-10 Routes configuration

This page allows you to:

- | View the information about existing routes.
- | Edit a route present in the route list.
- | Add a new route to the DNS relay's list.
- | Delete a present route.

This page lists the following information about existing routes:

- | Whether the route is valid ✓ or invalid ✗.
- | Destination IP address.
- | Gateway address.
- | Netmask.
- | Whether the route is advertised via RIP (true or false)

To edit the destination address, gateway address, netmask and advertise status of a route, click in the relevant text box, update the information then click the **Apply** button.

To edit the cost or interface settings for the route, click the [Advanced Options...](#) label to open the web page **advanced setting**.

Name	Value
Destination	192.168.0.0
Netmask	255.255.0.0
Gateway	192.168.1.1
Cost	1
Interface	none
Advertise	false

OK Reset
Cancel

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 4-11 Advanced setting of routes

Update the relevant values of route options, and then click the **OK** button.

To delete an existing route item, check the corresponding check box and click the **Apply** button.

To add a new route item, click the [Create new Ip V4Route...](#) label to open the web page **IP V4Route**. Enter the values of route options, and then click the **OK** button. Click the **Cancel** button to abort this action and return to the route configuration page.

Name	Value
Destination	0.0.0.0
Netmask	0.0.0.0
Gateway	
Cost	1
Interface	none
Advertise	false

OK Reset
Cancel

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 4-12 Create routes

& Note:

For DHCP or fixed IP service, the address of the next hop must be entered in the **Gateway** box (the box must not be left blank), while Interface can be the default **None** or any other value. For other services (i.e. IPoA, PPPoA, PPPoE), either **Interface** or **Gateway** must be specified with a value; if both of them are configured, only **Interface** takes effect.

4.7 Security Interface

Click **Security** in the Main menu and select the **Interface** tab in the Main Frame to open the **Security Interface Configuration** page.

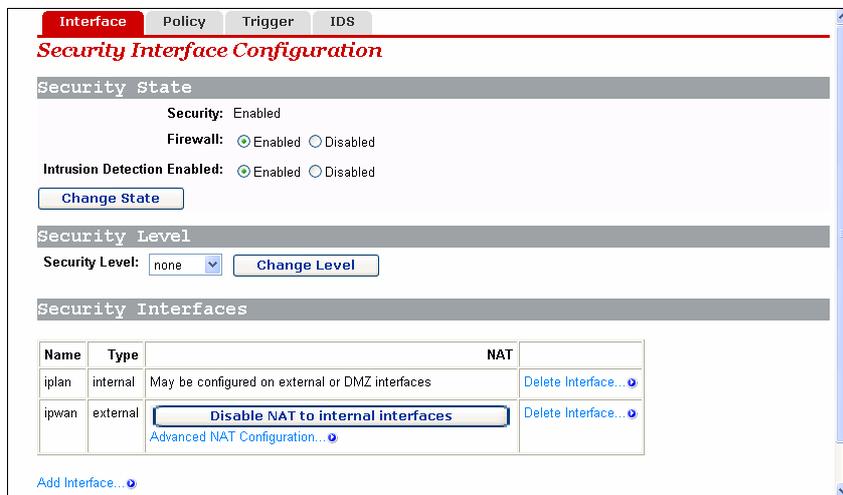


Figure 4-13 Security interface

This page allows you to:

- | Enable/disable the security.
- | Enable/disable the firewall.
- | Enable/disable the intrusion detection.
- | Assign the security level.
- | Add/delete a security interface.
- | Enable/disable NAT to internal interfaces.
- | NAT configuration.

To enable/disable the firewall, click the radio button labeled **Enabled/Disabled** corresponding to **Firewall**, then click the button.

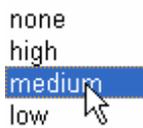
To enable/disable the intrusion detection, click the radio button labeled **Enabled/Disabled** corresponding to **Intrusion Detection**, then click the button.

To enable/disable the security, click the radio button  labeled **Enabled/Disabled** corresponding to **Security**, then click the  button.

& Note:

Firewall, intrusion detection and NAT can only be enabled if security is enabled.
Firewall, intrusion detection and NAT must be disabled if security is disabled.

The security level drop-down list contains entries defined as below, in which **None** level indicates that Internet users are not allowed to access the intranet, **High** level indicates that Internet users have part of the intranet services-access authority, **medium** level indicates even higher authority, and **Low** level indicates the highest authority. To set the proper security level, position the cursor over the entry and left-click to select it, and then click the  button.



none
high
medium
low

& Note:

Firewall must be enabled before security level can be configured.

To add a new security interface, click the [Add Interface...](#) label to open the web page **Add Interface**. Make sure that you have created a virtual interface before doing so. Refer to 4.4 LAN Setting for the way to create a virtual interface.

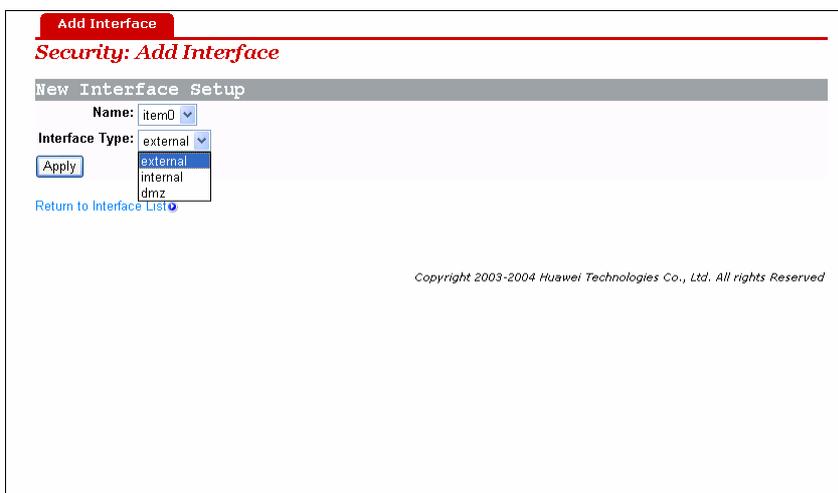


Figure 4-14 Security – add interface

Click on the **Name** drop-down list and select the LAN service that you want to base your security interface on. Only IP interfaces that have not been assigned a security type are displayed.

Click on the **Interface Type** drop-down list and specify what kind of interface it is depending on, that is, how it connects to the network: external, internal or DMZ.

Click the [Apply](#) button. The Security page is displayed, The **Security Interfaces** table displays information about each existing security interface, including the interface that you have just configured.

To delete a present security interface, click the corresponding [Delete Interface...](#) label to open the web page **Delete Interface**, and click the [Delete](#) button.

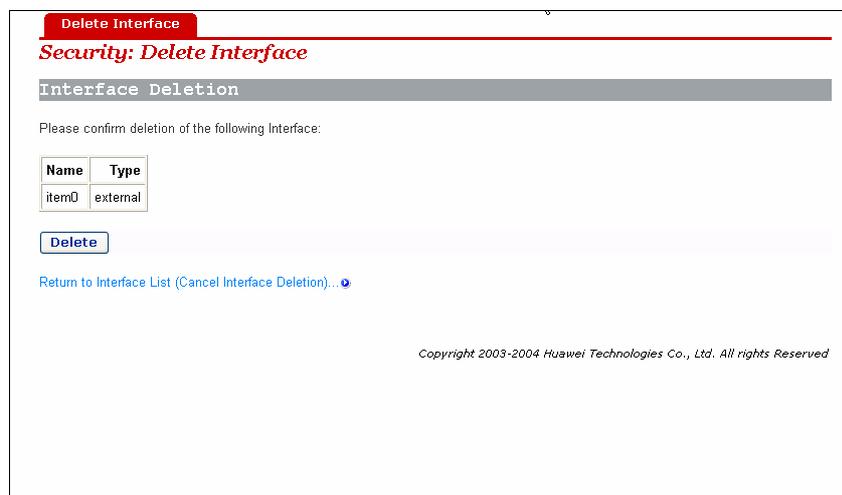


Figure 4-15 Security – delete interface

If the NAT is currently disabled, you may click the

[Enable NAT to internal interfaces](#) button to enable it. If the NAT is currently enabled, you may click the [Disable NAT to internal interfaces](#) button to disable it.

To perform advanced NAT configuration, click the [Advanced NAT Configuration...](#) label to open the web page **Advanced NAT Configuration**. If needed, modify the **Global Address Pools** and **Reserved Mappings** configurations.

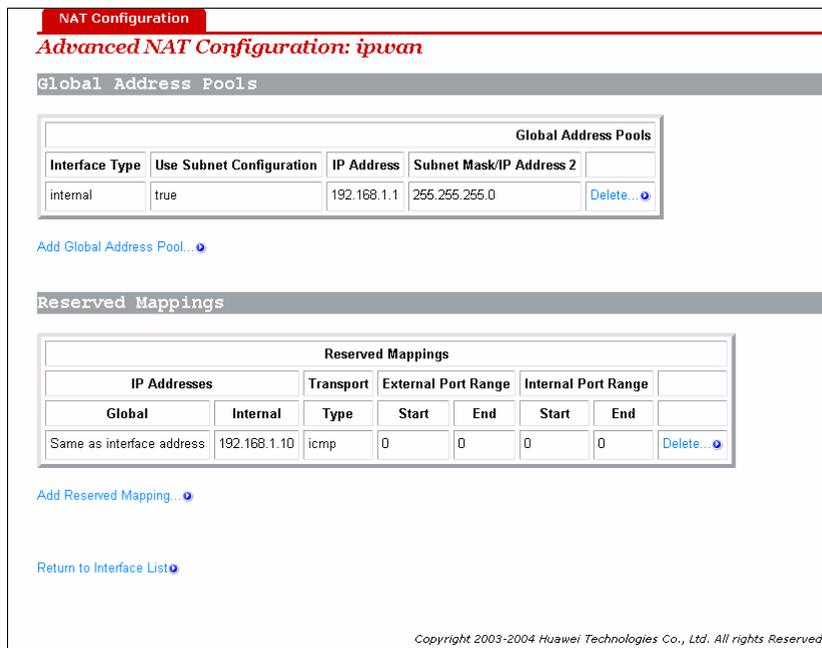


Figure 4-16 Advanced NAT configuration

& Note:

NAT can only be configured when at least one of the following pairs of interface types are defined:

- | external and internal
- | external and DMZ
- | DMZ and internal

& Note:

- | Advanced NAT configuration can only be performed when the NAT to internal interfaces is enabled.
- | Security must be enabled to configure NAT.

4.8 DMZ Configuration

The DMZ feature that DR series routers provide allows hosts in a DMZ zone to perform unlimited bi-directional communication with other Internet users or servers. This not only provides a security shelter for internal hosts to normally access the Internet, but also satisfies the needs to install servers in LANs for services such as FTP and web to fulfill two-way communication that small- to moderate-sized enterprises call for.

Follow these steps to configure DMZ:

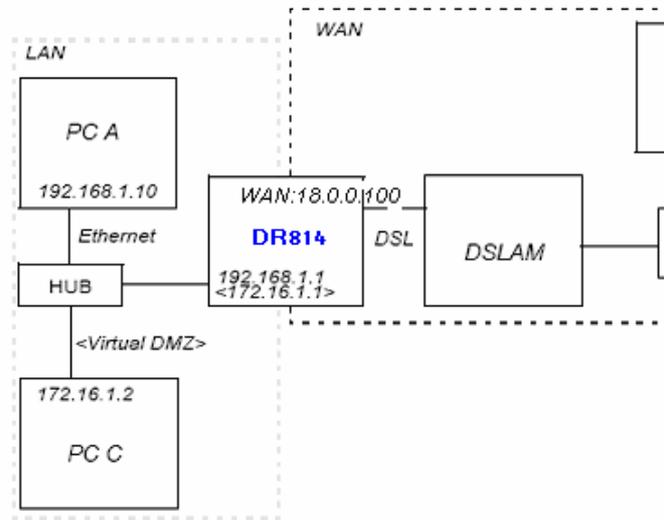


Figure 4-17 DMZ configuration

- 1 Create a virtual interface as instructed in 4.4 LAN Setting, enter the following parameters in the corresponding items and click the <Apply> button:

Create virtual interface

Create virtual interface

Configure new virtual interface:

IP Address: 172 . 16 . 1 . 1

Netmask: 255 . 255 . 0 . 0

[Apply](#)

Figure 4-18 Create a virtual interface

The result will appear in a web page, showing that a virtual interface with the name of item0 has been added into the list.

- 1 Add a security interface as instructed in 4.7 Security Interface, make settings according to the following figure, and then click the <Apply> button:

Add Interface

Security: Add Interface

New Interface Setup

Name: item0

Interface Type: dmz

[Apply](#)

[Return to Interface List](#)

Figure 4-19 Add a security interface

Where item0 is the virtual interface added at the last step.

- 1 Then, enter the **Port Filters** page of external-dmz (refer to 4.9 Security Policy), configure to ensure that users under the external interface can access the Internet services the DMZ zone specifies such as http, ftp, telnet, and so on. Meanwhile, configure port filtering policies for external-internal to disable users under the external interface from accessing host services under the internal interface.
- 1 Finally, configure to allow DMZ hosts to access DMZ zone. Make sure the IP address of the DMZ host is in the same segment as that of the above configured virtual interface (for example, configure the IP address as 172.16.1.100, the mask as 255.255.0.0), enable the corresponding Internet service, and then connect the host to the LAN port of the router, and configure the corresponding virtual server. As such, DMZ is completely and securely configured.

4.9 Security Policy

A policy is the collective term for the rules that apply to incoming and outgoing traffic between two interface types. Firewall must be enabled before you can create policies.

Click **Security** in the Main menu and choose the **Policy** tab in the Main Frame to open the **Security Policy Configuration** page.

Interface Type 1	Interface Type 2	Validators	Policy Configuration	
external	internal	Only listed hosts blocked	Port Filters...	Host Validators...
external	dmz	Only listed hosts blocked	Port Filters...	Host Validators...
dmz	internal	Only listed hosts blocked	Port Filters...	Host Validators...

[Return to Interface List](#)

Figure 4-20 Security policy configuration

This page allows you to:

- 1 Edit a security policy present in the **Current Security Policies** list.

To edit an existing security policy, click the [Port Filters...](#) label to open the web page **Port Filter** to configure the port filter rules, and/or click the [Host Validators...](#) label to open the web page **Host Validators** to configure the host validator rules.

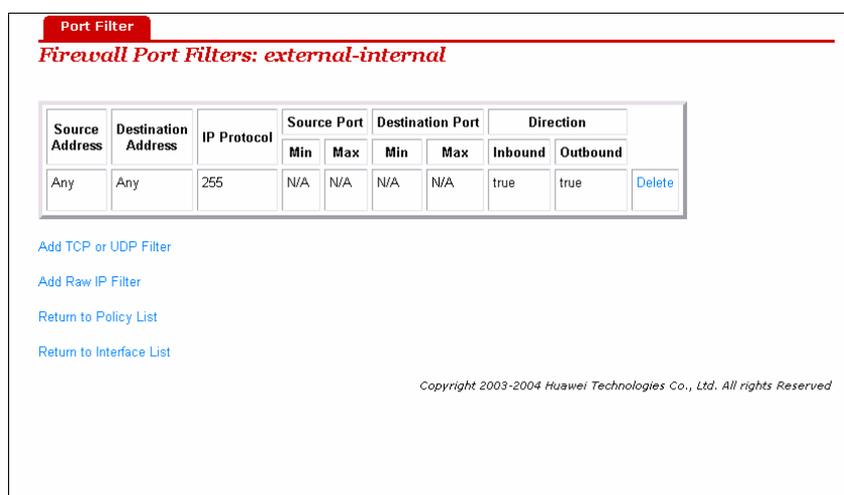


Figure 4-21 Firewall port

Firewall Add Host Validator: external-internal

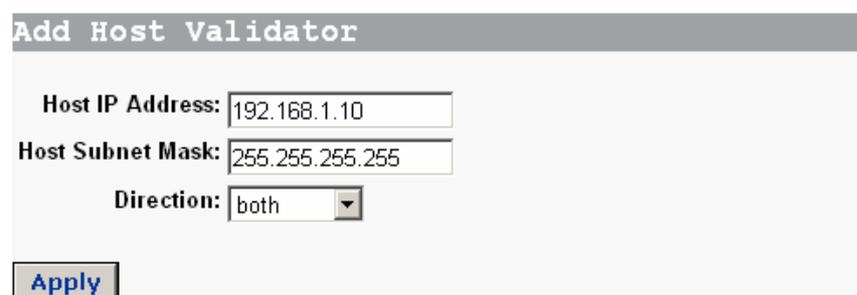


Figure 4-22 Host validator

& Definition:

A host validator can be used to restrict data streams from a WAN interface to a LAN interface or from a LAN interface to a WAN interface.

& Note:

Security policies take effect only after the firewall starts.

4.10 Trigger

Security triggers are used to deal with application protocols that create separate sessions. Some application protocols, such as Netmeeting, open secondary connections during normal operations. Triggers tell the security mechanism to expect

these secondary sessions and instruct it how to handle them. Triggers handle the situation dynamically, allowing the secondary sessions only when appropriate.

Click **Security** in the Main menu and choose the **Trigger** tab in the Main Frame to open the **Security Trigger Configuration** page.

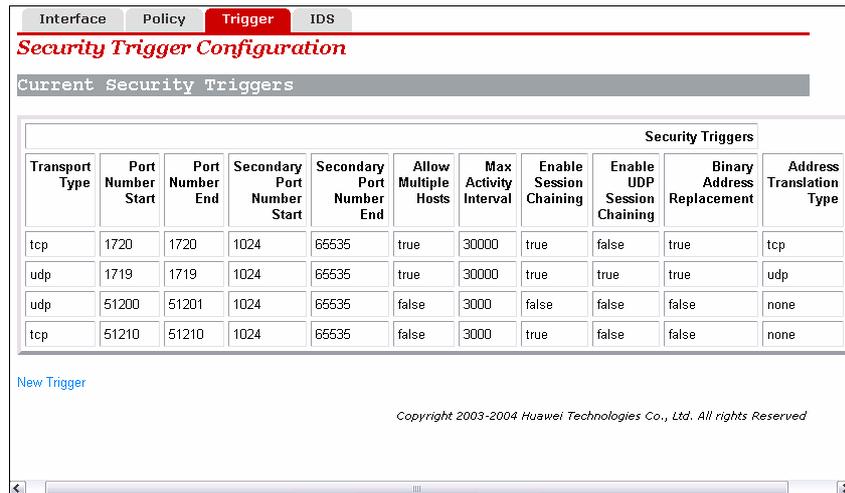


Figure 4-23 Security trigger

This page allows you to:

- 1 View security triggers present in the current security trigger list.
- 1 Create a new trigger and add it to the current security trigger list.
- 1 Delete an existing security trigger.

To create a new security trigger, click the [New Trigger](#) label to open the web page **Add Trigger**.

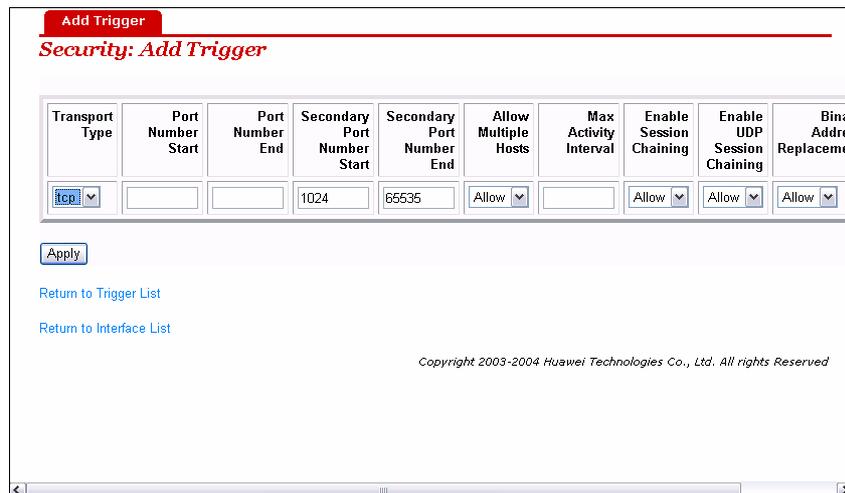


Figure 4-24 Add trigger

Configure the trigger as follows:

- | **Transport Type:** select a transport type from the drop-down list, depending on whether you are adding a trigger for a TCP or a UDP application.
- | **Port Number Start:** type the start of the trigger port range that the primary session uses.
- | **Port Number End:** type the end of the trigger port range that the primary session uses.
- | **Secondary Port Number Start:** type the start of the trigger port range that the secondary session uses.
- | **Secondary Port Number End:** type the end of the trigger port range that the secondary session uses.
- | **Allow Multiple Hosts:** select **Allow** if you want a secondary session to be initiated to/from different remote hosts. Select **Block** if you want a secondary session to be initiated only to/from the same remote host.
- | **Max Activity Interval:** type the maximum interval time (in milliseconds) between the use of secondary port sessions.
- | **Enable Session Chaining:** select **Allow** or **Block** depending on whether you want to allow multi-level TCP session chaining.
- | **Enable UDP Session Chaining:** select **Allow** or **Block** depending on whether you want to allow multi-level UDP and TCP session chaining. **Enable Session Chaining** must be set to **Allow** for this option to work.
- | **Binary Address Replacement:** select **Allow** or **Block** depending on whether you want to use binary address replacement on an existing trigger.
- | **Address Translation Type:** specify what type of address replacement is set on a trigger. **Binary Address Replacement** must be set to **Allow** for this option to work.

Once you have configured the trigger, click the button. The **Security Trigger Configuration** page is displayed, containing details of the trigger that you have just configured.

To delete an existing security trigger, click the corresponding label to open the web page **Delete Triggers**.

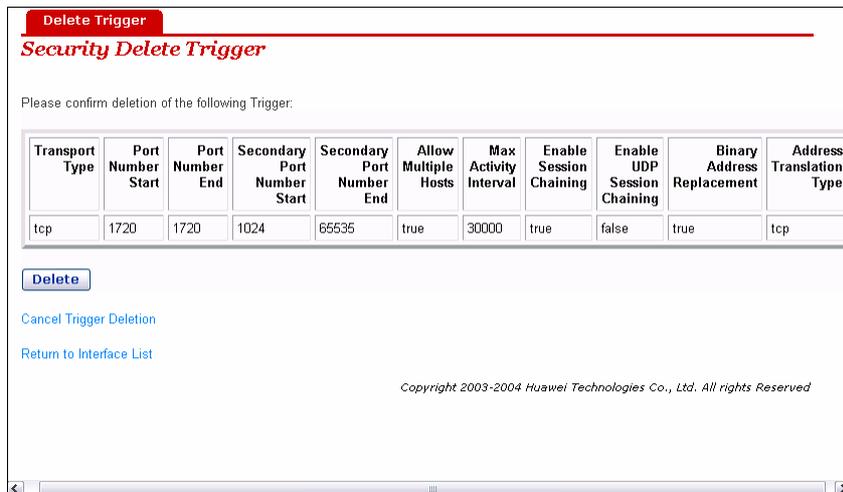


Figure 4-25 Delete trigger

Click the button to delete this trigger.

4.11 IDS

The IDS Settings protect your network from the following kinds of attacks:

- | DOS (Denial of Service).
- | Port Scanning.
- | Web Spoofing.

IDS also implements blacklisting. This stops external hosts that try to attack the network from accessing your device for a specific time limit.

Click **Security** in the Main menu and choose the **IDS** tab in the Main Frame to open the **Firewall Configure Intrusion Detection** page.

Interface Policy Trigger **IDS**

Firewall Configure Intrusion Detection

Use Blacklist	<input type="text" value="true"/>	
Use Victim Protection	<input type="text" value="true"/>	
Victim Protection Block Duration	<input type="text" value="600"/>	seconds
DOS Attack Block Duration	<input type="text" value="1800"/>	seconds
Scan Attack Block Duration	<input type="text" value="86400"/>	seconds
Scan Detection Threshold	<input type="text" value="5"/>	per second
Scan Detection Period	<input type="text" value="60"/>	seconds
Port Flood Detection Threshold	<input type="text" value="10"/>	per second
Host Flood Detection Threshold	<input type="text" value="20"/>	per second
Flood Detection Period	<input type="text" value="10"/>	seconds
Maximum TCP Open Handshaking Count	<input type="text" value="100"/>	per second
Maximum Ping Count	<input type="text" value="15"/>	per second
Maximum ICMP Count	<input type="text" value="100"/>	per second

Figure 4-26 IDS setting

This page allows you to:

- 1 Modify the current IDS configurations.
- 1 Clear the blacklist.

To change the current IDS configurations, enter the relevant values of IDS options, and then click the button.

To clear the blacklist, click the button.

& Note:

By default, the Security module is enabled.

4.12 SNTP

Configuring your device as an SNTP client allows you to obtain accurate time/date information from an associated SNTP server. If you are not attached to an SNTP server, you can set the time/date on your own device instead.

Click **Service** in the Main menu and choose the **SNTP** tab in the Main Frame to open the SNTP configuration page.

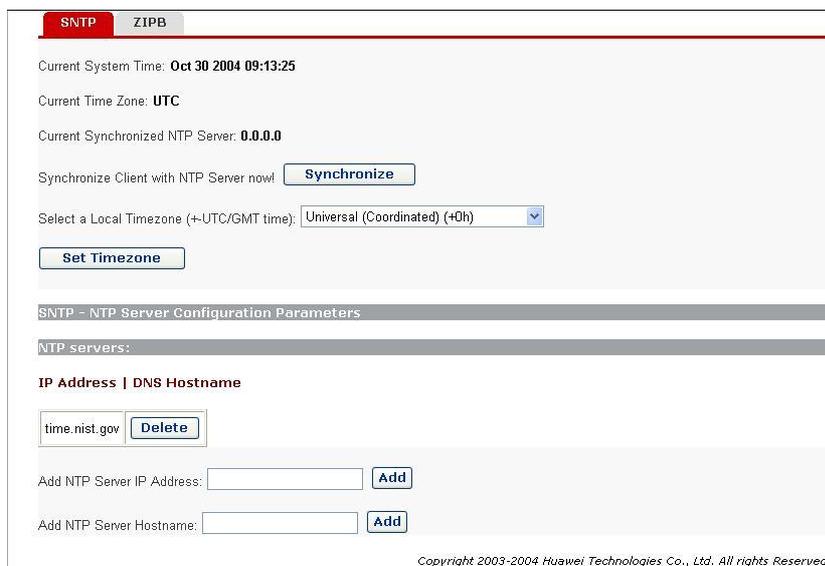


Figure 4-27 SNTP setting

This page allows you to:

- 1 View the current status about system time configuration.
- 1 Configure NTP servers on the Internet to which the ADSL router is able to synchronize its internal clock.

To synchronize the local time with the SNTP server, go to the top of the page and click the **Synchronize** button.

To add a NTP Server, enter the IP Address or the domain name of the SNTP server at the SNTP Server Configuration Parameters section of the page and click on the **Add** button.

To delete an existing NTP Server, click the corresponding **Delete** button.

To set the timezone, position the cursor over the relevant entry from the timezone drop-down list and left-click to select it, and then click the **Set Timezone** button.

4.13 ZIPB

ZIPB stands for "Zero Installation PPP Bridge". It is a way to ensure that a home user can be assigned a public IP address through the router, and to resolve the problem that all SOHO routers with NAT enabled cause part of the application unable to function normally.

Click **Service** in the Main menu and choose the **ZIPB** tab in the Main Frame to open the ZIPB configuration page.

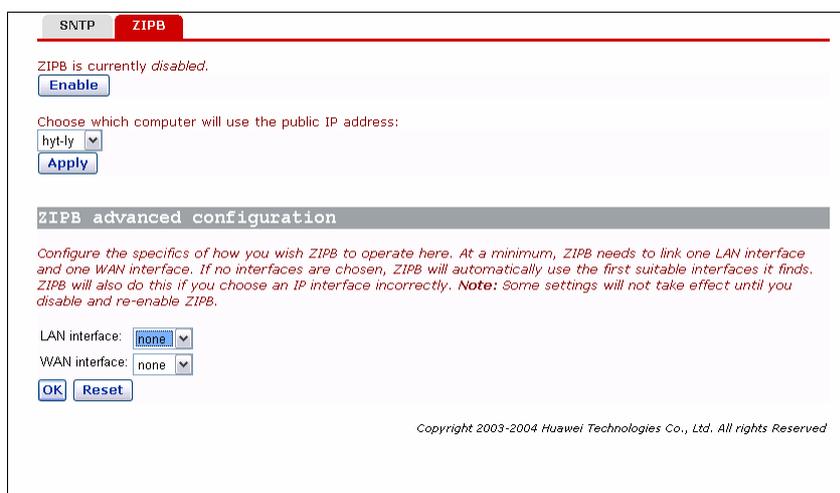


Figure 4-28 ZIPB setting

This page allows you to:

- 1 Enable/disable the ZIPB mode.
- 1 Perform advanced ZIPB configurations.

If the ZIPB is currently disabled, you may click the **Enable** button to enable it. If the ZIPB is currently enabled, you may click the **Disable** button to disable it.

To select which of your LAN computers will use the public IP address, click on the drop-down list below **Choose which computer will use the public IP address**, position the cursor over the entry and left-click to select a LAN computer, and then click the **Apply** button.

To perform advanced ZIPB configurations, proceed according to the following steps:

- 1 Select the LAN interface that ZIPB will run on: click on the **LAN interface** drop down list and select an interface.
- 1 Select the WAN interface that ZIPB will run on: click on the **WAN interface** drop down list and select an interface.

Once you have configured ZIPB, click the **OK** button.

& Note:

Make ensure that ZIPB is disabled before you configure ZIPB. Edit the configurations and click **OK**, the new configuration will take effect after you enable ZIPB.

Configuration changes on ZIPB will not be kept permanently, so you need to configure it again whenever the Router is restarted. In this way, remember to renew the IP address of the ZIPB host first.

4.14 Password

You can restrict access to your device's web pages using password protection. With password protection enabled, users must enter a username and a password before gaining access to the web pages.

By default, the username and password are set as follows:

Username: **admin**

Password: **admin**

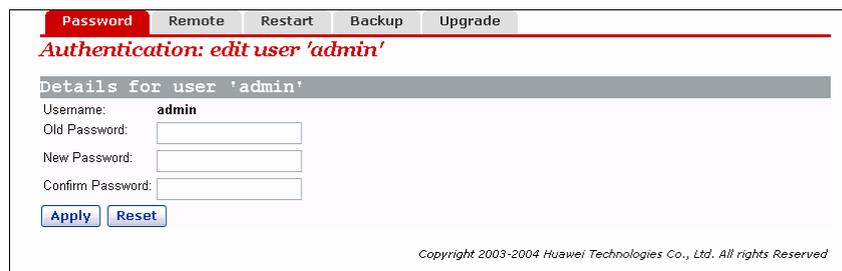
For more information, refer to 3 Getting Started with the Web Pages.

& Note:

For the default user ID admin, only the password can be changed.

Non-authorized users may try to guess your username and password. They will find it easier to guess the default username and password than to guess your own unique username and password. We recommend that you change the default password to your own unique setting.

Click **Device** in the Main menu and choose the **Password** tab in the Main Frame to open the password configuration page.



The screenshot shows a web-based configuration interface. At the top, there is a navigation bar with tabs: Password (selected), Remote, Restart, Backup, and Upgrade. Below the navigation bar, the page title is "Authentication: edit user 'admin'". Underneath, there is a section titled "Details for user 'admin'". This section contains the following fields: Username (pre-filled with "admin"), Old Password (empty), New Password (empty), and Confirm Password (empty). At the bottom of this section are two buttons: "Apply" and "Reset". At the very bottom of the page, there is a small copyright notice: "Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved".

Figure 4-29 Modify password

This page allows you to:

- 1 Change the password of the default user: admin.

To change the password, enter the new password, and then click the **Apply** button.

4.15 Remote Access

Click **Device** in the Main menu and choose the **Remote** tab in the Main Frame to open the remote administration configuration page.

This page allows you to:

- 1 Enable/disable the remote administration.
- 1 Set the value of idle timeout (if enabled).

If the remote administration is currently disabled, the following page is displayed .To enable the remote access, enter the idle timeout then click the **Enable** button.

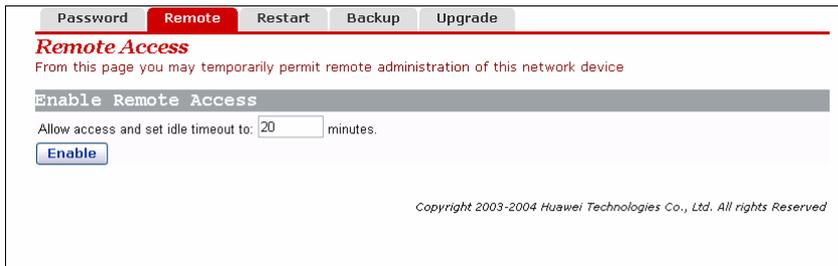


Figure 4-30 Remote access

If the remote administration is currently enabled, the following page is displayed. Whenever the remote administration is enabled, the system starts for timing; as soon the timer reaches the set timeout time, the remote connection is taken down. To disable the remote access, click the **Disable** button.

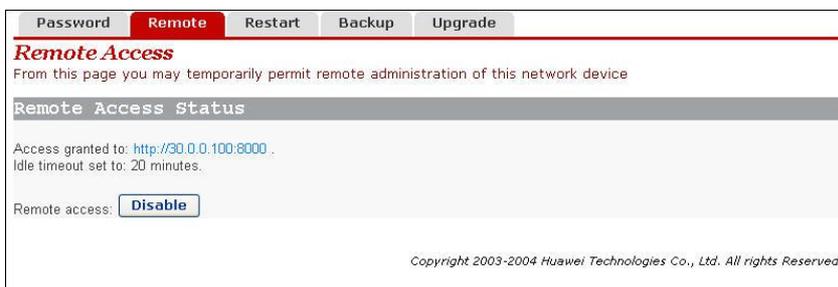


Figure 4-31 Disable remote access

4.16 Restart Router

Click **Device** in the Main menu and choose the **Restart** tab in the Main Frame to open the restart page.

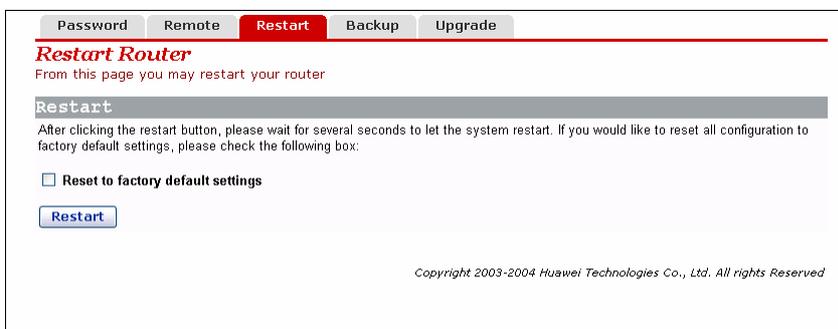


Figure 4-32 Restart

This page allows you to:

- | Restart the ADSL router.
- | Reset all configurations to default settings and restart the ADSL router.

If you would like to reset all configurations to default settings, check the **Restart to factory default setting** box . Click the button to restart the ADSL router.

& Note:

After clicking the restart button, wait for several seconds to let the system restart.

4.17 Configuration Backup/Restore

Click **Device** in the Main menu and choose the **Backup** tab in the Main Frame to open the configuration management page.



Figure 4-33 Backup/restore configuration

This page allows you to:

- | Backup the current configuration to a file on your computer.
- | Restore configuration from a previously saved file.

To backup the current configuration, click the button, the following page is displayed.

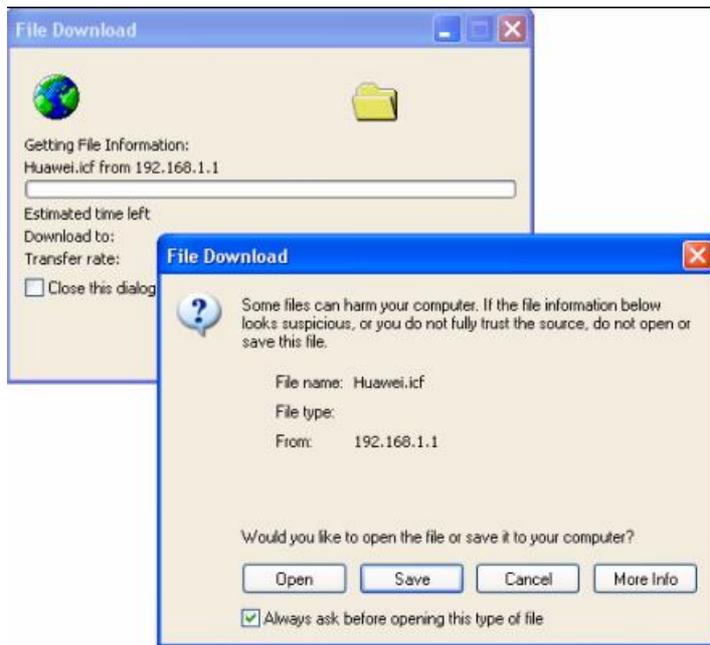
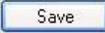


Figure 4-34 Download configuration file

Click the  button to pop up the following window:

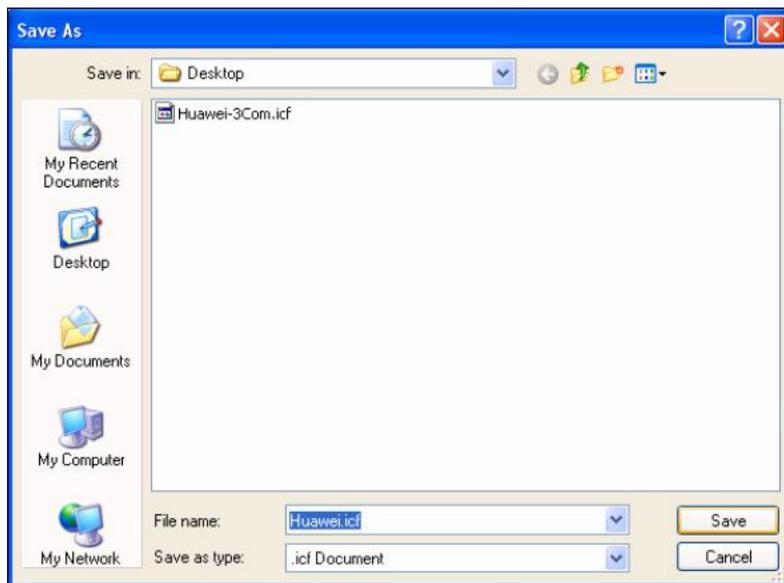
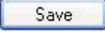


Figure 4-35 Save configuration file

Enter a proper filename, and then click the  button to backup the current configuration to the file.

To restore configuration from a previously saved file, click the  button to pop up the **Choose file** window.

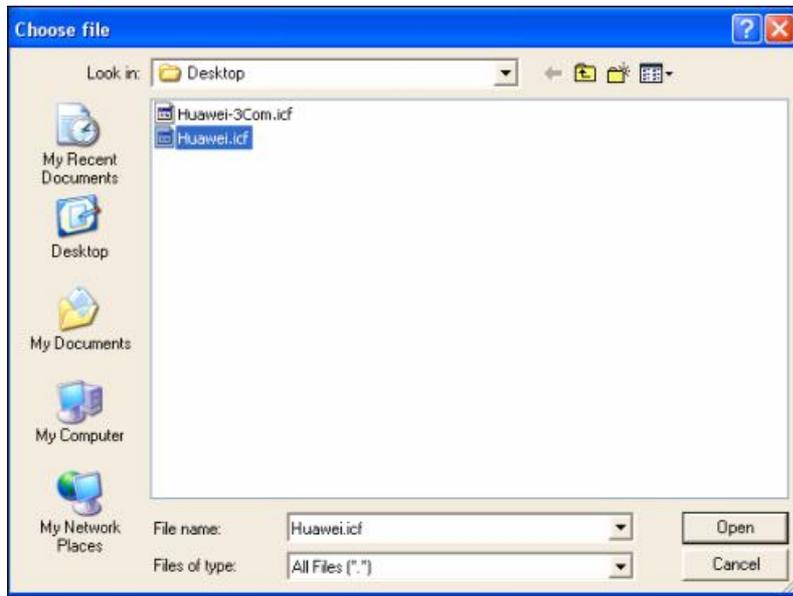


Figure 4-36 Select backup file

Click the button to open the selected configuration file, the following page is displayed. Click the button to restore configuration from the selected file.

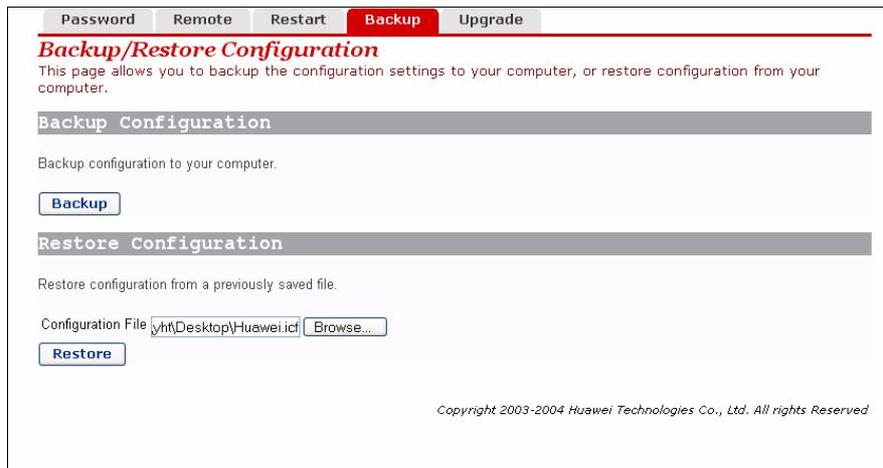


Figure 4-37 Restore configuration

4.18 Upgrade

Click **Device** in the Main menu and choose the **Upgrade** tab in the Main Frame to open the firmware upgrade page.



Figure 4-38 Firmware upgrade

This page allows you to update the system software on your network device from an image file which may be obtained from Huawei support website.

Enter the path to the image file location in the text box or click the button to locate the image file.

Click the button to open the selected firmware image file.

Click the button to update the system software on the ADSL router with the selected image file.

& Note:

The upgrade process takes about 2 minutes to complete, and the ADSL router will reboot.

After the router reboots, restore the configuration to the factory settings at first to make sure that the current configuration file matches!

Click the “Huawei” hyperlink to visit the support web site from where the update image file may be obtained.

4.19 Status

Click **Status** in the Main menu and choose the **Status** tab in the Main Frame to open the **Status** page.

Status Log Search Service

Status
This page shows the status of your connection

Status
PPPoE Connection: Connection established [Disconnect](#)
Connected time so far: 00:03:00s
WAN IP Address: 30.0.0.100
Local IP Address: 192.168.1.1

Advanced Diagnostics
Connection Authentication: PPPoE Username/Password
PPPoE Dial-On-Demand: Disabled
IP address of PPP server: 30.0.0.1

Port Connection Status

Port	Type	Connected	Line State
DSL	atm	✓	N/A
Ethernet	ethernet		N/A
Usb-ethernet	ethernet	✗	N/A

WAN Status
IP Address Type: Static or PPP
WAN Subnet Mask: 255.0.0.0
Default Gateway: 0.0.0.0
Primary DNS: 20.1.1.100

LAN Status
LAN Subnet Mask: 255.255.255.0
Act as Local DHCP Server: Yes
MAC Address: 00:0F:E2:00:4F:14

Hardware Status
Up-Time: 00:04:36s
Current Time:
Version: DR834V100DD004
CompileTime: Oct 30 2004 11:35:19
Vendor: Huawei

Defined Interfaces
PPPoE WAN uplink: [Show Statistics...](#) Port:dsl VPI/VCI: 0/35 ✓
RFC1483 WAN uplink: [Show Statistics...](#) Port:dsl VPI/VCI: 0/38
ethernet: [Show Statistics...](#)
usb-ethernet: [Show Statistics...](#)

Routing Table
[Route setup...](#)

Destination	Netmask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	iplan
127.0.0.0	255.0.0.0	0.0.0.0	loopback
30.0.0.0	255.0.0.0	0.0.0.0	ipwan
0.0.0.0	0.0.0.0	0.0.0.0	ipwan

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 4-39 Status page

The **Status** page displays useful information about the setup of the ADSL router, including:

- | Details of the ADSL router's Internet access settings
- | Some important system information (hardware information, version information)
- | Routing table
- | Current DSL state and Ethernet connection information
- | WAN Status
- | LAN Status
- | All interfaces' status

This page allows you to:

- 1 View the current status of the ADSL router.
- 1 Configure the port connection (DSL, Ethernet).

To configure the DSL port connection, click the **DSL** label in **Port Connection Status** region to open the web page **DSL**.

Name	Value
Connected	false
Operational Mode	Inactive
State	HandShake
Tx Bit Rate	0
Rx Bit Rate	0
Local SNRMargin	0.0 dB
Local Line Attn	0.0 dB
Local Tx Power	0.0 dB
Remote Line Attn	0.0 dB
Remote SNRMargin	0 dB
Activate Line	None
Standard	Multimode
Annex Type	AnnexA

Figure 4-40 DSL port configuration

The **DSL** page displays basic attribute information about the DSL port configuration.

To configure the basic attributes of DSL port, enter the proper values of attributes, then click the **Apply** button.

To configure the Ethernet port and USB port, follow the same step above.

4.20 Log

Click **Status** in the Main menu and choose the **Log** tab in the Main Frame to open the **Event log** page.

This page allows you to:

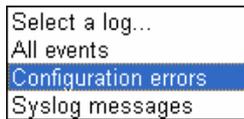
- 1 Clear the event entries according to the selected event type.
- 1 View the activity on the ADSL router since power-on according to the selected event type.



Figure 4-41 Log

The event type drop-down list contains entries defined as below. To select the proper event type, position the cursor over the entry and left-click to select it, and then click the

 button.



Click the  button to clear the selected event entries.

4.21 PVC Scan

Click **Status** in the Main menu and choose the **Search Service** tab in the Main Frame to open the PVC scan page.

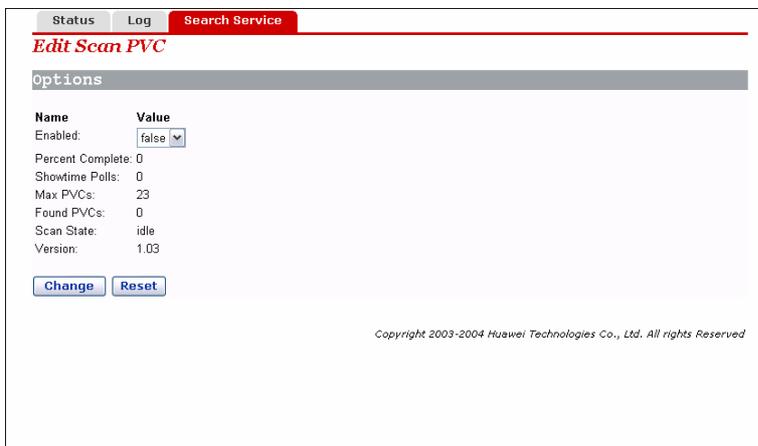


Figure 4-42 Search service

This page can be used to search for PVC settings not used currently. If the ISP has configured these PVCs, the device will automatically add the information about these PVCs into the WAN service list on the WAN setting page after the search. For PPPoE or PPPoA service, it is also necessary for the users to edit the automatically added services and to enter the username and password. The search takes over 5 minutes.

4.22 Save Configure

Click **Save Configure** in the Main menu to open the **Save configuration** page.

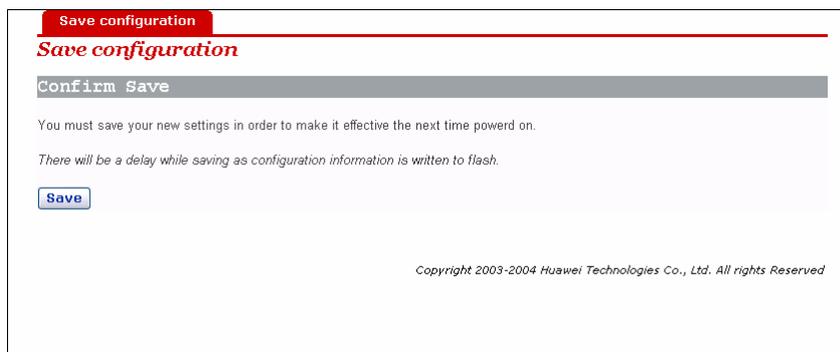


Figure 4-43 Save configuration

Click the **Save** button to write the current configuration to the flash memory.

& Note:

You must save your new settings for them to take effect the next time the device is powered on.

There will be a delay while configuration information is written to the flash memory.

5 Configuring Your Computers

This chapter provides instructions for configuring the Internet settings on your computers to work with the DR811/DR814 ADSL router.

5.1 Configuring Ethernet PCs

5.1.1 Before You Begin

By default, the ADSL router automatically assigns all required Internet settings to your PCs. You need only to configure the PCs to accept the information assigned.

& Note:

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the ADSL router to do so. Refer to “5.1.7 Assigning Static Internet Information to Your PCs” for instructions.

- | If you have connected your LAN PCs via Ethernet to the ADSL router, follow the instructions for the operating system installed on your PC:
 - | Windows® XP PCs
 - | Windows 2000 PCs
 - | Windows Me PCs
 - | Windows 95, 98 PCs
 - | Windows NT 4.0 workstations
- | If you have connected a PC via the USB port, refer to 5.2 Configuring a PC Connected by USB Port

5.1.2 Windows® XP PCs

- 1) In the Windows task bar, click the Start button, and then click Control Panel.
- 2) Double-click the Network Connections icon.
- 3) In the LAN or High-Speed Internet window, right-click on the icon corresponding to your network interface card (NIC) and select Properties. (Often, this icon is labeled

Local Area Connection). The Local Area Connection dialog box is displayed with a list of currently installed network items.

- 4) Ensure that the check box to the left of the item labeled Internet Protocol TCP/IP is checked and click Properties.
- 5) In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain DNS server address automatically.
- 6) Click OK twice to confirm and save your changes, and then close the Control Panel.

5.1.3 Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

- 1) In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.
- 2) Double-click the Network and Dial-up Connections icon.
- 3) In the Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select Properties. The Local Area Connection Properties dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
- 4) If Internet Protocol (TCP/IP) is not displayed as an installed component, click Install....
- 5) In the Select Network Component Type dialog box, select Protocol, and then click Add....
- 6) Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click OK. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
- 7) If prompted, click OK to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the ADSL router:

- 8) In the Control Panel, double-click the Network and Dial-up Connections icon.
- 9) In Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select Properties.
- 10) In the Local Area Connection Properties dialog box, select Internet Protocol (TCP/IP), and then click Properties.
- 11) In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain DNS server address automatically.
- 12) Click OK twice to confirm and save your changes, and then close the Control Panel.

5.1.4 Windows Me PCs

- 1) In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.
- 2) Double-click the Network and Dial-up Connections icon.
- 3) In the Network and Dial-up Connections window, right-click the Network icon, and then select Properties. The Network Properties dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.
- 4) If Internet Protocol (TCP/IP) is not displayed as an installed component, click Add....
- 5) In the Select Network Component Type dialog box, select Protocol, and then click Add....
- 6) Select Microsoft in the Manufacturers box.
- 7) Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click OK. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
- 8) If prompted, click OK to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the ADSL router:
- 9) In the Control Panel, double-click the Network and Dial-up Connections icon.
- 10) In Network and Dial-up Connections window, right-click the Network icon, and then select Properties.
- 11) In the Network Properties dialog box, select TCP/IP, and then click Properties.
- 12) In the TCP/IP Settings dialog box, click the radio button labeled Server assigned IP address. Also click the radio button labeled Server assigned name server address.
- 13) Click OK twice to confirm and save your changes, and then close the Control Panel.

5.1.5 Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

- 1) In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.
- 2) Double-click the Network icon.
- 3) The Network dialog box is displayed with a list of currently installed network components. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.
- 4) If TCP/IP is not displayed as an installed component, click Add...The Select Network Component Type dialog box appears.
- 5) Select Protocol, and then click Add.... The Select Network Protocol dialog box appears.

- 6) Click on Microsoft in the Manufacturers list box, and then click TCP/IP in the Network Protocols list box.
- 7) Click OK to return to the Network dialog box, and then click OK again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
- 8) Click OK to restart the PC and complete the TCP/IP installation. Next, configure the PCs to accept IP information assigned by the ADSL router:
- 9) Open the Control Panel window, and then click the Network icon.
- 10) Select the network component labeled TCP/IP, and then click Properties. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
- 11) In the TCP/IP Properties dialog box, click the IP Address tab.
- 12) Click the radio button labeled Obtain an IP address automatically.
- 13) Click the DNS Configuration tab, and then click the radio button labeled Obtain an IP address automatically.
- 14) Click OK twice to confirm and save your changes. You will be prompted to restart Windows.
- 15) Click Yes.

5.1.6 Windows NT 4.0 Workstations

First, check for the IP protocol and, if necessary, install it:

- 1) In the Windows NT task bar, click the Start button, point to Settings, and then click Control Panel.
- 2) In the Control Panel window, double click the Network icon.
- 3) In the Network dialog box, click the Protocols tab.
The Protocols tab is displayed with a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.
- 4) If TCP/IP is not displayed as an installed component, click Add....
- 5) In the Select Network Protocol dialog box, select TCP/IP, and then click OK.
You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
After all files are installed, a window appears to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
- 6) Click Yes to continue, and then click OK if prompted to restart your computer.

Next, configure the PCs to accept IP information assigned by the ADSL router:

- 7) Open the Control Panel window, and then double-click the Network icon.
- 8) In the Network dialog box, click the Protocols tab.
- 9) In the Protocols tab, select TCP/IP, and then click Properties.
- 10) In the Microsoft TCP/IP Properties dialog box, click the radio button labeled Obtain an IP address from a DHCP server.

- 11) Click OK twice to confirm and save your changes, and then close the Control Panel.

5.1.7 Assigning Static Internet Information to Your PCs

If you are like most users, you will not need to assign static Internet information to your LAN PCs. This information is automatically assigned by your ISP.

In some cases, however, you may want to assign Internet information to some or all of your PCs directly (often called “statically”), rather than allowing the ADSL router to do so. This option may be desirable (but not required) if:

- 1 You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a server providing network services to the outside).
- 1 You maintain different subnets on your LAN (subnets are described in “9 Appendix - Glossary”).

Before you begin, be sure to have the following information on hand, or contact your ISP if you do not know it:

- 1 The IP address and subnet mask to be assigned to each PC to which you are assigning static IP information.
- 1 The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the ADSL router. By default, the LAN port is assigned this IP address: **192.168.1.1**. (You can change this address, or acquire another address from your ISP. Refer to “6 IP Addresses, Network Masks, and Subnets” for more information.)
- 1 The IP address of your ISP’s Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions described previously relating only to checking for and/or installing the IP protocol to see if the IP protocol is stalled and install it in case it is not. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server and default gateway, click the radio buttons that enable you to enter the information manually.

& Note:

Your PCs must have IP addresses that place them in the same subnet as the ADSL router’s LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in “6 IP Addresses, Network Masks, and Subnets” to change the LAN port IP address accordingly.

5.2 Configuring a PC Connected by USB Port

5.2.1 Connecting a Computer to the USB Port by a USB cable

If you use the ADSL router's USB port to connect to a PC, you must install the provided USB driver on the PC. The driver enables Ethernet-over-USB communication with the ADSL router.

5.2.2 Installing the USB Driver

Ensure that the USB function of your PC is OK.

The Microsoft Windows 98, 98 SE, ME, 2000, and XP support this driver. The following installation instruction is based on Windows XP; you may refer to it when operating on other operating systems.

1. Insert the driver CD to your CDROM.

The CD shipped with the ADSL router contains the USB drivers. Insert it into your PC's CDROM.

2. Plug the USB cable from the device into the USB port of the PC.

The USB cable provided has a flat connector on one end (called Type A) and a square connector on the other (Type B). Connect the flat connector to your PC and the square connector to the ADSL router.



Figure 5-1 USB port outline

Plug the USB cable from the device into the USB port of the PC. The PC will detect the newly-attached device and display the *Found New Hardware Wizard* dialog box:



Figure 5-2 Found new hardware

3. Click on **Next>**. The PC will search the disc for the driver configuration file. When this file is found, the PC will begin installing the drivers for the device:



Figure 5-3 Install software

The following window is displayed warning that the device is not compatible with Windows XP:

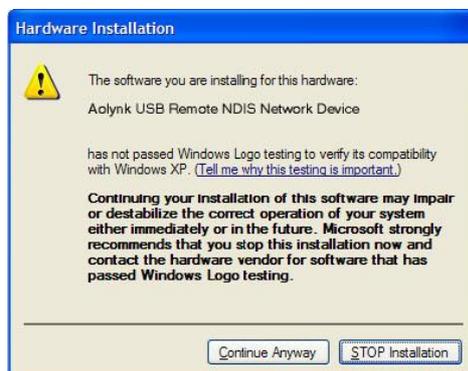


Figure 5-4 Driver warning

Click on *Continue Anyway* to proceed.

4. When the driver has been installed, the Found New Hardware Wizard confirms that the installation is complete for your device:



Figure 5-5 Install completed

5. Click on Finish. The toolbar will display the following message, confirming that the device has been installed correctly:

New hardware installed and ready to use

In the Windows XP Network Connections dialog box, the device is shown as a new LAN device called *Aolynk USB Remote NDIS Network Device*.

For example:



Figure 5-6 Windows XP device properties for the installed device

You have now finished installing the driver. You do not need to restart your computer.

5.2.3 Configuring IP Properties on PC Connected by USB Port

After the USB driver installation is complete, you must configure the PC so that its IP properties place it in the same subnet as the ADSL router's USB port. There are two ways to do this:

- 1. Configure the ADSL router so that it assigns an appropriate IP address to the PC. If you want to use this automatic assignment feature called DHCP server, you must configure the PC to accept dynamically assigned IP information. Follow the instructions in "5.1 Configuring Ethernet PCs" for the operating system installed on your PC.
- 1. If you want to assign a static IP address to the PC, follow the instructions described in "5.1.7 Assigning Static Internet Information to Your PCs" and use the following information:

In the Network Connections window, be sure to select the icon that corresponds to your new USB connection (not the one that corresponds to your Ethernet NIC). When you display properties for the icon, the following text should appear in the Connect Using text box:

Aolynk USB Remote NDIS Network Device

The USB port on the ADSL router is preconfigured with these properties:

USB port IP address: 192.168.1.1

USB port subnet mask: 255.255.255.0

Therefore, your PC must be configured as follows:

IP address: 192.168.1.n where n is a number from 2 to 254 that does not conflict with the DHCP address range.

Subnet mask: 255.255.255.0

6 IP Addresses, Network Masks, and Subnets

6.1 IP Addresses

& Note:

This section refers only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes.

IP addresses, the Internet version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called *dotted decimal notation*. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

6.1.1 Structure of an IP Address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information.

- | *Network ID*: Identifies a particular network within the Internet or intranet
- | *Host ID*: Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's *class* (refer to the following section). Table 7-1 shows the structure of an IP address.

Table 6-1 IP Address structure

Class	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

6.1.2 Network Classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Here are some important notes regarding IP addresses:

- 1 The class can be determined easily from field1:
 - field1 = 1-126: Class A
 - field1 = 128-191: Class B
 - field1 = 192-223: Class C

(field1 values not shown are reserved for special uses)
- 1 A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

6.2 Subnet Masks

& Note:

A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: a bit set to 1 means "this bit is part of the network ID" and a bit set to 0 means "this bit is part of the host ID."

Subnet masks are used to define *subnets* (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111.11111111.11111111.10000000

As with any class C address, all of the bits in field1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 1 to 126 hosts (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111.11111111.11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, and 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 1 to 62.

& Note:

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:

- | Class A: 255.0.0.0
- | Class B: 255.255.0.0
- | Class C: 255.255.255.0

These are called default because they are used when a network is initially configured, at which time it has no subnets.

7 Service Configuration

7.1 Configuration Overview

ATM is a connection oriented packet switching technology using fixed size packets, called cells. These cells consist of a header and a payload and are switched through a public or private ATM network depending on the contents of the header. End-to-end connections are formed by cross-connecting individual ATM segments in ATM switches.

Each ATM cell carries two labels called Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) as part of its header. An ATM channel, commonly referred to as virtual channel, is fully identified by these two labels. Therefore, multiple ATM channels can reside on your DSL line. All ATM connections are static, i.e. of type permanent virtual channel (PVC).

Following are 5 modes of ATM setting:

- | PureBridge
- | DHCP/StaticIP
- | PPPoA
- | IPoA
- | PPPoE

Click **WAN Setting** in the Main menu and choose the **WAN** tab in the Main Frame to open the WAN connection configuration page.

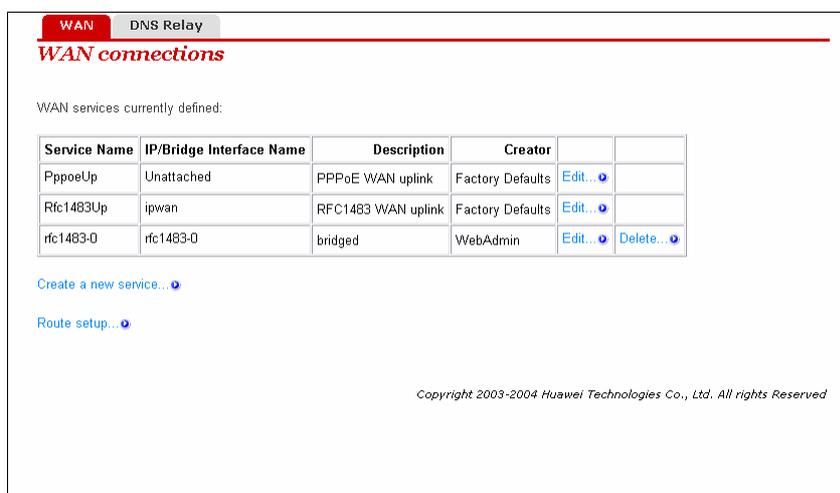


Figure 7-1 WAN connections

To add a new WAN service, click the [Create a new service...](#) label to open the web page **WAN Connection: create service**.

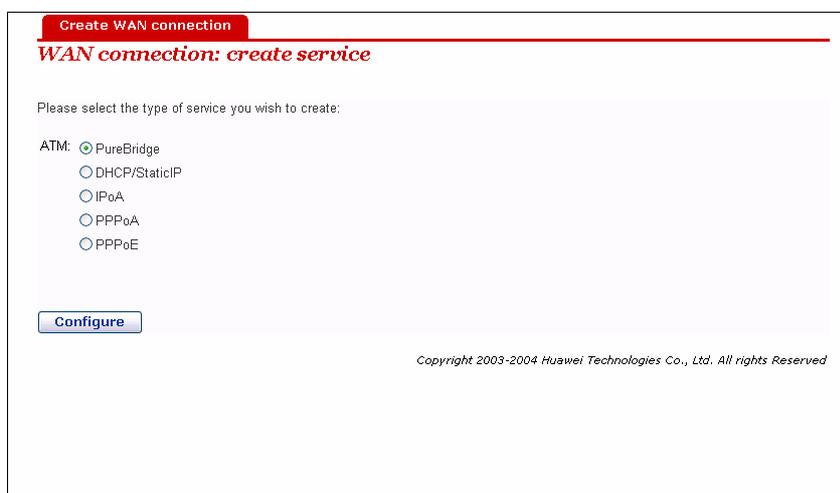


Figure 7-2 Create a new connection

7.2 PureBridge

To create a PureBridge WAN connection, click the radio button labeled **PureBridge**, then click the [Configure](#) button to open the web page **WAN Connection:PureBridge**.

Enter the proper values of connection options, and then click the [Apply](#) button.

WAN connection: PureBridge
Create WAN connection

Description:

VPI:

VCI:

Encapsulation method:

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 7-3 Pure bridge

7.3 DHCP/StaticIP

To create a DHCP/StaticIP WAN connection, click the radio button labeled **DHCP/StaticIP**, then click the button to open the web page **WAN Connection: DHCP/StaticIP**.

WAN connection: DHCP/StaticIP
Create WAN connection

Description:

VPI:

VCI:

Encapsulation method:

Obtain an IP Address Automatically

Use the following IP Address:

 WAN IP Address:

 Subnet Mask:

Enable NAT on this interface

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 7-4 DHCP/StaticIP

Enter the proper values of connection options, and then click the button.

7.4 IPoA

To create an IPoA WAN connection, click the radio button labeled **IPoA**, then click the button to open the web page **WAN Connection: IPoA**.

The screenshot shows a web interface titled "Create WAN connection" with a sub-header "WAN connection: IPoA". The form contains the following fields and options:

- Description:
- VPI:
- VCI:
- Encapsulation method: (dropdown menu)
- WAN IP address:
- Subnet Mask:
- Enable NAT on this interface
-

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 7-5 IPoA

Enter the proper values of connection options, and then click the button.

7.5 PPPoA

To create a PPPoA WAN connection, click the radio button labeled **PPPoA**, then click the button to open the web page **WAN Connection: PPPoA**.

The screenshot shows a web interface titled "Create WAN connection" with a sub-header "WAN connection: PPPoA". The form contains the following fields and options:

- Description:
- VPI:
- VCI:
- User name:
- Password:
- Auto Connect:
- User Idle Timeout (in minutes):
- Enable NAT on this interface
-

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 7-6 PPPoA

Enter the proper values of connection options, and then click the button.

7.6 PPPoE

To create a PPPoE WAN connection, click the radio button labeled **PPPoE**, then click the button to open the web page **WAN Connection: PPPoE**.

Create WAN connection

WAN connection: PPPoE

Description:

VPI:

VCI:

User name:

Password:

Auto Connect:

User Idle Timeout (in minutes):

Enable NAT on this interface

Copyright 2003-2004 Huawei Technologies Co., Ltd. All rights Reserved

Figure 7-7 PPPoE

Enter the proper values of connection options, and then click the button.

& Note:

- 1 Supply the **Service name** parameter for a PPPoE interface when it is required by the ISP. The ISP uses this to identify the type of connection to use for the interface.
 - 1 Each PPPoE interface is IP-enabled, i.e. it has an associated IP address. You may specify this IP address in the WAN IP address if the address is allocated statically by the ISP. If the IP address is obtained dynamically, specify this IP address as "0.0.0.0".
-

8 Troubleshooting

This chapter suggests solutions to problems you may encounter in installing or using the ADSL router, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

8.1 Troubleshooting Suggestions

Table 8-1 Troubleshooting suggestions

Problem	Troubleshooting Suggestion
LEDs	
Power LED does not illuminate	Verify that you are using the power cable provided with the device and that it is securely connected to the ADSL router and a wall socket/power strip.
Link LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the DSL port and your wall phone port.
LINK LAN LED does not illuminate after Ethernet cable is attached.	<p>Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the ADSL router. Make sure the PC and/or hub is turned on.</p> <p>Verify that you are using a straight-through Ethernet cable to the uplink port on a hub or a cross-over cable to a stand-alone PC. If you connect the device to an ordinary hub port (not uplink), you must use a straight-through cable. (To check: hold the connectors at each end of the cable side-by-side with the plastic spring facing down. Looking at the wires from left to right, if the first, second, third, and sixth wires are in the same color on the two connectors, then it is a straight-through cable. For a cross-over cable, wire 1 on one connector should be in the same color as wire 3 on the other. The same is true with wires 2 and 6.)</p> <p>Verify that your cable is sufficient for your network requirements. A 100 Mbps network (10BaseTx) should use cables labeled CAT 5. A 10Mbps network may tolerate lower quality cables.</p>
Internet Access	

Problem	Troubleshooting Suggestion
My PC cannot access Internet	<p>Firstly, check to see if ADSL Link LED is solid on; if it is not, check to see if the ADSL line is connected correctly.</p> <p>If the method for acquiring the IP and DNS of the host is set to Auto (Auto is recommended strongly), check to see if the IP address has already been obtained correctly, and if you can ping the IP address of the device's LAN interface (192.168.1.1 by default; refer to 8.2.1 ping to use the ping utility to check it out). If you cannot ping the interface, check to see if the Ethernet cable is OK.</p> <p>If the current computer is specified with a private IP address, make sure that it resides in the same segment as that of the device's LAN interface, the gateway is specified as the IP address of the device's LAN interface, and the DNS is specified as the IP address of the device's LAN interface or the DNS Server the ISP allocates. Similarly, the host should be able to ping the IP address of the device's LAN interface.</p> <p>If the host can communicate with the device normally but cannot connect to the Internet, login to the web page of the device (refer to Figure 4-39Status page) at first, and check to see if the WAN interface of the device has acquired the Internet IP address.</p>
My LAN PCs cannot display web pages on the Internet.	<p>Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the above item. If you specify that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the ADSL router is correct, and then you can use the ping utility to test connectivity with your ISP's DNS server.</p> <p>Generally, if a host can ping the Internet IP address, but cannot open the web pages, the DNS server of the ISP may be experiencing a failure for the time being. In this case, you can manually change the host's DNS to the IP address of a normally functioning DNS server, or login to the web page of the device and manually modify the configuration for DNS Relay (refer to 4.3 DNS Relay), and then check by using the nslookup command as instructed in 8.2.2 nslookup.</p>
Web pages	
I forgot/lost my password.	<p>If you have not changed the default password, try using "admin" as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing the Reset Default button on the rear panel of the device for at least 5 seconds. Then connect to the web page again, type the default User ID and password shown above. Warning: Resetting the device removes any custom settings and returns all settings to their default values.</p>
I cannot access the web pages from my browser.	<p>Use the ping utility, discussed in the following section, to check whether your PC can communicate with the device's LAN IP address (192.168.1.1 by default). If it cannot, check the Ethernet cabling.</p> <p>Verify that you are using Internet Explorer v5.0 or later, or Netscape Navigator v4.61 or later.</p> <p>Verify that the IP address defined for the PC is in the same subnet as the IP address assigned to the LAN port on the ADSL router.</p>

Problem	Troubleshooting Suggestion
My changes to the web pages are not being retained.	Be sure to confirm all changes by clicking the <Apply> button, and to enter the Save Configuration page and save the changes after completing all settings for them to take effect when the router is powered on again.

8.2 Diagnosing Problem Using IP Utilities

8.2.1 ping

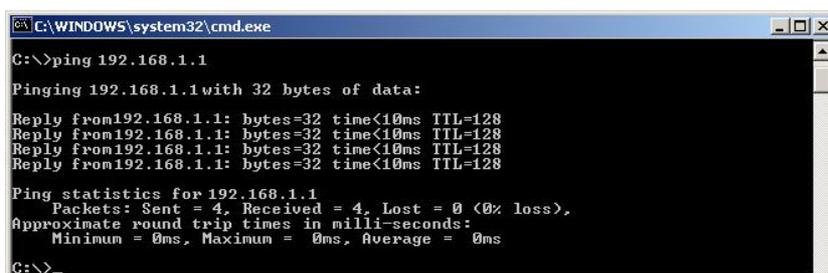
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends messages to the computer you specify. If the computer receives the messages, it sends messages in reply. To use the command, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the *Start* button, and then click *Run*. In the *Open* text box, type a statement such as the following:

ping 192.168.1.1

Click *OK*. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the messages, a *Command Prompt* window is displayed:



```

C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128

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

Figure 8-1 Using the ping utility

If the target computer cannot be located, you will receive the message *Request timed out*.

Using the ping command, you can test whether the path to the ADSL router is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP

address of a particular Internet location, you can use the *nslookup* command, as explained in the following section.

For most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

8.2.2 nslookup

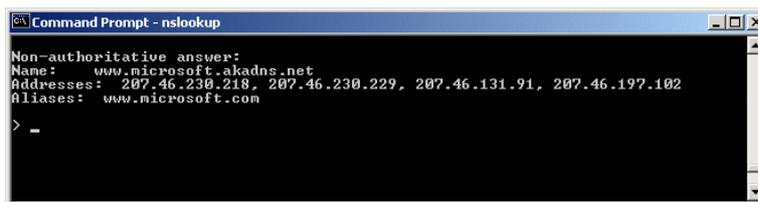
You can use the *nslookup* command to determine the IP address associated with an Internet site name. You specify the common name, and the *nslookup* command looks up the name in your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the *nslookup* command from the *Start* menu. Click the *Start* button, and then click *Run*. In the *Open* text box, type the following:

Nslookup

Click *OK*. A Command Prompt window is displayed with a bracket prompt (>). At the prompt, type the name of the Internet address that you are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown below:



```
Command Prompt - nslookup
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses: 207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases: www.microsoft.com
> -
```

Figure 8-2 Using the *nslookup* utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the *nslookup* utility, type **exit** and press **[Enter]** at the command prompt.

9 Appendix - Glossary

10BASE-T		A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See also data rate, Ethernet.
100BASE-T		A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See also data rate, Ethernet.
ADSL	Asymmetric Digital Subscriber Line	The most commonly deployed "flavor" of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.
ATM	Asynchronous Transfer Mode	A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See also data rate.
authenticate		To verify a user's identity, such as by prompting for a password.
binary		The "base two" system of numbers, which uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See also bit, IP address, network mask.
bit		Short for "binary digit," a bit is a number that can have two values, 0 or 1. See also binary.
bps		bits per second
bridging		Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The ADSL router can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See also routing.
broadband		A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
broadcast		To send data to all computers on a network.

DHCP	Dynamic Host Configuration Protocol	DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP server	Dynamic Host Configuration Protocol server	A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. <i>See DHCP.</i>
DNS	Domain Name System	The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, www.yahoo.com is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. <i>See also domain name.</i>
domain name		A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). A domain name is a key element of a URL, which identifies a specific file at a web site. <i>See also DNS.</i>
download		To transfer data in the downstream direction, i.e. from the Internet to the user.
DSL	Digital Subscriber Line	A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
Ethernet		The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. <i>See also 10BASE-T, 100BASE-T, and twisted pair.</i>
firewall		<p>A firewall is a method for protecting your computer or LAN from attacks and other unwelcome or malicious accesses from the outside (i.e. the Internet). Unauthorized users may attempt to attack your network in order to prevent you or others on your LAN from using.</p> <p>You can protect your network by blocking certain types of IP traffic commonly used by 'hackers' to transport attacks from the Internet to your LAN (incoming traffic). Similarly, you can restrict the types of IP traffic sent from your network to the Internet (outgoing traffic). Some firewall protection can be provided by packet filtering and Network Address Translation services.</p>
FTP	File Transfer Protocol	A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.
Gbps		Abbreviation for Gigabits ("GIG-uh-bits") per second, or one billion bits per second. Internet data rates are often expressed in Gbps.

host		A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol	HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. <i>See also web browser, web site.</i>
Hub		A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It usually includes a switch of some kind. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.
ICMP	Internet Control Message Protocol	An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IEEE		The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.
Internet		The global collection of interconnected networks used for both private and business communications.
intranet		A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP		<i>See TCP/IP.</i>
IP address	Internet Protocol address	The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a <i>network ID</i> that identifies the particular network the host belongs to, and a <i>host ID</i> uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. <i>See also domain name, network mask.</i>
ISP	Internet Service Provider	A company that provides Internet access to its customers, usually for a fee.
LAN	Local Area Network	A network limited to a small geographic area, such as a home, office, or small building.
LED	Light Emitting Diode	An electronic light-emitting device. The indicator lights on the front of the ADSL router are LEDs.
MAC address	Media Access Control address	The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example, <i>NN:NN:NN:NN:NN:NN</i> .
mask		<i>See network mask.</i>
Mbps		Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

NAT	Network Address Translation	A service performed by many routers that translates your network's publicly known IP address into a <i>private</i> IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.
network		A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a <i>LAN</i> , or very large, such as the <i>Internet</i> .
network mask		A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. A bits set to 1 means "select this bit" while a bit set to 0 means "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. <i>See also binary, IP address, subnet, "IP Addresses Explained" section.</i>
NIC	Network Interface Card	An adapter card that plugs into your computer and provides the physical interface to your network cabling, which for Ethernet NICs is typically an RJ-45 connector. <i>See Ethernet, RJ-45.</i>
packet		Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it comes from (source address) and where it should go (destination address).
ping	Packet Internet (or Inter-Network) Groper	A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
port		A physical access point to a device such as a computer or router, through which data flows into and out of the device.
PPP	Point-to-Point Protocol	A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the ADSL router uses two forms of PPP called PPPoA and PPPoE. <i>See also PPPoA, PPPoE.</i>
PPPoA	Point-to-Point Protocol over ATM	One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.
PPPoE	Point-to-Point Protocol over Ethernet	One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.
protocol		A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.
remote		In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
RJ-11	Registered Jack Standard-11	The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.

RJ-45	Registered Jack Standard-45	The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
routing		Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.
subnet		A subnet is a portion of a network. The subnet is distinguished from the larger network by a <i>subnet mask</i> that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. <i>See also network mask.</i>
subnet mask		A mask that defines a subnet. <i>See also network mask.</i>
TCP		<i>See TCP/IP.</i>
TCP/IP	Transmission Control Protocol/Internet Protocol	The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.
Telnet		An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.
TFTP	Trivial File Transfer Protocol	A protocol for file transfers. TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
twisted pair		The ordinary copper telephone wiring long used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. <i>See also 10BASE-T, 100BASE-T, Ethernet.</i>
upstream		The direction of data transmission from the user to the Internet.
USB	Universal Serial Bus	A serial interface that lets you connect devices such as printers, scanners, etc. to your computer by simply plugging them in. The ADSL router is equipped with a USB interface for connecting to a stand-alone PC.
VC	Virtual Circuit	A connection from your DSL router to your ISP.
VCI	Virtual Circuit Identifier	Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. <i>See also VC.</i>

VPI	Virtual Path Identifier	Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. <i>See also VC.</i>
WAN	Wide Area Network	Any network spread over a large geographical area, such as a country or continent. With respect to the ADSL router, WAN refers to the Internet.
Web browser		A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. <i>See also HTTP, web site, WWW.</i>
Web page		A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the <i>home page</i> . <i>See also hyperlink, web site.</i>
Web site		A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. <i>See also hyperlink, web page.</i>
WWW	World Wide Web	Also called <i>(the) Web</i> . Collective term for all web sites anywhere in the world that can be accessed via the Internet.
ZIPB	Zero Installation PPP Bridge	It is a way to ensure that a home user can be assigned a public IP address through the modem, and can then access the Internet without having to configure NAT on the modem, or install PPP software on the home computer. ZIPB mode becomes active when it has been enabled, IPCP negotiation has completed over the WAN PPP link, and a DHCPDISCOVER has been received on the modem LAN interface.