

ADE-4200 / ADW-4200 ADSL VPN/Firewall Router

User's Manual

Download from Www.Somanuals.com. All Manuals Search And Download.

Copyright

Copyright (C) 2003 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Compliance Statement

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the instructions provided with the equipment, may cause interference to radio and TV communication. The equipment has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If you suspect this equipment is causing interference, turn your Ethernet Switch off and reappears when you turn it back on, there is interference being caused by the Ethernet Switch.

You can try to correct the interference by one or more of the following measures:

- w Reorient the receiving radio or TV antenna where this may be done safely.
- w To the extent possible, relocate the radio, TV or other receiver away from the Switch.
- **w** Plug the Ethernet Switch into a different power outlet so that the Switch and the receiver are on different branch circuits.

If necessary, you should consult the place of purchase or an experienced radio/television technician for additional suggestions.

CE mark Warning

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

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Revision

User's Manual for PLANET ADSL VPN/Firewall Router: Model: ADE-4200A/B, ADW-4200A/B Rev: 1.0 (October 2003) Part No.: EM-AD4200

Table of Contents

CHAPTER 1. INTRODUCTION	1
1.1 AN OVERVIEW OF THE ADE-4200/ADW-4200	1
1.2 PACKAGE CONTENTS	
1.3 ADE-4200/ADW-4200 FEATURES	
1.4 ADE-4200/ADW-4200 APPI ICATION	
	-
CHAPTER 2. USING THE ROUTER	5
2.1 CAUTIONS FOR USING THE ADE-4200/ADW-4200	5
2.2 THE TOP PANEL LEDS	5
2.3 THE REAR PORTS	6
2.4 Cabling	7
CHAPTER 3. CONFIGURATION	8
3.1 BEFORE CONFIGURATION	8
3.2 CONNECTING THE ADE-4200/ADW-4200	
3.3 CONFIGURING PC IN WINDOWS	
3.3.1 For Windows 98/MF	
3.3.2 For Windows NT4.0	11
3.3.3 For Windows 2000	
3.3.4 For Windows XP	
3 4 FACTORY DEFAULT SETTINGS	16
3 4 1 Username and Password	16
3 4 2 I AN and WAN Port Addresses	17
3.5 INFORMATION FROM THE ISP	17
3.6 CONFIGURING WITH THE WEB BROWSER	17
361 STATUS	19
3.6.2 Quick Start	20
36.3 Configuration	20
3.6.3.1 LAN	
3.6.3.1.1 Ethernet	20
3.6.3.1.2 Wireless	21
3.6.3.1.3 Port Setting	22
3.6.3.1.4 DHCP Server	24
3.6.3.2 WAN	
3.6.3.2.1 ISP	
3.6.3.2.1.1 RFC 1483 fouted	20 26
3.6.3.2.1.2 RFC 1465 bildged	20 27
3.6.3.2.1.4 IPoA routed	
3.6.3.2.1.5 PPPoE routed	29
3.6.3.2.2 DNS	30
3.6.3.3 System	30
3.6.3.3.1 Time Zone	
3.6.3.3.2 Remote Access	
3.6.3.3 FIrmware Upgrade	
3.6.3.5 Restart Router	32 32
3 6 3 3 6 User Management	
3.6.3.4 Firewall	
3.6.3.4.1 General Settings	34
3.6.3.4.2 Packet Filter	36
3.6.3.4.2.1 Port Filters	36
3.6.3.4.2.2 Address Filters	37
3.6.3.4.2.3 Packet filter example	
3.6.3.4.3 Intrusion Detection	41
3.0.3.4.4 MAC AUDIESS FILLEI	44 /F
3.5.3.4.5 UKL Filler	40 46
3.5.3.4.5.2 Domain Filtering:	
3635 VPN	47

3.6.3.5.1 PPTP	48
3.6.3.5.1.1 PPTP for Remote Access	48
3.6.3.5.1.2 PPTP for LAN to LAN	49
3.6.3.5.1.3 An Example of Configuring a Remote Access PPTP VPN Dial-in Connection	50
3.6.3.5.1.4 An Example of Configuring a Remote Access PPTP VPN Dial-out Connection	54
3.6.3.5.1.5 An Example of Configuring a LAN-to-LAN PPTP VPN Connection	56
3.6.3.5.2 IPSec	58
3.6.3.5.2.1 IPSec configuration	58
3.6.3.5.2.2 An Example of Configuring a LAN-to-LAN IPSec VPN Connection	61
3.6.3.6 Virtual Server	63
3.6.3.6.1 An Example of Configuring a Web Server on the Local Network	65
3.6.3.6.2 An example of configuring the Web Server & the Router to be accessible remotely	66
3.6.3.7 Advanced	68
3.6.3.7.1 Routing Table	68
3.6.3.7.2 Dynamic DNS	69
3.6.3.7.2.1 Example of Configuring DDNS	69
3.6.3.7.3 Checking Emails	70
3.6.3.7.4 Device Management	71
3.6.3.7.4.1 Embedded Web Server	71
3.6.3.7.4.2 Universal Plug and Play (UPnP)	
3.6.3.7.4.3 SNMP Access Control	
3.6.4 Save Configuration to Flash	/2
3.6.5 Logout	73
CHAPTER 4. TROUBLESHOOTING	74
	75
	/ ၁
APPENDIX B. PRODUCT SUPPORT	76

Chapter 1. Introduction

1.1 An Overview of the ADE-4200/ADW-4200

The ADE-4200 ADSL VPN/Firewall Router and ADW-4200 ADSL Wireless VPN/Firewall Router provide office and residential users the ideal solution for sharing a high-speed ADSL broadband Internet connection on an 11Mbps wireless network or a 10/100Mbps Fast Ethernet backbone. They can support downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1Mbps. The products support PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with ISP.

They also serve as an Internet firewall, protecting your network from being accessed by outside users. Not only provide the natural firewall function (Network Address Translation, NAT), they also provide rich firewall features to secure a user's network. All incoming data packets are monitored and filtered. Besides, they can also be configured to block internal users from accessing to the Internet.

Furthermore, PPTP and IPSec VPN are also supported. Utilizing 56-bit DES and 168bit 3DES encryption, header authentication, and Internet Key Exchange (IKE) access control, their full IPSec VPN (virtual Private Network) capability provides complete data security and privacy for access and exchange of sensitive data. The PLANET ADE-4200 and ADW-4200 offer the security and flexibility to make fast and simple secure ADSL network connections.

1.2 Package Contents

- 1. One ADSL VPN/Firewall Router
- 2. One CD-ROM containing the on-line manual
- 3. One RJ-11 ADSL/telephone cable
- 4. One straight-through CAT-5 Ethernet cable
- 5. One AC-DC power adapter (output: 12V DC, 1A)
- 6. One Quick Start Guide

1.3 ADE-4200/ADW-4200 Features

ADE-4200/ADW-4200 provides the following features:

ADSL Multi-Mode Standard: Supports downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1024Kbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2).

Wireless Ethernet 802.11b access point: ADW-4200 Provides a wireless Ethernet

802.11b access point for extending the communication media to WLAN.

Fast Ethernet Switch: A 4-port 10/100Mbps fast Ethernet switch is supported in the LAN site and automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports is supported. An Ethernet straight or crossover cable can be used directly, this fast Ethernet switch will detect it automatically.

Multi-Protocol to Establish A Connection: Supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

Quick Installation Wizard: Supports a WEB GUI page to install this device quickly. With this wizard, an end user can enter the information easily which they from the ISP, then surf the Internet immediately.

Universal Plug and Play (UPnP) and UPnP NAT Traversal: This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices.

Network Address Translation (NAT): Allows multi-users to access outside resource such as Internet simultaneously with one IP address/one Internet access account. Besides, many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting and others.

Firewall: Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. The packet filtering and SPI are also supported. The hacker's attack will be recorded associated with timestamp in the security logging area. More firewall features will be added continually, please visit our web site to download latest firmware.

Domain Name System (DNS) relay: provides an easy way to map the domain name (a friendly name for users such as <u>www.yahoo.com</u>) and IP address. When a local machine sets its DNS server with this router's IP address, then every DNS conversion requests packet from the PC to this router will be forwarded to the real DNS in the outside network. After the router gets the reply, then forwards it back to the PC.

Dynamic Domain Name System (DDNS): The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply an account from this free Web server <u>http://www.dyndns.org/</u>. There are more than 5 DDNS servers supported.

Virtual Private Network (VPN): Allows a user to make a tunnel with a remote site directly to secure the data transmission among the connection. Users can use **embedded PPTP client/server and IPSec** supported by this router to make a VPN tunnel or the user can run the PPTP client in PC and the router already provides IPSec and PPTP pass through function to establish a VPN connection if the user likes to run the PPTP client in his local computer.

PPP over Ethernet (PPPoE): Provide embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. The Always ON, Dial On Demand and auto disconnection (Idle Timer) functions are provided too.

Virtual Server: Users can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, users can assign a PC in a LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse an inside web server directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

Rich Packet Filtering: Not only filters the packet based on IP address, but also based on Port numbers.

Dynamic Host Control Protocol (DHCP) client and server: In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN site, the DHCP server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

Static and RIP1/2 Routing: Supports an easy static table or RIP1/2 routing protocol to support routing capability.

SNTP: An easy way to get the network real time information from an SNTP server.

Web based GUI: supports web based GUI for configuration and management. It is user-friendly with an on-line help, providing necessary information and assist user timing. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable: the device can be upgraded to the latest firmware through the WEB based GUI.

Rich management interfaces: Supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal application through console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage a device.

1.4 ADE-4200/ADW-4200 Application

Internet Connection with Firewall:

They are the perfect solution to connect a small group of PCs to a high-speed broadband Internet connection. Multi-users can have high-speed Internet access simultaneously. With their policy-based firewall and Intrusion detection function, the internal network is secured from any hacker attack.

VPN Connectivity:

The ADE-4200 and ADW-4200 VPN connectivity support client-to-VPN gateway and VPN LAN-to-LAN connections. Using these connection capabilities, mobile workers may attach to and access LAN resources from the public Internet while they are working at home or at branches abroad. All corporate remote offices can deploy a ADE-4200 / ADW-4200 and establish secure connection with headquarters and share resources and information through the Internet in a safe and secure way.

Chapter 2. Using the Router

2.1 Cautions for using the ADE-4200/ADW-4200



Do not place the ADE-4200/ADW-4200 under high humidity and high temperature.

Do not use the same power source for ADE-4200/ADW-4200 with other equipment.

Do not open or repair the case yourself. If the ADE-4200/ADW-4200 is too hot, turn off the power immediately and have a qualified serviceman repair it.



Place the ADE-4200/ADW-4200 on a stable surface.

Only use the power adapter that comes with the package.

2.2 The Top Panel LEDs



ADE-4200



ADW-4200

LED	Meaning
PWR	Lit when power ON
SYS	Lit when system is ready
LAN port	Lit when connected to Ethernet device
1 ~ 4	Green for 100Mbps; Orange for 10Mbps
	Blinking when data transmit/received
WLAN (ADW-4200 only)	Lit green when the wireless connection is established. Flashes when sending or receiving data.
MAIL	Lit when there is email in the email account
PPP	Lit when there is a PPPoA/PPPoE connection
ADSL	Lit when successfully connected to an ADSL DSLAM

2.3 The Rear Ports



ADSL	Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network.
Console	Connect a PS2 or DB9 RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port). Please note that console cable is not provided on standard package.
LAN 1 — 4 (RJ-45 connector)	Connect an UTP Ethernet cable to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
Reset	After the device is powered on, press it to reset the device or restore to factory default settings. The operation is as below: 0-3 seconds : reset the device 3-6 seconds : no action 6 seconds or above : restore to factory default settings (this is used when you can not login to the router, e.g. forgot the password)
PWR	Connect the supplied power adapter to this jack.
Power Switch	Power ON/OFF switch

2.4 Cabling

The most common problem is bad cabling or ADSL line. Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. As a first check, verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Chapter 3. Configuration

The ADE-4200/ADW-4200 can be configured with your Web browser. The web browser is included as a standard application in the following operation systems, UNIX, Linux, Mac OS, Windows 98/NT/2000/Me, etc. The product provides a very easy and user-friendly interface for configuration.

3.1 Before Configuration

This section describes the configuration required by LAN-attached PCs that communicate with the ADE-4200/ADW-4200, either to configure the device, or for network access. These PCs must have an Ethernet interface installed properly, be connected to the ADE-4200/ADW-4200 either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet of the ADE-4200/ADW-4200. The default IP address of the ADE-4200/ADW-4200 is 192.168.1.254 and subnet mask is 255.255.255.0. The best and easy way is to configure the PC to get an IP address from the ADE-4200/ADW-4200. Also make sure you have UNINSTALLED any kind of software firewall that can cause problems accessing the 192.168.1.254 IP address of the router.

Please follow the steps below for PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows related manuals.



Any TCP/IP capable workstation can be used to communicate with or through the ADE-4200/ADW-4200 To configure other types of workstations, please consult the manufacturer's documentation.

3.2 Connecting the ADE-4200/ADW-4200

- 1. Connect the Router to a LAN (Local Area Network) and the ADSL/telephone network.
- 2. Power on the device
- 3. Make sure the PWR and SYS LEDs are lit steady & LAN LED is lit.
- **4.** Before proceeding to the next step, make sure you have **uninstalled** any software firewall.

3.3 Configuring PC in Windows

3.3.1 For Windows 98/ME

1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.

- Select TCP / IP -> NE2000 Compatible, or the name of any Network Interface Card (NIC) in your PC.
- 3. Click Properties.

Network
Configuration Identification Access Control
The following network components are installed:
NE2000 Compatible NetBEUI -> Dial-Up Adapter NetBEUI -> NE2000 Compatible
TCP/IP -> Dial-Up Adapter
📮 File and printer sharing for Microsoft Networks 📃 💽
Add Remove Properties
Client for Microsoft Networks
<u>File</u> and Print Sharing
Description TCP/IP is the protocol you use to connect to the Internet and wide-area networks.
OK Cancel

4. Select the IP Address tab. In this page, click the Obtain an IP address automatically radio button.

T	CP/IP Properties	×
	Bindings Advanced NetBIOS	1
	DNS Configuration Gateway WINS Configuration (IP Address	୬
	An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.	
	🗩 🖲 Obtain an IP address automatically	
1	C Specify an IP address:	
	IP Address:	
	Sybnet Mask:	
	OK Cancel	

- 5. Then select the DNS Configuration tab.
- 6. Select the **Disable DNS** radio button and click "OK" to finish the configuration.

TCP/IP Properties	2 ×
Bindings Advanced NetBIOS DNS Configuration Gateway WINS Configuration IP Addre	ess
© Disable DNS © Enable DNS	
Host: Domain: Domain:	
Add <u>R</u> emove	
Domain Suffix Search Order	
Remove	
OK Cancel	

3.3.2 For Windows NT4.0

- 1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
- 2. Select TCP/IP Protocol and click Properties.

VetWork Protoco	otocol		
NWLink IP>	//SPX Compatib	ole Transport	
TCP/IP Pro	tocol		
<u>A</u> dd	<u>R</u> emove	Properties	<u>U</u> pdate
Description:			
Transport Cont	rol Protocol/Inte	ernet Protocol. The d	lefault wide
diverse interco	nnected networ	ks.	
<u></u>			

3. Select the Obtain an IP address from a DHCP server radio button and click OK.

	erties			? X
IP Address DNS W	INS Addre	ess R	outing	
An IP address can be a by a DHCP server. If y ask your network admin the space below.	automatica iour netwo nistrator fo	ally ass ork doe or an ac	igned to th s not have ddress, and	iis network card a DHCP server, d then type it in
Adagter:	1			
🖉 Obtain an IP add	dress from	a DHC	P server	
	dress —		575	
IP Address:		- 20		
S <u>u</u> bnet Mask:		27	+	
S <u>u</u> bnet Mask: [Default <u>G</u> ateway: [(†) (†)	2) 75	+	
Subnet Mask:	() ()	5) 5-	+	A <u>d</u> vanced

3.3.3 For Windows 2000

- 1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
- 2. Double-click LAN Area Connection.



3. In the LAN Area Connection Status window, click Properties.

Connection	
Status:	Connected
Duration:	05:54:27
Speed:	10.0 Mbps
Packets:	Sent — En – Received 300 138
Properties	Disable

4. Select Internet Protocol (TCP/IP) and click Properties.

Local Area Connection 2 Properties
General Sharing
Connect using:
Realtek RTL8139(A) PCI Fast Ethernet Adapter
Configure
Components checked are used by this connection:
NWLink IPX/SPX/NetBIOS Compatible Transport Proto NetBEUI Protocol Internet Protocol (TCP/IP) Install Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Sho <u>w</u> icon in taskbar when connected
OK Cancel

- **5.** Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
- 6. Click OK to finish the configuration.

iis capability. Utherwise, you i ie appropriate IP settings.	need to ask y	vour ne	twork	administra	ator for
Obtain an IP address aut	omatically				
C Use the following IP add	ress:				
[P address:		15	<i>5</i> 5	53]
S <u>u</u> bnet mask:	Γ	÷	4		1
Default gateway:		4	Ψř.	2	1
Obtain DNS server addre	ess automatic	allu			
C Use the following DNS s	erver addres:	ses:—			
Preferred DNS server			±1.		1
Alternate DNS server:		a.	t.	-]

3.3.4 For Windows XP

- 1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click on Network Connections.
- 2. Double-click Local Area Connection



3. In the LAN Area Connection Status window, click Properties.

🕹 Local Area Co	nnection Status	? 🛛
General Support		
Connection		
Status:		Connected
Duration:		00:05:34
Speed:		100.0 Mbps
Activity	Sent — 👰 -	- Received
Bytes:	1,403	1,749
Properties	Disable	Close

4. Select Internet Protocol (TCP/IP) and click Properties.

General	Authentication	n Advanced	
Connec	et using:		
BB F	ealtek RTL81	39 Family PCI Fast Ethe	ernet NIC
This co	nnection uses I	the following items:	Configure
	Client for Micr File and Printo Internet Proto	rosoft Networks er Sharing for Microsoft col (TCP/IP)	Networks
	nstall	Uninstall	Properties
Desci	ription		-
Tran wide acro:	smission Contro area network p ss diverse inter	ol Protocol/Internet Pro protocol that provides o connected networks.	tocol. The default communication
(:	w icon in notific	ation area when conn	ected

5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons

eneral	Alternate Configu	uration				
'ou car his cap he appr	n get IP settings a ability. Otherwise, ropriate IP setting:	ssigned auto you need to s.	matically if y ask your n	your nel etwork (work su administi	pports ator for
о оь	tain an IP addres	s automatica	lly			
O Us	e the following IP	address: —				
IP ad	dress:					
Subn	et mask:				(9. S. S)	
Defa	ult gateway:				-	
о оь	tain DNS server a	address autor	matically			
OUs	e the following DN	4S server ad	ldresses: —			_
Prefe	rred DNS server:					
Alterr	ate DNS server:			i v		
					Adva	anced

6. Click OK to finish the configuration.

3.4 Factory Default Settings

Before configurating this ADE-4200/ADW-4200, you need to know the following default settings.

1. Web Configurator

Username: admin Password : admin

2. Device IP Network settings in LAN site

IP Address : 192.168.1.254

Subnet Mask : 255.255.255.0

3. ISP setting in WAN site

PPPoE

4. DHCP server

DHCP server is enabled. Start IP Address : 192.168.1.100 IP pool counts : 100

3.4.1 Username and Password

The default username and password are admin and admin respectively.



If you ever forget the password to log in, you may press the RESET button to restore the factory default settings..

3.4.2 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to
Subnet Mask	255.255.255.0	automatically get the
DHCP server function	Enabled	WAN port configuration from the ISP, but you have to
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	set the username and password first.
	(Actually, it can support up to 253 users.)	

3.5 Information from the ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, IPoA, or PPTP-to-PPPoA Relaying.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed).			
ΡΡΡοΑ	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed).			
RFC1483 Bridged	FC1483 BridgedVPI/VCI, VC-based/LLC-based multiplexing and configu this product into BRIDGE Mode.			
RFC1483 Routed	CHARACTER STATES (1483 Routed VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).			
ΙΡοΑ	VPI/VCI, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).			

3.6 Configuring with the Web Browser

Open the web browser, enter the local port IP address of this ADE-4200/ADW-4200, which defaults at **192.168.1.254**, and click "**Go**", a user name and password window prompt will appear. The default username and password are admin and admin.

۲	Please type	your user name and password.
3	Site:	192.168.1.254
	Realm	
	User Name	1
	Password	
	□ <u>S</u> ave this	s password in your password list

You will get a status report web page when login successfully.

🎒 http://192.168.1.254/ - M	licrosoft Internet Explorer			_ B >			
<u>F</u> ile <u>E</u> dit ⊻iew F <u>a</u> vorite:	s <u>T</u> ools <u>H</u> elp						
↔ → → · ④ Back Forward Sto	pp Refresh Home Se	😡 🔝 🧭 earch Favorites History	Mail Print Edit	- Discuss			
Address 🛃 http://192.168.1.2	54/			✓ Go Links			
PLANET Retworking & Communication	PLAN	IET ADE-4200	ADSL VPN/Firew	all Router			
Status			Status				
Quick Start							
Configuration	Host Name			Set Host Name 🕥			
Save Config to FLASH	System Up-Time	4 days, 21 hours					
	Current Time	Mon, 06 Oct 2003 - 08	6:36:26	Set Time ()			
Cogout	Hardware Version	ADSL GE-A v1.00 / H	e100/2xx CSP v2.3				
	Software Version	4.23					
Language	MAC Address	00:04:ED:04:10:9E					
English 🗾	Home URL PLANET Technology Corporation.						
	LAN						
		IP Address:	192.168.1.254	LAN Settings O			
		SubNetmask: 255.255.255.0					
	5. 5.	DHCP Server:	Yes	DHCP Server Settings O			
	WAN			ANANI O WANTER OF			
		US_PPPOE		WAN Settings O			
			0/33				
	-	PPPoE Connection:	Cable disconnected				
		P Address. SubNotmoole	0.0.0	1			
	÷.		0.0.0				
		Primary DNS:	139.175.55.244	DNS Settings 0			
	Port Status						
		Port Type Ethernet ethernet	Connected Line State				
		A1 adsl	×				
	Defined Interfaces						
		QS_WAN:	VPI/VCI:0/33	Rx: 0/ 0			
				Tx: 857/ 0			
		Ethernet:		Rx : 359080/ 0			
	<u> </u>			Tx : 9692/10			

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- n **Status** (ARP Table, PPTP Status, IPSec Status, Email Status, Event Log, Error Log and UPnP Portmap)
- n Quick Start
- n Configuration (LAN, WAN, System, Firewall, VPN, Virtual Server & Advanced)

- n Save Config to FLASH
- n Logout
- n Language (provides user interface in English language)

Click on the desired item to expand the page in the main navigation pane.

3.6.1 STATUS

The **Status** section provides and contains many items including device H/W and S/W information, LAN, WAN, Port status and all defined interfaces. It also provides useful information for users to review the status of the device.

ARP Table - you will see the data of the IP address of each PC in your LAN as well as its associated MAC address.

▼	Status ARP Table PPTP Status IPSec Status Email Status Event Log	IP A	RP entries	8			ARP Table
	 UPnP Portmap 	IP A	ddress	MAC Address	Interface	Static	
0	Quick Start	192	168.1.249	00:e0:18:fd:50:5a	iplan	no	
⊳	Configuration						
0	Save Config to FLASH						
0	Logout						
	Language English 💌						

PPTP Status - it gives you a quick overview of the PPTP connection status.

IPSec Status - it gives you a quick overview of the IPSec connection status.

Email Status - it gives you a quick view to know if there is email in your pre-defined email account. You will see the unread emails in the email server once you have successfully configured the "Check Emails" in **Configuration à Advance.**

Event Log - it displays valuable system event logging information and status after the power is turned on, such as ADSL line, WAN port, SNTP, Firewall, and etc.

Error Log - it shows the error message log. When you face a problem, please send this error log to support for quick feedback.

UPnP Portmap - it displays the Virtual Servers (or Port Mappings) that created by UPnP protocol implemented in Windows.

3.6.2 Quick Start

Status		Quick Start
Quick Start		
Configuration	Encapsulation:	PPPoE Scan
Save Config to FLASH	VPI:	
• Logout	VCI:	1483 Routed IP VC-Mux 1483 Routed IP II C
Language English	NAT:	(1483 LLC MER Classical IP (1577) 1483 Bridged IP VC-Mux
	IP Address:	1483 Bridged IP LLC red Pure Bridged VC-Mux Buro Bridged VC-Mux automatically)
	SubNetmask:	0.0.0
	Default Gateway:	
		DNS
	Primary DNS:	
	Secondary DNS:	
		РРР
	Username:	
	Password:	
	Apply Cancel	

If you use this device to access the Internet through the ISP, this web page is enough for you to configure this router and access the Internet without a problem. Please check Chapter 3.5 *Information from the ISP*, then enter the proper values into this web page, click the **Apply** button and then **Save Config to FLASH** in the left panel. After the router reboot, you may check the Status web page to check whether the router is connected to the ISP or not. In most cases, you can access the Internet immediately. If not, please refer to the sections below for more information.

3.6.3 Configuration

When you click this item, you get following sub-items to configure the ADSL router.

LAN, WAN, System, Firewall, VPN, Virtual Server and Advanced

These functions are described below in the following sections.

3.6.3.1 LAN

There are four items under the LAN section: Ethernet, Wireless, Port Setting and DHCP Server.

3.6.3.1.1 Ethernet

When you click the **Ethernet**, you get the following figure.

	Status	Ethernet
0	Quick Start	
	Configuration ▼ LAN Ethernet Wireless Port Setting DHCP Server ► WAN ► System ► Firewall ► VPN ● Virtual Server ► Advanced	Primary IP Address IP Address: 192 168 1 254 SubNetmask: 255 255 255 0 Secondary IP Address IP Address: 0 0 0 SubNetmask: 0 0 0 0
0	Save Config to FLASH	(Abbi)
•	Logout	Advanced Options
	Language English 💟	

It supports two Ethernet IP addresses in the LAN. With this function, the ADSL router can support two different LAN subnets to access the Internet at the same time. Usually, there is only one subnet in LAN, there is no need to configure a Secondary IP address. The 192.168.1.254 is the default IP address for this ADSL router. The Advanced **Options** will allow you to configure the routing protocol RIP version 1 or version 2 in receiving and sending direction.

3.6.3.1.2 Wireless

When you click Wireless, you will get the following figure. This option is only available for ADW-4200.

▶ Status		<u>Wireless</u>
Quick Start		
∇ Configuration ∇ LAN	ESSID:	wlan-ap
Ethernet Wireless	Regulation Domain:	N.America 💌
Port Setting DHCP Server	Channel ID:	Channel 1 (2.412 GHz)
► WAN	Default Tx Key:	0
► Firewall ► VPN	Passphrase:	Generate
○ Virtual Server ► Advanced	WEP Encryption:	O Disable ○ WEP64 ○ WEP128 Hex
• Save Config to FLASH	Кеу 0:	
Contemporary Logout	Key 1:	
Language	Key 2:	
English 💌	Кеу 3:	
	Hide_SSID:	false
	Reset:	false 💌
	Connected:	true
	Link Speed:	110000
	Card type:	Prism 2.5
	AP Firmware Version:	2.0.4
	Primary Firmware Version:	1.0.7
	Disable:	false

ESSID: Enter the unique ID given to the Access Point (AP), which is already built-in to the wireless broadband firewall gateway. To connect to this device, your wireless clients must have the same ESSID as the device.

Regulation Domain: There are five Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, and **Spain**. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Default Tx Key: Select the encryption key ID, please refer to Key (0-3) below.

Passphrase: This is used to generate WEP keys automatically by an input string and pre-defined algorithm in WEP64 or WEP128. You can input the same string in both AP and Client card to generate same WEP keys. Please note that you do not have to key in **Key (0-3)** as below when the **Passphrase** is enabled.

WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the wireless broadband firewall gateway offers highly secure data encryption, known as WEP. If you require high security in transmission, there are two alternatives to select from, WEP 40 and WEP 128.

Key (0-3): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the device. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is "-". Take WEP64 case for example, 11-22-33-44-55 is a valid key, 1122334455 is invalid instead.

Hide_SSID: When enabled, the Wireless AP is invisible from the site-surveying by Wireless clients. The wireless clients still can associate with this Wireless AP if entered with the same ESSID value.

Reset: Reset the Wireless AP function

3.6.3.1.3 Port Setting

When you click **Port Setting**, you get the following figure. This allows you to configure the port setting to solve some of the compatibility problems while connecting to the Internet.

	Status	Port Setting
0	Quick Start	
$\overline{\mathbf{v}}$	Configuration	Port1 Connection Type: Auto
	V LAN Ethernet	Port2 Connection Type: Auto
	Wireless Port Setting	Port3 Connection Type: Auto
	DHCP Server	Port4 Connection Type: Auto
	System Eirewall	Port1 Rate Limit: O Disable
	VPN Virtual Server	C Enable * 32kbps
	 Advanced 	Port2 Rate Limit: © Disable
0	Save Config to FLASH	C Enable * 32kbps
0	Logout	Port3 Rate Limit: O Disable
	Language English 💌	C Enable * 32kbps
		Port4 Rate Limit: O Disable
		C Enable * 32kbps
		IPv4 TOS priority Control: O Disable O Enable
		Set high priority TOS:
		□63 □62 □61 □60 □59 □58 □57 □56 □55 □54 □53 □52 □51 □50 □49 □48
		□ 47 □ 46 □ 45 □ 44 □ 43 □ 42 □ 41 □ 40 □ 39 □ 38 □ 37 □ 36 □ 35 □ 34 □ 33 □ 32
		Apply

Port # Connection Type: Five options to choose from: auto, 10M half-duplex, 10M fullduplex, 100M half-duplex or 100M full-duplex. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices. You can configure different types to solve the compatibility issues.

Port # Rate Limit: When it is enabled, enter a rate value that is configured as multiple of 32kbps. This function limits the inbound and outbound Ethernet throughput around the value that you specified.

IPv4 TOS priority Control: TOS, Type of Services, is the 2nd octet of IP packet. The bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet. The definition of these bits is listed blow:

Two bits: reserved One bit: high reliability One bit: high throughput One bit: No delay Three bits: IP priority (0 to 7)

This feature uses bits 0-5 to classify the packets' priority. If the packet is in high priority, it will flow first and will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the embedded Ethernet switch IC will check the 2nd octet of each IP packet. If the value in the TOS field matches in the checked values in the table (0 to 63), this packet will treat it as high priority.

3.6.3.1.4 DHCP Server

When you click **DHCP Server**, you get the following figure. You can disable or enable the DHCP server or enable the DHCP relay functions.



If you check **Disabled** and click **Next**, then click **Apply**. The DHCP server function is disabled. Each PC in the LAN should assign a fixed IP address and set the PC's gateway to the ADSL router.

If you check **DHCP Server** and click **Next**, you can configure parameters of the DHCP server including the IP pool (starting IP address and ending IP address), leased time for each assigned IP address, DNS IP address, Gateway IP address. Those messages are sent to the DHCP client when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router will find the IP address from the outside network automatically and forward it back to requesting PC in the LAN.

If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Click **Apply** to enable this function.

3.6.3.2 WAN

There are 2 items under the **WAN** section: **ISP** and **DNS**.

3.6.3.2.1 ISP

When you click **ISP**, you will get the following screen.

	> Status	WAN connections						
• ▼	Quick Start Configuration	WAN services currently defined:						
	V WAN	Name	Description	Creator	VPI	VCI		
	ISP DNS	rfc1483-0	RFC 1483 routed mode	WebAdmin	8	35	Edit 🕥	Delete 🕥
 ▷ System ▷ Firewall ▷ VPN ○ Virtual Server ▷ Advanced 		Create 🕥						
0	Save Config to FLASH							
•	Logout							
	Language English 💟							

The factory default is **rfc 1483-0**. If your ISP uses the same access protocol, please click **Edit** to input other parameters as below. If your ISP does not use rfc 1483-0, you can delete it by clicking **Delete**. Then you may click **Create** to create a connection to your ISP to surf the Internet. The following page is then shown.

	Status	ISP
• ⊽	Quick Start Configuration ▷ LAN ▼ WAN	Please select the type of service you wish to create:
	ISP DNS System Firewall VPN Virtual Server Advanced	 PPPoA routed PPPoE routed Next Quick Start
0	Save Config to FLASH	
•	Logout Language English V	

Select one of the access methods among the 5 listed items and click **Next** to configure the right connection method. Please refer to the following description and Section 3.5 Information from ISP.

Quick Start...) is a shortcut to the Quick Start page.

3.6.3.2.1.1 RFC 1483 routed

⊳	Status	<u>v</u>	VAN connections: RFC 1483 routed
0	Quick Start		
▼	Configuration	Description:	RFC 1483 routed mode
	► LAN ▼ WAN	VPI:	0
	ISP DNS	VCI:	0
	▶ System	NAT:	Enable 🔽
	▷ Firewall ▷ VPN	Encapsulation method:	LlcBridged
	 ○ Virtual Server ▷ Advanced 	⊙ Obtain an IP address	automatically via DHCP client
0	Save Config to FLASH	◯ Use the following IP a	address
0	Logout	IP Address:	
		Netmask:	
	Language	Gateway:	
	English 🔛	Apply	

Description: Give a name for this connection.

VPI and VCI: Enter the information provided by your ISP.

NAT: The NAT feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Encapsulation method: Select the protocol format, the default is LlcBridged. Select the one provided by your ISP.

DHCP client: Enable or disable the DHCP client, specify if the Router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click Obtain an IP address automatically via DHCP client to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

	Status		WAN connections: RFC 1483 bridged
•	Quick Start		
∇	Configuration	Description:	RFC 1483 bridged mode
	► LAN V WAN	VPI:	0
	ISP DNS	VCI:	0
	⊳ System	Encapsulation metho	od: LicBridged 🔽
	 Firewall VPN Virtual Server Advanced 	Apply	
•	Save Config to FLASH		
•	Logout		
	Language English 💌		

3.6.3.2.1.2 RFC 1483 bridged

Description: Give a name for this connection.

VPI and VCI: Enter the information provided by your ISP.

Encapsulation method: Select the protocol format, the default is LlcBridged. Select the one provided by your ISP.

3.6.3.2.1.4 PPPoA routed

	Status	<u>W</u>	AN connections: PPPoA routed
0	Quick Start		
V	Configuration	Description:	PPPoA Routed
	IDEN V WAN	VPI:	0
	ISP	VCI:	0
	► System	NAT:	Enable 💌
	▷ Firewall ▷ VPN	Username:	
	 ● Virtual Server ▶ Advanced 	Password:	
0	Save Config to FLASH	Use the following IP address:	(D.O.O.O' means 'Obtain an IP address automatically')
0	Logout	Authentication Protocol:	Chap(Auto)
		PPPoA Connection:	Always On 💌
	Language English 💌	User Idle Timeout (in minutes)	
		Apply	

Description: Give a name for this connection.

VPI/VCI: Enter the information provided by your ISP.

NAT: The NAT feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purpose. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

Use the following IP address: If your ISP gives you a fixed IP address through PPPoA, input the IP address on this field.

Authentication Protocol Type: Default is Auto.

PPPoA connection: This item provides 2 options.

Always on: if you want to establish a PPPoA session when starting up. It will

also automatically re-establish the PPPoA session when disconnected by the ISP.

¤ Connect to Demand: if you want to establish a PPPoA session only when there is a packet requesting access to the Internet.

User Idle Timeout (in minutes): Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Input 0 if you do not want to have idle timeout.

3.6.3.2.1.4 IPoA routed

Status	WAN composition of De A version
Quick Start	WAN connections: IPOA routed
 ▼ Configuration ► LAN ▼ WAN ISP DNS ► System ► Firewall ► VPN ♥ VPN 	Description: IPoA routed VPI: 0 VCI: 0 NAT: Enable © Obtain an IP address automatically via DHCP client
Advanced	C Use the following IP address
Save Config to FLASH	IP Address:
• Logout	Netmask:
Language English 💌	Gateway:

Description: Give a name for this connection.

VPI/VCI: Enter the information provided by your ISP.

NAT: The NAT feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Obtain an IP address automatically via DHCP client: If your ISP give you an IP address dynamically with IPoA, please select this item.

Use the following IP address: If your ISP give you an fixed IP address through IPoA, please select this item and manually configure the IP address, subnet mask and default gateway IP address.

3.6.3.2.1.5 PPPoE routed

	Status	WAN con	nections: PPP	oE routed
0	Quick Start			
∇	Configuration	Description:	PPPoE Routed	
	IDEN IN	VPI:	0]
	ISP DNS	VCI:	0]
	► System	NAT:	Enable 🔽	
	 Firewall VPN 	Username:		
	 ● Virtual Server ▶ Advanced 	Password:]
0	Save Config to FLASH	Service name:]
0	Logout	Use the following IP address:		(D.O.O.O' means 'Obtain an IP address automatically')
		Authentication ProtocolAuthentication Protocol:	Chap(Auto) 🔽	
	Language	PPPoE Connection:	Always On 🛛 🔽	
	English 🎽	User Idle Timeout (in minutes):	0]
		Apply		

Description: Give a name for this connection.

VPI/VCI: Enter the information provided by your ISP.

NAT: The NAT feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purpose. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

Use the following IP address: If your ISP gives you a fixed IP address through PPPoE, input the IP address on this field.

Authentication Protocol Type: Default is Auto.

PPPoE connection: This item provides 2 options.

Always on: if you want to establish a PPPoE session when starting up. It will also automatically re-establish the PPPoE session when disconnected by the ISP.

¤ Connect to Demand: if you want to establish a PPPoE session only when there is a packet requesting access to the Internet.

User Idle Timeout (in minutes): Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Input 0 if you do not want to have idle timeout.

3.6.3.2.2 DNS

The WAN-DNS is shown as below.

► Status	DNS
Quick Start	
 ▼ Configuration ► LAN ▼ WAN ISP DNS ► System ► Firewall ► VPN ● Virtual Server ► Advanced 	Primary DNS IP Address: Secondary DNS IP Address: Apply Cancel
Save Config to FLASH	
Logout	
Language English 🔽	

A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. In the Internet, every host has a unique and friendly name such as <u>www.yahoo.com</u> and an IP address. As the IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP will provide the DNS IP address automatically. You may leave it as blank. Or your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address.

If you choose one of the other three protocols — RFC1483 routed /bridged and IPoA. Check with your ISP, it may provide you with an IP address of DNS. You must enter the DNS IP address if you set the DNS of your PC to the LAN IP address of this router.

3.6.3.3 System

There are six items under the **System** section: **Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart Router** and **User Management.**

3.6.3.3.1 Time Zone

When you click **Time Zone**, you get the following figure.

⊳	Status	Time Zone
0	Quick Start	
▼	Configuration	💿 Enable 🔿 Disable
	► LAN ► WAN ▼ System Time Tame	Time Zone List: 💿 By City 🔘 By Time Difference
	Remote Access	Select a New Local Time Zone (+-UTC/GMT time):
	Firmware Upgrade	(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna 💟
	Backup/Restore Restart Router User Management Firewall VPN VIrtual Server	Enter new SNTP Server IP Address: 140.162.8.3
	► Advanced	Automatically adjust clock for daylight saving changes
0	Save Config to FLASH	
0	Logout	Resync Poll Interval
		Apply Cancel

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from the SNTP server from the outside network. Please choose your local time zone, click **Enable** and click the **Apply** button. You will get the correct time information after you ready establish a connection to the Internet. If you prefer to enter your own SNTP server, please enter and use it as the first choice.

Resync Poll Interval (in minutes) is the periodical interval of router's SNTP client to update (or re-synchronize) the current time with SNTP server after it synchronized with SNTP server.

3.6.3.3.2 Remote Access

When you click **Remote Access**, input the time and then click **Enable**, you may temporarily permit remote administration of the ADE-4200/ADW-4200. The maximum time is 120 minutes.



3.6.3.3.3 Firmware Upgrade

When you click **Firmware Upgrade**, it allows you to input the location of firmware stored on your PC and click the Upgrade button to upgrade to the new firmware.



3.6.3.3.4 Backup/Restore

When you click **Backup/Restore**, it allows you to save your current settings into a file on your PC. You can click the **Backup** to store the current settings on a file. If you like to restore it back, please input the location of this configuration file in the PC and click the **Restore** button to save it back.

▶ Status	Configuration Backup/Restore			
 Quick Start ▼ Configuration ▷ LAN ▷ WAN 	This page allows you to backup the configuration settings to your computer, or restore configuration from your computer.			
VAN V System Time Zone	Backup Configuration			
Remote Access Firmware Upgrade	Backup configuration to your computer.			
Backup/Restore Restart Router User Management	Backup			
Firewall VPN Virtual Server	Restore Configuration			
Advanced	Restore configuration from a previously saved file.			
Save Config to FLASH	Configuration File Browse.			
O Logout	"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.			
Language English 💌	Restore			

3.6.3.3.5 Restart Router

When you click **Restart Router**, you have two functions. One is to restart it with current settings and the other is to restart it with factory default settings if you check **Reset to**
factory default settings.



3.6.3.3.6 User Management

When you click **User Management**, you are able to edit existing user's database or to create other user accessing this device.

	Status				<u>Us</u>	er Management
● ▼	Quick Start Configuration	Curren	tly Defii	ned Users		
		Valid	User	Comment		
	V System Time Zone	true	admin	Default admin user	Edit 🕥	
0	Remote Access Firmware Upgrade Backup/Restore Restart Router User Management ► Firewall ► VPN ● Virtual Server ► Advanced Save Config to FLASH	Create.	0			
•	Language English					

3.6.3.4 Firewall

This product also serves as an Internet firewall, not only does it provide a natural firewall function (Network Address Translation, NAT), but it also provides rich firewall features to secure a user's network. Besides, it can also be configured to block internal

users from accessing the Internet. The functions include:

- 1. Firewall: prevent access from an outside network, the router provides three levels of security support.
 - I NAT natural firewall: it masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when NAT function is enabled.
 - I Firewall Security and Policy (General Settings): inbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing the local network.
 - I Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.
- 2. Access Control: prevent access from a local network.
 - I Firewall Security and Policy (General Settings): outbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing the Internet.
 - I MAC Filter rules: to prevent unauthorized computers accessing the Internet
 - I URL Filter: to block the unwanted websites from accessing inappropriate material from the local network.

To prevent unauthorized computers access to the Internet and local network, you can either choose not to enable Firewall, add the MAC address and URL filter rules by yourself, or enable the Firewall and modify the packet filter rules if required. The Packet Filter is categorized as Port Filters and Address Filters, configured to filter the packets based-on Applications (Port) and IP addresses of the computers respectively.

There are five items under the Firewall section: General Settings, Packet Filter, Intrusion Detection, MAC Address Filter and URL Filter.

3.6.3.4.1 General Settings

When you click **General Settings**, you get the following figure.



Firewall Security: When you enable the Firewall security function, you can select one of the firewall security policies. By default the firewall is set to disabled.

Firewall Policy: Select either All blocked/User-defined, High, Medium or Low security level to enable the Firewall. The different among these three security levels is the presetting of port filter rules in the Packet Filter.

All blocked/User-defined: no pre-defined port or address filter rule by default, it means all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to the Internet.

High, Medium and Low security level: By default, your system uses High, Medium and Low firewall security levels between the WAN and LAN. For example, when you select High, the Port Filters of the Packet Filter screen will be set automatically according to High security level settings.

Firewall Logging: When both the Firewall Security and Firewall Logging are enabled, the device will detect the blocked and/or intrusion packets, once the setting has been configured. Then the router will log the corresponding (blocking or intrusion detection) logs into the Event Log under Status.

Select the **Apply** button to save the setting.

Please note that the enabling of Firewall Security & selection of Firewall policy is belong to the second level of Firewall as described above, it blocks and redirects certain ports to limit the services that outside users can access with Port and Address Filter features. Please refer to **Intrusion Detection** section for security level 3 protection - to prevent your local area network (LAN) from malicious attacks, for example, port scan and Denial-of-Service (DoS).

3.6.3.4.2 Packet Filter

When you click **Packet Filter**, you get the following figure.

I		Status			<u>P</u>	acket Filter			
(0	Quick Start	-	<u> </u>		Nete			
1	V	Configuration	Type	Conf	iguration	Note			
		IDE LAN IDE WAN IDE System IVE Firewall	external < > internal	Port Filters O	Address Filters O	 By default, all protocol types and TCP/UDP ports are blocked. Only the listed IP addresses are blocked 			
		General Settings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN VItual Server Advanced							
(0	Save Config to FLASH							
(0	Logout							
		Language English 🔽							

You may configure to filter inbound (incoming) and outbound (outgoing) packets based on port or IP address.

If it is based on port, click Port Filters for more options. You may filter the packets based on PORT and packet type (TCP or UDP or any). For example, the protocol number 1 means ICMP. You may enter 1 to protocol number of Raw IP Filtering web page. Port ranges are supported.

If it is based on IP address, click Address Filters for more options. You may enter the IP address and again to select the inbound or outbound packets.

For example, to allow TCP packet, port 0 to 1000 passing router between WAN and LAN and blocks host IP address, 192.168.1.100. Then you have to configure the port filter \dot{a} add TCP filter > 0 to 1000 and ALLOW in both direction. Then click address filter \dot{a} add address filter \dot{a} enter host IP 192.168.1.100, subnet mask 255.255.255.255 (for this single host) and both direction.

3.6.3.4.2.1 Port Filters

The pre-defined port filter rules for high, medium and low security level are listed below. When user enables Firewall Security feature for high, medium or low security level, the Block WAN Request function (Ping packet) is enabled automatically.

Application	Protocol	Port Num	rt Number Firewall - I		ligh	Firewall - Medium		Firewall - Low	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	YES	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	YES	YES
FTP(21)	TCP(6)	21	21	NO	NO	NO	YES	NO	YES
Telnet(23)	TCP(6)	23	23	NO	NO	NO	YES	NO	YES
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES

NE\//S(110)		110	110	NO	NO	NO	VES	NO	VES
		119	119	NO	NO	NO	IES	NO	IES
RealAudio	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
(7070)	. ,								
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	NO	NO	NO	YES	YES	YES
T.120(1503)	TCP(6)	1503	1503	NO	NO	NO	YES	YES	YES
SSH(22)	TCP(6)	22	22	NO	NO	NO	YES	YES	YES
NTP(123)	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTPS(443)	TCP(6)	443	443	NO	NO	NO	YES	NO	YES
ICQ (5190)	TCP(6)	5190	5190	NO	NO	NO	NO	YES	YES

Note: Inbound: Internet to LAN, Outbound: LAN to Internet

3.6.3.4.2.2 Address Filters

There are no pre-defined address filter rules; you can add the filter rules to meet your requirements. There are two kinds of address filters, one is inbound, the other is outbound. The rules can be set to prevent unauthorized users (hosts or network) to access the Internet from LAN (outbound) and/or access LAN from the Internet (inbound).

3.6.3.4.2.3 Packet filter example

The following provides an example of configuring a web server in LAN when the firewall policy is set to High, Medium or Low security level.

The pre-defined port filter rule for HTTP is the same no matter if it is a high, medium or low security level. The default setting is allowed for outbound access, not allowed for inbound access. To setup a Web server located on the local network, when the firewall policy is set, you have to configure the Port Filters setting first.

When the firewall policy is set, the port filters screenshot is as below, the inbound HTTP access is not allowed.

 Þ	Status	····· H	TTP aj	plicat	ion	Filters			
٥	Quick Start							1	
V	Configuration		F ort F	liters					Not allowed for inbound
	Þ LAN Þ₩AN		Type	Start	End	Inbound	Outbound		(Internet to LAN) application
	⊳ System ⊽ Carroll	\sim	Б	80	80	false	eurt	Delete 👔	
_	Ganeral Settings		17	53	53	true	true	Delete 🕥	
	Intrusion Detection		Б	53	63	true	true	Delete 🔘	
URL Filter		Б	21	21	false	true	Delete 🐧		
	⊳ VPN ⊳ Advanced		Б	23	23	false	true	Delete 🐧	
0	Save Config to FLASH		6	25	25	false	true	Delete 🕥	
0	Logout		Б	110	110	false	true	Delete 📀	
	Longuage		Б	119	119	false	true	Delete 🕐	
	English 👻		17	7070	7070	true	true	Delete 🕐	
			1	NVΑ	N/A	false	true	Delete 🖸	
			Б	1720	1720	true	true	Delete 🕥	
			Б	1503	1503	true	true	Delete 🕥	
			6	22	22	true	true	Delete O	
			17	123	123	false	true	Delete 📀	
			6	443	443	false	true	Delete 📀	

1. Click Packet Filter, you will get the following figure.



Click Port Filters

2. Click Port Filters, the pre-defined port filter rules screen of low security level is shown as below.

⊳ Status						Port Filters	
Quick Start						<u> </u>	
Configuration	Port F						
Þ LAN Þ WAN	Туре	Start	End	Inbound	Outbound		
▶ System ▼ Circurrall	Б	80	8D	false	true	Delete 🔿 🕇	— Click Delete
General Settings	17	5 3	53	true	true	Delete 🕐	
Packet Filter Intrusion Detection	Б	53	53	true	true	Delete O	
URL Filter VRN Advanced	Б	21	21	false	true	Delete 🕥	
	Б	23	23	false	true	Delete	
Save Config to FLASH	6	25	25	false	true	Delete 💿	
Logout Language English 👻	6	110	110	false	true	Delete 🔘	
	Б	119	119	false	true	Delete 💿	
	17	7070	7070	true	true	Delete 🕐	
	1	N⁄A.	N/A	false	true	Delete 🖸	
	Б	1720	1720	true	true	Delete O	
	Б	1603	1503	true	true	Delete 🜑	
	6	22	22	true	true	Delete O	
	17	123	123	false	true	Delete 🕥	
	6	443	443	false	true	Delete O	
	 Status Quick Start Configuration LAN WAN System Firewall General Sattings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN Advanced Save Config to FLASH Logout Language English 	> Status Quick Start ? Configuration > LAN > WAN > System ♥ Firewall General Settings Packet Filter Intrusion Detection MAC Address Filter URL Filter ► VPN ► Advanced B Logout B English ● 11 5 6 17 1 6 17 10 5 6 17 1 5 6 17 1 5 6 6 6 6 6 6 6 6 6 7 8	 Status Quick Start Configuration LAN WAN System Firewall General Sattings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN Advanced Save Config to FLASH Language English ▼ Information Information	 Status Quick Start Configuration LAN WAN System Firewall General Sattings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN Advanced Save Config to FLASH Language English ▼ Information Information	 Status Quick Start Configuration LAN WAN System Firewall General Sattings Packet Filter URL Filter VPN Advanced Save Config to FLASH Logout Language English ▼ I10 <li< th=""><th> Status Quick Start Configuration LAN WAN System Firewall General Sattings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN Advanced Save Config to FLASH Language English Image State Struct Image Struct Imag</th><th> Status Ouick Start Configuration VAN WAN System Firewall General Sattings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN Advanced Sorve Config to FLASH Language English ♥ Intrusion Detection IA IA</th></li<>	 Status Quick Start Configuration LAN WAN System Firewall General Sattings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN Advanced Save Config to FLASH Language English Image State Struct Image Struct Imag	 Status Ouick Start Configuration VAN WAN System Firewall General Sattings Packet Filter Intrusion Detection MAC Address Filter URL Filter VPN Advanced Sorve Config to FLASH Language English ♥ Intrusion Detection IA IA

- 3. Click Delete to delete the HTTP rule.
- 4. Click Add TCP Filter.

	Status	Б	53	53	true	frue	Delete D
0	Quick Start	6	21	21	false	true	Delete 🕥
V	Configuration	6	23	23	false	true	Delete 👔
	▷ LAN ▷ WAN	6	25	25	false	1rue	Delete 👔
	t> System ⊽ Firewall	6	110	110	false	true	Delete 🕥
_	General Settings Packet Filter	Б	119	119	false	true	Delete 🕥
	Intrusion Detection MAC Address Filter	17	7070	7070	true	frue	Delete 🕥
	URL Filter	1	N⁄A	N/A	false	true	Delete 🕥
	▷ Advanced	Б	1720	1720	true	1rue	Delete 🕥
•	Save Config to FLASH	Б	1503	1503	true	1rue	Delete 🕥
0	Logout	Б	22	22	true	1rue	Delete 🕦
	Language	17	123	123	false	1rue	Delete 🕥
	English 💙	Б	443	443	false	1rue	Delete 🕦
		Add T(Add U Add R Return	CP Filte DP Filte awr IP F	er 🖸 1 91 🛈 ilter (0	— Click Ad	ld TCP Filter

5. Input the port number and set the inbound & outbound as Allow.



6. The port filter rule of HTTP is shown as below.

In Statur	l.	21	21	ыве	1 08	Delete	
 Quick Start 	6	23	23	false	true	Delete ()	
∇ Configuration	б	25	25	false	true	Delete 🕥	
ID> LAN ID> WAN	6	110	110	false	true	Delete 🕥	
I≫ System ▼ Firewali	6	119	119	false	true	Delete 🕥	
General Settings	17	7070	7070	true	true	Delete 🕥	
Intrusian Detection	1	N/A	N/A	false	true	Delete ()	
URL Filter	6	1720	1720	true	true	Delete	
D> VPN D> Advanced	6	1503	1903	true	true	Delete	
Save Config to FLASH	6	22	22	true	true	Delete	
D Logout	17	123	123	false	true	Delete 0	
Lanauaga	Б	443	443	false	true	Delete 🛆	
English 👻	6	En	90	true	true	Delete A	
	<u> </u>	<u> </u>	00	1100	1.00	Delete	
	Add T(CP Filte	r O				
	Add U	DP Filt	ər O			HTTP inbound &	outbound application
	Add R	aw IP F	ilter	0			
	Return	0					

7. Configure the Virtual Server to enable the HTTP service in the virtual server setting and input the WEB server's IP address. If you try to setup a remote management of router permanently, you may enter router's IP instead.

All Cool Act Act	Virtual	Server
------------------	---------	--------

Enable	Application	Protocol	Port	IP Address
	FTP	TCP	21	192.168.2.
	Telnet	TCP	23	192.168.2.
	SMTP	TCP	25	192.168.2.
	нттр	TCP	80	192.168.2.
	POP3	TCP	110	192.168.2.
	NNTP	TCP	119	192.168.2.
	NTP	UDP	123	192.168.2.
	HTTPS	TCP	443	192.168.2.
	IKE	UDP	500	192.168.2.
	T.120	TCP	1503	192.168.2.
	H.323	TCP	1720	192.168.2.

3.6.3.4.3 Intrusion Detection

The Intrusion Detection allows you to prevent your local area network (LAN) from malicious attacks, for example, port scan and Denial-of-Service (DoS). The purpose of such attacks is either to consume the computing resources of your router, or even to bring down the router and network.

The Intrusion Detection also supports the blacklisting feature to minimize system overhead that could be consumed in an attack, as well as protecting the network in the meantime. The blacklist is empty initially when the firewall enabled. The initiator of an attack will be blacklisted, that is, will be added to the blacklist. Whenever the router receives a packet from the Internet, it will check the blacklist first to see if the initiator is in the list. If it is, the packet will be dropped. A configurable value is associated with each type of the attack, the initiator will be removed from the list when it times out.

I		Status	<u>In</u>	trusior	n Detection
I	0	Quick Start			
I	▼	Configuration	Enable	true 💌	
I		► LAN ► WAN	Use Blacklist	true 💌	
I		▶ System	Use Victim Protection	true 💌	
I		V Firewall General Settings	Victim Protection Block Duration	600	seconds
I		Packet Filter Intrusion Detection	DOS Attack Block Duration	1800	seconds
I		MAC Address Filter	Scan Attack Block Duration	86400	seconds
I		 VPN Virtual Server Advanced 	Maximum TCP Open Handshaking Count	t 100	per second
			Maximum Ping Count	15	per second
I	0	Save Config to FLASH	Maximum ICMP Count	100	per second
I	0	Logout			
I			Apply		
		Language English	Clear Blacklist		

Enable: select True to enable intrusion detection. Strongly recommend to set TRUE for "Use Blacklist" and "Use Victim Protection" when enable "Intrusion Detection".

Use Blacklist: select True to use blacklist. If enabled, external host addresses will be saved into blacklist when the router detects the intrusion from these hosts.

Use Victim Protection: select True to use Victim Protection. If enabled, the router will protect the internal host (the host is the victim at this moment) from suspicious attacks.

Victim Protection Duration: after the router has detected that an internal host has been attacked, the router will record this external host IP into the Blacklist and block traffic with this host for a set time limit in order to protect the host.

DoS Attack Block Duration: after a DoS attack is detected, the router will record this external host IP into the Blacklist and block traffic with this host for a set time limit.

Scan Attack Block Duration: after a Scan attack is detected, the router will record this external host IP into the Blacklist and block traffic with this host for a set time limit.

Maximum TCP Open Handshaking Count: set the maximum number of unfinished TCP handshaking session per second. Once the maximum of unfinished TCP

handshaking session per second is reached, the router will consider the SYN flood attack occurs.

Maximum Ping Count: set the maximum number of PING packets per second. Once the maximum number of PING per second is reached, the router will assume that an Echo storm attack has occurred

Maximum ICMP Count: set the maximum number of ICMP packet per second. Once the maximum number of ICMP packet per second is reached, the router will consider that an ICMP flood attack has occurred

Some pictures are shown below which show the router attacked by others.

1. Attacked by other with TCP packet/Port 1052 from source IP: 64.152.73.206.

▼	Status ARP Table	Event Log
	PTP Status IPSec Status Email Status Event Log	Existing Session Somebody want to communicate with Router
	 Error Log UPnP Portmap 	Sep 18 20:31:30 home.gateway:firewall:info: Blocked Prot=6, 64.152.73.206:80 - 64.230.176.206:1052, AF Seq=-777651151, Ack=-490416013 -No Existing Session
0	Quick Start	
	Configuration	Sep 18 20:31:30 nome.gateway:firewall:info: Blocked Prot=1/8/0, 61.230.213.27 > 61.230.176.206 -Port Filter Defense
0	Save Config to FLASH	
0	Logout	Sep 18 20:31:31 home.gateway:firewall:info: Blocked Prot=6, 64.152.73.206:80 > 61.230.176.206:1052, AF Seq=-777651151, Ack=-490416013 -No Existing Session
	Language English <mark>▼</mark>	Sep 18 20:31:33 home.gateway:firewall:info: Blocked Prot=6, 64.152.73.206:80 > 61.230.176.206:1052, AF Seq=-777651151, Ack=-490416013 -No Existing Session
		Sep 18 20:31:37 home.gateway:firewall:info: Blocked Prot=6, 64.152.73.206:80 > 61.230.176.206:1052, AF Seq=-777651151, Ack=-490416013 -No Existing Session
		Refresh Clear

2. Attacked by ICMP PING request.



3. Attacked by NetBIOS_NAME_SERVICE_PORT packet from other source IP :

200.68.76.177 to port 137 (a netbios_ns port).

▼ Status ARP Table	Event Log
PPTP Status IPSec Status	61.230.176.206 -Port Filter Defense NetBIOS_NAME_SERVICE_PORT
Email Status Event Log Error Log	Sep 18 20:36:07 home.gateway:firewall:info: Blocked Prot=17, 200.68.76.177:1026 > 61.230.176.206:[137] -Default Defense
 UPnP Portmap Quick Start 	Sep 18 20:36:35 home.gateway:firewall:info: Blocked Prot=1/8/0, 61.231, 202.46 >
Configuration	Sep 18: 20:36:43 home gateway: firewall: info: Blocked Prot=17, 81, 74, 46, 100:21800
 Save Config to FLASH Logout 	> 61.230.176.206:137 -Default Defense
Language	Sep 18 20:37:10 home.gateway:firewall:info: Blocked Prot=1/8/0, 212.158.195.52 > 61.230.176.206 -Port Filter Defense
English 💌	Sep 18 20:37:10 home.gateway:firewall:info: Blocked Prot=1/8/0, 61.231.17.113 > 61.230.176.206 -Port Filter Defense
	Sen 18 20:37:30 home oateway:firewall:info: Blocked Prot=1/8/0_61_231_156_215 > 🗾
	Refresh Clear

3.6.3.4.4 MAC Address Filter

When you click the MAC Address Filter, you get the following figure.

	Status	MAC Address Filter
0	Quick Start	
▼	Configuration LAN	○ Enable Isable
	► Svstem	For LAN inbound ethernet frames.
	▼ Firewall General Settings	only the following Source MAC Address(es) are O Allowed 💿 Blocked
	Packet Filter	MAC Address
	MAC Address Filter	00:00:00:00:00
	 VPN Virtual Server 	
	► Advanced	
0	Save Config to FLASH	
0	Logout	
	Language English 💟	Apply

The MAC filtering function enables you to configure your router to block internal users (**MAC address**) from Internet access.

Enable/Disable: to enable or disable MAC Address Filter feature.

Allowed/Blocked: To allow or block the following MAC addresses to surf outside network only. If you check Allowed, please be sure your PC's MAC address is listed. If you check Blocked, please be sure your PC's MAC address is not listed.

MAC Address: There are 10 entries to enter the MAC addresses you want manage. If you select **Blocked**, the packet with the MAC address in the table will be dropped and others will be forwarded. If you select **Allowed**, the packet with the MAC address in the table will be forwarded and others will be dropped. Then select the **Apply** button to save the setting.

3.6.3.4.5 URL Filter

When you click the URL Filter, you get the following figure. There are no pre-defined URL filter rules; you can add the filter rules to meet your requirement.

	Status	URL Filter
0	Quick Start	
▼	Configuration LAN WAN System Firewall General Settings Packet Filter Inturing Detection	 Enable Always Block Block from 00 : 00 : 00 : 00 : 00 : 00 : 00 : 00
0	Intrusion Detection MAC Address Filter URL Filter ► VPN ● Virtual Server ► Advanced Save Config to FLASH Logout	 Keywords Filtering Details • Domains Filtering Details • Disable all WEB traffic except for Trusted Domains Enable Blocking Log
	Language English 💌	Apply Cancel

The URL filtering function enables you to block unwanted websites from accessing inappropriate material from the entire enterprise.

Enable / Disable: Check **Enable / Disable** radio button to activate or deactivate the URL filter function.

Always Block: Check this button, if you wish not to access this website through out the entire time. Or choose,

Block from: Check this button, if you only wish to block a URL in a specific time interval. For example, if you wish to temporarily block a URL from Monday 8:00am until Wednesday night at 7:40pm, in the space provided above, you should select **08:00**, **Monday** to **19:40**, **Wednesday**.

Keyword Filtering: Check if you want to enable the Keyword Filtering function and click **Details** button for further configuration options. Please refer below for more information.

Domain Filtering: Check if you want to enable the Domain Filtering function and click **Detail** button for further configuration options. Please refer below for more information.

Disable All WEB traffic except for Trusted Domain: It allows internal users to access only the specified/trusted domain. Please refer to the Domain Filtering section first, before checking this option.

Enable Blocking Log: Check this button to log the corresponding logs into the Event Log under Status.

Select the Apply button to save the setting.

3.5.3.4.5.1 Keyword Filtering

Status	URL Filter - Keywords Filtering		
Quick Start			
▼ Configuration	Keyword:		
⊳ WAN			
⊳ System	Арріу		
General Settings			
Packet Filter			
Intrusion Detection			
MAC Address Filter			
• Virtual Server			
► Advanced			
Save Config to FLASH			
Logout			
1			
Language			
English M			

The ADSL Router allows the administrator to block some WEB URLs containing certain keywords in this page. For example, if the keyword "xxx" is listed, the URL <u>http://www.new.site.com/xxx.html</u> would be blocked, even if it is not included in the domain filtering list. Keywords presented as site name are also blocked; that is, <u>http://www.xxxsite.com</u> can not be accessed from the LAN.

To add a keyword, enter it in the **Keyword** field and click **Apply**.

3.5.3.4.5.2 Domain Filtering:

▶ Status	URL Filter - Domains Filtering
 Quick Start ✓ Configuration ▷ LAN ▷ WAN ▷ System ▼ Eisenell 	Trusted Domain:
General Settings Packet Filter Intrusion Detection MAC Address Filter URL Filter ▶ VPN ♥ Virtual Server ▶ Advanced	Forbidden Domain: Name Domain Create O
Save Config to FLASH	Return O
Constant	

If the router is configured to allow internal users to access only certain specified domains, check add the domain name into the **Trusted Domain** list. If the router is configured to allow internal users to access all websites except for some forbidden domains, add the forbidden domain name into the **Forbidden Domain** list. These Forbidden Domains will be blocked, and users will no longer be able to access the websites from the LAN.

The checking procedure is like these steps.

- 1. Check the domain in the URL's string if it is in the trusted list. If yes, send it to outside world.
- 2. If not, check if it is listed in the forbidden list or the function, disable all WEB traffic except Trusted Domains, is checked, then drop this packet.
- 3. If the packet is not matched with above two items, the send it to outside world.

To add a domain name, enter its host name, such as <u>www.bad-site.com</u> into the text field under **Domain** and select either **Trusted Domain** or **Forbidden Domain**, then click **Apply**. The specified domain will be shown in the **Domain List**. DO NOT include <u>http://</u>, ONLY the sub-domain is allowed. For instance, taking "yahoo.com" as the trusted domain means that <u>www.yahoo.com</u>, <u>my.yahoo.com</u>, and <u>sports.yahoo.com</u> will also be trusted.

To remove a site that was previously added, select its name in the list box, and click the **Delete** button to eliminate it from the list.

3.6.3.5 VPN

The router supports VPN to establish secure, end-to-end private network connections over a public networking infrastructure. There are two types of VPN connections, the remote access and LAN-to-LAN VPN. Deploying a remote access VPN enables users to reduce the cost by leveraging the local dial-up infrastructures of the ISP, in addition,

transmitting data over a secure VPN tunnel. LAN-to-LAN VPN is an alternative WAN infrastructure that is used to connect offices and home offices to share network resources with each other over a secure VPN tunnel.

This router supports two kinds of VPN standards, Point-to-Point Tunneling Protocol (PPTP) and Internet Security Protocol (IPSec).

3.6.3.5.1 PPTP

There are two applications provided in PPTP, **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to select one of applications to continually setup.



3.6.3.5.1.1 PPTP for Remote Access

For the Remote Access Application, please refer to the figure below.

⊳	Status	PPTP Remote Access Connection		
0	Quick Start			
$\overline{\mathbf{v}}$	Configuration	Connection Name:		
	⊳ LAÑ ⊳ WAN	Type: Type: Dial out, Server IP Address (or Hostname):		
	⊳ System	O Dial in, Private IP Address Assigned to Dialin User:		
	► Firewall VPN	Username:		
	PPTP IPSec	Password:		
	 Virtual Server Advanced 	Auth. Type: Chap(Auto)		
0	Save Config to FLASH	Data Encryption: Auto 🗸 Key Length: Auto 🖌 Mode: stateful 💌		
0	Logout	Idle time: 0 minutes		
	Language English ▼	Apply		

Connection Name: Give a name for this connection.

Type: Check **Dial Out** to be a client, check **Dial In** to be a server. When this network router acts as a client, please input the remote **Server IP Address (or Hostname)** to establish a connection. When this network router acts as a server, please input the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is Auto.

Data Encryption: The data can be encrypted by MPPE algorithm. Default is **Auto**, it is negotiated when establishing a connection.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed in each 256 packets when you select Stateful mode. If you select Stateless mode, the key will not be changed in each packet.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. 0 means this connection is always on.

Click **Apply** after setting.

3.6.3.5.1.2 PPTP for LAN to LAN

For the LAN to LAN application, please refer to the figure below.

	Status	PPTP LAN TO LAN
• ⊽	Quick Start Configuration	Connection Name:
	▶ LAŇ ▶ WAN ▶ Svstem	Type: O Dial out, Server IP Address (or Hostname): O Dial in. Private IP Address Assigned to Dialin User:
	► Firewall VPN	Peer Network IP: Netmask:
	IPSec Virtual Server	Username: Password:
0	Advanced Save Config to FLASH	Auth. Type: Chap(Auto)
0	Logout	Idle time: 0 minutes
	Language English ▼	Apply

Connection Name: Give a name for this connection.

Type: Check **Dial Out** to be a client, check **Dial In** to be a server. When this network router acts as a client, please input the remote **Server IP Address (or Hostname)** to establish a connection. When this network router acts as a server, please input the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on above Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is Auto.

Data Encryption: The data can be encrypted by MPPE algorithm. Default is **Auto**, it is negotiated when establishing a connection.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establish a connection.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed in each 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the ADSL router when there is no activity on the line for a predetermined period of time. 0 means this connection is always on.

Click **Apply** after setting.

3.6.3.5.1.3 An Example of Configuring a Remote Access PPTP VPN Dial-in Connection

Background of the Example

A remote worker establishes a PPTP VPN connection with the head office using Microsoft's VPN Adapter, a piece of software included with Windows 2000/ME, etc. The router is installed in the head office, connected to a couple of PCs and Servers.

Application Diagram



Configuring PPTP VPN in the Office

The input IP address 192.168.1.200 will be assigned to the remote worker, please make sure this IP is not used in the Office LAN.



Configuring PPTP VPN in Remote Side

You can configure VPN client with commercial VPN client software package (e.g. SSH) or the Dial-up Adaptor in Windows. Please follow the steps below if you are a Windows 2000 user.

1. Click Network and Dial-up Connection and Make new connection

PLANET ADSL VPN / Firewall Router

🔊 Network and Dial-un Connections	- ALX
File Edit View Favorites Tools Advanced Help	
← Back - → - 🖬 @ Search P Folders ③History P S 🗙 🖄 🏢 -	
Address P Network and Dial-up Connections	▼ (∂G0
Address will hetwork and Dial-up Connections Petwork and Dial- up Connections Make New Connection wized hetwork Connection wized hetwork Connection wized hetworks. New Connection Create Shortcut	₹ (<i>α</i> ′ 60
Creates a new connection.	
🏦 Start 🛛 🔏 🗂 🖗 Network and Dial-up C.,.	🌾 🕮 10:02 AM

2. Follow the step and select "Connect to a private network through the Internet"

Network Connection Wizard			
Network Connection Type You can choose the type of network connection you want to create, based on your network configuration and your networking needs.			
Dial-up to private network Connect using my phone line (modem or ISDN).			
O Dial-up to the Internet Connect to the Internet using my phone line (modem or ISDN).			
Connect to a private network through the Internet Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.			
Accept incoming connections Let other computers connect to mine by phone line, the Internet, or direct cable.			
 Connect directly to another computer Connect using my serial, parallel, or infrared port. 			
< Back Next > Cancel			

3. Enter the IP address of the ADSL Router located in the office

Network Connection Wizard	
Destination Address What is the name or address of the destination?	S)
Type the host name or IP address of the computer or n connecting.	etwork to which you are
Host name or IP address (such as microsoft.com or 123	3.45.6.78):
< Bac	k Next > Cancel

4. Follow the step, the following screen appears. The setup is completed.

Network Connection Wizard			
S	Completing the Network Connection Wizard		
	Type the name you want to use for this connection:		
	Virtual Private Connection		
	To create this connection and save it in the Network and Dial-up Connections folder, click Finish.		
	To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.		
	Add a shortcut to my desktop		
	< Back Finish Cancel		

5. To make the connection, click the Virtual Private Connection icon in Dial-up Networking Group, and input the username & password set in ADSL Router.

Connect Virtual Private Connection			
User name:	username		
Password:	*****		
	Save Password		
Connect	Cancel Properties	Help	

3.6.3.5.1.4 An Example of Configuring a Remote Access PPTP VPN Dial-out Connection

Background of the Example

Corporate establishes a PPTP VPN connection with the file server located in the remote side. The router is installed in the office, connected with a couple of PCs and Servers.

Application Diagram



Configuring PPTP VPN in the Office

You can either input the IP address (69.1.121.33 in this case) or hostname to reach the Server.

	⊳	Status	Check Dial out	PPTP R	emote Access Cor	nection
<	00	Quick Starl Configuration > LAN > WAH > System > Firowall > Firowall PPTP IPSec O Virtual Server > Advanced Save Config to FLASH Legout Language English Y	Check Dial out Connection Name: Typs: Username: Password: Auth. Type: Data Encryption: Idle time: Apply	VPN-PPTPD Dial out, Server IP Dial in, Private I username e>eeeeee Chap(Auto) V Auto V D rninutes	Address (or Hostname): P Address Assigned to Dialin User. Key Length: Auto 💽	Dialect sever IP

Refer also to **PPTP VPN – remote access (dial-in)** for the other parameters.

PPTP Status

v	ARP Table	VPN/PPTP for Remote Access Application							
	IPSec Status Email Status	Name	Туре	Enable	Active	Session Connected	Cell Cennected	Encryption	
	Event Log	VPN_PPTP0	dialout	t 🖌	1	 ✓ 	×	encryption enabled mpps 128bits stateful mode	
•	Quick Start	VPNVPPTP for LAN-to-LAN Application							
Þ	Configuration	Name	Туре	Enable	Active	Session Connected	Call Connected	Encryption	
0	Logout	VPN_PPTP1	dialin	~	~	 	Confidence	encryption enabled mppe 128bits stateful mode	
	Language English 💌								

3.6.3.5.1.5 An Example of Configuring a LAN-to-LAN PPTP VPN Connection

Background of the Example

The branch office establishes a PPTP VPN tunnel with the head office to connect two private networks by leveraging the Internet infrastructure. The routers are installed in the head office and branch office accordingly.

Application Diagram



Configuring PPTP VPN in the Head Office

The input IP address 192.168.1.201 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Configuring PPTP VPN in the Branch Office

The input IP address 69.1.121.3 is the **Public IP** address of the router located in the head office. If you have a domain name assigned to this IP address - either you registered the DDNS (please refer to the **DDNS** section), or you have a static IP with a domain name, you can also use the Hostname instead of the IP address to reach the router.

Þ	> Status	Check Dial out		PPTP L	AN TO LAN	<u>N</u>	
V) Quick Start 7 Configuration ▷ LAN ▷ WAN ▷ System	Confrection Name Турв: 📀	VPN_PPTP1 Dialout, S Dialin, F	isrver IP Address (or Private IP Address A:	Hea Hostname): asigned to Dialin User:	69.1.121.3	r IP (WAII side)
<	PFIrewall PPTP IPSec O Virtual Server	Peer Network IP: Usemama: Passward:	192.168.1.0 Username	Hea	Nelmask:	256.255.255.0	
0	 ► Advanced Save Config to FLASI Logout 	H Auth. Type: Data Encryption: Idle time:	Chap(Auto) Auto	Key Length:	Auto 💌	Made: stateful	¥
	Language English 🛩	Apply					

Refer also to **Configuring PPTP VPN in the Head Office** for other parameters.

PPTP Status in the Head Office

Status ARP Table DHCP Table DOTE Status								
IPSec Status Email Status	Name	Туре	Enable	Active	Session Connected	Call Connected	Encryption	
Event Log Error Log	VPN_PPTP0	dialout	 Image: A second s	 Image: A start of the start of	 ✓ 	 ✓ 	encryption enabled mppe 128bits stateful mode	
o Quick Start	PN/PPTP for LAN-to-LAN Application							
 Configuration Save Config to FLASH 	Name	Турс	Enable	Active	Session Connected	Call Connected	Encryption	
o Logout	VPN_PPTP1	dialin	1	1	1	1	encryption enabled mppe 128bits stateful mode	
Language English 💌								

3.6.3.5.2 IPSec

The router supports IPSec VPN to establish secure, end-to-end private network connections over a public networking infrastructure. The specification is as below:

- w . Encapsulation: tunnel mode
- w . Support IKE authentication method: pre-shared key
- w . Security protocol: ESP and AH
- w . Authentication: MD5, SHA-1
- w . Encryption: DES, 3DES, AES
- w . Support PFS

3.6.3.5.2.1 IPSec configuration

When you click the IPSec, you get the following figure.



Click Create...

 ▶ Status Quick Start ▼ Configuration ▶ LAN 	Connection Name:	IPSec	
 ► WAN ► System ► Firewall ▼ VPN ₽PTP IPSec 	NetWork: © Single Addr O Subnet © IP Range	ress IP Address: IP Address: IP Address:	Netmask: End IP:
 O Virtual Server ► Advanced Save Config to FLASH Logout 	Secure Gateway Address(or Hostn NetWork: © Single Addr © Subnet O IR Reserve	ame); ress IP Address; IP Address; IP Address;	Netmask:
Language English ▼	Proposal ⓒ ESP Authentication: None ▼ Encryption: NULL ▼	C AH Authentication: MD5 💌	
	Prefect Forward Secrecy: Pre-shared Key: Apply	None 💌	
	Apply Advanced Options		

Connection Name: Give a name for this connection.

Local Network: Set the IP address, subnet or address range of the local network.

¤ Single Address: The IP address of the local host.

x Subnet: The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1.
 x IP Range: The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Remote Secure Gateway Address (or hostname): The IP address or hostname of remote VPN device that is connected and establishes a VPN tunnel.

Remote Network: Set the IP address, subnet or address range of the remote network.

Proposal: Select the IPSec security method. There are two methods to check the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Check ESP for a higher security, data will be encrypted and authenticated. Check AH, data will be authenticated but not encrypted.

Authentication: Authentication establishes the integrity of datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (MD5), Secure Hash Algorithm (SHA-1) or NONE. SHA-1 is more resistant to brute-force attacks than MD5, but it is slower.

MD5: A one way hashing algorithm that produces a 128-bit hash.

¤ SHA-1: A one way hashing algorithm that produces a 160-bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, DES, 3DES, AES and NONE. The NONE means it is a tunnel only, no encryption. 3DES and AES are more powerful but increases latency.

¤ DES: Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

¤ 3DES: Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

AES: Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman publickey cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel. There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit, MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

	Status	IPSe	ec_
• ⊽	Quick Start Configuration ▶ LAN ▶ WAN ▶ System ▶ Firewall	SA Lifetime: Phase 1(IKE): Phase 2(IPSec):	
	▼ VPN PPTP IPSec ● Virtual Server ► Advanced	ChangeReset	
0	Save Config to FLASH		
J	Language English		

Click Advanced Option to get the following figure.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

Phase 1 (IKE): To issue an initial connection request for a new VPN tunnel. Default 240 minutes, range from 5 to 15,000 minutes.

Phase 2 (IPSec): To negotiate and establish secure authentication. Default 60 minutes, range from 5 to 15,000 minutes.

A short SA time increases the security by forcing two parties to update the keys. However, every time the VPN tunnel re-negotiates, the access through tunnel will be temporarily disconnected.

3.6.3.5.2.2 An Example of Configuring a LAN-to-LAN IPSec VPN Connection

Background of the Example

The branch office establishes an IPSec VPN tunnel with the head office to connect two private networks by leveraging the Internet infrastructure. The routers are installed in the head office and branch office accordingly.

Application Diagram



Network Configuration and Security Plan

We want to setup a security channel between branch office and head office using LANto-LAN tunnel-mode connection. ESP, with MD5 as the authentication protocol and AES as the encryption protocol is decided as the policy of security plan. Pre-shared key is defined as 8 characters, 12345678.

	Branch Office	Head Office
Local Network ID	192.168.0.0/24	192.168.1.0/24
Local Router IP	69.1.121.30	69.1.121.3
Remote Network ID	192.168.1.0/24	192.168.0.0/24
Remote Router IP	69.1.121.3	69.1.121.30
IKE Pre-shared Key	12345678	12345678
VPN Connection Type	Tunnel mode	Tunnel mode
Security Algorithm	ESP:MD5 with AES	ESP:MD5 with AES

Configuring IPSec VPN in the Head Office

The local subnet (head office) is set as 192.168.1.0/24 (with netmask 255.255.255.0), while the remote subnet (branch office) is set as 192.168.0.0 (with netmask 255.255.255.0). The IP address 69.1.121.30 in "Secure Gateway Address" field is the **Public IP** address of the router located in the branch office. If you have a domain name assigned to this IP address - either you registered the DDNS (please refer to the **DDNS** section), or you have a static IP with a domain name, you can also use the Hostname instead of the IP address to reach the router. Set "Proposal" as ESP: MD5/AES, PFS as None and pre-shared key as as12345678 according the pre-defined security plan.



Configuring IPSec VPN in the Branch Office

The local subnet (branch office) is set as 192.168.0.0/24 (with netmask 255.255.255.0), while the remote subnet (head office) is set as 192.168.1.0 (with netmask 255.255.255.0). The IP address 69.1.121.3 in "Secure Gateway Address" field is the **Public IP** address of the router located in the head office. If you have a domain name assigned to this IP address - either you registered the DDNS (please refer to the **DDNS** section), or you have a static IP with a domain name, you can also use the Hostname instead of the IP address to reach the router. Set "Proposal" as ESP: MD5/AES, PFS as None and pre-shared key as as12345678 according the pre-defined security plan.



3.6.3.6 Virtual Server

In TCP/IP and UDP networks, a port is a 16-bit number, used by the host-to-host protocol to identify to which application program it must deliver incoming messages. Some ports have numbers that are pre-assigned to them by the IANA, and these are known as well-known ports. Servers follow the well-know port assignments so clients can locate them.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65536, but only ports numbers 0 to 1024 are reserved for privileged services and designated as well-known ports. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are as below, for further information, please see IANA web, http://www.iana.org/assignments/port-numbers.

Port Number	Protocol	Description
1	ICMP	PING
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)

53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	ТСР	World Wide Web HTTP
110	ТСР	POP3 (Post Office Protocol Version 3)
119	ТСР	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	ТСР	SNMP
443	TCP & UDP	HTTPS
1503	ТСР	T.120
1720	ТСР	H.323
4000	ТСР	ICQ
7070	UDP	RealAudio

Being a natural Internet firewall, this network router protects your network from being accessed by outside users. When it needs to allow outside users to access internal servers, e.g. Web server, FTP server, E-mail server or News server, this modem can act as a virtual server. You can set up a local server with specific a port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the Service Port number 80 (Web) to be mapped to the IP Address 192.168.1.2, then all the http requests from outside users will be forwarded to the local server with IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

When you click Virtual Server, you get the following figure.

⊳	Status			Virt	ual Server	
0	Quick Start]
V	Configuration	Enable	Application	Protocol	Port	IP Address
	► LAN ► WAN		FTP	ТСР	21	192.168.1.
	 Firewall VPN 		Telnet	ТСР	23	192.168.1.
	 ● Virtual Server ▶ Advanced 		SMTP	TCP	25	192.168.1.
0	Save Config to FLASH		HTTP	TCP	80	192.168.1.
0	Logout		POP3	ТСР	110	192.168.1.
	Language		NNTP	ТСР	119	192.168.1.
	English 🔛		NTP	UDP	123	192.168.1.
			HTTPS	TCP	443	192.168.1.
			IKE	UDP	500	192.168.1.
			T.120	TCP	1503	192.168.1.

Enable: Enable or disable this Virtual Server port.

Application: Input the application name for the port you define. This product provides

several pre-defined popular application and their port number.

Protocol: Select the properly protocol for the application.

Port: Input the port number for the application.

IP Address: Input the IP address that you want to allow accessing from outside users.

DMZ: The DMZ Host is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by the Firewall and NAT algorithms, then passed to the DMZ host when a packet is not sent by a hacker and not limited by the virtual server list.



If you have disabled the NAT option in the WAN-ISP section, this Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easy way is that the IP address assigned to each virtual server should not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it is still in the same subnet with the router.

3.6.3.6.1 An Example of Configuring a Web Server on the Local Network

To save time to configure, this router has listed the well-known protocol and port number that stands for the most popular applications on the Virtual Server table, e.g. Web (TCP/80), FTP (TCP/21), Telnet (TCP/23), SMTP (TCP/25), POP3 (TCP/110), IKE (UDP/500), etc. This is an example to configure a Web server, just check Enable, and input the IP address of the Web server.

Background of the Example

Setup the Web server in the office that can be visible to the outside network.

Configuring a Virtual Server

- 1. Set Web server IP address to a fixed IP = 192.168.1.100
- 2. Configure the Virtual Server

Status	Enable	Application	Protocol	Port	IP Address
Quick Start		FTP	тср	21	192,168,1
Configuration LAN WAN		Telnet	тср	23	192.160.1
System Elrewall		SMTP	TCP	25	197 168.1.
O Virtual Server		нтр	тср	BD	192.168.1.100
Save Config to ELASH		POP3	TCP	110	192.160.1.
Logout		NNTP	TCP	119	192.168.1.
Lannuane		NTP	UDP	123	192.168.1.
English 👻		нтра	TCP	443	192.168.1.
		KE	VDP	500	192.168.1.
		T.120	тср	1503	192.168.1.
		H.323	TCP	1720	192.168.1.
		рртр	TCP	1723	192.168.1.
		SIP	TCP/UDP	5060	192.168.1.
		CUSsaMe	TCP	7648	197 168 1

3.6.3.6.2 An example of configuring the Web Server & the Router to be accessible remotely

Background of the Example

Setup the Web server in the office that can be visible to the outside network. In the meantime, set the router to be accessible remotely through HTTP. Since they use the same protocol (TCP), we have to change the port number of either application to make these two services available. Please note the access method to the Web server and router is different in case 1 & 2, this is particularly related to port number setting, refer below for details.

Example 1: Configuring a Virtual Server

- 1. Set Web server IP address to a fixed IP (this is the IP of the PC running your web server software, e.g. 192.168.1.100)
- Change the embedded web server's HTTP port to 8080 by select Configuration -> Advanced -> Device Management.
- 3. Configure the Virtual Server as the following.

Chec	k E nable				IP address of Web server
t> Status	1	101104			192.168.1.
O Quick Start		SMTP	TCP	25	192.168.1.
Configuration		нттр	TCP	80	192.168.1.100
⊳ WAN ⊳ System		POP3	TCP	110	192.168.1.
► Firewall ► VPN		NNTP	TCP	119	192.168.1.
O Virtual Server Advanced		NTP	UDP	123	192.168.1.
Save Config to FLASH Longuit		HTTPS	TCP	443	192.168.1.
C Lugun		IKE	UDP	500	192.168.1.
Language English 🔽		T.120	TCP	1503	192.168.1.
		H.323	TCP	1720	192.168.1.
		PPTP	TCP	1723	192.168.1.
		SIP	TCP/UDP	5060	192.168.1.
		CUSeeMe	TCP	7648	192.168.1.
		Router-web	1cp 💌	8080 ~ 8080	192.168.1.254
			1cp 💌		192.168.1.
Check Ena Gi (re	/ ble /en a name mote acces	of the application s to router by Http	Select TCP (Protocol of))	Specify a port n Http)	umber for this application

Example 2: Configuring a Virtual Server

- 1. Set Web server IP address to a fixed IP = 192.168.1.100
- 2. Set Remote Access as Enable. User can access the router remotely through port 80.

⊳ Status	Remote Access
 Quick Start ∇ Configuration > LAN 	From this page you may temporarily permit remote administration of this network device
l> WAN ⊽ System	Enable Remote Access
Remote Access	Allow access for: 🗵 🔪 minutes.
Backup/Restore Restart Router	Enable
User Management Firewall Stress	Access time period from remote site
O Virtual Server ▷> Advanced	Check Enable
Save Config to FLASH	
Logout	
Language English ❤	

3. Since the port number 80 is used by the router, the Web server port number needs to be changed.



3.6.3.7 Advanced

There are four items under the Advanced section: Routing Table, Dynamic DNS, Checking Email and Device Management.

3.6.3.7.1 Routing Table

Click on the **Routing Table** and then choose **Create Router** to get the below figure to add a routing table.

Status	Create Route
Quick Start	
Configuration ▶ LAN ▶ WAN	Netmask
 System Firewall VPN Virtual Server 	via Gateway or Interface
Advanced Routing Table Dynamic DNS	Cost 1
Check Emails Device Management	OK Cancel
Save Config to FLASH	
Logout	
Language English 🔽	
	Status Quick Start Configuration LAN WAN System Firewall VPN Virtual Server Advanced Routing Table Dynamic DNS Check Emails Device Management Save Config to FLASH Logout

Destination: Enter the destination subnet IP.

Netmask: Subnet mask of destination IP addresses based on above destination subnet IP.

Gateway: Enter the gateway IP address which the packet is forwarded to.
DNS

Interface: Enter the interface which the packet is forwarded to.

Cost: This is the same meaning as Hop. Usually, leave it as 1.

3.6.3.7.2 Dynamic DNS

Click **Dynamic DNS** to get the below figure then check the "Enable" button to access the Dynamic DNS service.

⊳	Status		Dynamic
0	Quick Start		
▼	Configuration ► LAN	🔘 Enable	⊙ Disable
	▷ WAN ▷ System	Dynamic DNS:	www.dyndns.org (dynamic) 🔽
	 Firewall VPN 	Domain Name: Username:	
	O Virtual Server ▼ Advanced Routing Table	Password:	
	Dynamic DNS Check Emails Device Management	Period:	28 Day(s) 🔽
0	Save Config to FLASH	Apply Cancel	
0	Logout		
	Language English 💟		

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from their Web server <u>http://www.dyndns.org/</u>. There are several DDNS servers supported. Please first browse the website to apply an account then configure the Dynamic DNS settings on this page.

Enable / Disable: Enable or disable the Dynamic DNS function.

Dynamic DNS: Select the registered DDNS server. You have to first browse their website to apply username and password.

Domain Name, Username and Password: Enter the registered domain name, username and password.

Period: Set the time period for the Router to exchange information with the DDNS server. In addition to update periodically according to this period setting, the Router will take the same action automatically whenever the assigned IP changes.

3.6.3.7.2.1 Example of Configuring DDNS

Background of the Example

Setup a Web server in the office that can be accessed via Domain Name instead of the dynamic IP address.

Configuring DDNS

- 1. Set the Web server and FTP server IP address as described in section **Virtual Server**.
- 2. Apply an account from this free Web server http://www.dyndns.org/. There are more than 5 DDNS services supported by this router.
- 3. Configure DDNS as the following.

> Status	Check Enable	Dynami	c DNS
□ Quick Start ▼ Configuration	ÖEnable (🖲 Disable	
D≻ LAN D> WAN D> System	Dynamic DNS:	www.dyndns.org (dynamic) 🐋	Select the registered DDNS server
> Firewall > VPN	Domain Name: Username:	domain-prefix.dyndns.org	Input the registered domain name
Advanced	Password:		password
Dynamic DNS Check Emails Save Config to FLASH	Period:	28 Day(s)	to exchange information with the
	via wavi interno	ipwan 💉	update with the DD IIS server whenever the router IP address
Lugun	Apply Canc	el	(WAII side) changes.
Language English 💌		Select the name of the WAII connection. This is applicable when you create two or more WAII connections.	

3.6.3.7.3 Checking Emails

Click **Checking Emails** to get the below figure then check the "Enable" button to access the service.



Disable: Check to disable the ADSL router from getting the email.

Enable: Check to enable the ADSL router to get the email by providing the required information. Hence, the following fields will be activated and required.

Account Name: Enter the name of the account to which you have the POP access. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the password of the account

POP3 Mail Server: Enter your (POP) mail server name. If you have trouble with it, you would want to contact your ISP or your external mail server's administrator. For further assistance in tracking down this information, you will need to contact your Internet Service Provider or Network Administrator.

Interval: Enter the value in minutes to check your email account periodically.

Automatically dial-out for checking emails: When the function is enabled, your ADSL router will connect to your ISP automatically to check emails if your Internet connection dropped. Please be careful when using this feature if your ADSL service is charged by time.

3.6.3.7.4 Device Management

Click **Device Management** to protect and obtain system control while allowing device monitoring. This in turn provides enhanced security of the device.

	Status		Device N	lanagement
0	Quick Start			
∇	Configuration ▶ LAN ▶ WAN ▶ System	Embedded Web Server		
		* HTTP Port:	80	(80 is default HTTP port)
		Management IP Address:	0.0.0.0	('0.0.0.0' means Any)
	► Firewall ► VPN ► Vistor LC	Expire to auto-logout:	180	seconds
	▼ Advanced			
	Routing Table Universal Plug and Play (UPnP)			
	Check Emails	💿 Enable 🛛 🔿 Disable		
	Device Management	* UPnP Port:	2800	
0	Save Config to FLASH			
0	Logout	SNMP Access Control		
		Read Community:	public	IP Address: 0.0.0.0
	Language English 💟	Write Community:	password	IP Address: 0.0.0.0
		Trap Community:		IP Address:
		* : This setting will become	me effective after y	ou save to flash and restart the router.

3.6.3.7.4.1 Embedded Web Server

HTTP Port: Default value for HTTP port is 80. A desired value is also allowed. Simply specify a user-defined port number.

Management IP Address: Specify an IP address allowed to logon and access the router's web server. Note: IP 0.0.0.0 indicates all users who are connected to this

router are allowed to logon the device and modify data.]

Expire to auto-logout: Specify a time frame for the system to auto-logout the device.

For Example: User A changes HTTP port number to **100**, specified it's own IP address to be **192.168.1.55**, and set the logout time to be **50** seconds. Device will only allow User A which IP address is **192.168.1.55** to logon to the Web GUI by typing: **192.168.1.254:100**. After 50 seconds, the device will automatically logout User A.

3.6.3.7.4.2 Universal Plug and Play (UPnP)

Disable: Check to disable UPnP function.

Enable: Check to enable UPnP function.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. You may wish to modify this port value, only if this value conflicts with other ports already being used.

3.6.3.7.4.3 SNMP Access Control

Read Community: Specify a name in any string to be identified as the Read Community and an optional IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user with this IP address will be able to view the data.

Write Community: Specify a name in any string to be identified as the Write Community and an optional IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user with this IP address will be able to view and modify the data.

Trap Community: Specify a name in any string to be identified as the Trap Community and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user with this IP address will be notified Traps.

Please note SNMP software is required in order to utilize this section.

3.6.4 Save Configuration to Flash

After configuring this network router, you have to save all of the configuration parameters to FLASH.



3.6.5 Logout

To exit the website, choose Logout to exit completely. Please ensure that you have saved the configuration settings before logout.

Be aware that the router is restricted to only one local PC accessing the configuration Web pages. Once a current PC has logged onto the Web pages, other PCs cannot get access except waiting for the current PC to log out of the page. If the previous PC forgets to logout, the second PC can access the page after 3 minutes.

Chapter 4. Troubleshooting

If the ADE-4200/ADW-4200 Wireless ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save you time and effort but if the symptoms persist, then consult your service provider.

Problems Starting Up the ADE-4200/ADW-4200

Problem	Corrective Action
None of the LEDs are on when you turn on the ADE-4200/ADW- 4200	Check the connection between the adapter and the ADE-4200/ADW-4200. If the error persists, you may have a hardware problem. In this case you should contact technical support.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection failed.	Ensure that the cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the ADE-4200/ADW-4200 should be on. Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP. Reboot the ADE-4200/ADW-4200 . If you still have problems, you may need to verify these variables with the telephone company and/or ISP.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any station on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your ADE-4200/ADW-4200 and the station. Make sure you have uninstalled any software firewall.
	Verify that the IP address and the subnet mask are consistent between the ADE-4200/ADW-4200 and the workstations.

Appendix A. Specification

Product		ADSL VPN/Firewall Router	ADSL Wireless VPN/Firewall Router	
Model		ADE-4200A / ADE-4200B	ADW-4200A / ADW-4200B	
Hardwa	are			
Standard		ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) including - Annex A (ADSL over POTS for ADE-3100A/-4100A) - Annex B (ADSL over ISDN for ADE-3100B/ -4100B) G.992.2 (G.lite) with fast retrain		
Protocol		RFC 2364 - PPP over ATM (LLC/VCMUX) RFC 2516 - PPP over Ethernet (LLC/VCMUX) RFC 1577 - Classic IP over ATM (LLC/VCMUX) RFC 1483 - Bridged IP over ATM (LLC/VCMUX) RFC 1483 - Routed IP over ATM (LLC/VCMUX)		
AAL and ATM Support		Integrated ATM AAL5 support 255 VPI plus 65535 VCI address range		
Interop	erability	Interoperable with major DSLAM su	ippliers	
Ports	LAN	4 (10Base-T/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X)		
	Wireless	None	1 x 802.11b wireless access point	
	WAN	1 (RJ-1, 10/100Base-TX, Auto-Neg	otiation)	
LED In	dicators	PWR, SYS, LAN 1 to 4, MAIL, PPP, ADSL, WLAN (ADW-4200 only)		
Button		1 for reset/factory reset		
Console		1 x RS-232 Console		
ON/OF	F switch	1 x ON/OFF switch on rear panel		
Software				
Protocol		IP, NAT, PPTP, ARP, ICMP, DHCP, PPPoE, PPPoA, IPoA, PPTP client, RIP1/2		
Security		Native NAT firewall, Enhanced policy-based+ SPI firewall, Intrusion Detection, URL Filter, Blocking log, Virtual Server, DMZ		
VPN (IPSec)		MD5-HMAC/SHA1-HMAC/Certificates authentication, DES-CBC, 3DES-CBC encryption, Internet Key Exchange, Manual Key Negotiation		
Manag	ement	Web browser management, telnet, console, SNMP		
Environment Specification				
Dimension (W x D x H)		210 mm x 147 mm x 33 mm		
Power		12V DC, 1A		
Power Consumption		Maximum 10W, 34 BTU		
Temperature: Humidity		0~45 degree C (operating), -10~70 degree C (storage) 5%~ 95% (non-condensing)		
Emission		EMI: FCC part 15, CE		

Appendix B. Product Support

Most problems can be solved by using the *Troubleshooting* in Chapter 4. If you cannot resolve the problem with the *Troubleshooting* Chapter, please contact the dealer where you purchased this product. For any other questions, please contact *PLANET* directly at the following email address: support@planet.com.tw

You can also download upgraded driver or software utilities for free from PLANET's website at http://www.planet.com.tw

Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com