



P2P GEAR PRO Series

User Manual

English Version 2.0.0

Table of Contents

CHAPTER 1	INTRODUCTION	4
1.1	BENEFITS	4
1.2	PACKAGE CONTENT.....	5
CHAPTER 2	HARDWARE INSTALLATION.....	6
2.1	PANEL LAYOUT.....	6
2.1.1	Front LEDs (right to left).....	6
2.1.2	Rear Panel (right to left).....	7
2.2	PROCEDURE FOR HARDWARE INSTALLATION.....	8
2.2.1	Power On.....	8
2.2.2	Setup LAN Connection.....	8
2.2.3	Setup WAN Connection.....	8
CHAPTER 3	NETWORK SETTINGS FOR YOUR PC	9
3.1	FOR WINDOWS XP USERS	9
3.2	FOR WINDOWS 2000 USERS	11
3.3	FOR WINDOWS 98/ME USERS	13
CHAPTER 4	ACCESSING TO AXIMCOM P2P GEAR PRO	15
4.1	START-UP AND LOG IN.....	15
CHAPTER 5	BASIC SETTINGS	16
5.1	WAN SETUP.....	16
5.2	LAN SETUP.....	20
5.3	DHCP SETUP	21
5.4	DDNS SETUP.....	22
5.5	MAC ADDRESS CLONE SETUP	23
5.6	TIME SETUP	24
CHAPTER 6	WIRELESS SETTINGS	25
6.1	BASIC SETUP	25
6.1.1	Settings.....	25
6.1.2	SSID Settings.....	27
6.1.3	WEP.....	29
6.1.4	WPA Pre-shared Key / WPA2 Pre-shared Key.....	30
6.1.5	WPA / WPA2	31
6.2	ADVANCED SETUP.....	32
6.3	WDS SETUP.....	33
6.4	UNIVERSAL REPEATER SETUP	35
CHAPTER 7	SECURITY SETTINGS	36
7.1	SECURITY SETUP	36

7.2 VPN / PPTP SETUP.....	38
7.2.1 VPN / PPTP Settings.....	38
7.2.2 Add VPN / PPTP Rule.....	40
CHAPTER 8 iDBM AND ACCESS CONTROL SETTINGS.....	41
8.1 iDBM SETUP.....	41
8.1.1 iDBM Settings.....	41
8.1.2 Add SBM Rule.....	42
8.1.3 Add DBM Rule.....	43
8.2 ACL SETUP.....	44
8.2.1 ACL Settings.....	44
8.2.2 Add ACL Rule.....	45
8.3 iDBM PRIORITY SETUP.....	47
8.4 TurboNAT SETUP.....	48
8.5 MAC SETUP.....	49
8.5.1 MAC ACL Settings.....	49
8.5.2 Add MAC ACL.....	50
CHAPTER 9 APPLICATIONS SETTINGS.....	52
9.1 PORT RANGE FORWARD SETUP.....	52
9.1.1 Port Range Forward Settings.....	53
9.1.2 Add Port Range Forward Rule.....	54
9.2 STREAMING / VPN SETUP.....	55
9.3 UPnP / NAT-PMP SETUP.....	56
9.4 VNC KVM SETUP.....	57
9.5 BT DOWNLOAD SETUP.....	59
9.5.1 BT Download Settings.....	59
9.5.2 Add BT Seed.....	60
9.6 FTP SETUP.....	61
9.6.1 FTP Settings.....	61
9.6.2 Add FTP User Rule.....	62
CHAPTER 10 ADMIN.....	63
10.1 MANAGEMENT.....	63
CHAPTER 11 STATUS.....	65
11.1 TRAFFIC.....	65
11.2 SESSION.....	66
11.3 ROUTER INFORMATION.....	67
11.4 USER.....	69
11.5 LOG.....	70
CHAPTER 12 APPENDIXES – PRODUCT COMPARISON.....	71

CHAPTER 1 INTRODUCTION

AXIMCom P2P GEAR PRO Series is designed for landlords, cohabiting students, online gamers, P2P users, hotspots, Internet café owners, small offices, expatriates and any one encountering network instability issues. Equipped with award-winning iDBM (Intelligent Bandwidth Management), Session Manager, TurboNAT and MRTG functionalities, AXIMCom's P2P GEAR PRO Series is able to resolve network congestion issues, grant smooth/efficient bandwidth sharing and provide ease of network management. Furthermore, it supports Green Download and File Sharing which allow users to download files directly to an USD HDD without needing to turn on the PC and to share files stored in the USD HDD easily.

1.1 BENEFITS

- **iDBM - Intelligent Bandwidth Management**

Enabled with AXIMCom's patent-pending iDBM technology, AXIMCom P2P GEAR PRO is able to automatically monitor your bandwidth usage, prioritize traffic, and allocates bandwidth to all applications and users. At the same time, it also is able to provide users with the freedom to customize their bandwidth allocation to meet their desired special requirements. In short, iDBM is able to grant a smooth and efficient network sharing system no matter the circumstances or usage scenario.

- **Session Manager**

AXIMCom P2P GEAR PRO supports up to 17500 fast recycling sessions in order to guarantee stable network connection and to accommodate more users/applications in the network. (Session numbers vary between models.)

- **Green Download**

AXIMCom P2P GEAR PRO is equipped with an USB port to which users can connect an USB HDD. It allows users to download large files directly to the USB HDD without needing to turn on the PC!! It is not only convenient but also energy saving!

- **File Sharing**

Users in the local network can share files stored in the USB HDD easily and conveniently.

- **MRTG Monitoring**

Providing Throughput and Session MRTG graphs within the Graphic User Interface, this allows users to monitor bandwidth usage without difficulty and manage the network with total convenience and ease.

- **TurboNAT**

Embedded with the TurboNAT Engine, AXIMCom P2P GEAR PRO is able to increase NAT throughput to 95Mbps and achieve 225% the performance of traditional NAT.

- **Energy Saving**

With the low power consumption SOC chip adopted, AXIMCom P2P GEAR PRO provides a lower power consumption ability which saves not only energy, but also our environments.

- **Universal Repeater**

With the use of the University Repeater function, AXIMCom P2P GEAR PRO can enlarge your wireless coverage and eliminate dead spots in just a few steps. Hence, this allows users to be free from the hassles from the extremely complicated WDS settings. (Note: you need at least 2 units to use this function.)

- **Built-in PPTP Server** *(Applied to PGP-116N Only)*

With PPTP server enabled, P2P GEAR PRO provides a secured data connection in the most convenient way.

1.2 PACKAGE CONTENT

- One AXIMCom P2P GEAR PRO
- One User Manual CD
- One Quick Installation Guide
- One Power Adaptor
- One Ethernet Network Cable
- Two Detachable Dipole Antennas

CHAPTER 2 HARDWARE INSTALLATION

2.1 PANEL LAYOUT

2.1.1 Front LEDs (right to left)



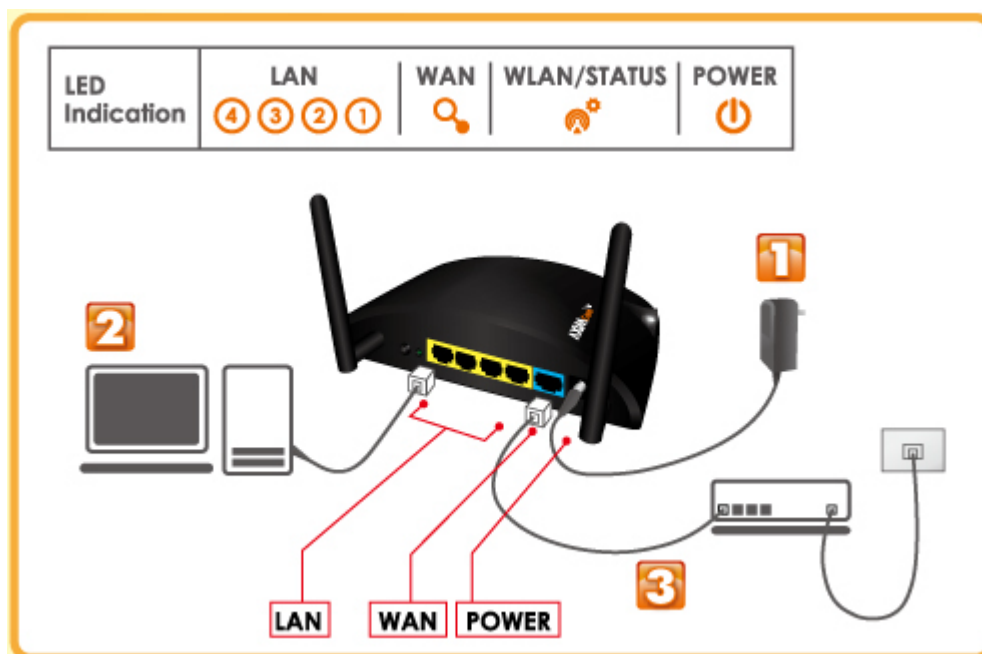
LED	Function	Color	Status	Description
LAN 	LAN Activity	Green	On	The LAN port is linked
			Off	The LAN port is not linked
			Blinking	Data is being transmitted via the LAN port
WAN 	WAN Activity	Green	On	AXIMCom P2P GEAR PRO is linked to the modem
			Off	AXIMCom P2P GEAR PRO is not linked to the modem
			Blinking	Data is being transmitted via the WAN port
WLAN/Status 	Wireless Activity	Green	On	Wireless connection is enabled
			Off	Wireless connection is disabled
		Red	On	AXIMCom P2P GEAR PRO is faulty, please contact our customer service team
			Blinking	USB device is detected or is being ejecting
Power 	Power Indication	Green	On	Power is on
			Off	Power is off

2.1.2 Rear Panel (right to left)



Ports	Description
Power	Power inlet
WAN	The port for connecting your DSL or Cable Modem
LAN	The ports for connecting your computers, printer or other devices for making a wired connection
Reset	When the status LED turns green without blinking, please press the Reset button for 3 seconds. Then, AXIMCom P2P GEAR PRO will restart automatically and reset the settings to factory default.
WPS	The button for ejecting the USB HDD safely, not for WPS setting.

2.2 PROCEDURE FOR HARDWARE INSTALLATION



2.2.1 Power On

Take the provided power adapter. Plug one end into P2P GEAR PRO's DC power port and the other end into a power outlet. AXIMCom P2P GEAR PRO will soon enter the working mode when its POWER LED and Status LED are constantly on.

2.2.2 Setup LAN Connection

Take an Ethernet cable. Plug one end of the cable into your computer's network port and the other end into one of AXIMCom P2P GEAR PRO's LAN ports.

2.2.3 Setup WAN Connection

Take another Ethernet cable. Plug one end of the cable into one of your modem's LAN ports and the other end into AXIMCom P2P GEAR PRO's WAN port.

CHAPTER 3 NETWORK SETTINGS FOR YOUR PC

Before using the AXIMCom P2P GEAR PRO, you have to configure your network settings in your computer. You can either use DHCP or Static IP for your TCP/IP Settings.

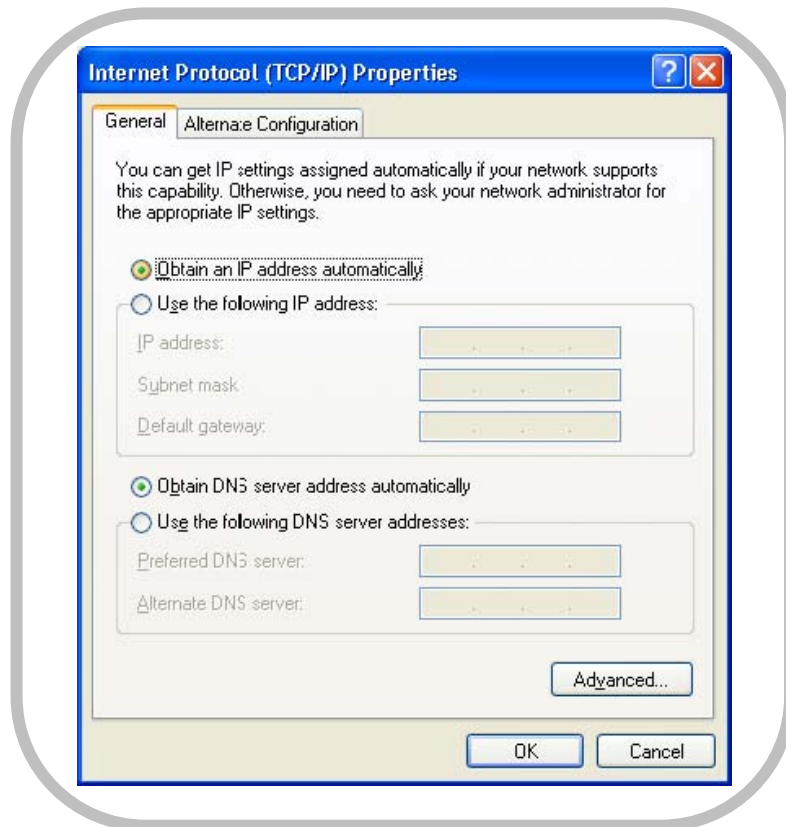
* **DHCP is recommended due to its relative ease in configuration.**

3.1 FOR WINDOWS XP USERS

1. Select **Start > Settings > Network Connections**
2. Click on **Local Area Connection** and choose **Properties**. You will now see the following screen.



3. Select **Internet Protocol (TCP/IP)** for your network card.
4. Click on **Properties**. You will see the following screen.



5. Enable DHCP or Static IP:

- To use DHCP

Select ***Obtain an IP Address automatically*** and ***Obtain DNS server address automatically***.

Then click **OK**. AXIMCom P2P GEAR PRO will now assign an IP address to your computer.

- To use Static IP

Select ***Use the following IP address*** and enter the followings.

IP address: **192.168.1.x** (x could be from 2 ~ 254)

Subnet mask: **255.255.255.0**

Default gateway: **192.168.1.1**

Now select ***Use the following DNS server addresses*** and enter the following.

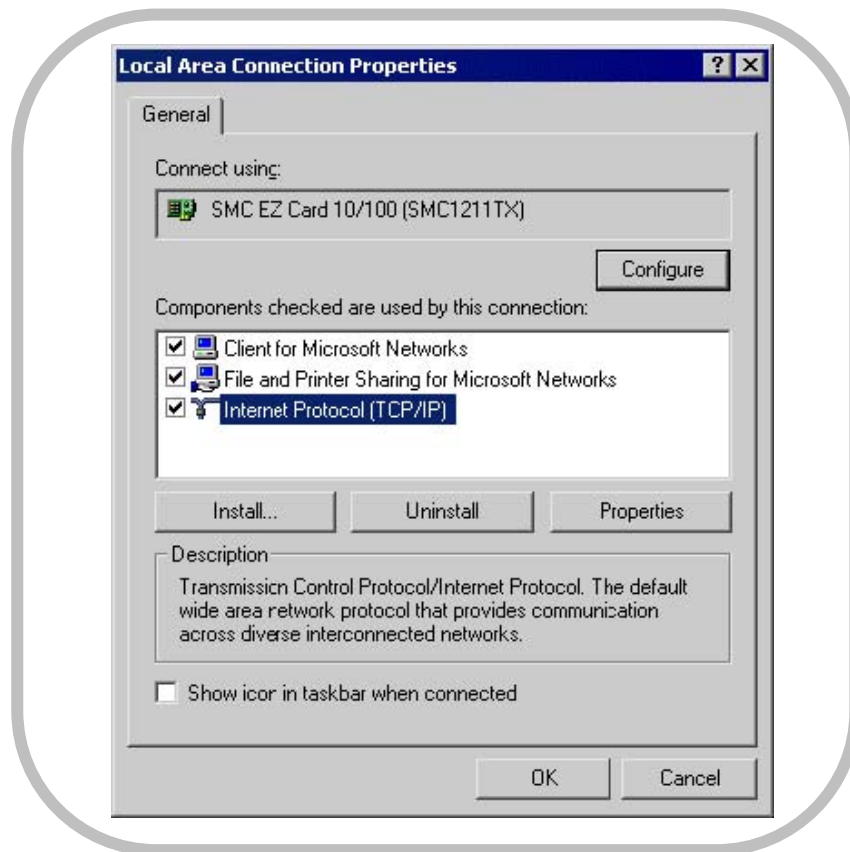
Preferred DNS server: **192.168.1.1**

Then click **OK**.

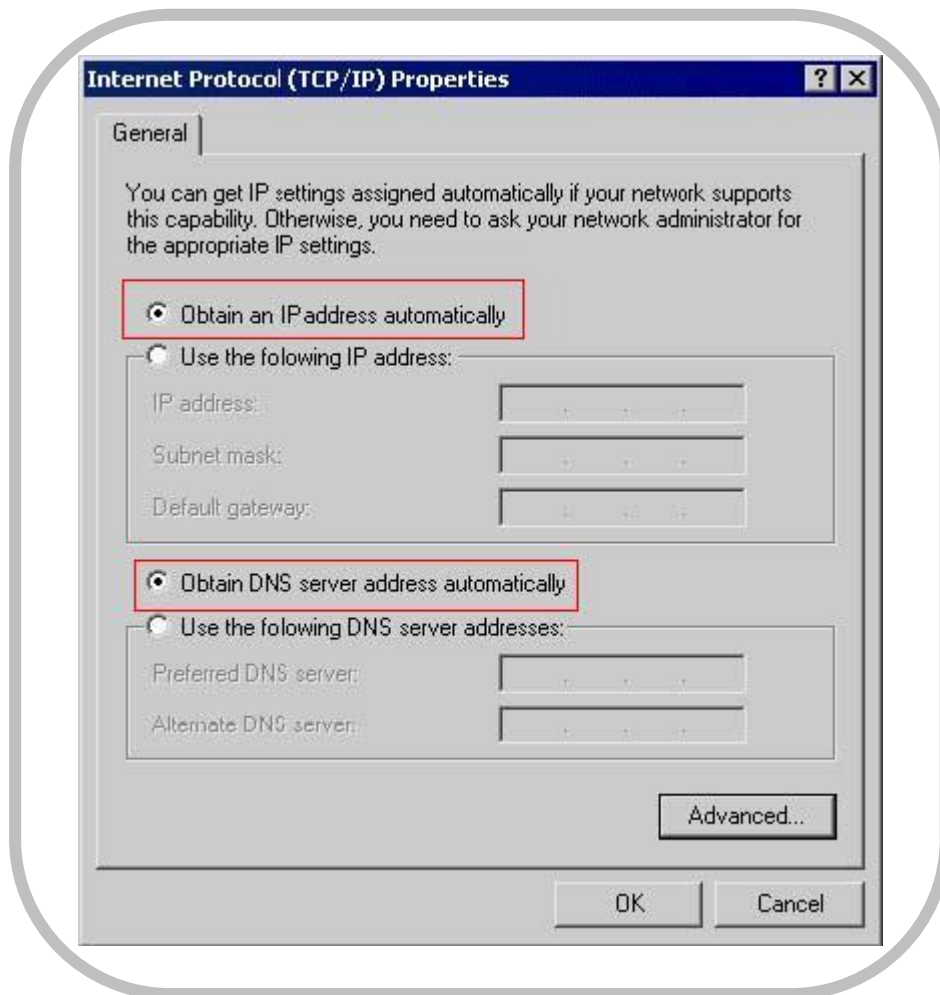
6. You have now finished the network settings for your computer. Please go to Chapter 4 to continue.

3.2 FOR WINDOWS 2000 USERS

1. Select **Start > Settings > Network and Dial-up Connection**
2. Right click on the **Local Area Connection** and select **Properties**. You will see the following screen.



3. Select the **Internet Protocol (TCP/IP)** for your network card.
4. Click on **Properties**. You will see the following screen.



5. Enable DHCP or Static IP:

- To use DHCP

Select ***Obtain an IP Address automatically*** and ***Obtain DNS server address automatically***.

Then click **OK**. AXIMCom P2P GEAR PRO will now assign an IP address to your computer.

- To use Static IP

Select ***Use the following IP address*** and enter the followings.

IP address: **192.168.1.x** (x could be from 2 ~ 254)

Subnet mask: **255.255.255.0**

Default gateway: **192.168.1.1**

Now select ***Use the following DNS server addresses*** and enter the following.

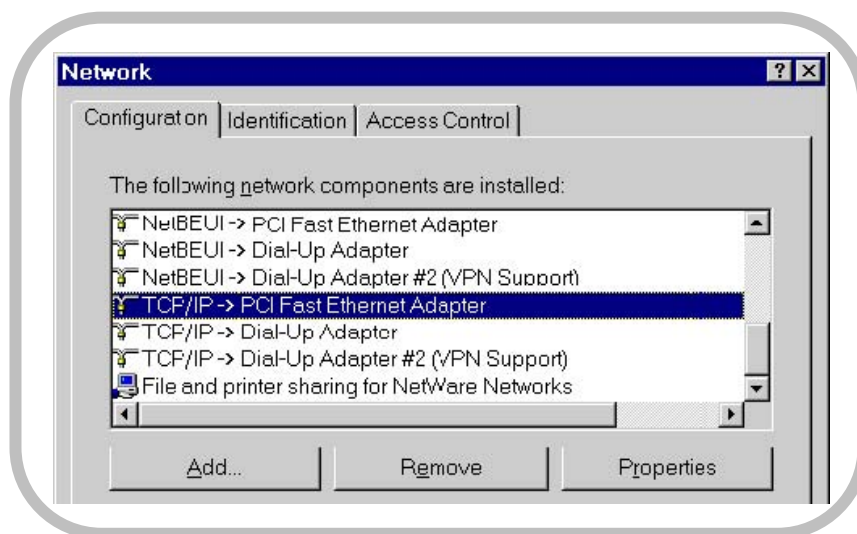
Preferred DNS server: **192.168.1.1**

Then click **OK**.

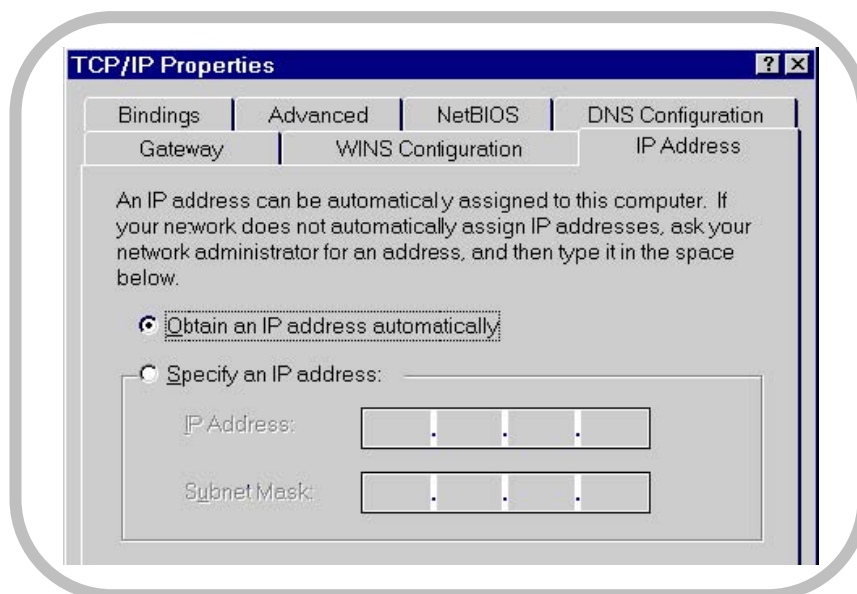
6. You have now finished the network settings of your computer. Please go to Chapter 4 to continue.

3.3 FOR WINDOWS 98/ME USERS

1. Select **Start > Settings > Network**. You will see the following screen.



2. Select **TCP/IP -> PCI Fast Ethernet Adapter** for your network card.
3. Click on **Properties**. You will now see the following screen.



4. Enable DHCP or Static IP:
 - To use DHCP
Select **Obtain an IP Address automatically**.
Then click **OK**. AXIMCom P2P GEAR PRO will now assign an IP address to your computer.

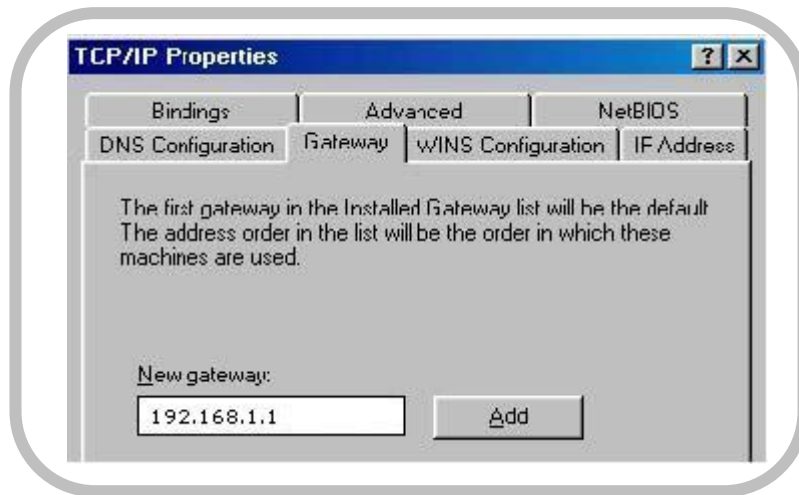
- To use Static IP

Select **Specify an IP address** and enter the followings.

IP address: **192.168.1.x** (x could be from 2 ~ 254)

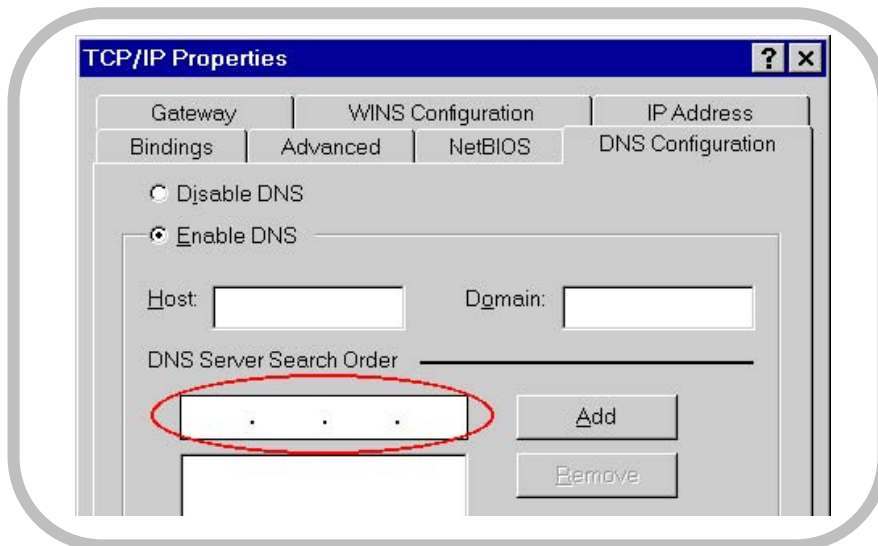
Subnet mask: **255.255.255.0**

Now click on **Gateway** tab. You will see the following screen.



Enter **192.168.1.1** in **New Gateway**, and click **Add**.

Now click on the **DNS Configuration** tab. You will see the following screen.



Enter **192.168.1.1** in **DNS Server Search Order** and click **Add**.

Then click **OK**.

5. You have now finished the network settings of your computer. Please go to Chapter 4 to continue.

CHAPTER 4 ACCESSING TO AXIMCOM P2P GEAR PRO

For Windows XP/2000 users, your computer should have obtained an IP address after configuring the network settings on your computer. Now you need to configure your AXIMCom P2P GEAR PRO.

4.1 START-UP AND LOG IN

1. Open your WEB browser. In the address box, enter [HTTP://192.168.1.1:8080]



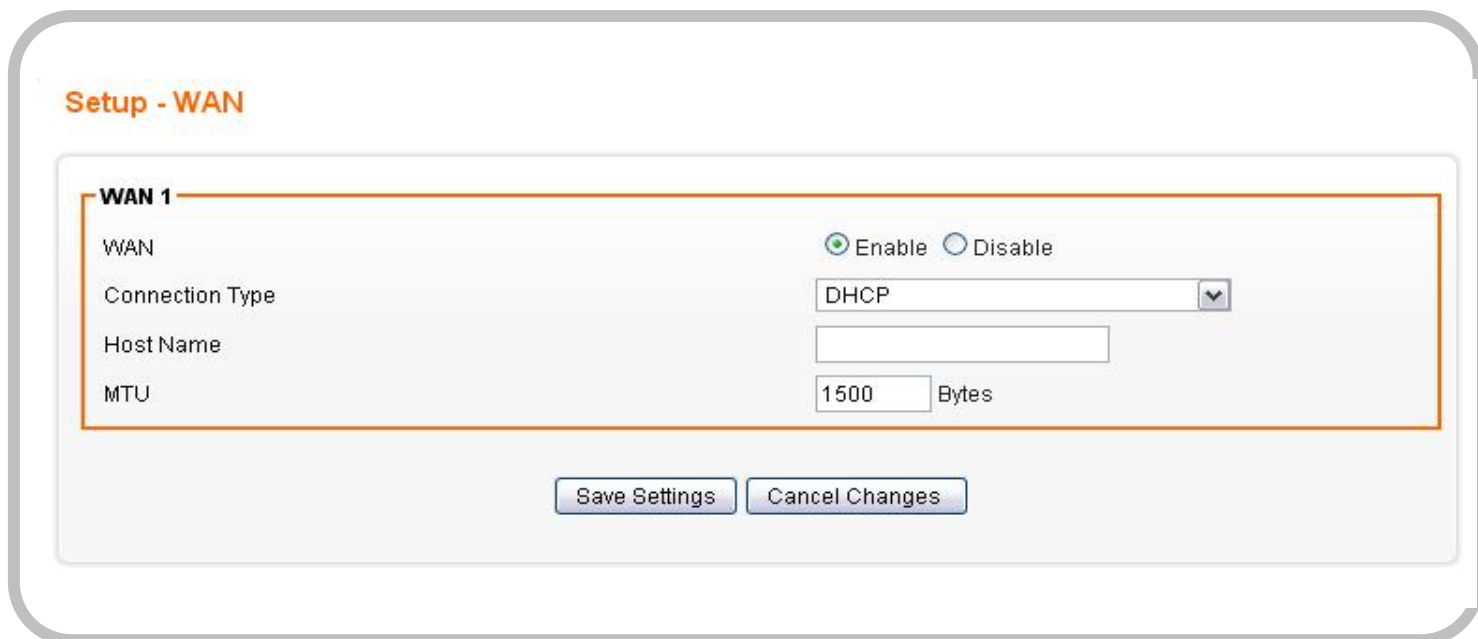
2. When you successfully connect to the configuration interface for AXIMCom P2P GEAR PRO, the login screen will pop up. Enter your username as [admin] and your password as [admin]. You will now see the start page of AXIMCom P2P GEAR PRO.



CHAPTER 5 BASIC SETTINGS

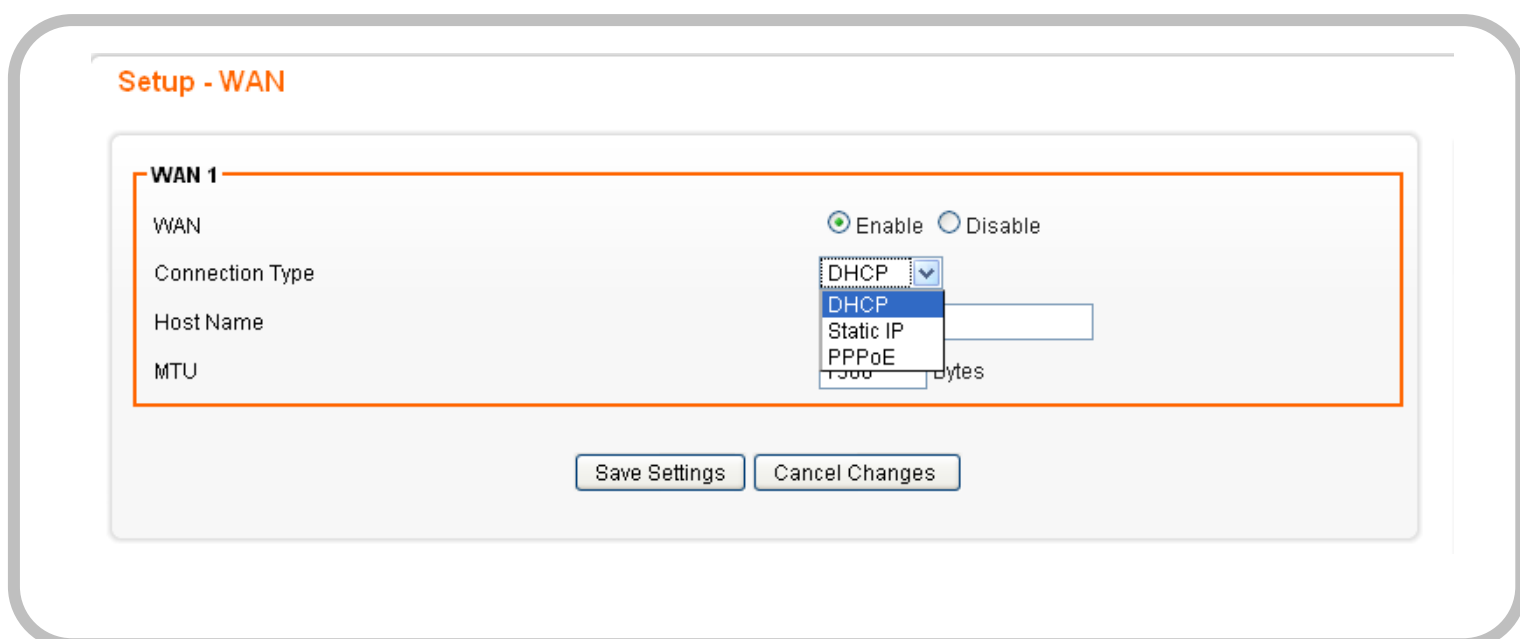
5.1 WAN SETUP

1. Click on [Setup] - [Basic setup] tab. You will see the following screen.



2. WAN Settings:

AXIMCom P2P GEAR PRO supports three connection types: DHCP, Static and PPPoE. Please ensure which connection type should be used, and select your internet connection type from the pull-down menu.



- Option 1: DHCP (automatic IP address assignment):

The IP address is automatically assigned to you by your ISP. DHCP is the default connection type for AXIMCom P2P GEAR PRO. You will see the following screen when you choose DHCP.

Setup - WAN

WAN 1

WAN Enable Disable

Connection Type ▼

Host Name

MTU Bytes

WAN	Select <i>Enable/Disable</i> to enable/disable WAN
Connection Type	DHCP
Host Name	Some ISP and DHCP servers ask for the Host Name of the DHCP client before assigning an IP address. In this case, please key in your Host Name.

- Option 2: Static (fixed IP address assignment):
The IP address, subnet mask, gateway, and DNS server are provided by your ISP.
Please enter the information accordingly.

Setup - WAN

WAN 1

WAN Enable Disable

Connection Type Static IP ▼

External IP Address

Netmask 255.255.255.0 ▼

Gateway

Static DNS 1

Static DNS 2

MTU Bytes

WAN	Select <i>Enable</i> / <i>Disable</i> to enable/disable WAN.
Connection Type	Static IP
External IP Address	The external IP addresses offered by the ISP.
Netmask	The netmask offered by the ISP.
Gateway	The gateway offered by the ISP.
Static DNS 1	The static DNS 1 offered by the ISP.
Static DNS 2	The static DNS 2 offered by the ISP.

- Option 3: PPPoE (connected by username/password):
If your ISP provides the username and password, please enter the information accordingly.

Setup - WAN

WAN 1

WAN Enable Disable

Connection Type PPPoE ▼

User Name

Password

On Demand: Max Idle Time 300 Seconds

Keep Alive: Redial Period

PPP Echo Interval 20 Seconds

PPP Echo Retry Threshold 20

PPPoE MTU 1492 Bytes

MTU 1500 Bytes

Provided by
your ISP

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	PPPoE
User Name	The user name offered by the ISP.
Password	The password offered by the ISP.
On Demand: Max Idle Time	PPPoE On Demand will only be activated when there is traffic. When there is no traffic within max. idle time (default: 300 seconds), PPPoE will be disconnected.
Keep Alive	PPP Keep Alive will maintain the PPP dial up connection.
PPP Echo Interval	PPP echo will ensure whether the link is still up or not (default interval 20 seconds)
PPP Retry Threshold	When PPP echo retry exceeds PPP Retry Threshold (default 20 times), the dial up connection would be recognized as down.
PPP MTU	PPP maximum transmission unit: up to 1492 bytes (PPP's header is 8 bytes).

5.2 LAN SETUP

1. Click on [Setup] – [LAN] tab. You will see the following screen.

Setup - LAN

LAN 1

Internal IP Address: 192.168.1.1

Netmask: 255.255.255.0

Spanning Tree Protocol (STP): Enable Disable

MTU: 1500 Bytes

Save Settings Cancel Changes

2. Configure your LAN following the instructions listed below.

Internal IP Address	Please key in Internal IP Address
Netmask	Select Netmask from the selection list.
Spanning Tree Protocol (STP)	Click Enable to avoid cyclic topology caused by incorrect connection of your internal network. (A cyclic topology will cause network breakdown.)
MTU	Maximum transmission unit: up to 1500 bytes.

5.3 DHCP SETUP

1. Click on [Setup] – [DHCP] tab. You will see the following screen.

AXIMCom P2P GEAR PRO provides DHCP server service in order to offer IP addresses to the computers within a LAN.

Setup - DHCP

DHCP - LAN 1

DHCP Service Enable Disable

DHCP Start IP Address 192.168.1.

Max DHCP Clients

Lease ▼

Domain

2. Configure your LAN following the instructions listed below.

DHCP Server	Select <i>Enable/Disable</i> to enable/disable DHCP Server.
DHCP Starting IP Address	The DHCP starting IP addresses offered by the DHCP Server.
Max DHCP Clients	The maximum number of the IP addresses supported by the DHCP server
Lease	Please choose lease time from the selection list. You can choose <i>1 Hour, 3 Hours, 6 Hours, 1 Day, 3 Days, or 7 Days</i> .
Domain	Please enter the domain name.

5.4 DDNS SETUP

DDNS (Dynamic Domain Name Service) allows an “internet domain name” to be assigned to a computer/router which has a dynamic IP address. This makes it possible for other internet devices to connect to the computer/router without needing to trace the changing IP addresses themselves. To enable DDNS, you will first need to sign up for DDNS services from DynDNS.org, TZO.com or ZoneEdit.com.

DDNS is useful when combined with the virtual server feature. It allows other internet users to connect to your virtual server by using a domain name, rather than an IP address. The DDNS service helps users to locate the right IP address by the domain name.

For example, you wish to set up a personal web server. However, you obtain a different IP address from your ISP every time you connect to the internet. The dynamic IP address you have will cause difficulty for other internet users to find your web server. In this case, you will need to enable DDNS, so other users can connect to you through a fixed domain name to disregard the potential varying IP addresses behind the server.

1. Register with one of the DDNS providers (DynDNS.org, TZO.com or ZoneEdit.com) before you configure DDNS on the AXIMCom P2P GEAR PRO.
2. Click on [Setup] – [DDNS] tab. You will see the following screen.

Setup - DDNS

Dynamic Domain Name Service - WAN 1

DDNS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DDNS Type	DynDNS.org ▼
User Name	<input type="text"/>
Password	<input type="text"/>
Host Name	<input type="text"/>
Action	<input type="button" value="Update"/>

- Configure your DDNS following the instructions listed below.

DDNS Service	Select <i>Enable</i> to enable DDNS service. Select <i>Disable</i> to disable DDNS service.
DDNS Type	Select the desired DDNS service provider from the list.
User Name	Enter your username
Password	Enter your password
Host Name	Apply for a domain name, and make sure it is allocated to you

5.5 MAC ADDRESS CLONE SETUP

Some ISPs only allow a registered MAC address to access to the internet. To bypass the rule, you need to set up a cloned MAC address for AXIMCom P2P GEAR PRO using the pre-registered MAC address.

- Click on [Setup] – [MAC Address Clone] tab. You will see the following screen.

- Configure your Internet Connection (WAN) MAC Clone following the instructions below.

Clone WAN MAC	If your ISP only grants access to a fixed MAC address, please select <i>Enable</i> . If your ISP does not enforce access control, please select <i>Disable</i> .
MAC Address	Type in the MAC Address which has been granted access by your ISP.

5.6 TIME SETUP

1. Click on [Setup] – [Time] tab. You will see the following screen.

Setup - Time

Time Synchronization

Time Synchronization Enable Disable

Time Server Type Time Server Pool Manual

Time Server Area

Time Server IP Address

Time Zone

Periodic Synchronization Enable Disable

Synchronization Interval

Action

2. Configure Time settings following the instructions below

Time Synchronization	Select <i>Enable/Disable</i> to enable/disable Time Synchronization
Time Server	Select Time Server according to your location. You can choose from Automatic, Asia, Europe, North America, South America, or Africa.
Time Zone	Select Time Zone according to your location. (Daylight Saving Time has been calculated and included in the selection).
Periodic Synchronization	Select <i>Enable/Disable</i> to enable/disable Periodic Synchronization
Synchronization interval	Select from <i>Every Hour, Every 6 Hours, Every 12 Hours, Every Day,</i> and <i>Every Week</i> .

CHAPTER 6 WIRELESS SETTINGS

6.1 BASIC SETUP

Multiple SSIDs allow the ability for separate security mode and key settings to be set by users for both convenience and increased protection. Users are able to configure their network devices to access the first SSID with the WPA2 PSK (Pre-Shared Key) and secret key, whilst share the second SSID with WEP and the periodically changed key for visitors. In addition, users are able to isolate these SSIDs to avoid malicious attacks and prevent certain access for visitors using the second SSID. This then provides users an extremely convenient approach to share the wireless access, provide access internet access for visitors, while possessing a strong security protection system at all times.

6.1.1 Settings

1. Click on [Wireless] – [Basic] tab. You will see the following screen.

Wireless - Basic

WLAN 1

Wireless Connection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Mode	B/G/N Mixed ▾
Transmission Power	100% ▾
Wireless Channel	Channel 6 [2.437GHz] ▾
Wireless Isolation Between SSIDs	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

WLAN 1 - SSID 1

Wireless SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless SSID Name	AXIMCom1
Wireless SSID Broadcasting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wi-Fi Multimedia (WMM)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Security Mode	Disable ▾

2. Configure wireless settings following the instructions below.

Wireless Connection	Select Enable if you would like to turn on the wireless signal Select Disable if you would like to turn off the wireless signal.
Wireless Mode	Select the wireless mode for 802.11b, 802.11g, 802.11n only, or mixed use.
Transmission Power	Select the transmission power class from <i>10%, 25%, 50%, 75%, and 100%</i> .
Wireless Channel	Select which channel to be located to.
Wireless Isolation Between SSIDs	Select Enable if you would like to omit the access from one SSID to another. Select Disable if you would like to allow the access from one SSID to another.

6.1.2 SSID Settings

Users are able to configure each SSID with its own attributes. Further, various security modes are available based on the user's needs and preference: Disable, WEP, WPA Pre-Shared Key, WPA, WPA2 Pre-Shared Key, and WPA2. However, it is important to note that all devices under the wireless network must use the same security mode.

You can configure the security settings of your wireless network to suit your desired preference. Different methods will grant different levels of security. Using encryption - data packet is encrypted before transmission - can prevent data packets from being intruded on by un-trusted parties. However, please note that the higher the security level is, the lower the data throughput becomes.

1. Click on [Wireless] – [Basic] tab. You will see the following screen.

Wireless - Basic

WLAN 1

Wireless Connection Enable Disable
Wireless Mode B/G/N Mixed
Transmission Power 100%
Wireless Channel Channel 6 [2.437GHz]
Wireless Isolation Between SSIDs Enable Disable

WLAN 1 - SSID 1

Wireless SSID Enable Disable
Wireless SSID Name AXIMCom1
Wireless SSID Broadcasting Enable Disable
Wi-Fi Multimedia (WMM) Enable Disable
Wireless Isolation Enable Disable
Security Mode
Disable
Disable
WEP
WPA PSK (Pre-Shared Key)
WPA (Radius)
WPA2 PSK (Pre-Shared Key)
WPA2 (Radius)

WLAN 1 - SSID 2

Wireless SSID

2. Configure SSID settings following the instructions below.

Wireless SSID	<p>Select <i>Enable</i> if you would like to turn on this SSID. Select <i>Disable</i> if you would like to turn off this SSID.</p>
Wireless SSID Name	<p>Enter the wireless station name you would like to have.</p>
Wireless SSID Broadcasting	<p>AXIMCom P2P GEAR PRO broadcasts SSID periodically. Select <i>Enable</i> to turn it on or <i>Disable</i> to turn it off. Enabling SSID Broadcasting brings convenience for users to find and connect AXIMCom P2P GEAR PRO. Disabling SSID broadcasting enhances the security by hiding SSID information.</p>
Wi-Fi Multimedia (WMM)	<p>Select <i>Enable</i> to prioritize different traffic types based on their characteristics. For example, VoIP or video traffic will have higher priorities over ordinary traffic.</p>
Wireless Isolation	<p>Select <i>Enable</i> if you would like to omit the access to other network devices connecting to this SSID. Select <i>Disable</i> if you would like to allow the access to other network devices connecting to this SSID.</p>

6.1.3 WEP

WLAN 1 - SSID 1

Wireless SSID Enable Disable

Wireless SSID Name

Wireless SSID Broadcasting Enable Disable

Wi-Fi Multimedia (WMM) Enable Disable

Wireless Isolation Enable Disable

Security Mode

Key Index

Key 1

Key 2

Key 3

Key 4

(The WEP Keys are ASCII strings of 5/13 digits, or HEX strings of 10/26 digits.)

If WEP is selected, WEP index and keys should be set manually.

WEP Key Index	WEP Key Index indicates which WEP key is used for data encryption.
WEP Key (1-4)	64-bit WEP: type 10 hexadecimal digits or 5 ASCII characters 128-bit WEP: type 26 hexadecimal digits or 13 ASCII characters.

6.1.4 WPA Pre-shared Key / WPA2 Pre-shared Key

WLAN 1 - SSID 1

Wireless SSID Enable Disable

Wireless SSID Name

Wireless SSID Broadcasting Enable Disable

Wi-Fi Multimedia (WMM) Enable Disable

Wireless Isolation Enable Disable

Security Mode ▼

Key

Encryption Method ▼

(The Key is an ASCII string of 8-63 digits, or a HEX string of 64 digits.)

If *WPA Pre-shared Key* or *WPA2 Pre-shared Key* is selected, Pre-shared Key is supposed to be set.

Pre-shared Key	Pre-shared Key serves as the credential for the packet encryption.
Encryption Mode	TKIP/AES are supported.

6.1.5 WPA / WPA2

WLAN 1 - SSID 1

Wireless SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Wireless SSID Name	<input type="text" value="AXIMCom 1"/>	
Wireless SSID Broadcasting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Wi-Fi Multimedia (WMM)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Wireless Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Security Mode	<input type="text" value="WPA (Radius)"/>	
Radius Server IP Address	<input type="text"/>	
Radius Server Port	<input type="text" value="1812"/>	<input type="text"/>
Radius Key	<input type="text" value="TKIP"/>	
Encryption Method	<input type="text" value="Disable"/>	
Rekey Method	<input type="text" value="3600"/>	
Rekey Time Interval	<input type="text" value="5000"/>	
Rekey Packet Interval	<input type="text"/>	

(The Key is an ASCII string of 8-63 digits, or a HEX string of 64 digits.)

If **WPA** or **WPA2** is selected, the radius server information should be set accordingly.

Radius Server IP Address	Enter the RADIUS server's IP address.
Radius Server Port	Enter the RADIUS server's port number. The default port is 1812 .
Radius Key	Enter the RADIUS server's IP Address.
Encryption Mode	Select TKIP or AES for the packet encryption.

6.2 ADVANCED SETUP

1. Click on [Wireless] – [Advanced] tab. You will see the following screen.

Wireless - Advanced

Region Setting

Region
US, Canada and Taiwan (channel 1 - 11)

WLAN 1

Fragmentation Bytes (256 ~ 2346)
RTS Seconds (1 ~ 2347)
DTim (1 ~ 255)
Beacon Interval Milliseconds (20 ~ 1024)
Header Preamble
Diversity

2. Configure wireless advanced settings following the instructions below.

Region	Choose the region you are currently located.
Fragmentation	Enter the fragmentation bytes. The default value is 2346 bytes.
RTS	Enter the RTS seconds. The default value is 2347 seconds.
DTim	Enter the DTim seconds. The default value is 1 .
Beacon Interval	Enter the interval to send a beacon. The default value is 100 milliseconds.
Header Preamble	Choose <i>Long</i> or <i>Short</i> header preamble.
Diversity	Choose the diversity, <i>-1</i> , <i>0</i> , <i>1</i> or <i>3</i> .

6.3 WDS SETUP

WDS (Wireless Distributed System) enables the wireless bridging amongst several wireless devices. The bridged devices are identified by the WDS MAC addresses.

1. Click on [Wireless] – [WDS] tab. You will see the following screen.

Wireless - WDS

WLAN 1

WDS Mode: Repeater (AP Enabled) (dropdown menu open showing: Disabled, Repeater (AP Enabled), Bridge (AP Disabled))

WDS 1

WDS MAC Address: [text input field]

Security Mode: Disable (dropdown menu)

WDS 2

WDS MAC Address: [text input field]

Security Mode: Disable (dropdown menu)

WDS 3

WDS MAC Address: [text input field]

Security Mode: Disable (dropdown menu)

WDS 4

WDS MAC Address: [text input field]

Security Mode: Disable (dropdown menu)

2. Configure WDS settings following the instructions below.

WDS	Select Enable to enable WDS function. Select Disable to disable WDS function.
MAC Address [1~4]	Enter the MAC addresses of the other bridged wireless devices. Maximum of 4 devices are allowed to be bridged together.

* Please make sure of the following settings in order to allow WDS to work effectively:

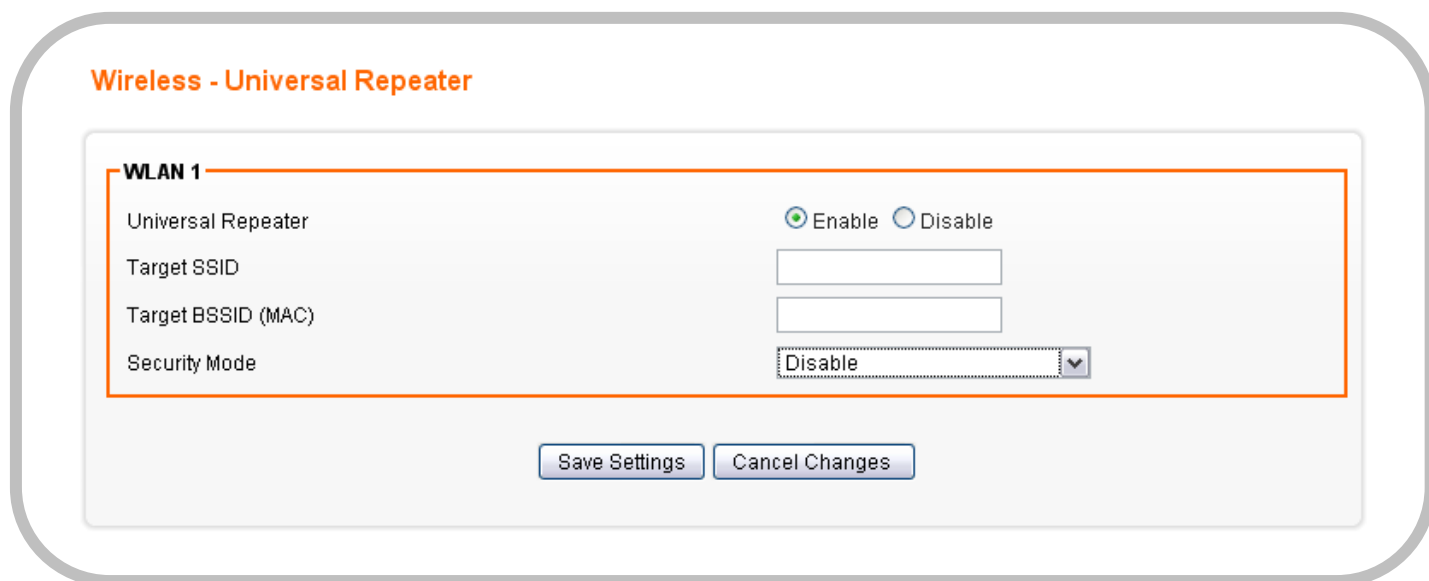
- (1) WDS bridged devices must use the same radio channel.
- (2) WDS bridged devices must use the same encryption mode and encryption keys.

Please Note: If one of the above fails, WDS devices cannot communication with each other.

6.4 UNIVERSAL REPEATER SETUP

The Universal Repeater function is similar with WDS in that it is used to essentially enlarge the area of wireless network coverage. However, unlike WDS, Universal Repeater offers simplicity in configuration requirements, as users only need to configure the current AP as a client, and to connect it to the second AP's SSID (or BSSID). However, you need to ensure that the two APs are using the same wireless channel and security mode (and key) for Universal Repeater to work effectively.

1. Click on [Wireless] – [Universal Repeater] tab. You will see the following screen.



Wireless - Universal Repeater

WLAN 1

Universal Repeater Enable Disable

Target SSID

Target BSSID (MAC)

Security Mode

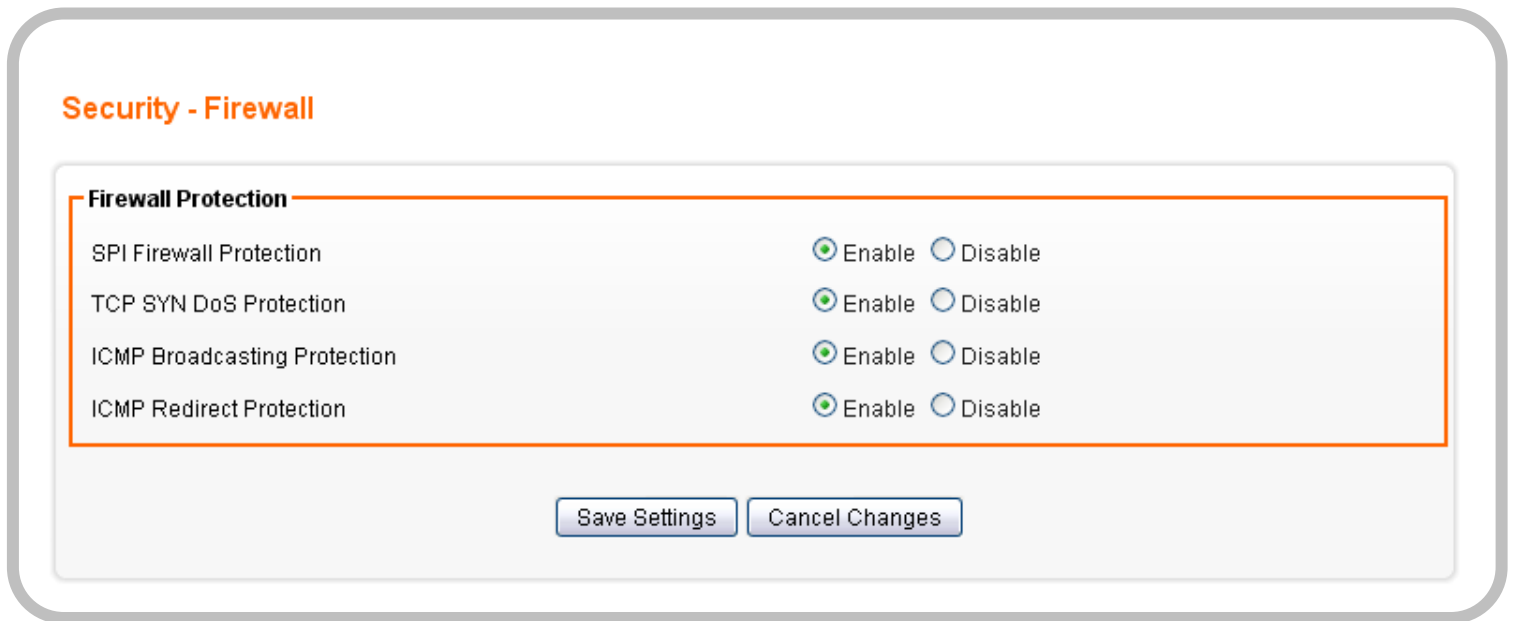
2. Configure universal repeater settings following the instructions below.

Universal Repeater	Select Enable to enable Universal Repeater function. Select Disable to disable Universal Repeater function.
Target SSID	Enter the target SSID to connect to.
Target BSSID (MAC)	Enter the target BSSID to connect to. The BSSID is optional if you setup the target SSID.
Security Mode	Choose the security mode the target AP uses, and enter the key if needed.

CHAPTER 7 SECURITY SETTINGS

7.1 SECURITY SETUP

1. Click on [Security] – [Firewall] tab. You will see the following screen.



2. Configure Security Settings following the instructions below.

SPI Firewall Protection	<p>Select Enable to enable SPI Firewall Protection.</p> <p>Select Disable to disable SPI Firewall Protection.</p>
TCP SYN DoS Protection	<p>Check to enable TCP SYN DoS Protection.</p> <p>Uncheck to disable TCP SYN DoS Protection.</p> <p>TCP SYN DoS attack sends a flood of TCP/SYN packets. Each of these packets are like a connection request, causing the server to consume computing resources (e.g. memory, CPU) to reply and to continuously wait for the incoming packets. Without TCP SYN Dos Protection, the resources in the server will be easily consumed completely. This will then consequently result in the dysfunction of the server.</p> <p>AXIMCom P2P GEAR PRO is able to detect TCP SYN DoS attacks and limits the resource consumption by lowering the incoming request rate by fast recycling the resource. Therefore, AXIMCom P2P GEAR PRO is still able to serve normal traffic while it is under such an attack.</p>
ICMP Broadcasting Protection	<p>Check to enable ICMP Broadcasting Protection.</p> <p>Uncheck to disable ICMP Broadcasting Protection.</p> <p>ICMP broadcasting attack is a type of DoS attacks. A flood of ICMP broadcasting packets is generated and sent to a server (like AXIMCom P2P GEAR PRO). Consequently, this server will suffer from a huge amount of interruptions and consumption of computing resources.</p> <p>AXIMCom P2P GEAR PRO is able to stop responding to ICMP broadcasting echo packets in order to avoid a potential ICMP broadcasting DoS attack.</p>
ICMP Redirect Protection	<p>Check to enable ICMP Redirect Protection.</p> <p>Uncheck to disable ICMP Redirect Protection.</p> <p>An ICMP redirect message is a way to change the existing routing path. Generally, ICMP redirect packets should not be sent, and so when there is the occurrence that ICMP redirect packets are sent, it is important to note that it is very likely to be used as a means for a network attack.</p>

7.2 VPN / PPTP SETUP

7.2.1 VPN / PPTP Settings

1. Click on [Security] – [VPN / PPTP] tab. You will see the following screen.

Security - VPN / PPTP

PPTP

PPTP Enable Disable

MTU Bytes

VPN Start IP Address

Max VPN Clients

Auto DNS Enable Disable

DNS

CHAP Enable Enable Disable

MSCHAP Enable Enable Disable

MSCHAP v2 Enable Enable Disable

MPPE128 Enable Enable Disable

Proxy ARP Enable Enable Disable

NAT Enable Enable Disable

User Rule

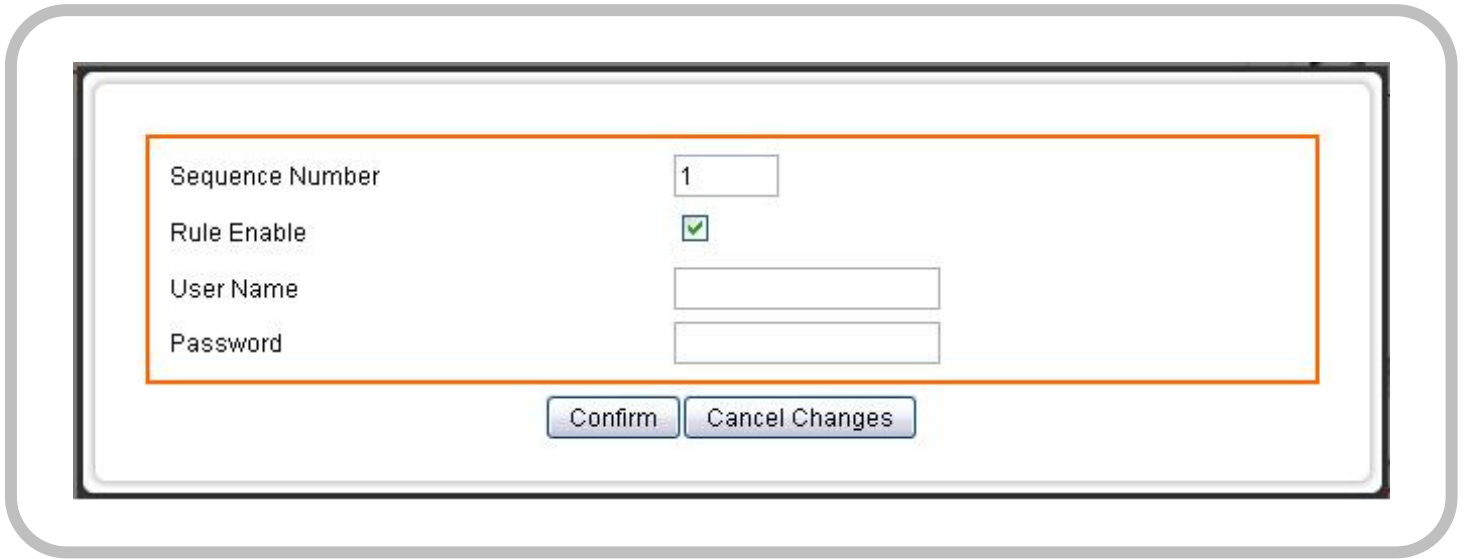
Rule Enable	User Name	Password
-------------	-----------	----------

2. Configure PPTP Settings following the instructions below.

PPTP	Choose <i>Enable/Disable</i> to enable/disable L2TP.
MTU	Enter MTU value. The default value is 1482 bytes.
VPN Start IP Address	Enter the VPN start IP address. The default value is 192.168.39.1 .
Max VPN Clients	Enter the max VPN clients.
Auto DNS	Choose <i>Enable/Disable</i> to enable/disable Auto DNS.
DNS	Enter DNS server if you choose <i>Disable</i> for Auto DNS.
CHAP Enable	Choose <i>Enable/Disable</i> to enable/disable CHAP for VPN authentication.
MSCHAP Enable	Choose <i>Enable/Disable</i> to enable/disable MSCHAP for VPN authentication.
MSCHAP2 Enable	Choose <i>Enable/Disable</i> to enable/disable MSCHAP2 for VPN authentication.
MPP128 Enable	Choose <i>Enable/Disable</i> to enable/disable MPP128 encryption.
Proxy ARP Enable	Choose <i>Enable/Disable</i> to enable/disable Proxy ARP.
NAT Enable	Choose <i>Enable/Disable</i> to enable/disable NAT.

7.2.2 Add VPN / PPTP Rule

1. Click on [Add] tab. You will see the following screen.



The screenshot shows a configuration window for adding a PPTP rule. It contains the following fields and controls:

- Sequence Number:
- Rule Enable:
- User Name:
- Password:
- Buttons: Confirm, Cancel Changes

2. Configure [Add PPTP] Settings following the instructions below.

Sequence Number	This defines the sequence of the PPTP rules.
Rule Enable	<i>Enable/Disable</i> this PPTP rule
User Name	Enter PPTP user name.
Password	Enter PPTP password.

CHAPTER 8 iDBM AND ACCESS CONTROL SETTINGS

8.1 iDBM SETUP

Intelligent Bandwidth Management (iDBM) provides two powerful and unique mechanisms to manage bandwidth: Static Bandwidth Management (SBM) and Dynamic Bandwidth Management (DBM). SBM provides users with the option to allocate a fixed amount of bandwidth for a specific computer or a particular application, while DBM intellectually manages the rest of the bandwidth while all the time satisfying the complicated bandwidth requirements/settings of SBM.

8.1.1 iDBM Settings

The essential configuration needed by iDBM is to specify accurately the bandwidth you have. iDBM would then dispatch bandwidth according to this information. Please Note: Improper bandwidth assignment may cause iDBM to work ineffectively.

1. Click on [iDBM / Access Control] – [iDBM] tab. You will see the following screen.

iDBM / Access Control - iDBM

Intelligent Dynamic Bandwidth Management (iDBM)

iDBM Enable Disable

DBM - WAN 1

Bandwidth Type (Download/Upload) ADSL 4M / 1M bps

Download Bandwidth 4096 K bps

Upload Bandwidth 1024 K bps

Reserved Buffering Bandwidth 25 %
(Too less reserved buffering bandwidth might cause congestion in a unstable network.)

Available Bandwidth 3072.0/7688.0 Kbps

Static Bandwidth Management (SBM)

Rule Name	Enable	IP Address	Application	External Interface	Bandwidth
SBM	✘	192.168.1.20		WAN1	20 %

Dynamic Bandwidth Management (DBM)

The rest bandwidth from setting SBM would be totally used for DBM.

DBM Available Bandwidth

WAN 1 3072.0/7688.0 Kbps

Rule Name	Rule Enable	DBM IP
-----------	-------------	--------

2. Bandwidth Settings:

Please adjust your bandwidth type according to your bandwidth (download/upload) subscribed from your ISP. Due to the unstable nature of network bandwidth supported by ISP, users are recommended to reserve a portion of bandwidth for buffering usage, and iDBM would then arrange the reserved bandwidth under heavy traffic.

Bandwidth Type (Download/Upload)	Select the correct bandwidth type according to your Internet service subscription. If the bandwidth type is not available on the list, select Custom .
Download Bandwidth	Enter the value to customize download bandwidth.
Upload Bandwidth	Enter the value to customize upload bandwidth.
Reserved Buffering Bandwidth	Enter the value to provide bandwidth buffer.

8.1.2 Add SBM Rule

1. Click on [Add] tab. You will see the following screen.

2. Configure [Add SBM] Settings following the instructions below.

Sequence Number	This defines the sequence of the SBM rules. If a packet fits the conditions set by the SBM rules, the packet will then be sorted according to the first SBM rule from the top of the list.
------------------------	--

Rule Name	Name of the SBM rule.
Rule Enable	Enable/Disable this SBM rule
Internal IP	Set up the internal IP for this SBM rule.
Protocol	Set up the protocol (TCP or UDP) for the ACL to be enabled.
External Interface	Please select which External Interface (WAN1 or WAN2) you want a packet to go through, IF the packet fits the condition of this SBM rule.
Service Port Range	Set up the Service Port Range (e.g., HTTP is TCP/80) for the SBM to be enabled.
Bandwidth Allocation	<i>By Ratio</i> or <i>By Bandwidth</i>
Ratio	The ratio of the whole bandwidth according to the External Interface.
Download	Enter the reserved download bandwidth.
Upload	Enter the reserved upload bandwidth.
Utilize Bandwidth More than Guaranteed	Check this box if you wish to allow the traffic conforming this SBM rule to be able to utilize the whole bandwidth when the bandwidth is idle.

8.1.3 Add DBM Rule

1. Click on [Add] tab. You will see the following screen.

The screenshot shows a configuration window for adding a DBM rule. It includes the following fields and controls:

- Sequence Number:** A text input field containing the value '2'.
- Rule Name:** An empty text input field.
- Rule Enable:** A checkbox that is checked.
- Internal IP Range:** Two text input fields labeled 'From:' and 'To:'.
- Buttons:** 'Confirm' and 'Cancel Changes' buttons at the bottom.

2. Configure [Add DBM] Settings following the instructions below

Sequence Number	This defines the sequence of the DBM rules.
Rule Name	Name of the DBM rule.
Rule Enable	Enable/Disable this DBM rule
Internal IP Range	Set up the internal IP range for this DBM rule.

8.2 ACL SETUP

Users can setup network access permission based on the LAN IP addresses, WAN IP addresses, and protocol/port numbers of the service. Please enable DBM function for the following applications: (a) the applications with heavy network traffic (e.g. P2P and FTP); (b) the applications requiring real-time response (e.g. online gaming, VoIP and streaming). You are allowed to set up at most 16 IP addresses to be managed by DBM.

8.2.1 ACL Settings

1. Click on [DBM / Access Control] – [ACL / DBM IP] tab. You will see the following screen. Please do not change the parameters unless you wish to customize it by yourself.

iDBM / Access Control - ACL

Access Control List (ACL)

ACL Enable Disable

Default ACL Action ALLOW DENY

Access Control List (ACL) Rule

Rule Name	Rule Enable	External Interface	Internal IP Range	Action
MSN Messenger	X	*	From: To:	DENY
MSN Messenger	X	*	From: To:	DENY
Yahoo! Messenger	X	*	From: To:	DENY

Add Delete Modify Up Down

Save Settings Cancel Changes

2. Configure Access Control List (ACL) Settings following the instructions below.

ACL	Select Enable to enable ACL. Select Disable to disable ACL.
Default ACL Action	Check Enable to enable a specific MAC Filter rule. Uncheck Enable to disable a specific MAC Filter rule. Type the MAC address to permit a device to access to the network. * Enabling MAC filtering blocks all MAC addresses which are not listed in the MAC Filter Rule. Be aware that adding the MAC address of your managing computer is required in order to access to AXIMCom P2P GEAR PRO.

8.2.2 Add ACL Rule

1. Click on [Add] tab. You will see the following screen.

The screenshot shows a configuration window for adding an ACL rule. The fields are as follows:

- Sequence Number: 4
- Rule Name: (empty text box)
- Rule Enable:
- External Interface: WAN1 (dropdown menu)
- Internal IP Range: From: (empty) To: (empty)
- External IP Range: From: (empty) To: (empty)
- Protocol: * (dropdown menu)
- Service Port Range: From: (empty) To: (empty)
- Action: ALLOW (dropdown menu)

Buttons: Confirm, Cancel Changes

2. Configure [Add Access Control List (ACL)] Settings following the instructions below

Sequence Number	This defines the sequence of the ACL rules. If a packet fits the conditions set by the ACL rules, the packet will then be sorted according to the first ACL rule from the top of the list.
Rule Name	Name of the ACL rule.
Rule Enable	Enable/Disable this ACL rule
External Interface	Please select which External Interface (WAN1 or WAN2) you want a packet to go through, IF the packet fits the condition of this ACL rule.
Internal IP Range	Set up the internal IP range for this ACL rule.
External IP Range	Set up the external IP range for this ACL rule.
Protocol	Set up the protocol (TCP or UDP) for the ACL to be enabled.
Service Port Range	Set up the Service Port Range (e.g., HTTP is TCP/80) for the ACL to be enabled.
Action	Select ALLOW / DENY .

3. Example

Example 1 : Enabling DBM for PCs with high throughput or high importance

For example, a family has 3 PCs. The 1st PC is used by parents to work at home, send and receive e-mails, and make VoIP calls. The IP address is set to 192.168.1.50 or it is assigned through MAC ACL.

The 2nd PC is used for continuous P2P download machine which consumes large bandwidth for a long period of time. The IP address is set to 192.168.1.51 or it is assigned through MAC ACL.

The 3rd PC is used for online gaming. The address is set to 192.168.1.52 or it is assigned through MAC ACL.

Now, we want to enable DBM so all 3 PCs can enjoy the optimized network service.

Rule Name	DBM management
Rule Enable	Enable
Internal IP Range	192.168.1.50:192.168.1.52

Example 2 : Filter and block MSN usage.

For example, a company does not wish to allow employees to use MSN. The system administrator can set up an ACL action: rejecting the traffic going out to External IP Range at 207.46.110.*/*.

Rule Name	MSN Blocking
Rule Enable	Enable
External Interface	* (All complies)
Internal IP Range	Keep it blank (All complies)
External IP Range	207.46.110.1:207.46.110.1.254 (IP address range for MSN server)
Protocol	TCP
Service Port Range	Keep it blank (All complies)
Action	DENY

8.3 iDBM PRIORITY SETUP

DBM transmits the important packets in high priority to optimize the network utilization. You can specify the types of packets for high priority.

1. Click on [iDBM / Access Control] – [iDBM Priority] tab. You will see the following screen.

iDBM / Access Control - iDBM Priority

iDBM Priority

iDBM Priority Enable Disable

Application Priority

TCP ACK Enable Disable

ICMP Enable Disable

DNS Enable Disable

SSH Enable Disable

Telnet (BBS) Enable Disable

TCP Max Segment Size Enable Disable

Save Settings Cancel Changes

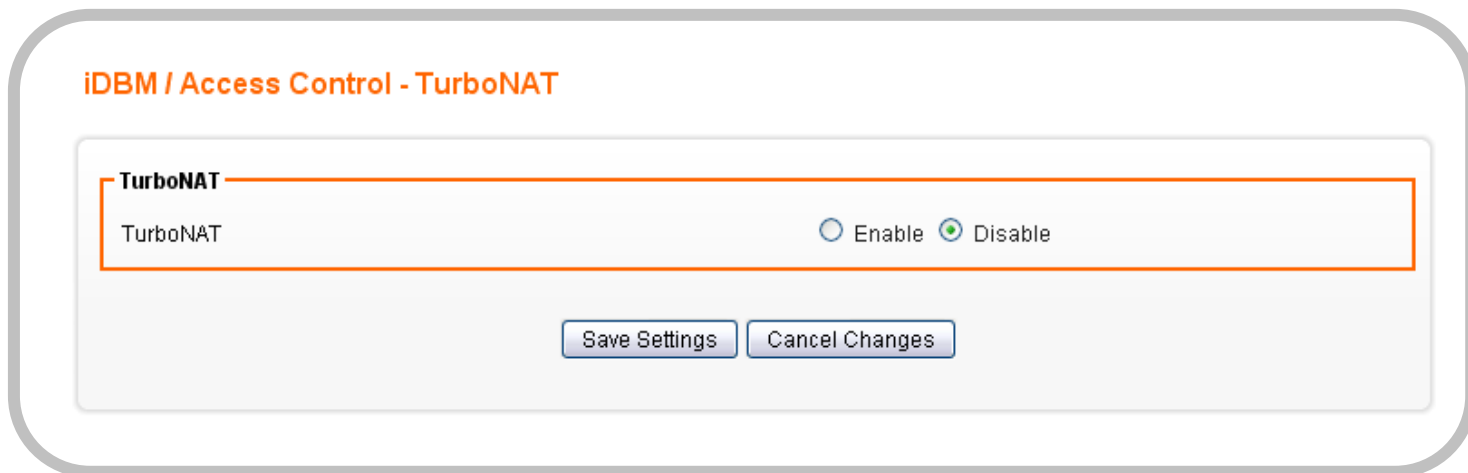
2. Configure [DBM Priority] Settings following the instructions below

TCP ACK	Select <i>Enable/Disable</i> to enable/disable TCP ACK priority
ICMP	Select <i>Enable/Disable</i> to enable/disable ICMP priority
DNS	Select <i>Enable/Disable</i> to enable/disable DNS priority
SSH	Select <i>Enable/Disable</i> to enable/disable SSH priority
Telnet (BBS)	Select <i>Enable/Disable</i> to enable/disable Telnet (BBS) priority
TCP Max Segment Size	Select <i>Enable/Disable</i> to enable/disable TCP Max Segment Size

8.4 TurboNAT SETUP

NAT is often the performance bottleneck in an IP sharing device. Generic routers are generally insufficient when dealing with a high-speed broadband network. Therefore, TurboNAT is designed to solve this problem. By accelerating the NAT performance, TurboNAT allows AXIMCom P2P GEAR PRO to fulfill the higher speed network and to reserve the system performance for other features such as ACL and VPN servers.

1. Click on [iDBM / Access Control] – [iDBM Priority] tab. You will see the following screen.



iDBM / Access Control - TurboNAT

TurboNAT

TurboNAT Enable Disable

2. Configure [DBM Priority] Settings following the instructions below

TurboNAT	Select <i>Enable/Disable</i> to enable/disable TurboNAT.
-----------------	--

8.5 MAC SETUP

8.5.1 MAC ACL Settings

AXIMCom P2P GEAR PRO's DHCP server can assign a specified IP address based on a corresponding MAC address. It is useful when your computers are running under DHCP but port forwarding is also set to forward certain types of packets to an IP address. For example, a web server (IP address is 192.168.1.5) exists and port 80 is forwarded to 192.168.1.5. This web server is running as a DHCP client. This feature can help the web server to always obtain 192.168.1.5 as its IP address and allow the port forwarding rule to work as planned.

1. Click on [DBM/Access Control] – [MAC] tab. You will see the following screen.

iDBM / Access Control - MAC

MAC ACL

MAC ACL Enable Disable

Default MAC ACL Action ALLOW DENY

MAC ACL Rule

Rule Enable	Action	ACL Enable	Static DHCP Enable	IP
-------------	--------	------------	--------------------	----

Add Delete Modify Up Down

Save Settings Cancel Changes

2. Configure [MAC ACL] Settings following the instructions below

MAC ACL	Check Enable to enable a specific MAC Address Binding rule. Check Disable to disable a specific MAC Address Binding rule. Type the MAC address to a specific IP address bonded.
Default MAC ACL Action	Check ALLOW to allow the ACL action. Check DENY to deny the ACL action.

8.5.2 Add MAC ACL

1. Click on [Add] tab. You will see the following screen.

The screenshot shows a configuration window for adding a MAC ACL. The fields are as follows:

- Sequence Number: 1
- Rule Name: (empty text box)
- MAC: (empty text box)
- Action: ALLOW (dropdown menu)
- ACL Enable:
- Static ARP Enable:
- Static DHCP Enable:
- IP: (empty text box)

Buttons: Confirm, Cancel Changes

2. Configure [Add MAC ACL] Settings following the instructions below

Sequence Number	This defines the sequence (priority) of all the MAC ACL actions.
Rule Name	Name of the MAC ACL Action.
MAC	Set up the MAC Address to which you would like to enable the MAC ACL action.
Action	ALLOW / DENY °
ACL Enable	Check / Uncheck to enable/disable this ACL action
Static ARP Enable	Check/Uncheck to enable/disable this Static ARP setting
Static DHCP Enable	Check/Uncheck to enable/disable this Static DHCP setting.
IP	The IP address corresponds to Static ARP or Static DHCP.

3. Example

Example 1 : Network management in a student dormitory

In a student dormitory, there are 5 PCs sharing the broadband network. In order to prevent the network from attacks, the system administrator sets up the MAC ACL Action to be DENY, and then assigns IP addresses to 5 PCs allowing them to access to the network.

- i. Check **Static DHCP Enable** to bind this MAC Address with a specific IP. Whenever the PC connects to the network, it will always be given this IP address. (This setting will allow the system administrator to enable DBM function on this PC easily later on.)
- ii. Check **Static ARP Enable** to protect the PCs from virus infection and attacks.

Rule Name	Dormitory List
MAC	00:12:34:56:78:9A (setting up the rule for this MAC Address)
Action	ALLOW
ACL Enable	Check to enable
Static ARP Enable	Check to enable
Static DHCP Enable	Check to enable
IP	192.168.1.13 (assign this IP address to the PC)

CHAPTER 9 APPLICATIONS SETTINGS

9.1 PORT RANGE FORWARD SETUP

By activating the port range forwarding function, remote users can access the local network via the public IP address. Users can assign a specific external port range to a local server. Furthermore, users can specify an internal port range associated in a port range forwarding rule. When AXIMCom P2P GEAR PRO receives an external request to access any one of the configured external ports, it will redirect the request to the corresponding internal server and change its destination port to one of the internal ports specified. Therefore, if users do not wish for destination port to be changed for a request, the internal port range should be left empty.

Certain applications in a LAN are available only after activating the port range forwarding, including servers and online gaming. When an Internet request wants to access a port, AXIMCom P2P GEAR PRO will dispatch it to the IP specified. Due to security reasons, users are suggested to limit the use of port range forwarding, and cancel it when the application is not used.

By enabling DMZ Host Function, you can set up a DMZ host at a particular computer exposed to the Internet. In this way, some applications, especially online games (if the traffic port numbers of the applications are always changing), can be easily accessed.

9.1.1 Port Range Forward Settings

1. Click on [Applications] – [Port Range Forward] tab. You will see the following screen.

Applications - Port Range Forward

DMZ - WAN 1

DMZ Enable Disable

DMZ IP Address

Port Range Forwarding

Port Forwarding Enable Disable

Port Range Forwarding Rule

Rule Name	Rule Enable	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range
HTTP	✘	WAN1	TCP	From:80 To:80	192.168.1.20	From: To:
HTTPS	✘	WAN1	TCP	From:443 To:443	192.168.1.20	From: To:
POP3	✘	WAN1	TCP	From:110 To:110	192.168.1.20	From: To:
POP3S	✘	WAN1	TCP	From:995 To:995	192.168.1.20	From: To:
SMTP	✘	WAN1	TCP	From:25 To:25	192.168.1.20	From: To:
SMTPS	✘	WAN1	TCP	From:465 To:465	192.168.1.20	From: To:
SSH	✘	WAN1	TCP	From:22 To:22	192.168.1.20	From: To:

2. Configure [DMZ] Settings following the instructions below

DMZ	Select Enable to enable DMZ function. Select Disable to disable DMZ function.
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port / Public IP address above.

3. Configure [Port Range Forwarding] Settings following the instructions below

Port Forwarding	Select Enable / Disable to enable/disable Port Forwarding
------------------------	--

9.1.2 Add Port Range Forward Rule

1. Click on [Add] tab. You will see the following screen.

The screenshot shows a configuration window for adding a port range forwarding rule. The fields are as follows:

- Sequence Number: 9
- Rule Name: (empty text box)
- Rule Enable:
- External Interface: WAN1 (dropdown menu)
- Protocol: TCP (dropdown menu)
- External Port Range: From: [] To: []
- Internal IP: []
- Internal Port Range: From: [] To: []

At the bottom of the form are two buttons: 'Confirm' and 'Cancel Changes'.

2. Configure [Add Port Range Forwarding Rule] Settings following the instructions below

Sequence Number	This defines the sequences (priorities) of the port forwarding rules. If a packet fits the conditions setup by the port forwarding rules, the packet will then be forwarded according to the 1 st rule from the top of the list.
Rule Name	Enter the name of the port forwarding rule.
Action	Check/Uncheck to enable/disable this port forwarding rule.
External Interface	Choose WAN1 or WAN2 as the External port forwarding interface.
Protocol	Choose TCP, UDP or TCP/UDP for the rule to be applied.
External Port Range	Set up the External Port Range for the rule to be applied.
Internal IP	Set up the Internal IP for the rule to be applied.
Internal Port Range	Set up the Internal Port Range for the rule to be applied.

9.2 STREAMING / VPN SETUP

You can enhance your media streaming quality by enabling RTSP, MMS, and H.323 protocols. Moreover, VPN Pass-through functionality can also be enabled.

1. Click on [Applications] – [Streaming / VPN] tab. You will see the following screen.

Applications - Streaming / VPN

Streaming
RTSP Enable Disable
MMS Enable Disable

Video Conference
H.323 Enable Disable

VPN
IPSec Enable Disable
PPTP Enable Disable

2. Configure [Streaming] Settings following the instructions below.

RTSP	Select <i>Enable/Disable</i> to enable/disable RTSP
MMS	Select <i>Enable/Disable</i> to enable/disable MMS

3. Configure [Video Conference] Settings following the instructions below

H.323	Select <i>Enable/Disable</i> to enable/disable H.323
-------	--

4. Configure [VPN] Settings following the instructions below

IPSec Pass-through	Select <i>Enable/Disable</i> to enable/disable IPSec Pass-through
PPTP Pass-through	Select <i>Enable/Disable</i> to enable/disable PPTP Pass-through

9.3 UPnP / NAT-PMP SETUP

Applications - UPnP / NAT-PMP

UPnP

UPnP

Enable Disable

NAT-PMP

Enable Disable

UPnP Port

5555

Save Settings

Cancel Changes

1. Configure [Applications] – [UPnP] Settings following the instructions below

UPnP	Select <i>Enable/Disable</i> to enable/disable UPnP
NAT-PMP	Select <i>Enable/Disable</i> to enable/disable NAT-PMP
UPnP Port	Enter the number for UPnP port.

9.4 VNC KVM SETUP

VNC KVM allows the VNC viewer on Internet to easily connect to the VNC servers on a LAN. Please see the graphical illustration listed below. In this way, users can conveniently connect to the computers at home/office network from anywhere in the world. (Please note that VNC KVM function has to work with UltraVNC viewer/server.)



1. Click on [Applications] – [VNC KVM] tab. You will see the following screen.

Applications - VNC KVM

VNC KVM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
VNC KVM	
<input type="button" value="Save Settings"/> <input type="button" value="Cancel Changes"/>	

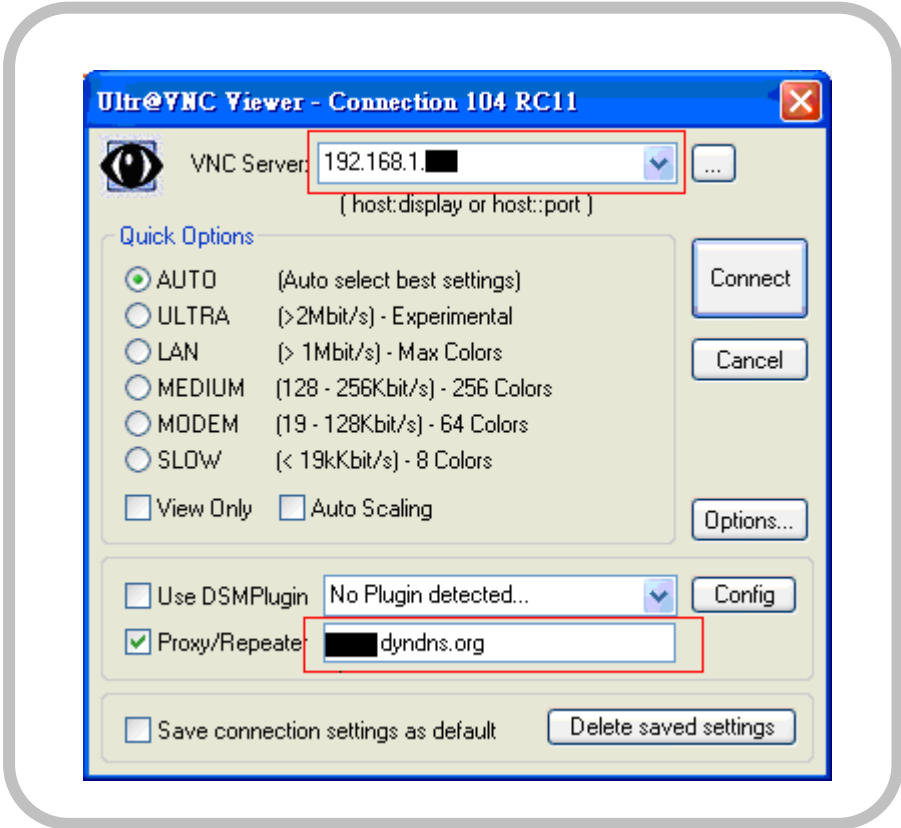
2. Configure [Applications] – [VNC KVM] Settings following the instructions below.

VNC KVM	Select <i>Enable/Disable</i> to enable/disable VNC KVM
---------	--

- Download UltraVNC and install it.

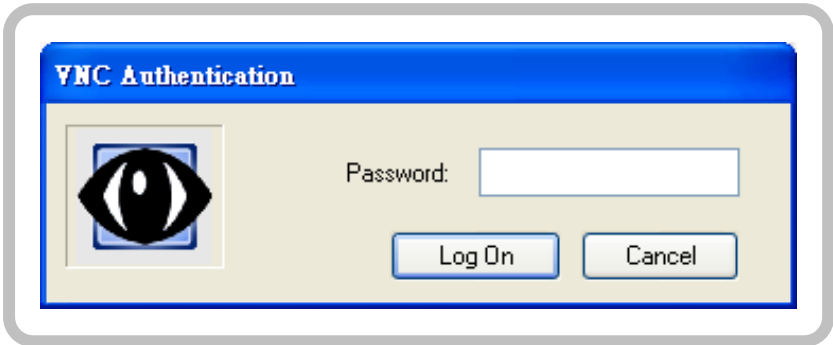


- Run UltraVNC Viewer and configure the application as below.



VNC server	Input the internal IP address of the VNC server.
Proxy/Repeater	Check the item and input the external IP address of AXIMCom P2P GEAR PRO

- If it is connected successfully, the VNC server in the LAN will ask for your password. After entering the password, you will see a VNC window. Now, you can run remote desktop management on this VNC Server,



9.5 BT DOWNLOAD SETUP

P2P GEAR PRO is equipped with BT download functionality which allows users to download without needing to turn on a PC or a NAS server. By plugging an USB HDD or flash drive onto P2P GEAR PRO and adding BT seeds via the GUI, P2P GEAR PRO will automatically download the BT files with regards to the seeds.

9.5.1 BT Download Settings

1. Click on [Applications] – [BT Download] tab. You will see the following screen.

Applications - BT Download

BT Download

BT Download Enable Disable

Maximum Peer Num

BT Port Range From: To:

DHT Port

Maximum Download Rate Mbps

Maximum Upload Rate Mbps

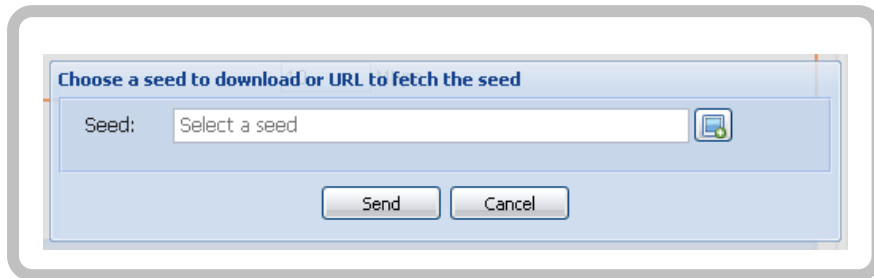
File Name	File Size	Downloaded	Progress	Upload Speed	Download Speed	Status
-----------	-----------	------------	----------	--------------	----------------	--------

2. Configure [Applications] – [BT Download] Settings following the instructions below.

BT Download	Select <i>Enable/Disable</i> to enable/disable BT download.
Maximum Peer Num	Enter the maximum number of BT peer.
BT Port Range	Enter the port range for BT download.
DHT Port	Enter the port of DHT.
Maximum Download Rate	Enter the maximum download rate.
Maximum Upload Rate	Enter the maximum upload rate.

9.5.2 Add BT Seed

1. Click on [Add] tab. You will see the following screen. Choose the seed file and click [Send].
2. You will then see the BT seed listed on the table.



9.6 FTP SETUP

9.6.1 FTP Settings

1. Click on [Applications] – [FTP] tab. You will see the following screen.

Applications - FTP

FTP

FTP Enable Disable

User Rule

Rule Enable	User Name	Password
-------------	-----------	----------

2. Configure [Applications] – [FTP] Settings following the instructions below.

FTP	Select <i>Enable/Disable</i> to enable/disable FTP Server.
-----	--

9.6.2 Add FTP User Rule

1. Click on [Add] tab. You will see the following screen.

The screenshot shows a configuration window for adding an FTP user rule. It contains the following elements:

- Sequence Number:** A text input field containing the number '1'.
- Rule Enable:** A checkbox that is checked with a green checkmark.
- User Name:** An empty text input field.
- Password:** An empty text input field.
- Buttons:** Two buttons at the bottom: 'Confirm' and 'Cancel Changes'.

2. Configure [Add FTP] Settings following the instructions below.

Sequence Number	This defines the sequence of the FTP user rule
Rule Enable	<i>Enable/Disable</i> this FTP user rule
User Name	Enter FTP user name
Password	Enter FTP password

CHAPTER 10 ADMIN

10.1 MANAGEMENT

1. Click on [Admin] – [Management] tab. You will see the following screen.

Admin - Management

Administration Interface

Language: English

Administrator Password: [Masked]

Re-type Password: [Masked]

Remote Management: Enable Disable

Management Port: HTTP 8080

Reboot

Reboot:

Configuration

Configuration Export:

Default Configuration Restore:

Configuration Import: [Input Field]

Firmware

Firmware Upgrade: [Input Field]

2. Configure [Administration Interface] Settings based on the instructions listed below.

Language	Select the language of administration Interface you wish to use.
Administrator Password	Maximum input is 36 alphanumeric characters (case sensitive) * Please change the administrator's password if the remote management is enabled. Otherwise, a malicious user can access the management interface. This user can then have the ability to change the settings and damage your network access.
Re-type Password	Enter the password again to confirm.
Remote Management	Select <i>Enable</i> to enable Remote Management. Select <i>Disable</i> to disable Remote Management If the remote management is enabled, users who are not in the LAN can connect to AXIMCom P2P GEAR PRO and configure it from the Internet.
Management Port	HTTP port which users can connect to. (default port is 8080)

3. Configure [Configuration] Settings based on the instructions listed below

Configuration Export	Click <i>Export</i> to save your current configuration settings in a file.
Default Configuration Restore	Click <i>Restore</i> to recover the default system settings.
Configuration Import	Click <i>Browse</i> and <i>Import</i> to load previous configuration settings.

4. Configure [Firmware] Settings based on the instructions listed below

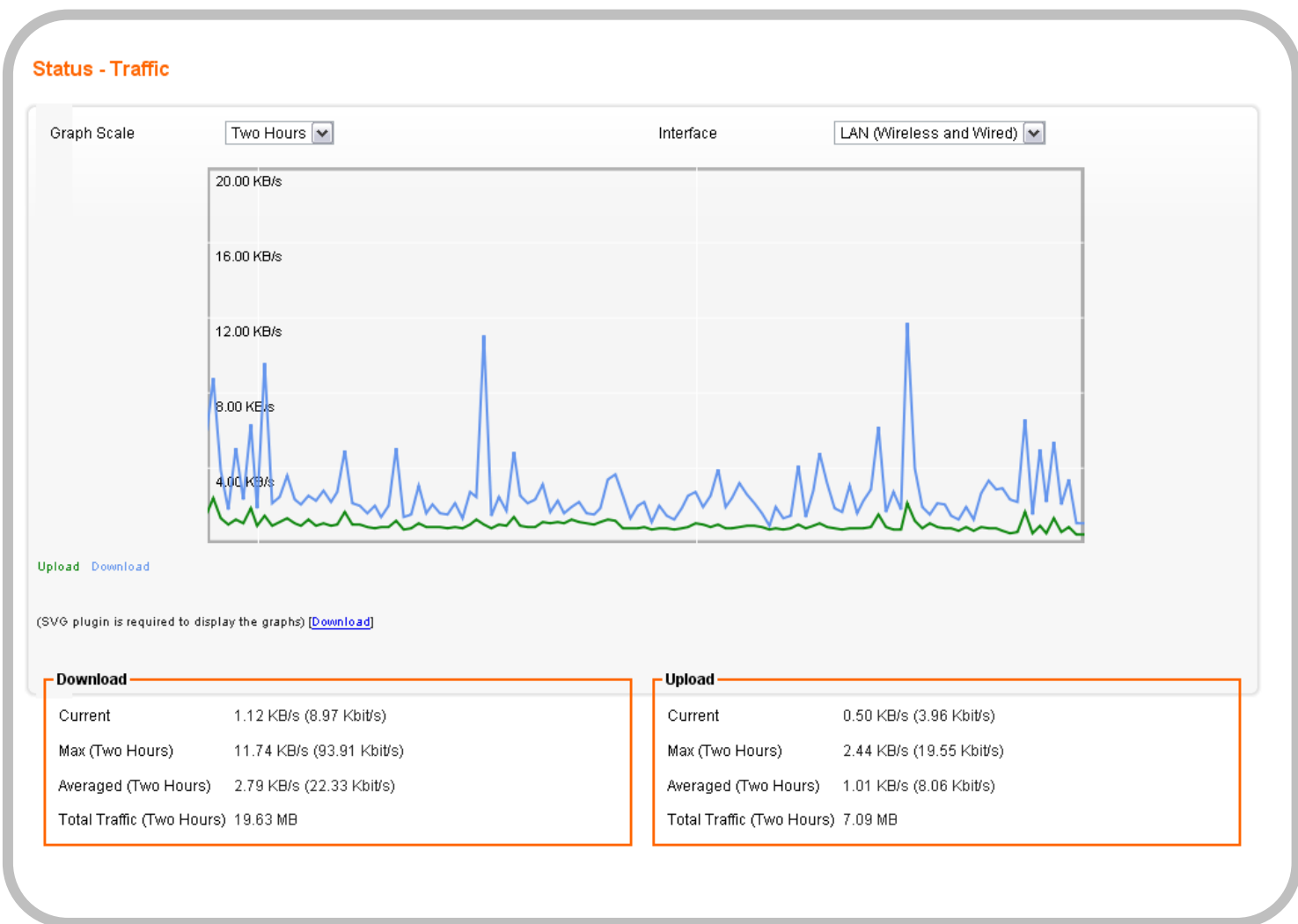
Firmware Upgrade	Click <i>Browse</i> and <i>Upgrade</i> to upgrade the firmware.
-------------------------	---

CHAPTER 11 STATUS

You can access and view all the system information regarding AXIMCom P2P GEAR PRO from here.

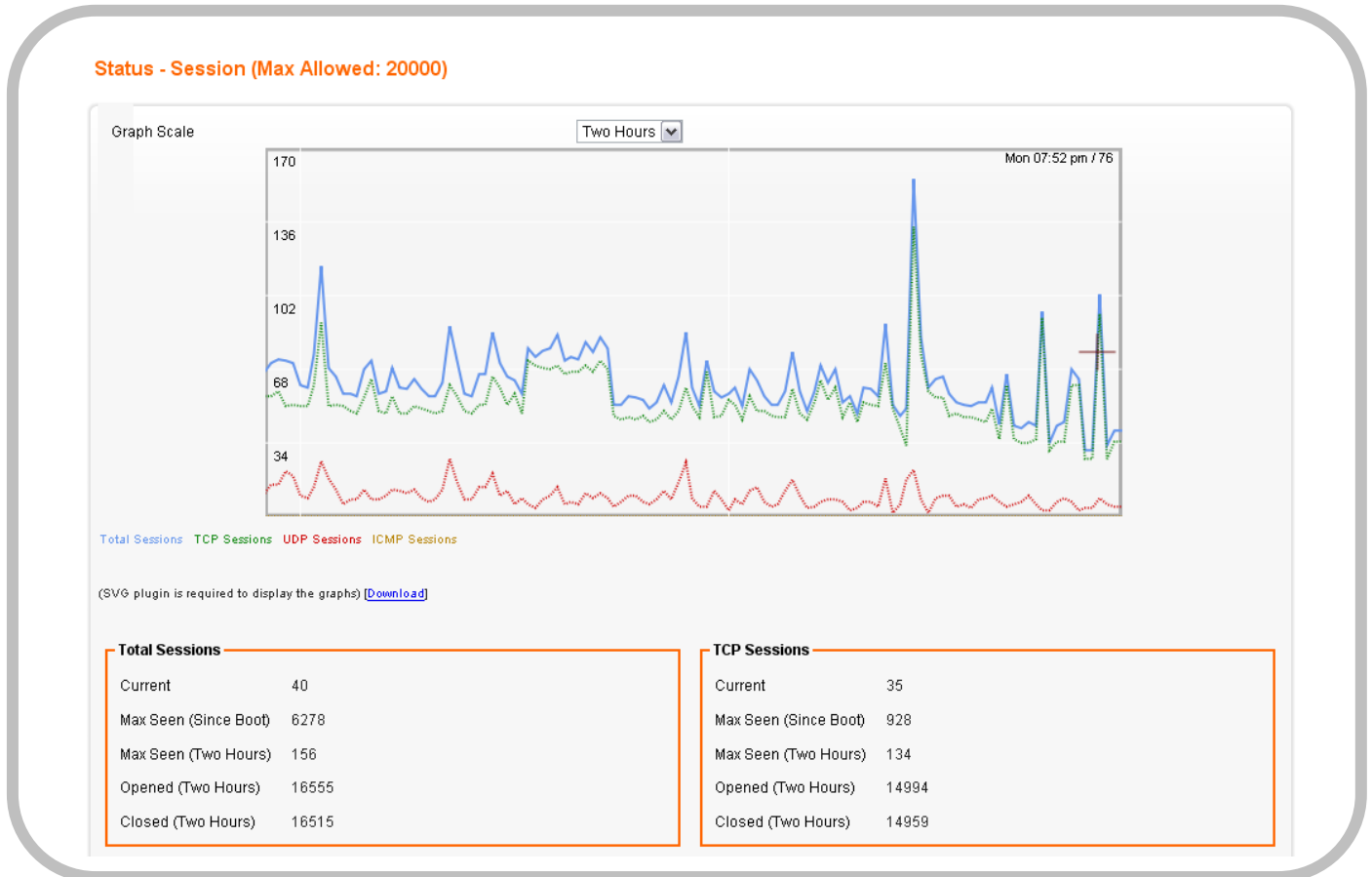
11.1 TRAFFIC

1. Click on [Status] – [Throughput] tab, and then choose the graph scale from two hours, one day, one week, and one month. You will now see the following graph.
2. You can now monitor your download and upload throughput.



11.2 SESSION

1. Click on [Status] – [Session] tab and choose the graph scale from two hours, one day, one week, and one month. You will now see the following graph.
2. TCP, UDP, ICMP, and total session information is displayed.



11.3 ROUTER INFORMATION

1. Click on [Status] – [Router] tab. You will see the following screen.

Router Information

Model Name	AXIMCom Product: PGP-108N
Firmware Version	2.0.0 (C.1)
License	Unauthorized(-5931)
Current Time	Fri, 19 Jun 2009 15:33:12
Running Time	2 hours, 34 mins

WAN 1

MAC Address	00:12:0E:B0:73:0A
Connection Type	pppoe
IP Address	118.166.52.130
Subnet Mask	32
Gateway	61.217.32.254

LAN 1

MAC Address	00:12:0E:B0:73:08
IP Address	192.168.1.1
Subnet Mask	24
DHCP Service	Enabled
DHCP Start IP Address	192.168.1.20
DHCP End IP Address	192.168.1.27
Max DHCP Clients	8

2. Router Information

Model Name	Product model name is shown.
Firmware Version	The firmware version this device is running.
License	"Authorized" should be shown. If "Unauthorized" is shown, please contact the seller or AXIMCom for a replacement.
Current Time	Current system time
Running Time	The period of time AXIMCom P2P GEAR PRO has been running.

3. LAN

MAC Address	MAC Address
IP Address	Internal IP Address
Subnet Mask	The number of subnet mask in the internal network
DHCP Service	DHCP service enabled or disabled
DHCP Start IP Address	DHCP Start IP address
DHCP End IP Address	DHCP End IP address
Max DHCP Clients	The maximum IP addressed which can be assigned to PCs connecting to the network

4. Wireless Network

Wireless Mode	Access Point
Wireless SSID	SSID of this Wi-Fi station
Wireless Channel	Wireless Channel in use (default is 6)
MAC Address	MAC Address

5. WAN

MAC Address	MAC Address
Connection Type	The current connection type (PPPoE, Static IP, and DHCP)
IP Address	WAN IP Address
Subnet Mask	Number of subnet mask.
Gateway	IP address of the gateway

11.4 USER

1. Click on [Status] – [User] tab. You will see the following screen.

Status - User

DHCP Table (3 users)

Name	IP Address	MAC Address	Expiration Time
cyba	192.168.1.34	00:15:af:ee:2f:bd	19:48:11
maode-ibook-g4	192.168.1.21	00:11:24:ed:21:1e	19:11:48
eeehp	192.168.1.23	00:1b:24:37:0a:e3	21:39:49

2. DHCP Table

Name	DHCP client name
IP Address	IP address which is assigned to this client
MAC Address	MAC address of this client
Expiration Time	The remaining time of the IP assignment

3. ARP Table

IP Address	IP address assigned by Static ARP matching
MAC Address	MAC address in the Static ARP matching
ARP Type	Static or dynamic

11.5 LOG

1. Click on [Status] – [Log] tab. You will see the following screen.





Setup - Log

System Log

```
Jan 1 00:00:07 FS-service: boot [OK]
Jan 1 00:00:07 HOTPLUG-service: boot [OK]
Jan 1 00:00:07 USB-service: boot [OK]
Jan 1 00:00:11 lan1: up [OK] [192.168.1.1]
Jan 1 00:00:11 License-client: boot [OK]
Jan 1 00:00:11 WEB-server: boot [OK]
Jan 1 00:00:12 DHCP-server: boot [OK]
Jan 1 00:00:12 SSH-server: boot [OK]
Jan 1 00:00:12 STATS-server: boot [OK]
Jan 1 00:00:12 CRON-service: boot [OK]
Jan 1 00:00:26 ACL: service [boot] OK
Jan 1 00:00:26 TurboNAT: boot [OK]
Jan 1 00:00:26 wan1: down [OK] []
Jan 1 00:00:27 WANG: stop [OK]
Jan 1 00:00:27 wan2: down [OK] []
Jan 1 00:00:27 WANG: stop [OK]
Jan 1 00:00:28 MON-server: boot [OK]
Jan 1 00:14:51 wan2: down [OK] []
Jan 1 00:14:51 WANG: stop [OK]
Jan 1 00:18:07 wan1: up [OK] [118.166.47.8]
Jan 1 00:18:20 ACL: WAN [service] start
Jan 1 00:18:20 WANG: start [OK]
Jan 1 00:18:20 DDNS-client: start [Failed]
Jan 1 00:18:20 UPnP-server: start [OK]
Jan 1 08:18:20 NTP-client: start [OK]
```

Refresh

CHAPTER 12 APPENDIXES – PRODUCT COMPARISON

 Intelligent Bandwidth Management Series				
Feature	Description	PGP-108T	PGP-108N	PGP-116N
iDBM Intelligent Bandwidth Management	On-the-fly upload/download monitoring	●	●	●
	Real-time traffic prioritization (gaming, VoIP, streaming, etc.)	●	●	●
	Dynamic bandwidth allocation (P2P, gaming, VoIP, etc.)	●	●	●
	Intelligent P2P traffic bandwidth allocation	●	●	●
	Optimal bandwidth utilization	●	●	●
	Bandwidth limitation by IP address	●	●	●
	Bandwidth limitation by protocol / port	●	●	●
MRTG Monitoring	TurboNAT	●	●	●
	Real-time throughput MRTG	●	●	●
Green Download	Real-time session MRTG	●	●	●
	BT download	●	●	●
	DHT seeds support	●	●	●
	Multi-language seeds support	●	●	●
	Large file download support (>4GB)	●	●	●
File Sharing	Web-based remote download management	●	●	●
	FTP Server	●	●	●
VNC KVM	iSCSI Server	-	-	●
	Remote desktop management	-	-	●
VPN	Windows XP SP2 / Vista / Mac OS X compatible	-	-	●
	VPN tunnels	-	-	4
	PPTP (MPPE 128-bit encryption)	-	-	●
	MS-CHAP v2	-	-	●
VPN NAT	VPN pass-through (PPTP and IPsec NAT-T)	●	●	●
Wireless	Energy saving	-	●	●
	Standards	-	802.11b/g/n	802.11b/g/n
	Max. data rate	-	300Mbps	300Mbps
	WDS (Wireless Distribution System)	-	●	●
	WPA, WPA2, WPA-PSK, WPA2-PSK, WEP 64 /128-bit	-	●	●
	Universal repeater	-	●	●
	Wireless LAN isolation	-	●	●
	802.1X authentication	-	●	●
Session Management	Multiple SSID and hidden SSID broadcasting	-	●	●
	Concurrent sessions	15000	15000	17500
Streaming Media Technology	LRU (Least Recently Used) idle session recycling	●	●	●
	Support P2P streaming (Joost, PPStream, etc.)	●	●	●
	Support RTSP and MMS protocols	●	●	●
	Support Real, Quick Time, Windows Media Players	●	●	●
WAN Protocol	H.323 video conferencing support	●	●	●
	DHCP, Static IP and PPPoE	●	●	●
Network Features	MAC address cloning	●	●	●
	DHCP client / relay / server	●	●	●
	Dynamic DNS (DynDNS, TZO, ZoneEdit, NO-IP, etc.)	●	●	●
	UPnP	●	●	●
	DNS cache / proxy	●	●	●
	NTP (Network Time Protocol)	●	●	●
Firewall	STP (Spanning Tree Protocol)	●	●	●
	SPI (Stateful Packet Inspection) firewall	●	●	●
	Anti-DoS and Anti-spoofing protection	●	●	●
	Instant messaging filtering	●	●	●
	L2 / L3 / L4 ACL filtering	●	●	●
	Static DHCP and static ARP IP-MAC binding	●	●	●
System Management	DMZ and port forwarding (virtual server)	●	●	●
	Web-based management	●	●	●
	Configuration backup and restore	●	●	●
	Firmware upgrade and downgrade	●	●	●
Hardware	Multiple language support	●	●	●
	WAN port(s)	1 × 10/100M	1 × 10/100M	1 × 10/100M
	LAN port(s)	4 × 10/100M	4 × 10/100M	4 × 10/100M
	USB port(s)	1 × USB 2.0	1 × USB 2.0	1 × USB 2.0

Note: '–' Not available '●' Available